SEPS-AKA: A SECURE EVOLVED PACKET SYSTEM AUTHENTICATION AND KEY AGREEMENT SCHEME FOR LTE-A NETWORKS

Zaher Jabr Haddad[1], Sanaa Taha[2] and Imane Aly Saroit Ismail[2]

[1]Department of Computer Science, Faculty of Applied Science,
Al-Aqsa University, Gaza, Palestine
zj.haddad@alaqsa.edu.ps
[2]Information Technology Department, Faculty of Computers and Information,
Cairo University, Cairo, Egypt
staha@fci-cu.edu.eg, i.saroit@ fci-cu.edu.eg

ABSTRACT

In this paper, we propose a secure authentication of the Evolved Packet System Authentication and Key Agreement (EPS-AKA) for the LTE-A network. Our scheme is proposed to solve the problem of sending the IMSI as a clear text, and hence prevents the mobility management entity attack. We will use public key (PK) cryptography to protect the transmitted messages, the RSA scheme computation to compute a temporary value to the IMSI, and nonce to generate challenge messages toward the opposite side. Our scheme does not need to change the original framework and the infrastructure of the LTE-A network, although a ciphered IMSI is transmitted. The authentication procedure is performed by the HSS to authenticate the UEs and the MME; therefore, the impersonating of the MME and UEs is not possible. Our evaluation demonstrates that the proposed scheme is secure and achieves the security requirements of the LTE-A subscribers such as privacy, authentication, confidentiality and integrity. In our scheme, we try to maintain the problems defined in the previous related works.

KEYWORDS

Long Term Evolution – Advanced, Authentication and Key Agreement, Home Subscriber Server, Mobility Management Entity, User Equipment.

1. INTRODUCTION

The Long Term Evolution-Advanced (LTE-A) network is a packet based system specified by the Third Generation Partnership Project (3GPP) towards fourth-generation (4G) mobile; in order to meet more subscriber needs. Among those communications, LTE-A is the next generation of the cellular communication system that meets more subscriber needs, such as: 1) wider bandwidth that supports up to 100MHz via aggregation of 20 MHz blocks, 2)Multi Input Multi output (MIMO) that allows the use of multiple antennas in the transmitter and the receiver in order to

Natarajan Meghanathan et al. (Eds) : WiMONe, NCS, SPM, CSEIT - 2014
pp. 57–70, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.41206

improve the communication performance, 3) coordinate Multiple transmission (CoMP) that allows coordinates scheduling, beam-forming and joint processing transmission, 4)Heterogonous Network (Het-Net) that supports enhanced inter-cell interference coordinate (eICIC) to deal at the interference issues at the cell edge, and 5)relaying capabilities that achieves self-backhauling of the radio signal between a base station and User Equipment (UE) [1].

The EPS-AKA is the authentication protocol used by the LTE-A network to perform the authentication and key agreement security services. EPS-AKA protocol was improved to prevent malicious attacks such a redirection, rogue base station, and Man in the middle attacks. A malicious attack can be any action intents of acquiring, destroying, modifying or accessing a transmitted data without permission. However, the lack of privacy and denial of services attack still a big weakness of the EPS-AKA protocol. This LTE-A's security weakness is represented in the processes of registration, synchronization failure, and roaming to a new mobility management entity (MME), when the MME requests the international mobile subscriber identity (IMSI) of the User Equipment (UE). Therefore the IMSI disclosure may incur severe problems [2].

Many attacks may violate the vulnerabilities of the authentication in the LTE-A network such as [3][4]:

a) Replay Attack, which attains to perform maliciously or fraudulently repeated or delayed transmitted messages in order to increase the flow in the network and therefore, may make system toppled [3][4].
b) Denial of service (DoS) attack, which attains to make a machine or network resources unavailable to legitimate users [3][4].
c) Man in the Middle (MITM) attack, which makes independent connection between two victims in order to intercept or inject fake messages [3][4].
d) Impersonation attack, which attempts to use a fake identity to gain unauthorized access to network system through legitimate access identification [3][4].

