Sādhanā (2018) 43:128
https://doi.org/10.1007/s12046-018-0891-1

A privacy-preserving authentication protocol with secure handovers for the LTE/LTE-A networks

GARIMA SINGH* and DEEPTI SHRIMANKAR

Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology, Nagpur 440010, India
e-mail: garimasingh.mit2006@gmail.com

MS received 23 July 2017; revised 19 September 2017; accepted 3 December 2017; published online 3 July 2018

Abstract. Long-Term Evolution/Long-Term Evolution Advanced (LTE/LTE-A) is the latest mobile communication technology that is offering high data rates and robust performance to the subscribers. Since LTE/LTE-A standards are established on the Internet Protocol (IP) connectivity and provide compatibility with the heterogeneous networks, these new features create availability of the new security challenges in the LTE/LTE-A networks. Taking into consideration the issues of serious signalling congestion and security loopholes in LTE/LTE-A networks, the authors propose an Efficient Authentication and Key Agreement Protocol for Evolved Packet System (EAKA-EPS) with secure handover procedures. The proposed protocol achieves outstanding results in terms of the optimization of computation and signalling overhead. With this, the protocol guarantees the needed security requirements like protected wireless interface and strong mutual authentication between the entities, and ensures access stratum secrecy at the time of handovers. The formal verification results of the proposed scheme over the security verification and simulation tool "Automated Validation of Internet Security Protocols and Applications (AVISPA)" show that the suggested protocol is safe against various malicious attacks, which are still possible in LTE/LTE-A networks. To the best of the authors' knowledge, the suggested approach is the first approach that provides perfect secrecy with less computation and communication overhead in the LTE/LTE-A networks.

Keywords. Mobile networks; cryptography; LTE security; authentication and key agreement; confidentiality; integrity; LTE handovers.

1. Introduction

A recent increase in the usage of novel mobile applications has led to the continuous traffic increase and skyrocketing bandwidth demands [1]. In response, 3rd Generation Partnership Project (3GPP) standardized Long-Term Evolution/Long-Term Evolution Advanced (LTE/LTE-A) technology has evolved as the next generation of the mobile communication technology [2–11]. Designers of the LTE/LTE-A technology have announced Evolved Packet System (EPS) as the Fourth Generation (4G) of the mobile communication network, which has been recently deployed worldwide and its installations and applications (Machine type Communications, Internet of Things) are increasing rapidly. EPS is a completely packed switched mobile network, which implements a flat architecture with limited network components. As shown in figure 1, EPS architecture is composed of two major entities: an access network called Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and the Internet Protocol (IP)-based Evolved Packet Core (EPC). After considering the performance and implementation issues, some design decisions were made by 3GPP [12–14]. For instance, EPS is distributed into two separation frameworks: one is User plane (U-plane) framework and another is Control plane (C-plane) framework. The control plane framework is used to carry the signalling traffic (control messages) over the S1-C path that is established between the UE (User Equipment) and the MME (Mobility Management Entity), whereas the User plane framework carries user data traffic over the S1-U path that is established between the UE and the Serving Gateway (S-GW). These modifications, over the legacy technologies, establish physically separated paths for both types of traffic and separate key management for confidentiality and integrity protection. In an effort to make EPS secure, two layers, Access Stratum (AS) layer and Non-Access Stratum (NAS) layer, protect the traffic passing through the EPS as shown in figure 1. NAS security executes between the UE and the MME and provides integrity and confidentiality protection to the NAS signalling data in control plane, whereas AS security executes between the UE and the eNodeB and provides integrity and confidentiality

*For correspondence

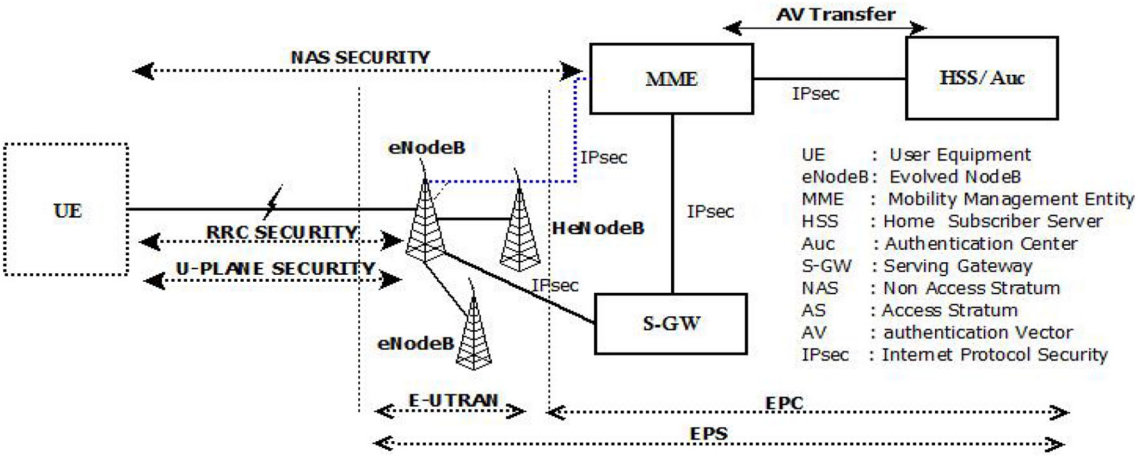

Figure 1. Security architecture of the Evolved Packet System.

protection to the Radio Resource Control (RRC) signalling data in control plane and confidentiality protection to the IP packets in user plane. Beyond the MME, Internet Protocol Security (IPsec) protocols are responsible for protecting all the insecure links.

Although LTE /LTE-A networks implement a strong security model called Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol that is proposed by 3GPP in its release 9 (TS 33.401 V11.1.0.) [12–15], still it has multiple security loopholes and performance-decreasing factors (detailed description of the security loopholes is given in section 1.1) and need further enhancements.

1.1 *Security loopholes in the LTE/LTE-A networks*

For the trustworthy development of the LTE/LTE-A networks, the researchers are actively engaged with the research works focused on the unanswered security vulnerabilities of the LTE/-LTE-A networks. In this section the authors illustrate these security vulnerabilities of the LTE/LTE-A networks, and solutions for them are provided later.

1. Attack against the subscriber's identity: When analysing the security gaps of the LTE/LTE-A networks, the wireless interface between the UE and the eNodeB cannot be ignored. Because of the packet switched behaviour of the LTE/LTE-A, this wireless interface is always at a risk of eavesdropping or manipulation. In some unavoidable situations (like when a subscriber registers first time to the network or the network is not able to link TMSI to the subscriber or if there is synchronization failure between the source MME and the target MME), UE cannot refuse to transfer IMSI instead of TMSI in its attach request. The EPS-AKA scheme transmits this attach request in a plain text form over the wireless interface [16]. Thus, an intruder can easily retrieve IMSI from this unprotected attach request by either using IMSI catchers or decoding attach request manually [44–46]. Shaik *et al* [17] demonstrated in his research that unprotected transmission of the paging messages over the wireless interface may also lead to the subscriber's identity leak. SPAN representation of IMSI leak attack on EPS-AKA is shown in figure 2.
2. Denial of Service (DoS) attack: DoS attack prevents legitimate subscribers from getting the intended services and resources. The EPS-AKA scheme and the schemes suggested in [15, 43, 45, 48] allow unprotected transmissions of the authentication messages over the wireless interface. Thus, an adversary is able to capture and launch active attacks against these unprotected authentication messages that will automatically lead to the UE authentication failure and UE will not get intended services. In another way, for the purpose of preventing communication and increasing destruction, adversaries can collect a large number of valid IMSIs for launching a large number of false attach requests within the LTE/LTE-A network. Here, MME has to execute each received attach request and perform all the needed operations. This will exhaust the computational capacity and LTE/LTE- A resources and create congestion over the network, which will automatically lead to the DoS

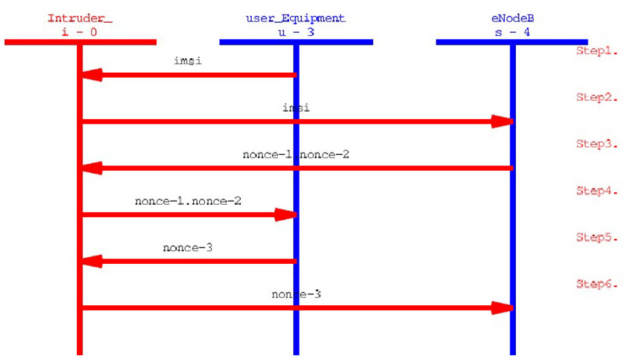

Figure 2. SPAN (AVISPA) representation of IMSI leak attack on EPS-AKA.

attack. In [5, 17, 22, 46] researchers demonstrated in detail about the feasibility of the DoS attack in the LTE/LTE-A networks.

3. Man in the Middle (MitM) attack: By applying the MitM attack, an intruder is able to create an independent connection between the two entities in order to intercept and inject messages. MitM attack is feasible over the LTE/LTE-A networks. For instance, an intruder sends a fake attach request using the legitimate identity of a mobile station to the MME. In response, MME forwards authentication vectors back to the intruder. After receiving authentication vectors, the intruder waits for an attach request from the legitimate UE. When UE asks for the attachment, the intruder interrupts and forwards previously received authentication parameters to the UE. In this way, the intruder is able to authenticate itself to the UE as a legitimate network and creates an independent connection between the UE and the network; execution of the MitM attack on EPS-AKA protocol is shown in figure 3.
4. Vulnerable handover scheme: Handover in LTE/LTE-A should ensure forward key separation (FKS) and backward key separation (BKS) to prevent exploitation of the session keys. However, in LTE/LTE-A, on intra-MME handover, target eNodeB receives fresh Next-Hop (NH) key and NH Chaining Counter (NCC) value from the MME within the path switch message after the radio link handover [13]. Thus, these new parameters can be used only to generate keying material for the next handover. In EPS-AKA, the source eNodeB computes a session key for the target eNodeB using fresh parameters (NH, NCC) received on previous handover. Thus, in the presence of the rouge base stations, horizontal key derivation never ensures FKS and vertical key derivation achieves FKS with well-defined limitation of the two-hop only [13]. Even then, rouge eNodeB may disrupt updating of NCC values that may lead to the desynchronization attack in LTE/LTE-A networks [18–20].
5. Replay attack: Replay attacks were executed on the legacy networks (GSM, UMTS) and are still feasible in LTE/LTE-A networks. As per [15], an intruder can capture the authentication parameters sent by the MME over the wireless interface and replay them to the UE. In this way, an intruder can verify the presence of the subscriber through the received error message response. The EPS-AKA scheme and the schemes suggested in [15, 48] allow unprotected transmissions of the authentication parameters. Hence, the schemes are vulnerable to the replay attack.
6. Redirection attack/overbilling attack: Let us make an assumption that an adversary is controlling a device that can function as a base station and entices UE to camp on its radio channel. This rouge base station can redirect subscriber's service request to the foreign network instead of the home network and is charged accordingly, which will lead to the overbilling attack in the LTE/LTE-A networks. In another scenario, with the intention of breaching user traffic security, the rouge base station may redirect user traffic to a network where security is either weak or not provided. On access authentication, the EPS-AKA approach and the approaches suggested in [15, 43, 45, 48] never verify authenticity of the base stations; thus, this weak mutual authentication creates space for the redirection attack and the overbilling attack in the LTE/LTE-A networks. The researchers in [37, 45] demonstrated how redirection attack may occur in the LTE/LTE-A networks.
7. High bandwidth consumption/storage overhead: High bandwidth consumption and signalling overhead between the MME and the HSS is one of the performance-decreasing factors of the EPS-AKA protocol. If UE resides in MME for a long span of duration and exhausts all its authentication vectors received from the network, then MME requests again to the HSS for another sets of the authentication vectors. This generates high signalling overhead and high bandwidth consumption between the MME and the HSS. With this, it creates additional storage overhead at the MME for storing n sets of the authentication vectors [46].
8. Single-key dependency: In general, cryptographic keys have defined lifetime to limit the key exposure and compromise. If the EPS-AKA scheme or the scheme suggested in [15, 43, 44, 48] is used, then the security of the LTE/LTE-A networks is dependent on a single permanent symmetric key (K) that is shared between the USIM and the HSS at the time of manufacturing. If somehow this key is compromised, then the whole system security will be on risk and it will be feasible for an opponent to be authenticated by the LTE/LTE-A network.

