SAK-AKA: A Secure Anonymity Key of Authentication and Key Agreement protocol for LTE network

Shadi Nashwan
Department of Computer Science and Information, Aljouf University, Saudi Arabia

Abstract: *3rdGeneration Partnership Project (3GPP) has proposed the Authentication and Key Agreement (AKA) protocol to achieve the security requirements of Evolved Packet System (EPS) in the Long Term Evolution (LTE) network, called (EPS-AKA) protocol. Nevertheless, the EPS-AKA protocol is still has some drawbacks in authentication process due to inherit some weaknesses from the predecessor protocols. This paper proposes a secure anonymity Key of Authentication and Key Agreement (SAK-AKA) protocol for LET network to enhance the security level of EPS-AKA protocol. The same security architecture of EPS-AKA is used by the proposed protocol without adding extra cost to the system. Specifically, the SAK-AKA protocol increases the difficulty of defeating the authentication messages by complete concealing of IMSI with perfect forward security. The extensive security analysis proves that the SAK-AKA protocol is secure against the drawbacks of current EPS-AKA protocol. Moreover, the performance analysis in terms of the bandwidth consumption, the authentication transmission overhead and the storage consumption demonstrates that the SAK-AKA protocol relatively is more efficient than the current EPS-AKA protocol.*

Keywords: *3GPP, LTE network, IPsec protocol, UMTS-AKA protocol, EPS-AKA protocol.*

Received March 21, 2017; accepted May 28, 2017

1. Introduction

The 3rdgeneration Partnership Project (3GPP) has proposed the Long Term Evolution (LTE) network as the promising technology of current mobile communication networks. The LTE network has added two main entities to enhance the Quality of Service (QoS) in the 3GPP environment. The first entity is called Evolved Universal Terrestrial Radio Access Network (E-UTRAN). The second entity is the Internet Protocol (IP) that is deployed in Evolved Packet Core (EPC).

The E-UTRAN improves the access technology with high data rate, low latency, and flexible bandwidth while the IP offers full interworking with heterogeneous wireless networks [1]. In the LTE network architecture, the User Equipment (UE) connects to the EPC via E-UTRAN. Specifically, the e-UTRAN is a mesh network contains a set of Evolved NodeB (eNBs). The latter modulates and demodulates the radio signals to connect with the UEs. The EPC is comprised of Mobility Management Entity (MME), Serving Gateway (SGW), Packet Data Network Gateway (P-GW), Home Subscriber Serve (HSS), Authentication Center (AuC) and Policy Charging Rules Function (PCRF). In order to fetch the users profile information that are stored in the HSS database, the MME communicates with HSS for user authentication, mobility management, handover management, EPS bearer management and Non-Access Stratum (NAS) signaling. The P-GW communicates with the outside IP networks. The PCRF is responsible about the rules and policies of QoS, user charging and access the network resources. The S-GW forwards data between the eNBs and the P-GW. The AuC is resided within the HSS to map the user identifier and the pre-loaded shared key as well as to perform the key derivation functions during the authentication sessions [9]. Figure 1 illustrates the LTE network architecture.

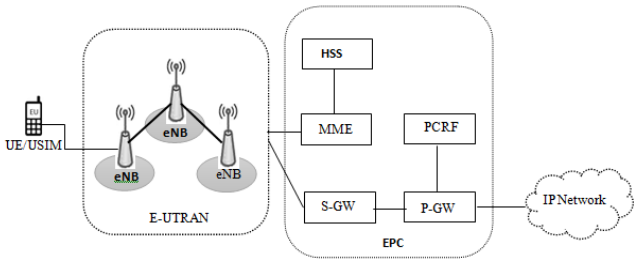


Figure 1. LTE Network architecture.

The security principles of LTE network follow the same principles of the predecessor 3GPP networks [18].

New security features and enhancements have been deployed in the LTE network to be more flexible and reliable. The mutual authentication, the confidentiality and the integrity are achieved between the UE and Serving Network (SN) based on the NAS, Access Stratum (AS) and User Plane (UP) security protections. In addition to, all the communication

messages among the eNB, the SGW and the MME are protected through the Internet Security Protocol (IPsec) [19, 20]. To achieve the security features of the LTE network, the Evolved Packet System- Authentication And Key Agreement (EPS-AKA) protocol is used by the UE to authenticate himself with the serving network mutually. Despite the attractive security requirements in the LTE network, the EPS-AKA protocol inherits some security drawbacks from predecessor protocol, i.e., UMTS-AKA protocol.

Consequently, the EPS-AKA protocol cannot resist several types of attack. EPS-AKA protocol sends some authentication parameters as clear text during the UE registration process and synchronization failure process of handoff procedure to connect with a new MME.

Therefore, the adversary easily can catch the International Mobile Subscriber Identity (IMSI) to obtain the subscriber information [2, 3, 5, 7, 13, 17].

Several Drawbacks related to Denial Of Services (DOS) and fully dependent on the pre-shared secret key (K) have been existed in EPS-AKA protocol [6, 14, 16]. Considering these security weaknesses, this paper proposes a secure anonymity key of authentication and key agreement protocol (SAK-AKA) for LET network.

Specifically, the SAK-AKA protocol achieves the security requirements of the EPS and can prevent the existing drawbacks such as false base station attack, redirection attack, man in the middle attack, and DOS attacks [10, 15].

The rest of this paper is organized as follows: section 2 discusses the related works. The proposed protocol is introduced in section 3 .The security and performance analysis of the SAK-AKA protocol is demonstrated in section 4 and 5 respectively. Finally, this paper will be concluded in section 6.

2. Related Work

Numerous works have been carried out to solve the drawbacks of the AKA protocol in the 3GGP networks. In 2013, Lai *et al.* [11] introduced a secure and efficient group AKA protocol for LTE networks, called (SE-AKA) protocol. The SE-AKA protocol is a hybrid key-based protocol and provides strong security features including the key forward/backward secrecy (KFS/KBS). Hence, the public key infrastructure (PKI) is adapted to prevent the sending of IMSI as clear text.

Once the first UE in the group is registered in the network and fetches the authentication vector from the HSS, no need to go back to the HSS for fetching another vector. However, the protocol is suffered from the long delay and large computational overhead in the MME, this because the SE-AKA protocol shifts all computations after the first UE in the group completes the firs from the HSS to the MME. Arkko *et al.* [4] presented A USIM compatible 5G AKA protocol with perfect forward secrecy. The protocol takes the advantages of running the Diffie-Hellman between the UE and the MME. Nevertheless, identity protection was not completely taken into consideration, thus it does not resolve the security issues in defeating the false base station, impersonate, redirection and Man-in-the-Middle (MitM) attacks. In 2016, Degefa *et al.* [8] proposed Enhanced Authentication and Key Agreement protocol called (Enhanced-AKA) for SAE/LTE network. In Enhanced-AKA, the serving network generates the AVs Instead of the home network. The Enhanced-AKA is an interesting authentication scheme to overcome the almost security drawbacks in current EPS-AKA. The Enhanced-AKA is an interesting authentication scheme to overcome most of the security drawbacks in current EPS-AKA.