In this paper, a novel scheme is proposed to solve the problem of sending the IMSI as a clear text, and hence prevents the mobility management entity attack. In our scheme, we will use three levels of security. First, nonce is used to generate challenge messages toward the opposite side. Second, PK cryptography is used to protect the transmitted messages. Third, the RSA scheme computation is used to compute a temporary value to the IMSI.

The remainder of this paper is organized as follows: Section II illustrates the related work. The system models, including network, threat, and trust models, are presented in Section 3. In section 4 the preliminaries are discussed. In section 5, the proposed system, SEPS-AKA, is introduced. In sections 5 and 7, the security analysis and performance evaluation are discussed, respectively. In section 8, conclusion and future work are provided.

2. RELATED WORK

In [5], Park et al., introduce number of possible security risks may be caused due to the open nature of the 4G networks. First, a large number of external connectivity points with peer operator, third-party applications providers, the public Internet, and with numerous heterogeneous technologies accessing the infrastructure, serves as potential security holes if the security technologies do not fully interoperability. Second, multiple service providers share the core network infrastructure, meaning that compromise of a single provider may result in collapse of the entire network infrastructure. Third, service theft and billing fraud can take place if there are third-parties masquerading as legitimate ones [5]. New end-user equipment's can also become a source of malicious (e.g., DoS) attacks, viruses, worms, spam mails and calls. In particular, the

Spam over Internet Telephony (SPIT), the new spam for VoIP [5], becomes a serious problem just like the e-mail spam today. For example, SPITs targeting VoIP gateways can consume available bandwidth, thereby severely degrading QoS and voice quality. Clearly, the open nature of VoIP makes it easy for the attackers to broadcast SPITs similar to the case of spam emails. Other possible VoIP threats include: (1) spoofing that misdirects communications, modifies data, or even transfers cash from a stolen credit card number, (2) SIP registration hijacking that substitutes the IP address of packet header with attacker's own, (3) eavesdropping of private conversation that intercepts and crypt-analyzes IP packets, and (4) phishing attacks that steal user names, passwords, bank accounts, credit cards, and even social security numbers.

In [6], Purkhiabani et al. propose a new scheme to preserve the privacy of the IMSI by encrypting it using a temporary random number (MSR) during its transmission into the EUTRAN interface. In addition, HSS generates only one Authentication Vector (AV) to use in each authentication process in order to preserve the bandwidth of the CN. Therefore, the UE sends a message, which contains a concatenation of MSR, IMSI, and MSMAC, to the MME, which in turn forwards this message to the HSS. The MSR is a random number generated by the UE, and MSMAC= $f1_k$(MSR), where f1 is a cryptographic function used to generate 128-bit output using 128-bit input key. After receiving the transmitted message, the HSS verifies the IMSI, generates and sends back one AV to the MME, and hence, the original authentication and key agreement are performed. In this scheme, the use of same framework of the original LTE-A authentication scheme, decreases the HSS bandwidth consumption, the protection of the IMSI, and bandwidth preserving of the CN. But as the MSR is generated by the UE, this increases the possibility of malicious UE and MME. Moreover, the bandwidth consumption is moved from the CN to the radio interface.

In [7], Hamandi et al. propose a scheme to solve the privacy problem in the LTE-A authentication scheme to prevent the masquerading of the MME. Authors employ the public key infrastructure to provide more powerful MME and HSS elements. MME generates and sends a random number, RANDMME, to the UE to compute a vector of parameters, and then returns a message to the MME, which in turn adds its identity and digital signature and forwards the message to the HSS. At receiving, the HSS verifies the identities of both the MME and IMSI, and then generates a new random mobile subscriber identity, RMSI, to concatenate with the AVs. Both AVs and RMSI are sent back to the MME in order to complete the original authentication and key agreement procedures. In this scheme, a ciphered IMSI is sent, a virtual number (TMSI) is used in the next hops instead of the IMSI, and legal MME identity is protected by digital signature. However, EUTRAN consumption is increased. In addition, the initiation procedure is started from the MME, which also allows the possibility of the presence of malicious MME. Additionally, this scheme is not integrated with the original mobility procedures, such as handover and localization [7].