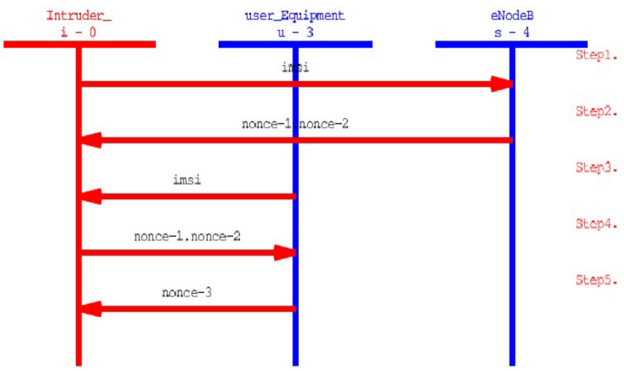

Figure 3. SPAN (AVISPA) representation of MitM attack on EPS-AKA.

1.2 *Related works*

There are many studies claiming multiple security vulnerabilities in the LTE/LTE-A networks. Shaik *et al* [17]

uncovered various security loopholes in the LTE access network protocols. They demonstrated the feasibility of inexpensive, practical attacks like subscriber's location leak and DoS attack using the low-cost commercial LTE devices on the real networks. Rupprecht *et al* [21] conducted a comprehensive survey on the LTE security and found two implementation vulnerabilities: the first class of vulnerability contained network authentication, while the second class contained user traffic encryption; with this, the researchers demonstrated feasibility of the MitM attack without the need of authentication requirements. Rupprecht *et al* demonstrated that attackers are able to deploy fake base stations in the LTE network, which may lead to the feasibility of redirection attack. Park and Park [22] surveyed LTE technology and concluded that this technology inherits security problems from the legacy technologies and its migration to IP-network exposes it to the IP-specific security threats. Researchers exposed the feasibility of redirection attack on user traffic, attack on the lifetime of the UE to make it shorter and resynchronization attack. Cao *et al* [23] surveyed the security aspect of the LTE/LTE-A networks and uncovered various security vulnerabilities of the standard AKA protocol.

In order to achieve the objectives of the secure communication and better performance, in the existing literature, several authentication and key agreement protocols have been suggested [24–44]. Most of these suggested approaches demand changes in the LTE/LTE-A environment and require additional cryptographic algorithms. Abdrabou *et al* [45] suggested a symmetric-key-based approach named Modified Evolved Packet System Authentication and key agreement protocol (MEPS-AKA) to mitigate existing security issues. Their approach was based on simple password exponential key exchange. A pre-authentication is performed that generates dynamic keys for each access to the network. This approach introduced a communication overhead increase (in bits) up to 62% in authentication procedure. Degefa *et al* [46] proposed another symmetric-key-based protocol called Enhanced-AKA, which enhances the security level and performance of the LTE/SAE networks. The approach requires a secretly shared key identity (KI) between the UE and the HSS to fulfill the security needs of the subscriber. The approach was efficient as per the bandwidth consumption and reduction in storage overhead at MME, but could not resolve the issues like deployment of the rouge base station, DoS attack and MitM attack in LTE/LTE-A networks. In addition, if IPsec is not enabled on EPC this approach, it provides chances for the exposure of pre-shared LTE key (K). To recover K, an adversary can sniff KI over the air interface and secret key (s) from the core interface, and apply brute force attack on K using known function f', KI and key (s) over a quantum supercomputer. Ekene *et al* [47] suggested a PKI (Public Key Infrastructure)-based authentication approach called EC-AKA, in which IMSI will never be sent in the plain text manner in an attach request. Thus, subscriber identity is safe from the disclosure. In this approach, transmission of AUTN, Rand and RES parameters is executed in clear text, which makes this protocol vulnerable to all those attacks that are possible over the unprotected wireless interface. Hamandi *et al* [48] proposed a hybrid protocol with a modified key to protect privacy concerns of the subscribers; the main objective of the approach was to assure that subscriber's identity could not be tracked. This approach considered the issue of limited energy for the UEs. In this research, for UE authentication, MME generates a random number and forwards it to the UE. UE also generates a random number and feeds both the random numbers with previously shared key K to the key generation function. As a result, an anonymity key is generated, which is used for the ciphering of IMSI. In addition, the protocol used a newly introduced sequence numbers (SQN_{HSK}) for the identification of key K against the UE on the HSS. Thus, this approach increased the computational as well as managerial overhead for maintaining the newly introduced SQNs. In addition, some parameters that were assumed to be secure can be obtained from the authentication vectors. For instance, RMSI was confidential to the HSS and UE, but it could be easily obtained from the AUTN parameter. Zhang and Fang [37] demonstrated that 3GPP AKA protocol is vulnerable to the false base station attack, which may lead to the feasibility of redirection attack. They suggested an AP-AKA protocol that is flexible according to whether or not UE has unused parameters. This AP-AKA approach mitigates redirection attack and eliminates the need of synchronization between the UE and the HSS. However, the issues of DoS attack, MitM attack and redirection attacks are not considered in this approach. Hamandi *et al* [15] proposed a modified subscriber's privacy-sensitive LTE-AKA approach to prevent various active and passive attacks in LTE network. The approach is a hybrid approach that employs both symmetric and asymmetric encryptions and its main objective is to secure subscriber's identity. The approach suggested the use of three identities MUTI, GRid and E-IMSI instead of two, which increased the difficulty level of linking static–dynamic identities of the subscriber, which presented a new temporary UE ID reallocation scheme in order to maintain user privacy. However, this scheme does not prevent high bandwidth consumption between the HSS and the MME and storage overhead is high on the MME.

1.3 *Our contributions*

In the present research, an attempt is made to do the following:

- Proposing a security and performance-enhanced access control protocol with efficient handover schemes. The suggested approach mitigates most of the security

issues that still exist in the LTE/LTE-A networks. The protocol strongly authenticates to the LTE/LTE-A entities (UE, eNodeB, MME, HSS) and ensures AS layer secrecy.

- Security analysis and verification of the proposed scheme are performed on the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Results shows the security capabilities of the protocol against various malicious attacks.
- We compare the Efficient Authentication and Key Agreement Protocol for Evolved Packet System (EAKA-EPS, suggested approach) performance with those of other existing approaches in terms of the bandwidth consumption, computational overhead and signalling overhead. Results indicate that the suggested approach guarantees outstanding performance while achieving more security requirements.

2. The proposed protocol

To meet the goal of perfect secrecy in the LTE/LTE-A networks, the authors try to suggest an EAKA-EPS approach that will remove redundant computations and minimize the use of PKI to achieve the goal of perfect secrecy. Following assumptions are considered for EAKA-EPS: (i) IPsec is enabled on the wired interface of the EPS, (ii) UE and MME store asymmetric key pairs (PK_{ue}, PK_{ue}^{-1}, PK_{mme}, PK_{mme}^{-1}) and when UE enters into the area of the MME, MME shares its public key PK_{mme} with the UE and (iii) UE, MME, HSS have functions f_1, f_2, f_3, f_4, f_5 and KDF stored on them.

2.1 *EAKA-EPS*

Security services included in the proposed scheme are mutual authentication and key agreement, NAS key agreement for NAS security set-up and AS key agreement for AS security set-up. The proposed authentication and key agreement protocol is shown in figure 4 and in order to create a clear picture of the key computations, it is diagrammatically depicted in figure 5. Protocol execution is as follows:

1. UE → MME: Attach Request ($E\{IMSI||UE\text{-}Net\text{-}Cap||T1||PK_{ue}||MAC\text{-}1\}PK_{mme}$): For initial attachment, UE sends encrypted attach request message to the MME via eNodeB. This attach request includes IMSI, UE network capabilities, timestamp (T_1), MAC − 1 and PK_{ue} (public key of the UE) where $MAC\text{-}1 = f_1(IMSI||UE\text{-}Net\text{-}Cap||T_1||PK_{ue})$ is the message authentication code computed by the UE; eNodeB attaches its security certificate (C_{eNodeB}) issued by the Certification Authority (CA) to

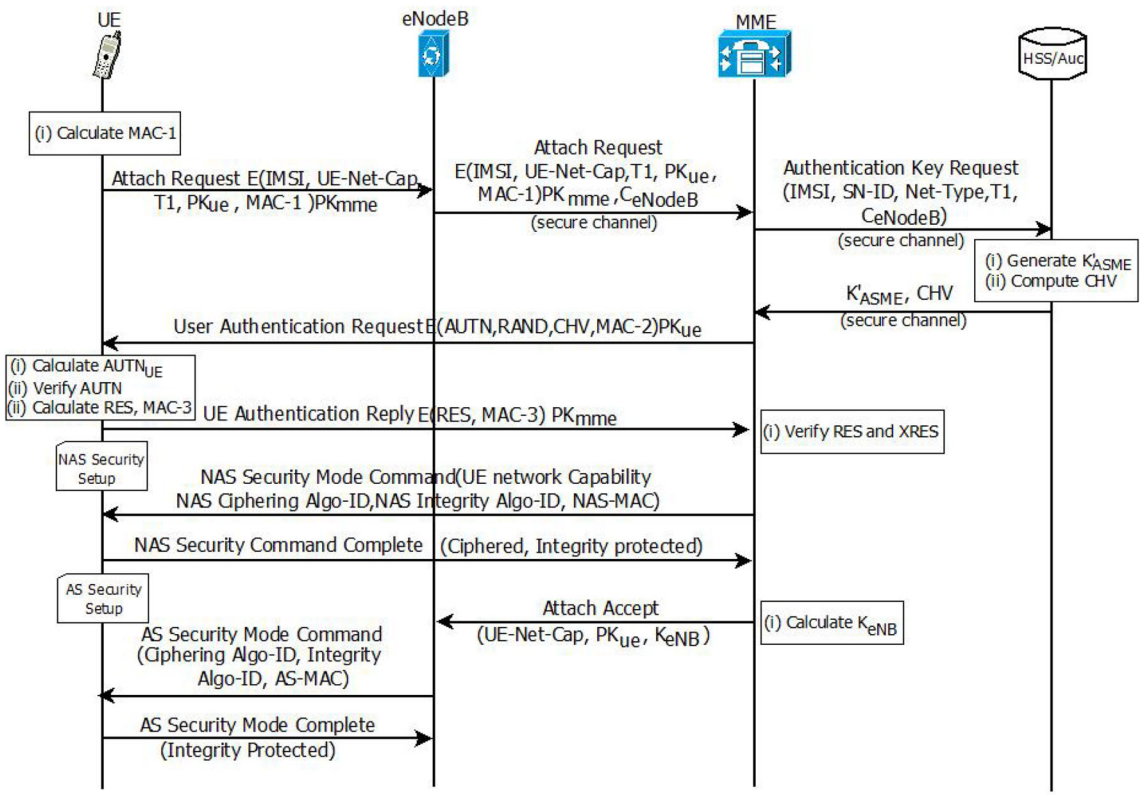

Figure 4. An Efficient Authentication and Key Agreement Protocol for Evolved Packet System (EAKA-EPS).