However, the protocol is suffered from the large computational overhead in the MME, this because the Enhanced-AKA shifts all computations from the HSS to the MME after the UE is registered to the serving network.

3. SAK-AKA Protocol

This section introduces a secure anonymity key authentication and key agreement protocol for LTE networks (SAK-AKA) to improve the security level of EPS-AKA protocol with the same security architecture and without adding extra cost to the system. The SAK-AKA is similar to the EPS-AKA protocol whereas all the authentication stages are managed by the MME. SAK-AKA is divided into two states; Initial Authentication Processes Session (IAPS) and Subsequence Authentication Processes Session (SAPS). The enhancement of SAK-AKA is accomplished by newly introduced authentication parameters and cryptographic functions.

3.1. Preparation and Initialization.

Both of the Tables 1 and 2 show the used notations and authentication functions of SAK-AKA protocol respectively. Both of the User Equipment/ Universal Subscriber Identity Module (UE/USIM) and MME execute the Network path function (Np) to generate the unique Identifier of Network Path (NPID). The latter is used to identify the path of UE/USIM connection through the eNB to MME using the eNB identifier (eNBID) and the MME identifiers (MMEID). In the HSS, the Unique Session Identifier (USID) is pointing to the pre-loaded shared Key (K) and International Mobile Equipment Identity (IMEI).

The value of USID has to be changed after each successful execution of the IAPS by the HSS based on the Reallocated Function (RF). The HSS encrypts the new USID using expected session identity function (f8) while the UE/USIM decrypts the XUSID using session identity function (f8*). The Random umber of User Equipment (RUE) is generated using (f0) for each IAPS execution by the UE/USIM the Subsequent random function (f0+) to increment the value of RUE

by C. the latter is a constant value that is determined by the network operator. According to the values of IMSI and USID, both of the UE/USIM and the HSS execute the SKDF function to derive the Session Key (SK), where the SKDF is one way function known by UE/USIM and HSS only. The HSS performs the Expected sequence number function (f7) to encrypt the SQN while the UE/USIM decrypts the XSQN using (f7*). Both of the UE/USIM and HSS executes the (f1) and (f1*) to generate the message authenticate code whether for request authentication messages or response authentication messages. Base on the SK, both of the UE/USIM and HSS execute the key derivation functions. The key derivation functions (f3), (f4), (f5) and (KDF) are executed to drive the Cipher Key (CK), Integrity Key (IK), Anonymity Key (AK) and key derivation KASME, respectively. The latter will be used to generate further subsequence shared keys and the AK is used to conceal the USID for each SAPS execution.

Table 1. SAK-AKA notations.

Notation	Definition
MMEID	The Unique identifier of MME.
eNBID	The Unique identifier of eNB.
NPID	The Unique identifier of Network Path.
IMSI	International Mobile Subscriber Identity.
IMEI	International Mobile Equipment Identifier
USID	Unique Session Identifier.
XUSID	Expected Unique Session Identifier.
RUE	Random number.
XRUE	Expected random number.
MAX-U	User Message authentication code generated by UE.
XMAX-U	Expected user message authentication code generated by HSS.
MAX-H	Network Message authentication code generated by HSS.
XMAX-H	Expected network message authentication code generated by UE.
RES	Response message generated by HSS.
XRES	Expected response message generated by UE.
SQN	Sequence number.
XSQN	Expected sequence number.
Count	Number of remains authentication vectors in the MME.
AUTN	Authentication token.
CK	Cipher key.
IK	Integrity key.
SK	The Session Key.
K	The pre-loaded shared key as in EPS-AKA protocol.
AK	Anonymity key
C	Constant value.
K_{ASME}	The key derivation.

Table 2. SAK-AKA protocol functions.

F	Description	Input	Output
f0	Random generating function	-	RUE
f0+	Subsequent random function	RUE + C	RUE
SKDF	session Key derivation function	K, (IMSI ⊕ USID)	SK
Np	Network Path function	(eNBID ⊕ MMEID)	NPID
f1	Network authentication function	SK, (IMSI ⊕ NPID ⊕ IMEI ⊕ RUE)	MAC-U/XMAC-U
f1+	User authentication function	SK, (SQN RUE)	MAC-H/XMAC-H
f2	Subsequent authentication function	SK, RUE	XRES, RES
f3	Cipher key derivation function	SK, RUE	CK
f4	Integrity key derivation function	SK, RUE	IK
f5	Anonymity key derivation function	SK, RUE	AK
f6	Expected Random function	SK, RUE	XRUE
f6*	Response Random function	SK, XRUE	RUE
f7	Expected sequence number function	SK, SQN	XSQN
f7*	Sequence number function	SK, XSQN	SQN
f8	Expected session identity function	SK, new USID	XUSID
f8*	Session identity function	SK, XUSID	USID
KDF	key derivation function	SQN, NPID, CK, IK	KASME
RF	Reallocation function	old USID	new USID

3.2. IAPS State

In IAPS, the MME relays the access request message to the HSS which is sent from UE/USIM through the eNB. The access request message includes USID, XRUE, MAC-U and NPID. The HSS retrieves the authentication parameters to generate the AVs. Then the HSS answers the MME by send back the response message over the secure channel. Upon the received response message, the MME selects the AUTN of the first AV and sends it back to UE/USIM. The latter verifies the response message. Finally, new-shared keys are generated between the UE/USIM and the MME for signaling and user plan data protection.

Figure 2 illustrates the five stages of the IAPS.

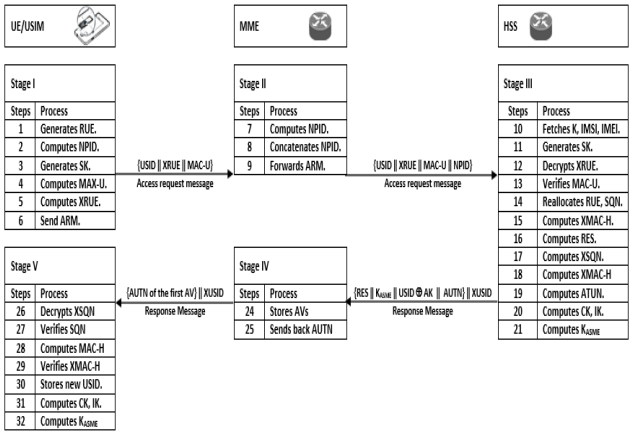


Figure 2. Initial authentication processes session (IPAS).