In [8], Abdo et al. define four security weaknesses in the original LTE AKA protocol: IMSI catching, tracking user temporary identity due to linkability and security network authentication. In addition, the authors propose two countermeasures to use in order to solve these problems: Public Key Infrastructure (PKI) and pseudonyms based approaches. The advantage of this work is the security capabilities that are performed using the PKI. However, there is a critical problem that is the first hop dependency, where the UE depends on a pre-stored cipher Key (CK) and identity Key (IK) to generate the initial pseudonyms. CK and IK are generated by the pre-shared cryptographic function using the pre-shared secret key (K) between UE and HSS and a random challenge RAND that is generated by the HSS, therefore, the HSS should performs some computations before initialization phase, and surely this depends on the IMSI.

In [9], Abdo et al. propose a scheme called EPS mutual authentication and Crypt-analyzing (SP-AKA), which is a self-certified based protocol, in order to solve the positive capturing of the IMSI during user identification and key agreement protocols. Authors use the PKI to encrypt the transmitted AKA messages. Hence, provide a high security level, but the fake MME is still a problem.

In [10], Lai et al. propose a new scheme for group base communication authentication called a secure and efficient group authentication and key agreement protocol for LTE networks (SE-AKA). This scheme uses the Elliptic curve Diffie-Hellman to achieve the key forward/backward secrecy and also adapts asymmetric cryptosystem to protect user privacy. For group authentication, SA-AKA uses a group temporary key (GTK), which employs a well-known keys generation algorithm, Diffie-Hellman, and also provides a strong security level where subscriber must meet the restrictions of the authenticated group, before network authentication. The problems of this scheme are the consumption of the MME where the Elliptic curve Diffie-Hellman consumes time to generate and distribute the public keys between group members, while the main role of the MME is to work as a gateway between the HSS and the UEs. Also, the proposed group is considered as an uncontrolled area in the network and used to break the security of the network since the authentication permissions are invoked to the group authority instead of the HSS.

In [11], Zheng el at. propose a hybrid AKA scheme that uses a trusted model platform and PKC to adapt the AKA. This scheme uses a password associated with fingerprint and PKC to achieve the authentication between the UE and HSS.

In our scheme, we try to maintain the problems defined in the previous related works. Our proposed scheme does not need to change the original framework and the infrastructure of the LTE-A network, although a ciphered IMSI is transmitted. The authentication procedure is performed by the HSS to authenticate the UEs and the MME; therefore, there is no possibility for any occurrence of fake MME and UEs.

3. SYSTEM MODEL

In this section, we describe the system models for the SEPS-AKA including, the network model and the threat model.

3.1. Network Model

In this subsection, we will explain the LTE-A network architecture and the original authentication and key agreement protocol used in the LTE-A network

3.1.1 LTE-A Network Architecture

The architecture of the LTE-A network is mainly composed of two components as depicted in Figure 1; the Evolved Packet Core (EPC) and Evolved Universal Terrestrial Radio Access Network (EUTRAN). [2][16].

The EPC represents the wired part in the network, which is responsible for the overall control of UEs and the bearer establishment. Each entity in the EPC has a responsibility as follows;

- MME to manage bearer and connection.
- HSS to maintain the user subscription data and MME identities.
- Packet Data Network (PDN) and Packet Data Network Gateway (PGW) to perform mobility anchor and internetworking within the 3GPP and non-3GPP technologies respectively.

- Policy Control and Charging Rule function (PCRF) to control decision making of flow and Quality of Service (QoS).

EUTRAN is the Radio Access Network (RAN) in the LTE-A system; mainly two components are included [2][16];

- UE which is the mobile phone handset.
- Evolved Node B (eNB) presents the Base Transceiver System (BTS) and the Base Station Subsystem (BSS) in the non-3GPP technologies.