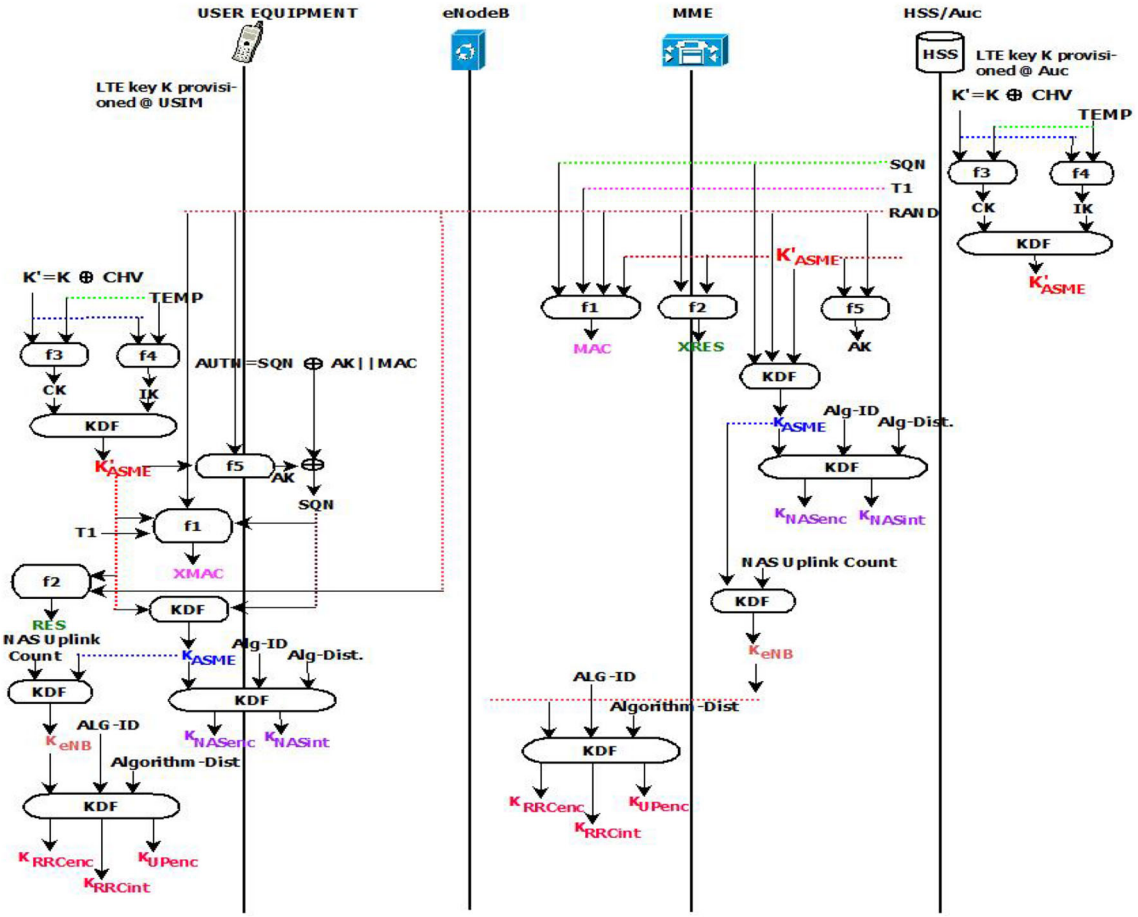

Figure 5. Key generation model of EAKA-EPS Protocol. Key K'_{ASME} is a temporary key assigned to the MME by the HSS that authorizes the MME for the authentication of the UEs.

the received attach request (E{IMSI||UE-Net-$Cap||T_1||\text{PK}_{ue}||\text{MAC}-1\}\text{PK}_{mme}||\text{C}_{eNodeB}$) and forwards it to the MME over a secure channel. MME decrypts the received message with its private key and checks the integrity of the received attach request.

2. MME → HSS: Authentication Key Request (IMSI, Network-type, SN-ID, T_1, C_{eNodeB}): For getting a temporary authentication key that will authorize to the MME for providing authentication to the UEs, MME forwards authentication key request (IMSI, Network-type, SN-ID, T_1, C_{eNodeB}) to the HSS. This authentication key request includes the network type of the UE and identity of the serving network (SN-ID) with timestamp T_1 and certificate of the eNodeB (C_{eNodeB}).
3. HSS → MME: Authentication Key Response (K'_{ASME}, CHV): In response to the authentication key request, HSS authenticates to the eNodeB and MME by verifying the validity of the C_{eNodeB} and SN-ID. If eNodeB and MME are genuine entities then HSS generates a Certificate Hash Value (CHV) = $f_2(T_1, C_{eNodeB})$, key generating key $K^{'}$ = (CHV $\oplus K$), temporary value TEMP = (SN-ID $\oplus$ CHV), Integrity Key (IK) = $f_3(K^{'}$, TEMP) and Cipher Key (CK) = $f_4(K^{'}$, TEMP). With this, using a key derivation function over CK and IK, HSS computes a temporary authentication key K'_{ASME} = KDF(CK, IK). HSS forwards computed temporary authentication key K'_{ASME} and CHV to the MME.
4. MME → UE: Authentication Request (E{AUTN, Rand, CHV, MAC-2}PK_{ue}): After receiving temporary authentication key (K'_{ASME}), MME generates a random variable (Rand), assigns an SQN and computes remaining authentication vectors as follows:

- An anonymity key AK = f_5 (K'_{ASME}, Rand), where f_5 is a key generating function.
- Message authentication code MAC = f_1 (K'_{ASME}, SQN, T_1, Rand), where f_1 is an authentication function.
- An authentication token AUTN = SQN⊕AK||MAC.
- An expected response XRES = $f_2(K'_{ASME}$, Rand), where f_2 is an authentication function.
- Access security management entity key K_{ASME}= KDF (K'_{ASME}, Rand, SQN), where KDF is a one-way hash function for key derivation.
- Finally, set of the authentication vectors AV = (RAND, AUTN, XRES, K_{ASME}).

MME computes MAC-2 = f_1(AUTN, Rand, CHV) and confidentially forwards a user authentication request that includes authentication parameters (E{AUTN, RAND, CHV, MAC-2}PK_{ue}) to the UE.

5. UE → MME: Authentication Request Reply (E{RES, MAC-3}PK_{mme}): UE recovers authentication parameters and checks the integrity of the received message by computing MAC-2' in a similar manner as that of MME computed MAC-2. If MAC-2 = MAC-2', UE also computes K', TEMP, CK, IK and key K'_{ASME} in a similar way as that computed by HSS (shown in figure 5); otherwise, UE rejects the authentication request. UE computes $AUTN_{UE}$ and authenticates to the eNodeB, MME and HSS by checking whether $AUTN_{UE}$ = AUTN or not. After the successful authentication of the network components, UE generates authentication response RES = f_2(K'_{ASME}, Rand), key K_{ASME} = KDF (K'_{ASME}, Rand, SQN) and MAC-3 = f_1(RES). UE forwards signed response (RES) to the MME in ciphered and integrity-protected manner. MME recovers the response (RES) and verifies integrity of the received message. If integrity holds, MME verifies whether XRES = RES or not; if equality holds then UE will be an authenticated entity, otherwise not. After successful mutual authentication of all the entities and sharing of the key K_{ASME}, NAS security set-up procedure starts.
6. UE↔ MME: NAS security set-up. MME sets up NAS security as mentioned by 3GPP. MME selects NAS security algorithms and generates NAS security keys as shown in figure 5. NAS encryption key K_{NASenc}= KDF(K_{ASME}, NAS ciphering algorithm distinguisher, Algorithm-ID) and NAS integrity key K_{NASint} = KDF(K_{ASME}, NAS integrity algorithm distinguisher, Algorithm-ID). MME forwards ciphered and integrity-protected NAS security set-up command to the UE with selected algorithms. UE also generates NAS security keys and forwards NAS security set-up complete command back to the MME.
7. UE↔eNodeB: AS security set-up.
For setting-up AS security, MME computes a session key K_{eNB} = KDF(K_{ASME}, NAS Uplink Count) and forwards attach accept command (UE network capabilities, PK_{ue}, K_{eNB}) to the eNodeB. Then eNodeB selects AS security algorithms and generates AS security keys: RRC integrity key K_{RRCint} = KDF (K_{eNB}, AS-algorithm-ID, AS-integrity-algorithm-distinguisher), RRC cipher key K_{RRCenc} = KDF (K_{eNB}, AS- algorithm-ID, AS-encryption-algorithm-distinguisher) and user plane cipher key K_{UPenc} = KDF (K_{eNB}, AS-algorithm-ID, AS-user-plane-encryption-algorithm-distinguisher); eNodeB forwards integrity-protected AS security set-up command to the UE. UE computes AS keys and forwards integrity-protected AS security set-up complete command back to the UE.

2.2 *The j^{th} authentication between the same serving network and UE*

In EAKA-EPS, when UE stays under the MME for a long span of duration and sends its j^{th} authentication request to the registered network, previously shared (between the UE and the MME) access security management entity key (K_{ASME}) will now work as temporary authentication key K'_{ASME}. This key (K'_{ASME}) is known only to the previously HSS authenticated entities. Further, for the j^{th} authentication and key agreement, MME generates a random number (Rand), assigns an SQN and computes authentication vectors (AUTN, XRES and K_{ASME}) as depicted in figure 5 using (K'_{ASME}). MME forwards authentication vectors to the UE in the ciphered and integrity-protected manner and achieves mutual authentication in a similar manner as discussed in section 2.1. Thus, MME need not request back to the HSS for the authentication vectors; HSS will not be overloaded with the authentication of the UE and less bandwidth; signalling will be consumed between the MME and the HSS and storage overhead will be very less on the MME.