In stage 1, the UE/USIM initiates the authentication parameters of the access request message. Therefore, the UE/USIM executes the f0, Np, SKDF, f6 and f1 functions to generate RUE, NPID, SK, XRUE and MAX-U parameters respectively. The UE/USIM transmits the access request message to the MME through the eNB, the access request message shall include USID, XRUE, and MAC-U parameters. In stage 2, upon receipt of the access request message, the MME can determine the eNBID. Therefore, the MME executes Np function to compute NPID. In order the HSS can compare the NPID sent from UE/USIM with the NPID sent from MME, the MME adds the NPID to the received message. The MME forwards the access request message to the HSS over the secure channel where the message shall include USID, XRUE, MAC-U and NPID. In stage 3, the HSS retrieves K, IMEI and IMSI that are assigned to the UE/USIM from the AuC/HSS through the authentication parameters that are relayed from the MME. HSS invokes SKDF function to generate SK.

Then, the HSS decrypts XRUE using f6* function. Consequently, the HSS can execute f1 function to compute XMAX-U value. Then the HSS can verify whether the MAC-U value that is relayed by MME is equal to the MAC-U that is generated by UE/USIM, i.e. if XMAC-U = MAC-U.

Once the verification passes, the HSS replies the response authentication message to MME. In this stage, the HSS verifies the authentication parameters IMSI, IMEI, eNBID, MMEID and RUE indirectly when XMAC-U = MAC-U. Then the HSS performs a set of computations to generate the authentication vectors (AV's) and to prepare the response authentication message. The HSS Increases the value of the RUE using f0+ and assigns new SQN value for each authentication vector. Subsequently, the HSS executes f1*, f7, f2, f3, f4, f5 and KDF to compute the XMAX-H, XSQN, RES, CK, IK, AK and KASME, respectively. Finally, each authentication vector AV[i] shall include RES, KASME, USID ⊕ AK and AUTN where AUTN contains XSQN and XMAC-H. In order to change the value of SK and concealment the UE/USIM identifier for next IAPS, the HSS executes RF and then f8 function. RF function is used to assign a new USID and f8 function will be used to encrypt the new USID. After computing the authentication vectors, the HSS sends back the authentication response message with the XUSID to the MME. In stage 4, according to the received authentication message, the MME stores the ordered array of authentication vectors, and then forwards the first ATUN with the XUSID to the UE/USIM through eNB. In stage 5, when the UE/USIM receives the authentication response message, the UE/USIM executes f0+ to compute the new RUE and f7* to extract the SQN, then executes f1* to compute MAC-H. After stage V is completed, the UE/USIM can access the service of the serving network. In order to verify the freshness of the AUTN, the UE/USIM checks the SQN value and the XMAC-H.

If the SQN is not in correct rang or MAC-H is not equal to the XMAC-H, an authentication reject message will be sent to the MME from the UE/USIM. After the successful verification between the UE/USIM and MME, the UE/USIM decrypts the XUSID using f8* and stores the new USID for next IAPS, and then generates CK, IK and KASME as in the HSS side where the KASME now is shared between the UE/USIM and MME.

3.3. SAPS State

The SAPS is accomplished between the UE/USIM and MME without go back to request another AVs from the HSS. The UE/USIM invokes the SAPS according to the current value of the counter variable. Specifically, the UE/USIM determines the number of unused pre computed authentication vectors in the data base of MME, while the counter variable is in correct range, the UE/USIM invokes the SAPS, else the UE/USIM Initiates the IAPS (the number of per computed AVs is determined by the network operator). The UE/USIM sends the subsequent authentication request massage to the MME. The subsequent authentication request message shall include the XRES and the USID XOR with the AV. The MME verifies XRES value to decide whether the UE/USIM is a legitimate. Figure 3 illustrates the three stages of the SAPS.

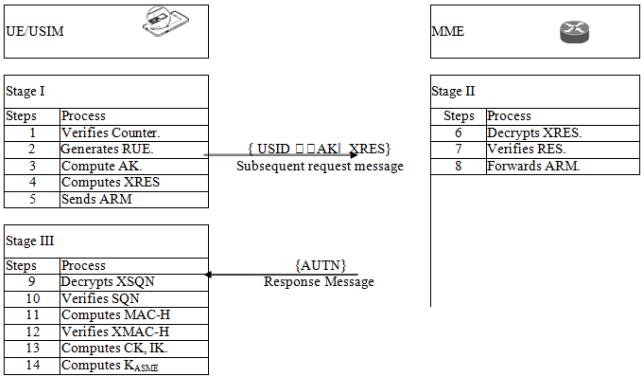


Figure 3. Subsequence authentication processes session (SAPS).

In stage 1, UE/USIM executes f0+ and f5 to compute RUE and generate AK respectively for each SAPS execution. Then the UE/USIM executes f2 to compute the XRES value, then the UE/USIM sends the subsequent access request message to the MME, the subsequent access request message shall include USID XOR with the AV and XRES. In stage 2, when the MME receives the subsequent access request message from the UE/USIM, the MME verifies the XRES parameter, i.e., (XRES=RES). If the verification succeeds then the MME sends back the ATUN to the UE/USIM, else reject the subsequent request. In stage 3, due to the received subsequent response message from the MME, the UE/USIM executes f7* and f1 functions to extract the SQN and compute the MAC-H respectively. Consequently, the UE/USIM verifies the integrity and the freshness of the AUTN. If the verification succeeds, the UE/USIM Computes the CK, IK and KASME using f3, f4 and KDF functions respectively.

3.4. Reallocation Function (RF)

In order to prevent the possible attacks that are associated with the user anonymity problem, the SAK-AKA protocol introduces a USID to conceal the IMSI completely. The USID points to the IMSI, IMEI and K of UE/USIM in the HSS/AuC, the new identifier is reallocated by the HSS using RF after each successful execution of IAPS.

The HSS/AuC contains two predefined disjoint sets, the first one represents the unused USID's while the second set represents the current used USID's.

Thus, the HSS reallocates a new value for the USID by swapping the elements between these sets to prevent assigning USID to different subscribers in the same time. The old USID will be saved for pre-defined period of time without reallocating to another UE/USIM until the encrypted value of the new USID is delivered to the UE/USIM and the next IAPS is executed successfully.

3.5. Allocation Session Key Function (SKDF)

In general, to reduce the risks of the single key problem in the AKA protocols, the proposed protocol is not fully dependent on the per-loaded shared key K between the UE/USIM and the HSS/AuC. The SAK-AKA protocol renews the session key (SK) periodically by introducing a new Session Key Derivation Function (SKDF). After the HSS reallocates a new USID for next IAPS, both of the UE/USIM and the HSS execute the SKDF function to create a new session Key Derivation (SK). Therefore, the input parameters of the SKDF function will be changed according to the new USID, consequently the SK will be renewed after each successful execution of IAPS periodically. The SKDF is recommended to be one way function and is known to the UE/USIM and the HSS only.