2.3 *Key management for X_2-handover*

A modified X_2-handover key chaining model that is expected to provide FKS and BKS in LTE/LTE-A networks is shown in figure 6. For AS security set-up, UE and MME derive a session key K_{eNB} and MME forwards this session key to the eNodeB in attach accept message. UE and eNodeB use K_{eNB} for generating subsequent AS keys. On X_2 handover in LTE/LTE-A networks, for efficiency, source eNodeB generates a temporary key K_{eNB}* for the target eNodeB (Eq. (1)) using its currently active K_{eNB} and sends handover request (K_{eNB}*, PK_{ue}) to the target eNodeB. For maintaining the uniqueness of the session key and to ensure FKS, target eNodeB generates a random number (Rand) and its session key K_{eNB} using a key derivation function on received temporary key K_{eNB}* and generated Rand value (Eq. (2)). Target eNodeB generates all the subsequent AS keys using the generated session key (K_{eNB}), for providing secure communication in AS with UE.

$$K_{eNB}* = \mathrm{KDF}(K_{eNB}, \alpha) \tag{1}$$

$$K_{eNB} = \mathrm{KDF}(K_{eNB}*, \mathrm{Rand}) \tag{2}$$

where α represents cell level values like PCI and EARFCN-DL. Target eNodeB sends Rand value within prepared handover command message to the UE via source eNodeB in a protected manner (as shown in figure 6). UE recovers Rand and generates session key K_{eNB}* and subsequent AS keys in a similar way as target eNodeB is generated. The proposed approach provides FKS/BKS at X_2 handovers without the involvement of the MME. In addition, unlike the standard AKA (EPS-AKA) there is no need for NH key

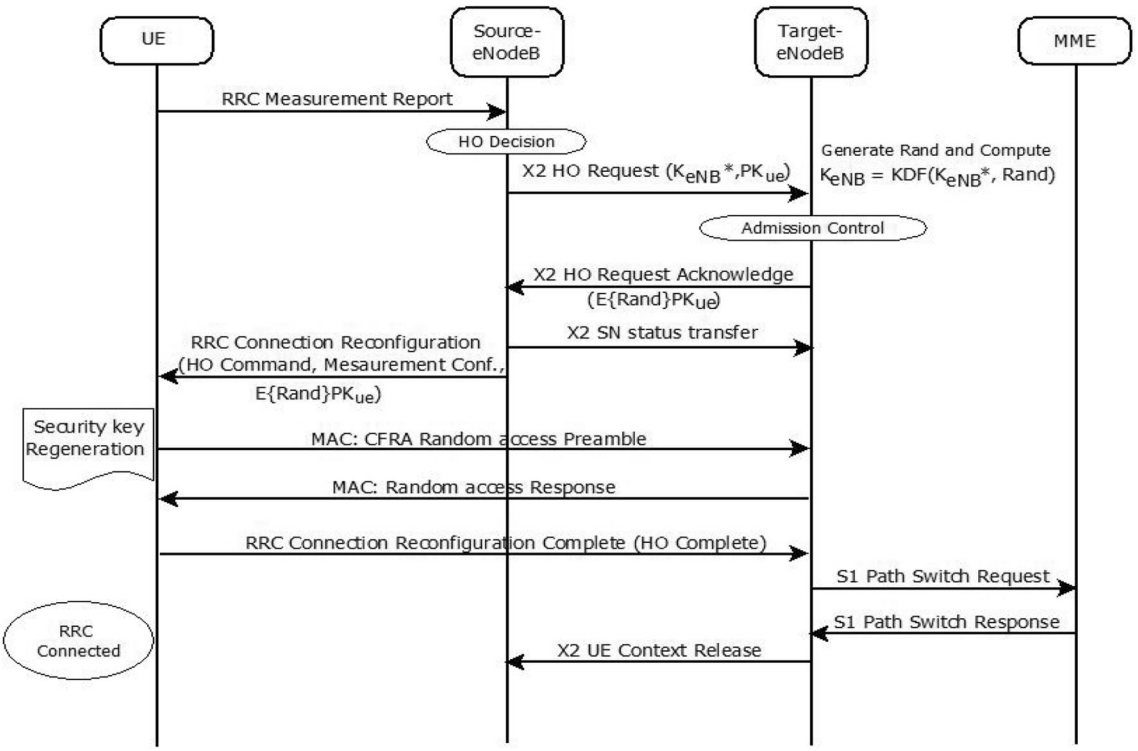

Figure 6. X_2-handover key chaining model.

computations and NCC synchronization. Thus, this approach prevents feasibility of desynchronization attack on the network, maintains secrecy of the AS data and minimizes computational and managerial overhead between the eNodeB and the MME.

2.4 *Key management for S_1-handover*

The proposed S_1-handover key chaining model is shown in figure 7. On S_1 handover, the source eNodeB sends S_1 handover required message to the source

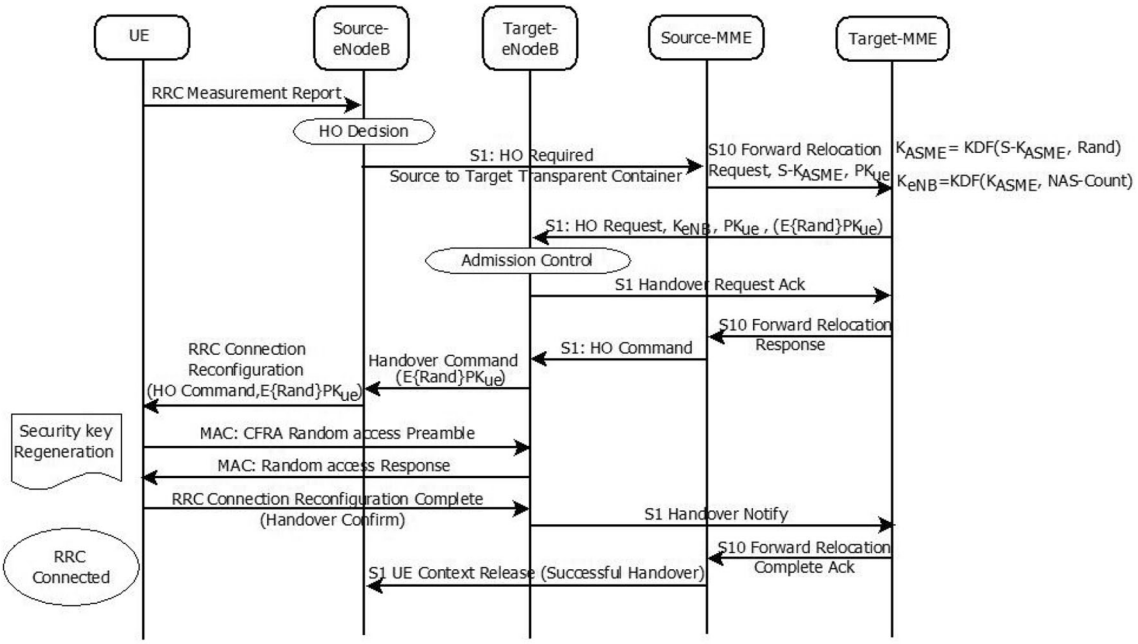

Figure 7. S_1-handover key chaining model.

MME. Upon reception of S_1 handover required message, source MME sends $S10$ relocation request message to the target MME. This $S10$ relocation request message contains key S-K_{ASME}(currently active K_{ASME} on source MME) and the public key of UE (PK_{ue}). Upon reception of relocation request the target MME generates a random number (Rand); with this target, MME computes key K_{ASME} = KDF(S-K_{ASME}, Rand), key $K_{eNB} = (K_{ASME}$, NAS-Uplink-Count) and NAS security keys. The target MME sends K_{eNB}, PK_{ue} and encrypted random number ($E\{\text{Rand}\}PK_{ue}$) to the target eNodeB within S_1 handover request message. Upon reception of S_1 handover request message, target eNodeB generates AS security keys with the help of received K_{eNB} and forwards encrypted random number ($E\{\text{Rand}\}PK_{ue}$) within handover command to the UE via source eNodeB. Upon reception of handover command, UE recovers random number generated by the target MME (Rand) and regenerates security keys in a similar manner as the target MME and the target eNodeB generated.

3. Security analysis

In this section, the authors illustrate some correctness proofs for the proposed approach with its achievements.

3.1 *Theorem 1*

The protocol achieves resistance to the subscriber's identity leak, DoS attack and MitM attack.

Proof: The EAKA-EPS comes up with the asymmetric key cryptography and uses the UE's and MME's asymmetric key pairs (PK_{ue}, PK_{ue}^{-1}, PK_{mme}, PK_{mme}^{-1}) for providing secrecy over the wireless interface. An adversary cannot compromise the secret keys (PK_{ue}^{-1},PK_{mme}^{-1}) because these keys are never transmitted over air in the LTE/LTE-A network. In EAKA-EPS, before transmitting IMSI over the wireless interface, UE encrypts it with the public key (PK_{mme}) of the MME and MME receives IMSI encrypted with its public key (MME← UE: $E\{\text{IMSI}\}PK_{mme}$) from the UE. Here, an adversary is not able to capture IMSI over the wireless interface until he is not having the secret key (PK_{mme}^{-1}) corresponding to the (PK_{mme}). Hence, only MME can recover IMSI from the attach request. In a similar way, the protocol enables secure transmissions over the wireless interface and intruder is not able to sniff any information over this wireless interface. These secure transmissions prevent subscriber's identity leak and ensures data confidentiality in AKA procedure, as per the findings in section 1.1; these confidential transmissions also offer resistance to the DoS attack and the MitM attack. □

3.2 *Theorem 2*

The protocol achieves optimization to the bandwidth consumption/storage overhead over the core network.

Proof: The EAKA-EPS protocol optimizes the bandwidth consumption in the LTE/LTE-A networks by enabling MME to generate the authentication parameters by itself without going back to the HSS. For providing UE's authentication authority to the MME, HSS assigns a temporary authentication key K'_{ASME} to the MME and MME uses this key to generate the authentication parameters. When UE stays under the MME for a long span of duration and sends its j^{th} authentication request to the registered serving network, previously shared access security management entity key (K_{ASME}) works as a temporary authentication key K'_{ASME} and MME uses it to generate the authentication parameters for the j^{th} authentication of the UE. In the proposed approach, if UE is once registered to the MME then MME need not go back to the HSS for the authentication parameters, which reduces the bandwidth consumption and additional storage overhead over the core network. □

3.3 *Theorem 3*

The protocol preserves the FKS/BKS at the time of handovers.

Proof: As illustrated under the "key management for the X_2-handover" subsection, the source eNodeB computes a temporary key $K^*_{eNB} = \text{KDF}(K_{eNB}, \alpha)$ for the target eNodeB using the one-way key derivation function (KDF), which ensures backward key separation in the LTE/LTE-A networks. The source eNodeB sends handover request that includes computed K^*_{eNB} to the target eNodeB. For ensuring the FKS between the session keys, target eNodeB computes its own session key $K_{eNB} = \text{KDF}(K^*_{eNB}$, Rand) using the received K^*_{eNB} and the fresh confidential parameter (Rand) under the KDF. With this, the target eNodeB shares fresh keying parameter (Rand) with the UE in a confidential manner. On handover, the proposed protocol allows session key generation on the target eNodeB using fresh, confidential keying material (Rand). Hence, the protocol achieves FKS/BKS on X_2 handovers, which ensures resistance to the desynchronization attack and achieves the AS secrecy in the LTE/LTE-A networks. □

3.4 *Theorem 4*

The protocol achieves resistance to the Replay attack.

Proof: In the proposed approach, UE includes a fresh timestamp (T_1) value in its initial attach request to prevent the replays of the messages. When HSS receives the attach request, HSS verifies the freshness of the request by

Table 1. Comparison of the proposed protocol with existing protocols suggested by other researchers.

Comparison criteria fulfilled	Original EPS-AKA	EC-AKA [48]	SE-EPS-AKA [43]	MEPS-AKA [44]	Enhanced EPS-AKA [45]	M-LTE-AKA [15]	EAKA-EPS (proposed)
Secure against IMSI Leak	No	Yes	Yes	Yes	Yes	Yes	Yes
Secure against MitM attack	No	Yes	Yes	Yes	Yes	Yes	Yes
Secure against DoS attack	No	No	No	Yes	No	No	Yes
Secure against redirection attack	No	No	No	Yes	No	No	Yes
Existence of FKS/BKS	No	No	No	No	Yes	No	Yes
Secure against impersonation attack	No	Yes	Yes	Yes	Yes	Yes	Yes
Secure against desynchronization attack	No	No	No	No	Yes	No	Yes
Secure against replay attack	No	No	Yes	Yes	Yes	No	Yes
Existence of strong mutual authentication	No	No	No	No	No	No	Yes
Single secret key dependency problem resolved	No	No	No	No	Yes	No	Yes
HSS is overloaded for UE authentication	Yes	Yes	Yes	Yes	No	Yes	No
Data confidentiality protection in AKA procedure	No	Yes	No	Yes	No	No	Yes
Integrity protection in AKA procedure	No	Yes	No	Yes	No	No	Yes
Optimized storage overhead at the MME	No	No	No	No	Yes	No	Yes
Bandwidth consumption between the MME and the HSS	High	High	High	High	Smaller	High	Smallest

checking the validity of the timestamp T_1. If the timestamp T_1 is out of order then HSS will reject the attach request, otherwise HSS will process the request, because if HSS believes the fresh (T_1) then HSS also believes the fresh ($X||T_1$). When UE receives the authentication parameters, UE verifies authenticity of the serving network by computing AUTN_{UE} using the fresh (T_1) sent by the UE in its attach request. If the user authentication request is a replay then it will automatically lead to authentication failure ($\text{AUTN}_{UE} \neq \text{AUTN}$). Hence, the proposed approach ensures resistance to the replay attack in the LTE/LTE-A networks. □

3.5 *Theorem 5*

The protocol ensures strong mutual authentication and resistance to the redirection attack and overbilling attack in LTE/LTE-A networks.

Proof: To achieve the goal of strong mutual authentication between the LTE/LTE-A entities, the EAKA-EPS protocol uses the challenge–response mechanism. HSS verifies authenticity of the eNodeB and the serving network by checking the validity of received eNodeB certificate (C_{eNodeB}) and the serving network identity (SN-ID). For verifying the authenticity of the HSS, UE computes authentication token AUTN_{UE} in a similar manner as AUTN is computed. If $\text{AUTN}_{UE} = \text{AUTN}$, it means HSS is an authenticated entity and eNodeB and MME are HSS-verified entities. For UE authentication, UE computes RES in a similar manner as MME computes XRES and sends RES to the MME; MME checks whether RES = XRES or not. If both values are equal, it implies that UE is an authenticated entity. Here, adversaries cannot compute the same values for the authentication parameters without the knowledge of secret key K'_{ASME}. Thus, the proposed approach prevents deployment of fake base stations in the LTE/LTE-A networks, which mitigates the issues of the redirection attack and the overbilling attack in the network. □

3.6 *Theorem 6*

The protocol ensures resistance to the single-key dependency problem.

Proof: The existing EPS-AKA protocol is dependent on the secrecy of the permanent LTE key K. If anyhow K is compromised then whole system security will be compromised. Taking this into consideration, the proposed approach uses dynamic key generating key K' ($K' = f_2(T_1, C_{eNodeB}) \oplus K$) instead of the permanent

LTE key *K* for computing all the subsequent keys. Thus, the issue of single-key dependency has been resolved in the proposed EAKA-EPS approach. Many researchers suggested various approaches for achieving perfect secrecy in the EPS; the pros and cons of these approaches are discussed in detail in section 1.1. The authors compared some of the existing approaches with the proposed approach, and comparison results are shown in table 1. Comparison is performed on the basis of the attacks prevented by the approaches and performance enhancement factors included by these approaches. Comparison results show that the proposed approach achieves security against most of the malicious attacks currently feasible in LTE/LTE-A networks. □

4. Formal verification results

According to 3GPP, all the wired channels are secure (IPsec enable) in LTE/LTE-A networks, Hence, the authors simulated the wireless interface only on AVISPA over the Intel(R) Core(TM) i5 2.60 GHz, 4 gigabyte RAM, under ubuntu 12.04 operating system. AVISPA integrates different back-ends like On-the-Fly Model-Checker (OFMC) and CL-based Attack Searcher (CL-AtSe). These back-ends are complementary to each other rather than equivalent and force perfect cryptography, which implies that an attacker cannot recover information from the encrypted message without the knowledge of the corresponding decryption key [49]. The protocol is written in the "High Level Protocol Specifications Language" to be tested on AVISPA back-end servers. "SAFE" and "NO ATTACK FOUND" are the keywords that indicate that the protocol achieves specified goals and it is safe against the automatically created attacks by AVISPA. AVISPA also simulates the behaviour of Dolev-Yao intruder model (network is fully controlled by an intruder) [50]. All the messages transmitted by agents are accessible to the intruder and an intruder can analyse, modify and intercept messages sent by the agents. The primary goals of the proposed protocol are secure transmission of the data over the wireless interface and strong mutual authentication between the LTE/LTE-A components. In the model of the proposed protocol, there are two roles user_Equipment and eNodeB as shown in listings 1 and 2, respectively, and the desired goals of the protocol are declared in Listing 3. Verification results (OFMC, CL-AtSe) of the proposed protocol on AVISPA are found to be safe and shown in figures 8 and 9. From the results we can conclude that proposed protocol accomplishes goals of the mutual authentication and secrecy over the wireless interface under the test of AVISPA.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/EAKA-EPS1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 5 nodes
  depth: 4 plies
```

Figure 8. Results reported by the OFMC back-end.

Listing 1. Role of user_equipment.

```
role user_Equipment(U,S       : agent,
          Snd, Rec            : channel(dy),
          $K_enc$             : symmetric_key,
          $K_int$             : symmetric_key,
          IMSI,UE_cap         : text,
          F5,F2               : function,
          $P_ue$              : public_key
          )
played_by U def=
 local
          State               : nat,
          MAC1,KSI            : text
          MAC2,MAC3,T1        : text,
          CHV                 : message,
          AUTN,Rand,RES,Cenb  : text,
          $K$                 : symmetric_key
 const
          im_conf ,u1,u2      : protocol_id
 init
      State := 1
 transition
  1. State  = 1 /\ Rec(start) =|>
      State':= 2 /\ Snd(P_ue)

  2. State  = 2 /\ Rec({K_enc'.K_int'}_P_ue)
                    =|>
      State':= 3 /\ Snd({IMSI.UE_cap'.KSI'.T1
                    '.MAC1'}_K_enc)
                 /\ secret(IMSI,im_conf,{U,S})

  3. State  = 3 /\ Rec({AUTN'.Rand'.CHV'.
                    MAC2'}_K_enc)=|>
      State':= 4 /\ RES':=xor(F2(K.Rand),CHV)
                 /\ Snd({RES'.MAC3'}_K_enc)
                 /\ wrequest(U,S,u1,AUTN)
                 /\ witness(S,U,u2,RES)
end role
```

Listing 2. Role of eNodeB.

```
role eNodeB(S,U          : agent,
            Snd, Rec     : channel(dy),
            $K_enc$      : symmetric_key,
            $K_int$      : symmetric_key,
            IMSI, UE_cap: text,
            F2,F5        : function,
            $P_ue$       : public_key
           )
played_by S def=
  local
        State                      : nat,
        MAC1,KSI,MAC2,MAC3,T1      : text,
        CHV                        : message,
        AUTN,Rand,RES,Sq ,Cenb     : text
  const
   kenc_conf, kint_conf, autn_conf: protocol_id
   rand_conf, u1,u2,chv_conf: protocol_id
  init
        State := 1
  transition
    1.  State  = 1 /\ Rec(P_ue)=|>
        State':= 2 /\ Snd({K_enc'.K_int'}_P_ue)
                   /\ secret(K_enc,kenc_conf,
                  {U,S})
                   /\ secret(K_int,kint_conf,
                  {U,S})
    2.  State  = 2 /\ Rec({IMSI.UE_cap'.KSI'.
                        T1'.MAC1'}_K_enc) =|>
        State':= 3 /\ CHV':=F5(K_enc.Cenb')
                   /\ Snd({AUTN'.Rand'.CHV'.
                   MAC2'}_K_enc)
                   /\ secret(AUTN',autn_conf,
                  {U,S})
                   /\ secret(Rand',rand_conf,
                  {U,S})
                   /\ secret(CHV',chv_conf,
                  {U,S})
                   /\ witness(S,U,u1,AUTN)
     3.  State  = 3 /\ Rec({RES'.MAC3'}_K_enc)
                    =|>
        State':= 4 /\ Snd(Sq)
                   /\ wrequest(U,S,u2,RES)
end role
```

Listing 3. Goals of the model.