3.6. Key Derivation in S-AKA protocol

To support cryptographic and integrity services of the NAS and AS, the key hierarchy is organized in the SAK-AKA protocol into three different levels according to the authentication entities. Table 3 illustrates the key derivation of the SAK-AKA.

Table 3. key derivation of the SAK-AKA protocol.

Keys level	Authentication entities	Keys
Level 1	UE/USIM, HSS	K
	UE/USIM, HSS	SK
	UE/USIM, HSS	CK, IK
	UE/USIM, MME, HSS	KASME
Level 2	UE/USIM, eNB, MME	KNASenc, KNASint
Level 3	UE/USIM, eNB	KRRCenc, KRRCint, KUPenc

In the first level, the key K is used to derive the SK in the UE/USIM and the HSS, then both of the CK key and the IK key are derived from the SK in the UE/USIM and the HSS. When the mutual authentication process between the UE/USIM and the HSS is completed successfully, both of UE/USIM and HSS agree on the KASME key by binding the CK key, IK key and other parameters to the KDF function based on the SK key, then the KASME is delivered to the MME from the HSS. Therefore, the CK and IK are not used directly for cryptographic and integrity services, but are used to generate the successive keys that will be used to protect the signaling and user data for the NAS traffic and the AS traffic. In the second level, the KASME is used to derive the keys KNASenc, KNASint and KeNB by the UE/USIM and the MME, then the KeNB is delivered to the eNB from the MME. Both of the KNASenc and KNASint are used to protect the signaling messages between the UE/USIM and the MME. Similarly, the three Keys KRRCenc, KRRCint and KUPenc are derived from KeNB by the UE/USIM in the third level, the KRRCenc and the KRRCint are used for encryption and integrity to control traffic between the UE/USIM and the eNB respectively. While the KUPenc is used to encrypt the user traffic. Except the keys of the first level in key hierarchy, the SAK-AKA protocol follows the ESP-AKA protocol in terms of the key derivation. The SAK-AKA protocol renews all the keys from up to down in the key hierarchy using one-way denervation functions after each successful execution of IAPS.

Therefore, the key is used for one security context during the SAPS, if one key in bottom level is compromised does not mean the other keys will be deduced whether in the same level or upper level.

4. Security Analysis of SAK-AKA

In this part, the security analysis is performed to demonstrate that the SAK-AKA protocol can meet the security requirements of the LTE network. In addition to, explain how the major improvements of the SAK-AKA protocol can resist the different known attacks.

The SAK-AKA protocol deploys the same security architecture of the EPS-AKA protocol through uses some authentication functions of EPS-AKA protocol.

Moreover, it uses new authentication functions to increase the security level and to be more secure against the drawbacks that are related to user anonymity problems than the current EPS-AKA protocol as the follows:

4.1. Mutual Authentication

In SAK-AKA protocol, the mutual authentication is achieved between the UE/USIM and the serving Network whether in IAPS or SAPS authentication sessions. More precisely, UE/USIM and HSS authenticate each other by verifying the MAC-U and the MAC-H in the IAPS respectively. In the SAPS, the MME authenticates UE/USIM by verifying the XRES value and the UE/USIM authenticates MME by MAC-H value.

Table 4. Mutual authentication in SAK-AKA protocol.

Verification messages	Authenticator Entities	Verification Parameters
XMAC-U = MAC-U	HSS	USID, IMSI, IMEI, NPID, K, SK, RUE.
XMAC-H = MAC-H	UE/USIM	SK, RUE, SQN.
XRES = RES	MME	USID, SK,RUE,AV.

As shown in Table 4, successful verification not only means both of authentication entities can obtain the same results from the same functions, but also must be depends on the freshness and correctness of the input parameters of the these functions. Therefore, when the verification process succeeds, implicitly the authentication parameters have been verified by the authenticator entity. Note that, the communication channel between MME and HSS is secure channel.

4.2. User Privacy

To ensure the privacy of the user in the LTE network, the IMSI should not be transferred without protection.

In the EPS-AKA protocol, the IMSI is transferred

as clear text in many instances between the UE/USIM and the serving network. Therefore, the adversary can obtain IMSI and track the UE/USIM to attack the user privacy. This paper performs new USID which points to the IMSI and the per-loaded shared K in the HSS/AuC. The USID is used to generate session key SK, i.e. SK= (K, (IMSI ⊕ USID)).

The HSS executes RF function to assign new USID to generate different SK for each IAPS execution. In each SAPS execution, the USID is concealed by different anonymity key AV, i.e., (USID ⊕ AK). Thus, the user privacy is enhanced in SAK-AKA protocol where the IMSI is concealed completely whether in the IAPS or the SAPS.

4.3. Confidentiality and Data Integrity

The proposed protocol follows the same security architecture of the EPS-AKA protocol to achieve the confidentiality and data integrity services. The proposed protocol executes the cipher and IKs derivation functions in the UE/USIM and the HSS to generate CK key and IK key respectively. These keys are not actually used for encryption and integrity operations, but are used in the UE/USIM and HSS to derive KASME. After the KASME is delivered to the MME from the HSS, both of the MME and the UE/USIM derive further keys using the KASME.

The derived keys are used to provide the cryptographic and the integrity operations for NAS traffic and AS traffic between the UE/USIM - MME and UE/USIM-eNB respectively.

4.4.Secure Key Derivation

The EPS-AKA protocol is fully dependent on the secrecy of the pre-loaded shared Key (K) between the UE/USIM and the HSS/AuC. The K is a static key which is used to derive all the remaining keys CK, IK, and KASME among all authentication entities in future. The SAK-AKA protocol introduces new session Key Derivation Function (SKDF) which is preferred to be one-way function to derive the Session Key (SK). The latter is considered a dynamic key which is renewed periodically in each time the IAPS will be executed with different fresh USID. Therefore, the SK cannot compromised by the adversary. The SK is used to execute the Key derivation functions. Consequently, the remaining keys (CK, IK and KASME) cannot also retrieved by the adversary.

4.5. Perfect forward secrecy

In the EPS-AKA protocol, the CK, IK, AK, SNID and SQN are used as input parameters for the KDF function to generate the local master KASME based on a single long-term Key (K). Moreover, all remaining keys that are used to execute the cryptographic and integrity functions are generated based on the KASME. Therefore, all the keys that are used to perform the NAS and AS operations depend on a single Key. Once an adversary compromises the K, he can generate the keys of the whole system.

Therefore, the EPS-AKA protocol cannot guarantee the perfect forward security property. In the SAK-AKA protocol, the perfect forward secrecy property is guaranteed where the long-term Key (K) is not used directly to generate the system keys, rather it is used just to generate the SK. The latter is used to generate KASME using the KDF function.