```
goal
  secrecy_of im_conf,kenc_conf,kint_conf,
             autn_conf,rand_conf,chv_conf
  authentication_on u1
  authentication_on u2
end goal
```

5. Performance evaluation

In this section, the authors analyse the proposed scheme from three important metrics: bandwidth consumption, computational cost and storage overhead by comparison to existing authentication and key agreement schemes.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/EAKA-EPS.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Figure 9. Results reported by the CL-ATSE back-end.

5.1 *Bandwidth consumption between the MME and the HSS*

To analyse signalling overhead and bandwidth consumption between the MME and the HSS a simple fluid flow mobility model has been customized [46, 51]. The mobility model says that the traffic flow in a region is directly proportional to the length of the registration area (L), density of UEs in the region (ρ) and the velocity of the UE movement (v). The mobility model assumes that the direction of movement is distributed over [0–2π]. Thus, the rate of registration area crossing (R) is given as (Eq. (3))

$$R = \frac{\rho * v * L}{\pi}. \tag{3}$$

Traffic because of the arrival rate of the authentication requests is generated due to the mobility of UEs into the new registration area. Thus, the authentication requests (R) generated per registration area (as per assumptions in table 2) is 3.757/s. Req_{auth} is the total number of requests arriving for the authentication at the HSS in every second.

Thus, the total number of authentication requests at the HSS is generated as follows (Eq. (4)):

$$\text{Req}_{auth} = R \times \text{Ar} = 375.7/\text{s}. \tag{4}$$

Computation of bandwidth consumption between the HSS and the MME is sufficient to show the bandwidth optimization in the proposed scheme. Bandwidth consumption between the HSS and the MME ($\text{BW}_{MME \leftrightarrow HSS}$) can be

Table 2. Parameters to calculate traffic rate to the LTE database.

Parameter	Assumption value
Number of registration areas (Ar)	100
Square registration area size	$(6.657\ \text{km})^2 = 44.3$ sq km
Length of registration area (L)	25.3 km
Mean density of UE (ρ)	350/sq km
Total number of UE	$100 * 44.3 * 350 = 1.55$ million
Average velocity of UE (v)	4.8 km/h

measured in terms of the number of bits involved in the exchanged massages for the authentication. Thus, the bandwidth consumption between the MME and the HSS can be calculated as follows (Eq. (5)):

$$\text{BW}_{MME\leftrightarrow HSS} = \sum \text{bits(core traffic)} \times \text{Req}_{auth} \tag{5}$$

$$\sum \text{bits(core traffic)} = \sum_{i=1}^{i=n} |\text{message}_i| \tag{6}$$

where n is the total number of messages communicated between the MME and the HSS for the UE authentication and $|\text{message}_i|$ represents the bit length of the ith message. Accordingly, the bandwidth consumption of the various approaches is as follows.

5.1a *Bandwidth analysis of the EPS-AKA (standard scheme) protocol*: In this scheme, MME receives authentication vectors from the HSS by sending two messages: message_1, where MME forwards request for the authentication vectors to the HSS, and message_2, where HSS forwards n sets of the authentication vectors to the MME. The total number of bits (bit size of the parameters is shown in table 3) involved in authentication procedure are

$$\begin{aligned}\text{message}_1 &= |\text{IMSI}| + |\text{SNID}| = 128 + 48 = 176 \text{ bits}\\ \text{message}_2 &= \text{AV}(|\text{XRES}| + |\text{AUTN}| + |\text{Rand}| \\ &\quad + |K_{ASME}|)n = 544n \text{ bits}.\end{aligned}$$

Table 3. Bit size of the parameters.

Parameters	Size	Parameters	Size
PU_{UE}, PR_{UE}	128	RES	32
AMF	16	TEMP	128
IMSI	128	AK	48
AUTN	128	SN-ID	48
Rand	128	MAC	64
K_{ASME}, K'_{ASME}	256	T_1	48
K_{enc}, K_{int}	128	SQN	48
K_{eNB}	256	NCC	8
NH	256	K_{eNB}*	256
KI	128	M-ID	32
SK	128	C_{eNodeB}	128

In EPS-AKA, bandwidth consumption for the single authentication request is $176 + 544n$ bits. Hence, the overall bandwidth consumption ($\text{BW}_{MME\leftrightarrow HSS}$) between the MME and the HSS in the EPS-AKA approach is 1.42 Mbits/s (Eq. (5)), where required sets of the authentication vectors (n)/request are 7.

5.1b *Bandwidth analysis of the Fikadu's approach (enhanced-AKA)*: In this approach, messages that incur bandwidth between the MME and the HSS for UE authentication are message1, where MME requests the HSS for sending the secret key, and message2, where HSS forwards secret key (s), KI and IMSI back to the MME.

$$\begin{aligned}\text{message}_1 &= 2|\text{SN-ID}| + |\text{KI}| + |\text{IMSI}| + |\text{Rand}_{UE}| \\ &\quad + |\text{M-ID}| = 512 \text{ bits}\\ \text{message}_2 &= |s| + |\text{KI}| + |\text{IMSI}| = 384 \text{ bits}.\end{aligned}$$

Bandwidth consumption for single authentication request is 896 bits. The overall bandwidth consumption ($\text{BW}_{MME\leftrightarrow HSS}$) between the MME and the HSS for enhanced AKA is 0.27 Mbits/s (Eq. (5)).

5.1c *Bandwidth analysis of the Hamandi's approach (modified LTE-AKA)*: In this scheme, messages that incur bandwidth between the MME and the HSS for the authentications are message1, where MME requests the HSS for the authentication vectors, and message2, where HSS forwards n copies of the authentication vectors back to the MME.

$$\begin{aligned}\text{message1} &= |\text{Uid}| + |\text{SN-ID}| = 176 \text{ bits}\\ \text{message2} &= (\text{AV}(|\text{Rand}| + |\text{XRES}| + |\text{K}_{ASME}| \\ &\quad + |\text{AUTN}| + |\text{IMSI}| + |\text{SK}|)n) = 800n \text{ bits}.\end{aligned}$$

Bandwidth consumption for the single authentication request is $176+800n$ bits. Hence, the overall bandwidth consumption ($\text{BW}_{MME\leftrightarrow HSS}$) between the MME and the HSS for modified LTE-AKA is 2.0 Mbits/s (Eq. (5)), where required sets of authentication vectors (n)/request are 7.

5.1d *Bandwidth analysis of the EAKA-EPS (proposed approach)*: In the proposed scheme, messages that incur bandwidth between the MME and the HSS for the authentication are message1, where MME forwards a request for temporary authentication key to the HSS, and message2, where HSS forwards temporary authentication key with CHV parameter back to the MME:

$$\begin{aligned}\text{message1} &= |\text{SN-ID}| + |\text{IMSI}| + |T1| + |C_{eNodeB}| = 352 \text{ bits},\\ \text{message2} &= (|\text{K}'_{ASME}| + |\text{CHV}|) = 384 \text{ bits}.\end{aligned}$$

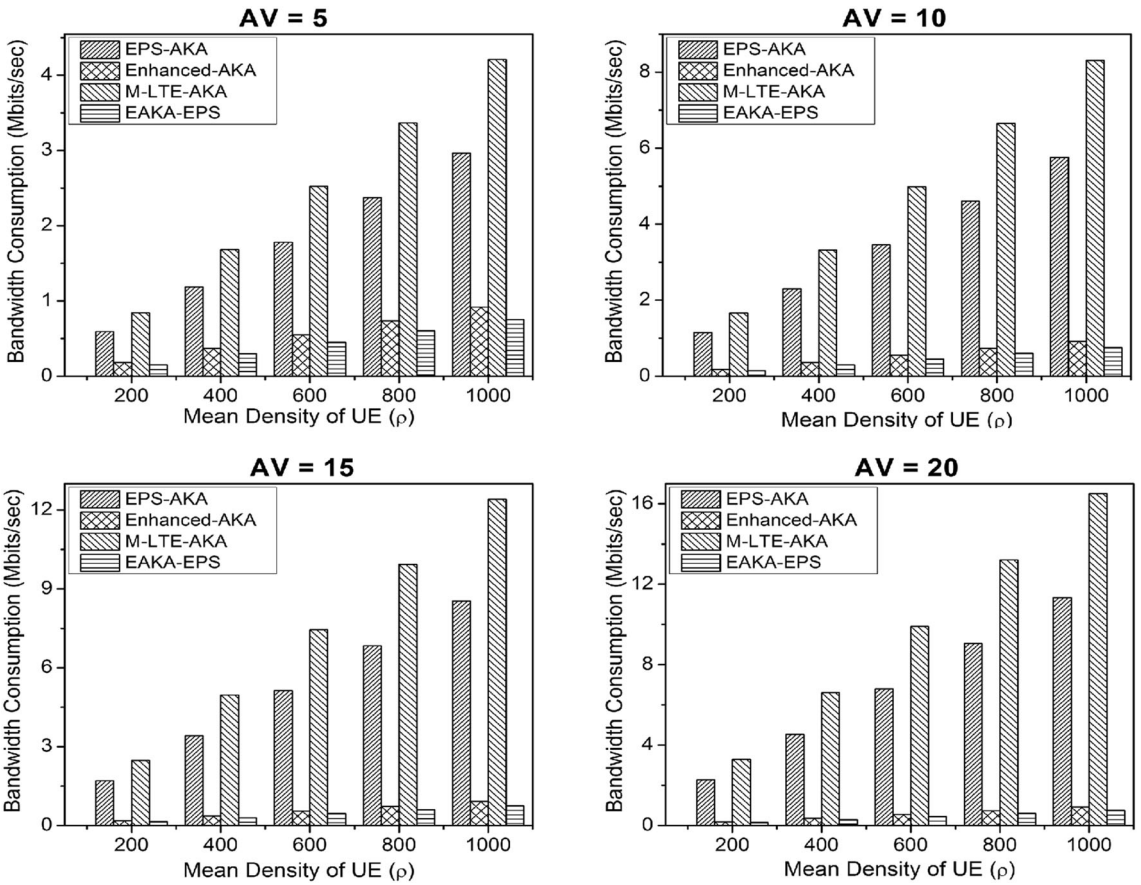

Figure 10. Bandwidth consumption between HSS and MME in various approaches suggested by researchers, when needed number of authentication vectors (n) are: AV = 5, AV = 10, AV = 15 and AV = 20. EAKA-EPS reduces bandwidth consumption to 81% between UE and MME for the first authentication of the UE.

Bandwidth consumption for the single authentication request is 736 bits. Hence, the overall bandwidth consumption ($BW_{MME \leftrightarrow HSS}$) between the MME and the HSS for the proposed approach is .26 Mbits/s (Eq. (5)). Calculations show that the proposed approach reduces bandwidth consumption between the HSS and the MME to 81% in comparison with the standard AKA protocol. In addition, for the j^{th} authentication request from the registered UE, bandwidth consumption will be 0% because MME need not request back the HSS for the authentication parameters. Comparison between all these approaches is depicted in figure 10 corresponding to the mean density of UEs/registration area. From figure 10 the authors can conclude that the proposed approach achieves the goal of less bandwidth consumption between the MME and the HSS in comparison with the EPS-AKA approach and the approaches suggested by other researchers.

5.2 *Computational cost*

For the calculations of the computational cost, the authors compare security functions that are executed for providing authentication to the UE. Although, all security functions carry different computational costs, here, for all the security functions, computation cost is assumed to be 1 [37]. Other operations will not be considered because their computational cost is very less. All the protocols are analysed under the same standards for maintaining the fairness in the computation. Computational overhead is calculated individually for the UE, MME and the HSS against the security functions performed.