Therefore, all the remaining keys of the system are depending on the SK. An adversary who may know the long-term key K cannot generate the SK which is renewed periodically in each time the IAPS will be executed. Consequently, an adversary cannot compute all the remaining keys of the system. Thus the SAK-AKA protocol supports the property of perfect forward security.

4.6. Resistance Against Redirection Attack

The adversary can simulate the eNB and impersonate the UE/USIM. In the EPS-AKA protocol, the SNID is delivered to HSS from MME only. Thus, the adversary can redirect the connection to unsecured network with low level of protection. In the proposed protocol, the NPID is delivered to the HSS through access request message from both of the UE/USIM and the MME.

Therefore, the HSS can easily verify the network identity that the UE/USIM is looking to access. If the (XMAC-U= MAC-U) then the NPID that is encrypted with other authentication parameters by UE/USIM is equal to the NPID that is attached by the MME. In the SAK-AKA protocol, because of the MAC-U is encrypting using a freshness SK where the IMSI is completely concealing, the adversary cannot reply or modify the NPID and therefore, the proposed protocol resists against redirection and replay attacks.

4.7. Resistance Against MitM Attack

The EPS-AKA suffers from the MitM attack problem. In order to receive authentication token message (AUTN ‖ RAND) from the serving network, an adversary uses a legitimate subscriber identifier IMSI to send access request message. An adversary stores the received authentication token message and waits until a legitimate UE/USIM transmits legal access request message to the serving network, an adversary intercepts the legal request message and then the adversary sends the stored message to a legitimate UE/USIM. The latter sends back to the adversary the response authentication message RES, then the adversary forwards the response message to the serving network as a response to the authentication token that has been sent initially from the serving network.

Therefore, the adversary is authenticated by the

serving network. The SAK-AKA protocol can deal with this problem in simple way, due to the subscriber identity (IMSI), the USID, Network Path Identity (NPID) and the UE identity IMEI are included in the access request message as a cipher text. An adversary cannot acquire all of these parameters to construct this message due to lack of the dynamic Session Key (SK).

4.8.Resistance Against DoS Attack

The Denial-of-Service (DoS) attacks can be occurred by modifying unprotected authentication messages or by sending a large number of the access request messages.

In the latter case, the attacker sends a large number of request messages based on a large number of legitimate IMSI's that are collected in advance.

Consequently, the serving network will be destroyed due to exhaust computation capacity and congest bandwidth. In the former case, the attacker modifies the access request messages to cause authentication failures. Despite the difficulty of resisting all cases of DoS attack in the same time, the S-AKA protocol though encrypting and concealing the IMSI prevents the attacker from acquire the IMSI's. The attacker cannot encrypt the authentication parameters due to lack of the fresh SK, but it may try to replay a whole access request message. In this case, the HSS can reject the request message whereas the USID is renewed periodically in each time the IPAS and SAPS are executed without verifying the authentication parameters.

4.9.Security Requirements and Achievements

The security requirements can be summarized of the EPS-AKA protocol into the following security services [1, 3].The AKA protocol shall provide a high level of security in terms of mutual authentication, confidentiality, integrity and the privacy. Consequently, the AKA should provide high level of protection to prevent the attacks.

Table 5. Statues of Security requirements.

Security requirements	EPS-AKA	SAK-AKA
Mutual Authentication	Hold	Hold
Integrity	Hold	Hold
Confidentially	Hold	Hold
Privacy	Does not Hold	Hold
Renew the session key periodically	Does not Hold	Hold
Single key problem	Hold	Does not Hold
secure against Man in the middle attack	Does not Hold	Hold
secure against replay attack	Does not Hold	Hold
secure against redirection attack	Does not Hold	Hold
secure DOS attack	Does not Hold	Hold
Perfect Forward security	Does not Hold	Hold

According to the discussions in previous sections, Table 5 summarizes the security requirements that have achieved through the proposed protocol as comparison factors with EPS-AKA protocol. These factors demonstrate that the SAK-AKA protocol can provide the most of security requirements compared to the current protocol.

5. Performance Analysis of SAK-AKA

In this part, the performance analysis is carried out to compare between the SAK-AKA protocol and the EPS-AKA protocol in terms of the bandwidth consumption overhead, authentication transmission overhead and the storage overhead. The proposed protocol has simulated in MATLAB running on a 2.10 GHz processor with 4GB memory computing machine. Table 6 illustrates the assumptions of the HSS coverage area.

Table 6. Assumptions of the HSS coverage area.

Assumptions	Assumptions values
Mean density of UE/USIM ρ.	300/km^2
Total number of UE/USIM.	$128 \times 54.76 \times 300 \approx 2.1$ millions
Size of registration Area.	$(7.4\text{ km})^2 = 54.76\text{ km}^2$
Average rate of originating service request.	1.4/hr/user
Average rate of terminating service request.	1.4/hr/user
Average speed of UE/USIM $\mathcal{V}$.	5.2 km/hr
Number of registration area.	128.
Border covered length ℓ.	36 km.

5.1. Bandwidth Consumption Overhead

In order to analyze the bandwidth consumption of the proposed protocol, the arrival rate of the UE/USIM for registration events in each registration area is computed using to the following equation [8, 12].

$$\mathcal{R} = \frac{\rho \mathcal{V} \ell}{\pi} \quad (1)$$

According to the assumptions in table 6, the registration arrival rate R = (300/km2 × 5.2 km/hr × 36 km)/3.14 ≈ 4.7 UE/USIM per second. Thereafter, the total arrival rate in the serving network TR=R× number of registration area=4.7×128≈602 UE/USIM's in each second. Consequently, the serving network should be able to authenticate 602 UE/USIM's per second which represents the number of authentication request per second (q). Therefore, the total bandwidth transmission (TBω) of authentication messages for all new registration requests whether in EPS-AKA protocol or SAK-AKA protocol is calculated as follows:

$$\text{TB}\omega = \sum_{i=1}^{n} |\text{Message } i| \times q \quad (2)$$

Table 8 shows the bit size of authentication messages for new registration request in the EPS-AKA protocol based on the bit size of authentication parameters in Table 7. Thus, the total bandwidth of the new authentication requests for all mobile subscribers in EPS-AKA protocol is calculated as follows:

$$\begin{aligned} \text{TB}\omega &= \sum_{i=1}^{5} |\text{Megs } i| \times q \\ &= 4114\text{ bits} \times 602/\text{sec} = 2.362\text{ Mbits/sec} \end{aligned} \quad (3)$$

Table 7. Bit size of authentication parameters in the EPS-AKA.

Parameters	Size
IMSI	128 bits
SNID	48 bits
AUTN	128 bits
RAND	128 bits
XRES/RES	64 bits
K_{ASME}	256 bits
RES	64 bits

Table 8. Bit size of authentication messages in the EPS-AKA protocol for new registration requests.

Msgs	Description	Message parameters	Bits size
M1	Authentication request sent from UE/USIM to MEE.	IMSI	128 bits
M2	Authentication vectors request sent from MME to HSS.	IMSI ‖ SNID	176 bits
M3	Authentication vector response sent from HSS to MME.	IMSI ‖ RAND ‖ AUTN ‖ XRES ‖ K_{ASME}	3520 bits
M4	Authentication token response sent from the MME to UE/USIM.	RAND ‖ AUTN	256 bits
M5	Authentication response sent from UE/USIM to MME.	RES	64 bits

Table 10 shows the bit size of authentication messages for new registration request in the SAK-AKA protocol based on the bit size of authentication parameters in table 9.Thus, the total bandwidth of the new authentication requests for all mobile subscribers in SAK-AKA protocol is calculated as below:

$$\begin{aligned} TB\omega &= \sum_{i=1}^{4} |\text{Megs } i| \times q \\ &= 3440 \text{ bits} \times 602/\text{sec} = 1.974 \text{ Mbits/sec.} \end{aligned} \quad (4)$$

Table 9. Bit size of authentication parameters of the SAK-AKA.

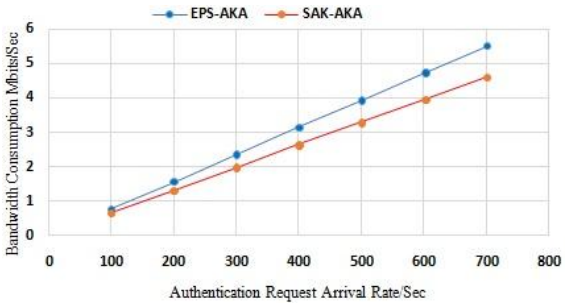
Parameters	Bit Size
USID	64 bits
AV	64 bits
XRES/RES	64 bits
XRUE	128 bits
MAC-U	128 bits
NPID	48 bits
K_{ASME}	256 bits
AUTN	176 bits

Table 10. Bit size of authentication messages in the SAK-AKA protocol for new registration requests.

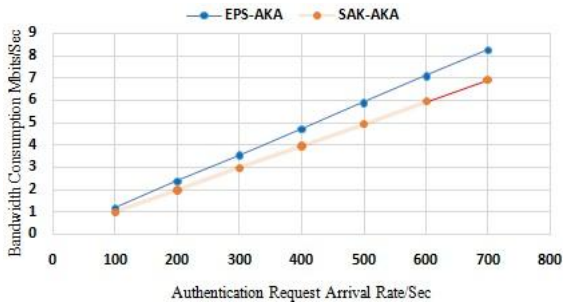
Msgs	Description	Message parameters	Bits size
M1	Authentication request sent from UE/USIM to MEE.	USID ‖ XRUE ‖ MAC-U	320 bits
M2	Authentication vectors request sent from MME to HSS.	USID ‖ XRUE ‖ MAC-U ‖ NPID	368 bits
M3	Authentication vector response sent from HSS to MME.	{USID □ AK ‖ AUTN ‖ XRES ‖ K_{ASME} } ‖ XUSID	2560 bits
M4	Authentication response sent from the MME to UE/USIM.	AUTN ‖ XUSID	192 bits

The results of total bandwidth consumption of ESP-AKA protocol and SAK-AKA show that the latter in IAPS saves ≈ 16.4 % of bandwidth consumption of the authentication messages between the UE/USIM's and serving network for registration requests. Despite that the SAK-AKA protocol adds new authentication parameters to enhance the security level of the EPS-AKA protocol, it can save more bandwidth consumption. The reason is that the SAK-AKA protocol decreases the number of authentication messages from five messages to four messages where the access request message in the IAPS includes the MAC-U parameters. Figures 4-a, 4-b, 4-c, and 4-d compares the bandwidth consumption between the EPS-AKA protocol and SAK-AKA protocol. From the figure, the proposed protocol provides lesser bandwidth consumption than the EPS-AKA protocol with different arrival rates at the MME and with different number of authentication vectors.

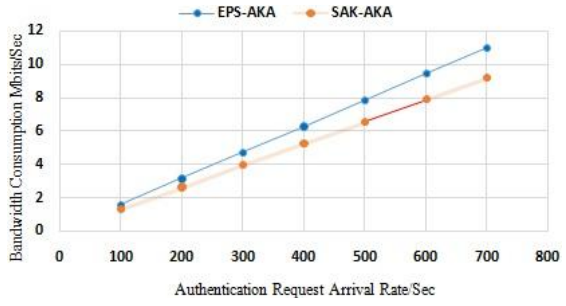
a) Bandwidth Consumption for AV=5



b) Bandwidth Consumption for AV=10.



c) Bandwidth Consumption for AV=15.



d) Bandwidth Consumption for AV=20.

Figure 4.Bandwidth consumption variation.

Suppose all the UE/USIM's already have registered in the serving network and there is no need to generate new authentication vectors from the HSS. In other meaning, the authentication vectors are available in the MME for all Intra-domain handoff authentication events and session authentication. From [13], the

arrival rate of Intra-domain handoff authentication ($\lambda 1$) can be calculated as follows:

$$\lambda 1 = \lambda u \times \sum_{i=1}^{4} \mathrm{P}ri([\mathrm{N}ai] - 1) \quad (5)$$

Where $\mathrm{P}r$, is the probability of UE/USIM events (i), λu is Poisson process which represents the call arrival rate, $\mathrm{N}a$ is the average numbers of registration area passed by an UE/USIM in current serving network in event (i).

Suppose all the UE/USIM's events are originate and terminate in the same registration area ($\mathrm{P}r = 1$) then $\lambda 1$.

$$\lambda 1 = \lambda u \times \mathrm{P}r([\mathrm{Na}] - 1) \quad (6)$$

From [8], the session authentication request arrival rate $\lambda 2$ is equal to the arrival call rate of UE/USIM ($\lambda 2 = \lambda u$) where λu = 8.7/sec/registration area and Na = 10.Table 11 illustrates the bits size of authentication messages in the EPS-AKA protocol for subsequent authentication requests. Therefore, the total bandwidth of the subsequent authentication requests for all UE/USIM's in the EPS-AKA protocol is calculated as indicated below:

$$\mathrm{TB}\omega = 128 \times (\lambda 1 + \lambda 2) \times \sum_{i=1}^{3} |\mathrm{Megs}\, i| \approx 0.95\ \mathrm{Mbits/sec} \quad (7)$$

Table 11. Bit size of authentication messages in the EPS-AKA protocol for subsequent requests.