5.2a *Computational cost analysis of the EPS-AKA (standard approach) protocol*: Computational cost corresponding to the security functions executed on the UE, MME and the HSS for providing authentication to the UE is as follows:

$$\begin{aligned} \text{UE:}(f_1 + f_2 + f_3 + f_4 + f_5 + 2\text{KDF}) &= 7, \\ \text{MME: No. security functions} &= 0, \\ \text{HSS: AV}(f_1 + f_2 + f_3 + f_4 + f_5 + 2\text{KDF})n &= 7n. \end{aligned}$$

For single authentication request, total number of security functions executed on the EPS-AKA are $7+7n$, where n is the required number of authentication vectors/UE. Thus,

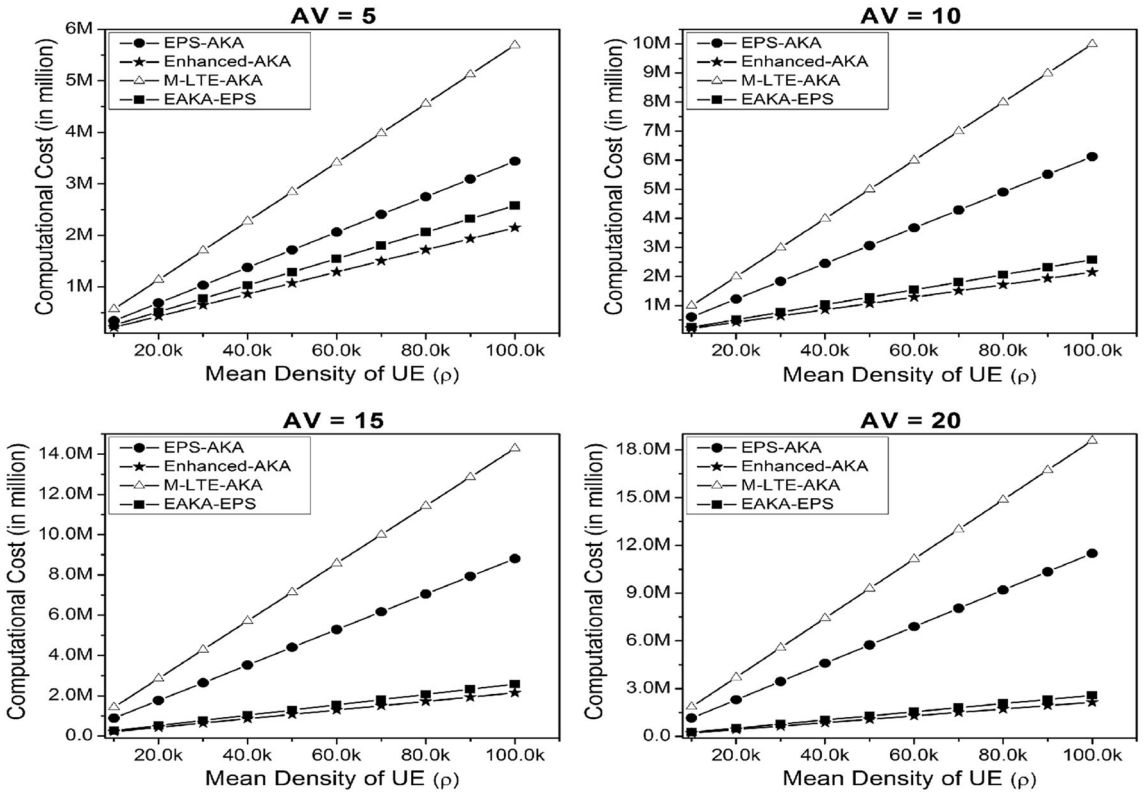

Figure 11. Comparison of computational cost of various approaches suggested by researchers. When needed number of authentication vectors (n) are: AV = 5, AV = 10, AV = 15 and AV = 20.

the overall computation number of the EPS-AKA against the security functions is as follows:

$$\text{computational cost } (\text{Cc}) = \text{Req}_{auth}(7 + 7n)/\text{s}.$$

5.2b *Computational cost analysis of the Fikadu's approach-(enhanced-AKA)*: Computational cost corresponding to the security functions executed on the UE, MME and the HSS for providing authentication to the UE is as follows.

$$\begin{aligned}\text{UE: } (f' + \text{Enc} + f_1 + f_2 + f_3 + f_4 + 2f_5 + \text{KDF} + \text{Denc}) &= 10,\\ \text{MME: } (f_1 + f_2 + f_3 + f_4 + f_5 + \text{KDF} + \text{Enc} + \text{Dec}) &= 8,\\ \text{HSS: } (f' + \text{KDF}) &= 2.\end{aligned}$$

For single authentication request, total number of security functions executed in Fikadu's approach is 20. Thus, the overall computation number of the fikadu's approach against the security functions is as follows:

$$\text{computational cost } (\text{Cc}) = \text{Req}_{auth}\,(20)/\text{s}.$$

5.2c *Computational cost analysis of the Hamandi's approach*: Computational cost corresponding to the security functions executed on the UE, MME and the HSS for providing authentication to the UE are as follows.

$$\begin{aligned}&\text{UE: } (\text{Enc} + 2f_k + \text{MAC} + \text{KDF} + f_1 + f_2 + f_3 + f_4 + f_5 + 2\text{KDF}) = 12,\\ &\text{MME: no. security functions} = 0,\\ &\text{HSS: Dec} + \text{AV } (3\text{KDF} + f_1 + f_2 + f_3 + f_4 + f_5)\\ &n = 1 + 8n.\end{aligned}$$

For single authentication request, the total number of security functions executed in Hamandi's approach is $13+8n$, where n is the required number of authentication vectors/UE. The overall computational cost of Hamandi's approach against the security functions is as follows:

$$\text{computational cost } (\text{Cc}) = \text{Req}_{auth}(13 + 8n)/\text{s}.$$

5.2d *Computational cost analysis of the EAKA-EPS (proposed approach) protocol*: Computational cost corresponding to the security functions executed on the UE, MME and the HSS for providing authentication to the UE are as follows.

$$\begin{aligned}&\text{UE : } (\text{Enc} + \text{MAC} + f_1 + f_2 + f_3 + f_4 + f_5 + 2\text{KDF} + \text{Dec} + \text{Enc} + \text{MAC}) = 12,\\ &\text{MME:} (\text{Dec} + f_1 + f_2 + f_3 + f_5 + \text{KDF} + \text{Enc} + \text{MAC} + \text{Dec}) = 9,\\ &\text{HSS: } (f_3 + f_4 + \text{KDF}) = 3.\end{aligned}$$

For single authentication request, total number of security functions executed on EAKA-EPS is 24; hence, the overall computation number of EAKA-EPS against the security functions is as follows:

$$\text{computational cost } (\text{Cc}) = \text{Req}_{auth}\,(24)/\text{s}.$$

Figure 11 shows the overall computational cost of various suggested approaches corresponding to the mean density of the UEs/registration area. From the comparison results (figure 11) the authors can conclude that proposed approach achieves the goal of less computational overhead in comparison with the standard AKA. Computational overhead is a little bit more in comparison with the Fikadu's approach (enhanced-AKA), but due to the security needs fulfilled by the suggested protocol it is bearable.

5.3 *Storage overhead in the serving network*

Memory consumption is incurred due to the introduced new asymmetric keys, which are stored on the UE and the MME. Due to the secure wireless interface, IMSI transmission is secure and it replaces the need of dynamic TMSI assignment to the UE. With this, the suggested approach supports only horizontal key derivation; thus there is no need of NH keys and NCC values to be computed and stored on the MME and UE. Somewhere the storage overhead at the UE and the MME is compensated. In contrary to the suggested approach, the standard AKA approach stores 1.94 bits/s $(\text{AV}(|\text{XRES}| + |\text{AUTN}| + |\text{Rand}| + |K_{ASME}|)n \times 375.5)$ at the MME, where the required number of authentication vectors (n) is 10. However, for providing authentication to the UEs, authors' approach needs to store only 0.09 bits/s ($|K'_{ASME}| \times 375.5$) at the MME. Storage overhead at MME for various suggested and standard approaches is depicted in figure 12 corresponding to the mean density of UEs/registration area, and from these results the authors conclude that EAKA-EPS achieves the goal of the storage overhead reduction at the serving network.

6. Implementation/simulation needs

Scope of the current research is to propose a more secure authentication and key agreement scheme for the LTE/LTE-A networks and to verify the security of the proposed

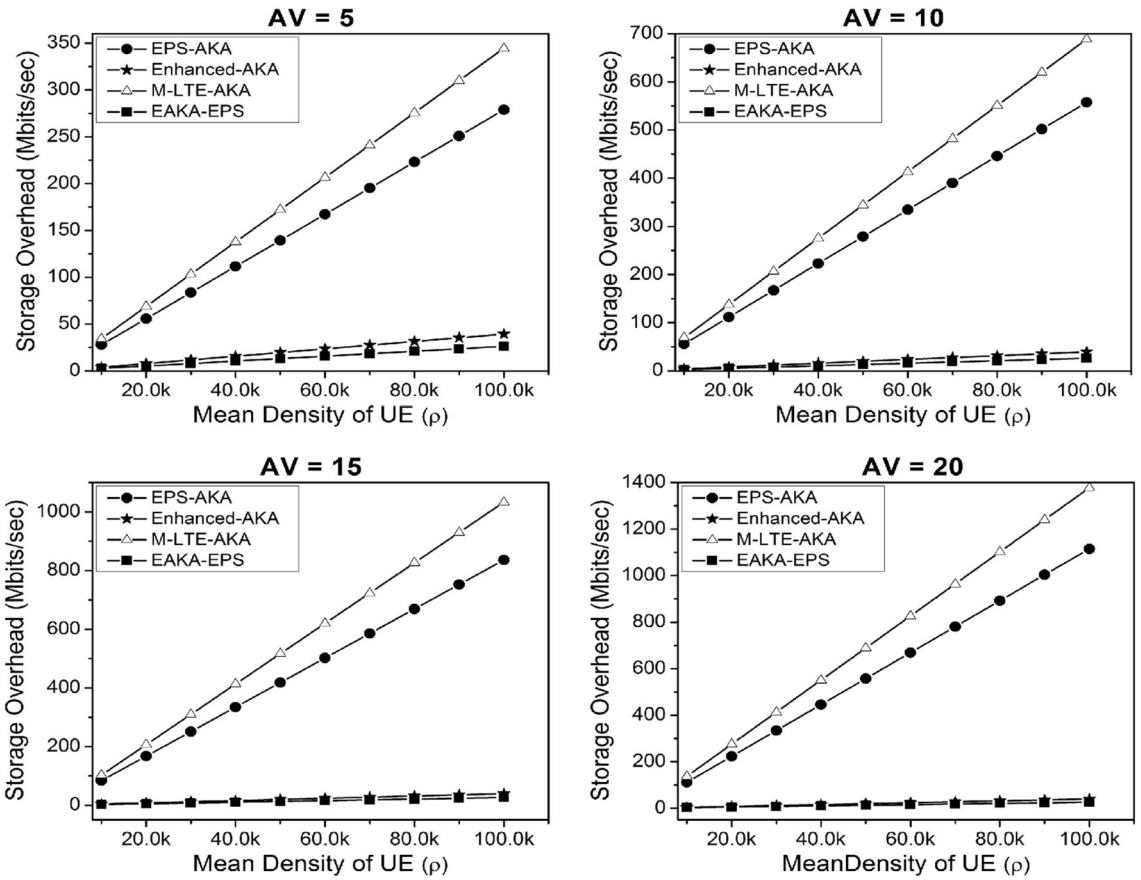

Figure 12. Comparison of storage overhead at MME for various approaches suggested by the researchers. Needed number of authentication vectors (n) are AV = 5, AV = 10, AV = 15 and AV = 20.

scheme on AVISPA with its performance analysis. However, for the proof-of-concept, EAKA-EPS protocol can be simulated on Network Simulator-3 (ns-3) version 3.17 and measurements can run on Intel(R) Core(TM) i5 CPU@2.60 GHz, 4 gigabyte RAM, under ubuntu 12.04 operating system.

7. Conclusion

In this research, the authors propose an Efficient Authentication and Key Agreement Protocol for Evolved Packet System, called EAKA-EPS. To the best of the authors' knowledge, EAKA- EPS achieves all the specified objectives successfully within the defined scope. The proposed approach is a hybrid approach that includes both symmetric and asymmetric key encryptions but minimizes the use of the asymmetric encryption due to its excessive overhead. Unlike the other approaches, EAKA-EPS enables secure transmissions over the wireless interface, maintains strong mutual authentication between the entities and achieves AS secrecy at the time of X_2 handovers. Moreover, the suggested approach was proven to thwart subscriber's identity leak, DoS attack, MitM attack, replay attack, desynchronization attack and redirection attack. This new approach is formally verified on AVISPA and verification results are proven to be safe. Its performance analysis demonstrates that the suggested approach achieves the subscriber's security needs and better performance in terms of bandwidth consumption, memory consumption and involved computational cost. Moreover, the EAKA-EPS protocol is applicable to the current architecture of LTE/SAE networks without the need of special software implementations. Finally, the researchers conclude that the suggested approach is powerful for the recent and upcoming generations of the mobile networks because of its novel features.

Acknowledgements

The authors are thankful to The Director, VNIT Nagpur, for his constant encouragement to publish this paper. The authors also wish to thank the Department of Electronics and Information Technology (Deity), Ministry of Communication and Information Technology, Government of India, for financial assistance.

References

[1] Bikos A and Sklavos N 2013 LTE/SAE security issues on 4G wireless networks. *IEEE Secur. Priv.* 11(March–April 2013): 55–62

[2] Cichonski J and Franklin J M 2016 *LTE architecture overview and security analysis*. Draft NISTIR 8071, U.S. Department of Commerce

[3] Ahmadian Z, Salimi S and Salahi A 2010 Security enhancements against UMTS-GSM interworking attacks. *Comput. Netw.* 54(13): 2256–2270

[4] Carla L, Fantacci R, Gei F, Marabissi D and Micciullo L 2016 LTE enhancements for public safety and security communications to support group multimedia communications. *IEEE Netw.* 30(1): 80–85