Msgs	Description	Message parameters	Message size
M1	Authentication request message sent from UE/USIM to MEE.	IMSI	128 bits
M2	Authentication token response message sent from the MME to UE/USIM.	RAND ‖ AUTN	256 bits
M3	Authentication response message sent from UE/USIM to MME.	RES	64 bits

Table 12 illustrates the bits size of authentication messages in the SAK-AKA protocol for subsequent authentication requests. Therefore, the total bandwidth of the subsequent authentication requests for all mobile subscribers in proposed protocol is calculated as indicated below:

$$\mathrm{TB}\omega = 128 \times (\lambda 1 + \lambda 2) \times \sum_{i=1}^{2} |\mathrm{Megs}\, i| \approx 0.54\ \mathrm{Mbits/sec} \quad (8)$$

Table 12. Bit size of authentication messages in the SAK-AKA protocol for subsequent requests.

Megs	Description	Message parameters	Message size
M1	Authentication request message sent from UE/USIM to MEE.	USID □ AK ‖ RES	128 bits
M2	Authentication token response message sent from the MME to UE/USIM.	AUTN	128 bits

The results of total bandwidth consumption of ESP-AKA protocol and the SAK-AKA show, the latter saves in the SAPS ≈ 43% of bandwidth consumption of the authentication messages between the UE/USIM's and serving network for subsequent authentication requests. The reason is that the SAK-AKA protocol decreases the number of subsequent authentication messages from three messages to two messages. The results of total bandwidth consumption of ESP-AKA protocol and the SAK-AKA show, the latter saves in the SAPS ≈ 43% of bandwidth consumption of the authentication messages between the UE/USIM's and serving network for subsequent authentication requests. The reason is that the SAK-AKA protocol decreases the number of subsequent authentication messages from three messages to two messages.

5.2.Authentication Transmission Overhead

The authentication transmission overhead in the SAK-AKA protocol is similar to the current protocol. From [11], the Authentication Transmission Overhead of current protocol (AtO) is expresses as:

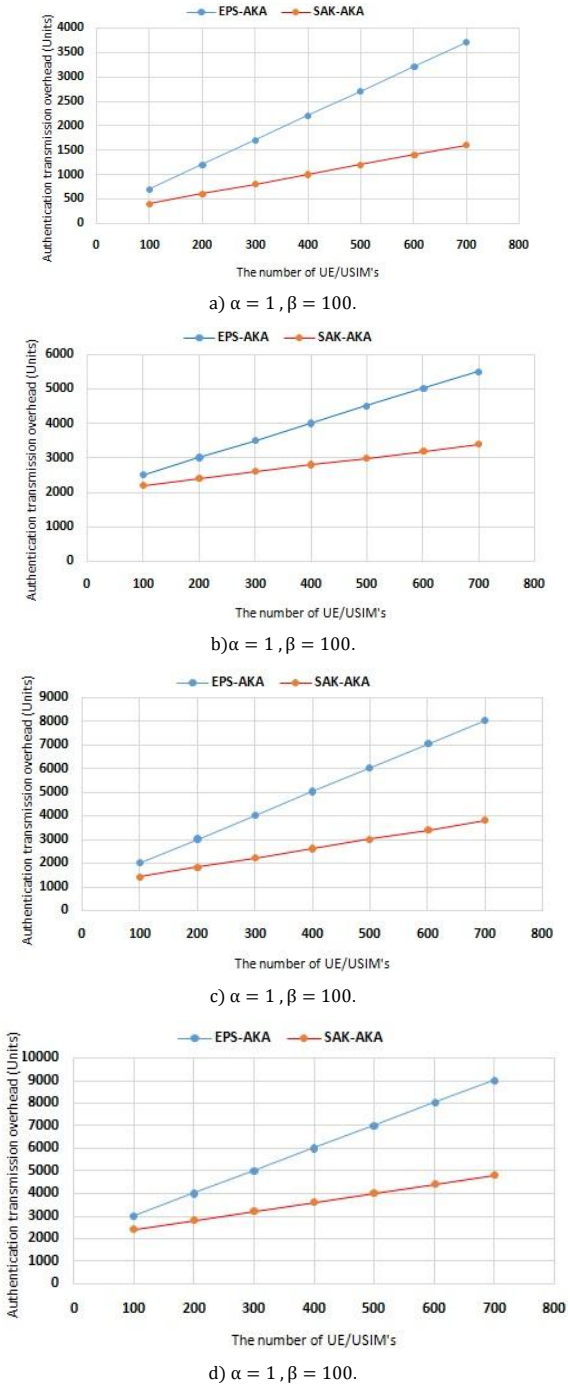
$$\mathrm{AtO} = 5n\alpha + 2n\beta \quad (9)$$

Both of α, β units represent the overhead of authentication message delivery between the n UE/USIM's and the MME, and between the MME and the HSS respectively. $\beta \gg \alpha$, because we assume that the location of the MME is far away from the HSS.

Where there are 5 messages between the UE/USIM and MME, 2 messages between the MME and HSS. In the proposed protocol, the AtO is expresses as:

$$\mathrm{AtO} = 2n\alpha + 2n\beta \quad (10)$$

Where, there are 2 messages between the serving network entities and 2 messages between UE/USIM's and the MME.



a) $\alpha = 1, \beta = 100$.

b) $\alpha = 1, \beta = 100$.

c) $\alpha = 1, \beta = 100$.

d) $\alpha = 1, \beta = 100$.

Figure 5. Authentication transmission overhead.

As shown in Figures 5-a to 5-d, the proposed protocol always achieves lower AtO than EPS-AKA protocol. This is because the number of authentication messages between the UE/USIM and MME is reduced in SAKA-AKA protocol from 5 messages to 2 messages.

5.3. Storage consumption.

In this part, we consider that (η) is the arrival rate of authentication requests in the serving network. In addition, we compare between the proposed protocol and the EPS-AKA protocol in term of the Storage consumption (Sc). The latter represents the occupied storage space in the serving network during the protocol execution time. For each authentication session in both protocol, the UE/USIM needs one authentication vector.

Therefore, the arrival rate of authentication request is equal to the number of authentication vectors.

Consequently, the storage consumption(Sc) can be calculate as follows:

$$\mathrm{Sc} = \eta \times size\,(\mathrm{AV}) \tag{11}$$

For the EPS-AKA protocol, the length of authentication vector is 704 bits, therefore the storage consumption ($\eta \times 704$ bits). For S-AKA protocol, the storage consumption will occupy ($\eta \times 576$ bits) where the $size(\mathrm{AV}) = 576$ bits.

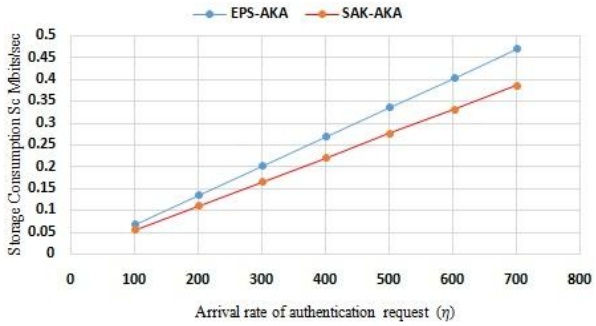


Figure 6. Storage consumption variation.

Figure 6 compares the storage consumption between the EPS-AKA protocol and SAK-AKA protocol base on different arrival rates of authentication request. According to this figure, it can be seen that the S-AKA protocol has reduced the storage usage than the EPS-AKA protocol. In general, if the arrival rate of authentication request increased, the storage consumption will be increased proportionally in both protocols.

6. Conclusions

In this paper, we have proposed a secure anonymity key of AKA protocol (SAK-AKA) for LTE network to enhance the security level of current protocol (EPS-AKA). Compared with the EPS-AKA protocol, the proposed protocol can provide strong security features including complete concealing of IMSI with perfect forward security. The SAK-AKA protocol increases the difficulty of compromising the authentication parameters to solve the authentication messages detection problem. The USID is changed periodically in each authentication session by the HSS and is used to prevent the transmission of IMSI within the request authentication messages. The proposed protocol through introduces the session Key derivation function (SKDF) that is used to generate a fresh session key (SK) based on the USID, all authentication functions generate fresh authentication parameters in all authentication session based on the SK.As extensive discussion under the security analysis section, the SAK-AKA protocol is secure against the redirection attack, MitM attack, replay attack and DoS attack.

Moreover, the performance analysis in different terms have been discussed. In the SAK-AKA protocol the bandwidth consumption is considerably reduced, the transmission authentication messages is decreased and the storage consumption of authentication sessions can also be reduced. In summary, the SAK-AKA protocol is more secure and more efficient for LTE than the EPS-AKA protocol.

References

[1] Ahmadi S., *LTE-Advanced: A practical System to Understand 3GPP LET Released 10 and 11 Radio Access Technologies*, Elsevier, 2014.

[2] Ajagaonkar K., Bhalerao A., Fakir Sh., Jagadale V., and Phadatare D., "Advanced Subscriber Identity in 3GPP Mobile Systems," *International Research Journal of Engineering and Technology*, vol. 3, no. 5, pp. 2458-2463, 2016.

[3] Al-fayoumi M., Nashwan S., and Yousef S., "A New Hybrid Approach of Symmetric/Asymmetric Authentication Protocol for Future Mobile Networks," *in Proceeding of 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, New York, pp. 29, 2007.

[4] Arkko J., Norrman K., Naslund M., and Sahlin B.," A USIM compatible 5G AKA protocol with perfect forward secrecy," *in proceeding of 13th IEEE international Symposia on Parallel and Distributed Processing with Application*, Helsinki, pp. 1205-1209, 2015.

[5] Aymen Z., "QoS-based Performance and Resource Management in 3G Wireless Networks in Realistic Environments," *The International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 1-9, 2013.

[6] Choudhary A. and Bhandari R., "Analysis of UMTS (3G) Authentication and Key Agreement Protocol (AKA) for LTE (4G) Network", *International Journal on Recent and innovation Trend in Computing Communication*, vol. 3, no. 4, pp. 2146-2149, 2015.

[7] Copet P., Marchetto G., Sisto R., and Costa L., "Formal verification of LTE-UMTS and LTE-LTE handover," *Computer Standards and Interfaces*, vol. 5, pp. 92-106, 2017.

[8] Degefa F., Lee D., Kim J., Choi Y., and Won D., "Performance and Security Enhanced Authentication and Key Agreement Protocol for SAE/LTE Network," *Computer Networks*, vol. 94 pp. 145-163, 2016.

[9] Forsberg D., Horn G., Moeller W., and Niemi V., *Lte Security*, John Wiley and Sons, 2013.

[10] Kareem N., "Implementation of Enhanced AKA in LTE Network," *International Journal of Computer Science and Mobile Computing*, vol. 4, no. 5, pp. 1124-1132, 2015.

[11] Lai Ch., Li H., Lu R., and Shen X., "SE-AKA: A Secure and Efficient Group Authentication and Key Agreement Protocol for LTE Networks," *Computer Networks*, vol. 57, pp. 3482-3510, 2013.

[12] Liang W. and Wang W., "A Quantitative Study of Authentication and QoS in Wireless IP Networks," *in Proceeding of IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, Miami, pp. 1478-1489, 2005.

[13] Loriya H., Kulshreshta A., and Keraliya D., "Security analysis of Authentication and Key Agreement Protocol for LTE Network," *International Research Journal of Engineering, Science and Technology*, vol. 3, no. 1, 2016.

[14] Nashwan S. and Alshammari B., "Mutual Chain Authentication Protocol for SPAN Transactions in Saudi Arabian Banking," *International Journal of Computer and Communication Engineering*, vol. 3, no. 5. pp. 326-333, 2014.

[15] Purkhiabai M. and Salahi A., "Enhanced Authentication and Key Agreement Procedure of Next Generation 3GPP Mobile Networks," *International Journal of Information and Electronic Engineering*, vol. 2, no. 1, pp. 69-77, 2012.

[16] Sarmah S., Kalita P., and Devi J., "A New Approach to Authentication and Key Agreement in LTE 3GPP," *International Journal of Computer Science Research and Technology*, vol. 1, no. 4, 2013.

[17] Yang X., Huang X., and Liu J., "Efficient Handover Authentication with User Anonymity and Untraceability for Mobile Cloud Computing," *Future Generation Computer Systems*, vol. 62, pp. 190-195, 2016.

[18] 3gpp-ts, 21.133 V4.1.0, 3rd Generation Partnership Project, Universal Mobile Telecommunications System (UMTS) , 3G security; Security threats and requirements (2001-12), Release 4.3GPP Organizational Partners.

[19] 3gpp-ts, 33-401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, 3GPP System Architecture Evolution (SAE); Security architecture (2008-10), Release 10. 3GPP Organizational Partners.

[20] 3gpp-ts, 35.216, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 and UIA2; Document 2: SNOW 3G specification (2009-12), Release 9. 3GPP Organizational Partners.

Shadi Nashwan received his B.Sc. degree in Computer Science from Alazhar University, Palestine, in 2001, and M.Sc. degree in Computer Science from university of Jordan, Jordan, in 2003, and Ph.D. degree in Computer Science from Anglia Ruskin University, UK, in 2009. He is head of Computer Science and Information department, Aljouf University, KSA. His research focuses on authentication protocol wireless network, mobility management, and wireless network security. He has published several papers in the area of authentication protocol, recovery techniques and mobility management.