[5] Seddigh N, Nandy B, Makkar R and Beaumont J F 2010 Security advances and challenges in 4G wireless networks. In: *Proceedings of the 2010 Eighth International Conference on Privacy, Security and Trust*, pp. 62–71

[6] Thuana V D, Jønvikb T, Jørstadc I, Boninge F and Thanhe V D 2009 Strong authentication using dual SIM. In: *Proceedings of the 2009 13th International Conference on Intelligence in Next Generation Networks: Beyond the Bit Pipes, ICIN 2009*, pp. 2–5

[7] Abdeljebbar M and Kouch R E 2014 Fast authentication during handover in 4G LTE/SAE networks. *IERI Procedia* 10: 11–18

[8] Mohapatra S K, Swain B and Das P 2015 Comprehensive survey of possible security issues on 4G networks. *Int. J. Netw. Secur. Appl.* 7(2): 61–69

[9] Damnjanovic A, Montojo J, Wei Y, Ji T, Luo T, Vajapeyam M, Yoo T, Song O and Malladi D 2011 A survey on 3GPP heterogeneous networks. *IEEE Wirel. Commun.* 18(3): 10–21

[10] Ghosh A, Mangalvedhe N, Ratasuk R, Mondal B, Cudak M, Visotsky E, Thomas T A, Andrews J G, Xia P, Jo S H, Dhillon H S and Novlan T D 2012 Heterogeneous cellular networks: from theory to practice. *IEEE Commun. Mag.* 50(6): 54–64

[11] Jover R, Lackey J and Raghavan A 2014 Enhancing the security of LTE networks against jamming attacks. *EURASIP J. Inform. Secur.* 2014(1): 7

[12] 3rd Generation Partnership Project *Technical specification group services and system aspects*. 3GPP System Architecture Evolution (SAE) Security Architecture Release 11, 3GPP TS, vol. 33.401, p. V11.5.0

[13] 3rd Generation Partnership Project *Technical specification group services and system aspects*. 3GPP System Architecture Evolution (SAE) Security Architecture Release 8, 3GPP TS, vol. 33.401, p. V8.8.0

[14] 3rd Generation Partnership Project *Technical specification group service and system aspects*. Network Domain Security Authentication Framework Release 6, 3GPP TS, vol. 33.310, p. V1.1.0

[15] Hamandi K, Abdo J B, Elhajj I H, Kayssi A and Chehab A 2016 A privacy-enhanced computationally-efficient and comprehensive LTE-AKA. *Comput. Commun.* 98: 20–30

[16] Abdo J B, Chaouchi H and Aoude M 2012 Ensured confidentiality authentication and key agreement protocol for EPS. In: *Proceedings of the 2012 Symposium on Broadband Networks and Fast Internet, RELABIRA 2012*, pp. 73–77

[17] Shaik A, Borgaonkar R, Asokan N, Niemi V and Seifert J P 2016 Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In: *Proceedings of NDSS*, pp. 21–24

[18] Pan M, Lin T and Chen W 2015 An enhanced handover scheme for mobile relays in LTE-A high-speed rail networks. *IEEE Trans. Veh. Technol.* 64(2): 743–756

[19] Han C and Choi H 2014 Security analysis of handover key management in 4G LTE/SAE networks. *IEEE Trans. Mob. Comput.* 13(2): 457–468

[20] Sinclair N, Harle D, Glover I A, Irvine J and Atkinson R C 2013 An advanced SOM algorithm applied to handover management within LTE. *IEEE Trans. Veh. Technol.* 62(5): 1883–1894

[21] Rupprecht D, Jansen K and Pöpper C 2016 Putting LTE security functions to the test: a framework to evaluate implementation correctness. In: *Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT 16)*

[22] Park Y and Park T A 2007 Survey of security threats on 4G networks. In: *Proceedings of the Workshop on Security and Privacy in 4G Networks*

[23] Cao J, Ma M, Li H, Zhang Y and Luo Z 2014 A survey on security aspects for LTE and LTE-A networks. *IEEE Commun. Surv. Tutor.* 16(1): 283–302

[24] Yaping D, Hong F, Xianzhong X, Jihua Z, Yucheng Z and Jinling S 2009 A novel 3GPP SAE authentication and key agreement protocol. In: *Proceedings of IC-NIDC 2009*

[25] Forsberg D, Leping H, Tsuyoshi K and Alanärä S 2007 Enhancing security and privacy in 3GPP E-UTRAN radio interface. In: *Proceedings of the IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC07*

[26] Lee M F, Smart N P, Warinschi B and Watson G J 2014 Anonymity guarantees of the UMTS/LTE authentication and connection protocol. *Int. J. Inform. Secur.* 13(6): 513–527

[27] Lin Y B, Chang M F, Hsu M T and Wu L Y 2005 One-pass GPRS and IMS authentication procedure for UMTS. *IEEE J. Sel. Areas Commun.* 23(6): 1233–1239

[28] Huang C M and Li J W 2009 Reducing signaling traffic for the authentication and key agreement procedure in an IP multimedia subsystem. *Wirel. Pers. Commun.* 51(1): 95–107

[29] Ntantogian C and Xenakis C 2009 One-pass EAP-AKA authentication in 3G-WLAN integrated networks. *Wirel. Pers. Commun.* 48(4): 569–584

[30] Rahman M M and Heydari S S 2012 A self-healing approach for LTE evolved packet core. In: *Proceedings of the 2012 25th IEEE Canadian Conference on Electrical and Computer Engineering: Vision for a Greener Future, CCECE 2012*

[31] Zhang Y and Fujise M 2006 An improvement for authentication protocol in third-generation wireless networks. *IEEE Trans. Wirel. Commun.* 5(9): 2348–2352

[32] Fanian A, Berenjkoub M and Gulliver T A 2009 A new mutual authentication protocol for GSM networks. In: *Proceedings of the Canadian Conference on Electrical and Computer Engineering*, pp. 798–803.

[33] Chang C C, Lee J S and Chang Y F 2005 Efficient authentication protocols of GSM. *Comput. Commun.* 28(8): 921–928

[34] Saxena N and Chaudhari N S 2013 SAKA: a secure authentication and key agreement protocol for GSM networks. *CSI Trans. ICT* 1(December): 1–11

[35] Aydemir Ő and Selçuk A A 2005 A strong user authentication protocol for GSM. In: *Proceedings of the Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE*, pp. 150–153

[36] Caragata D, El Assad S, Shoniregun C and Akmayeva G 2011 UMTS security: enhancement of identification, authentication and key agreement protocols. In: *Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, December*, pp. 278–282

[37] Zhang M Z M and Fang Y F Y 2005 Security analysis and enhancements of 3GPP authentication and key agreement protocol. *IEEE Trans. Wirel. Commun.* 4(2): 734–742

[38] Islam S and Ajmal F 2009 Developing and implementing encryption algorithm for addressing GSM security issues. In: *Proceedings of the 2009 International Conference on Emerging Technologies, ICET 2009*, pp. 358–361

[39] Hytönen V, Puchko O, Höhne T and Chapman T 2012 Introduction of multiflow for HSDPA. In: *5th International Conference on New Technologies, Mobility and Security—Proceedings of NTMS 2012 Conference and Workshops*

[40] Haddad Z J, Sanaa T and Ismail I A S 2014 SEPS-AKA: a Secure Evolved Packet System Authentication And Key Agreement scheme for LTE-A networks. In: *Proceedings of WiMONe*, pp. 57–70

[41] Prasad M and Manoharan R 2015 A robust secure DS-AKA with mutual authentication for LTE-A. *Appl. Math. Sci.* 9(47): 2337–2349

[42] Prakash K and Muniyal B 2015 EPMOS based secure mobile communication in LTE/SAE networks. In: *Proceedings of the 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)*, pp. 101–105

[43] Zemao C, Junge Z and Biyi H 2012 Optimizing PKI for 3GPP Authentication and Key Agreement. In: *Proceedings of the 2012 Fourth International Conference on Multimedia Information Networking and Security*, pp. 2–5

[44] Li X and Wang Y 2011 Security enhanced authentication and key agreement protocol for LTE/SAE network. In: *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2011*, pp. 0–3

[45] Abdrabou M A, Elbayoumy A D E and El-Wanis E A 2016 LTE authentication protocol (EPS-AKA) weaknesses solution. In: *Proceedings of the 2015 IEEE 7th International Conference on Intelligent Computing and Information Systems, ICICIS 2015*, pp. 434–441

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

[47] Ekene O E, Ruhl R and Zavarsky P 2016 Enhanced user security and privacy protection in 4G LTE network. In: *Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, pp. 443–448

[48] Hamandi K, Sarji I, Chehab A, Elhajj I H and Kayssi A 2013 Privacy enhanced and computationally efficient HSK-AKA LTE scheme. In: *Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops, WAINA 2013*, pp. 929–934

[49] Takkinen L 2006 Analysing security protocols with AVISPA. In: *Proceedings of the TKK T-110.7290 Research Seminar on Network Security*

[50] Dolev D 1983 On the security of public key protocols. *IEEE Trans. Inform. Theory* 29(2): 198–208

[51] Mohan S 1996 Privacy and authentication protocols for PCS. *IEEE Pers. Commun.* 3(5): 34–38