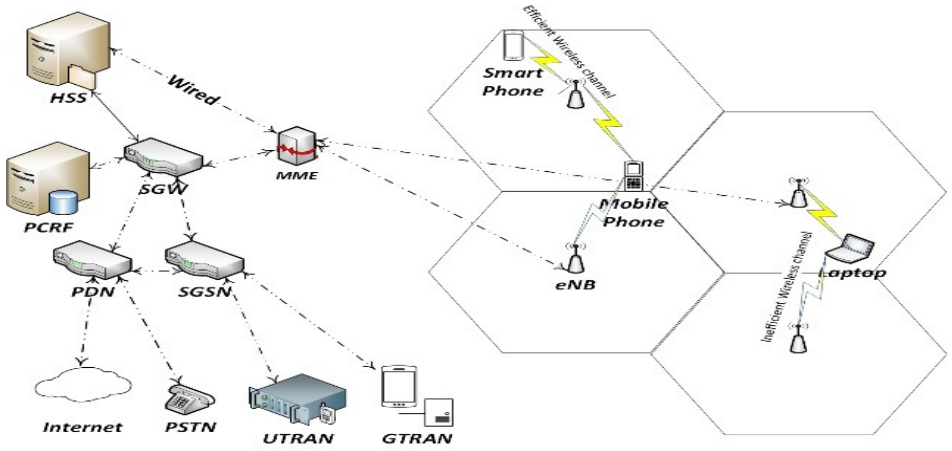

Figure 1: LTE-A Network Model

Number of eNBs is interconnected via the EUTRAN to manage multiple cells and to allow the interaction between different protocol layers in order to perform the radio resource management, header compression, securely capabilities and connectivity functions.

The security of cellular communication is a very important issue to subscribers. Attacker can exploit any security flaw to perform their goals. Telecommunication, video and audio streaming, mobile banking, data transmission, commences and etc. are a mobile application that may be attacked and hence causes a sophisticated problems. Authentication is the security issue that verifies users to the network. The problem in this issue allows unauthorized users to access the network.

Consider the system and the communication models of the LTE-A as depicted in Figure 1, the MMEs are the connection link between the HSS and the UEs. In our propose scheme, we do not introduce any modification on the original infrastructure of the LTE-A. Only we introduce a soft modification on the parameters and algorithms that are adapted in the system entities; such as the RSA scheme in the UEs and the HSS, to generate and regenerate parameters, and the certificate authority, to distribute PKs to between MMEs and UEs [2][16].

3.1.2. LTE-A Authentication Procedure

EPS-AKA authentication procedure was proposed in the 3GPP release 9 for LTE networks. EPS-AKA can broadly be divided into two stages: (1) authentication data distribution, and (2) user authentication and key agreement. The former enables the home network (HN) of a mobile equipment (ME) to distribute authentication data to the serving network (SN) where the ME device is visiting. The latter is to establish new session keys between the ME and the SN. The EPS-AKA protocol works as follows [10]:

a) An UE sends an access request message to the MME.
b) Upon receiving a request, the MME launches an authentication procedure by asking the UEs identity (IMSI).
c) In response to the MME, the UE sends its identity (IMSI).
d) The MME sends an authentication data request message containing IMSI to the HSS for acquiring Authentication Vectors (AVs).
e) The HSS first generates AVs for the MME, an AV comprising a RAND, XRES, AUTN and KASME in steading of IK and CK in UMTS AV. The AV is expressed as AV = RAND||XRES||KASME||AUTN, and AUTN = SQN $\oplus$(AK || AMF || MAC), where $\oplus$ is a simple bitwise XOR and || is a simple concatenation operations.
f) The HSS sends back an authentication data request message including the generated AV (for the corresponding UE), so that the MME is authorized to authenticate the requesting UE.
g) Upon receipt of authentication vectors, the MME sends RAND and AUTN piggy-backed on authentication request to the UE, enabling the ME to verify the correctness of SQN and compute the RES.
h) The UE verifies the correctness of SQN by computing MAC and comparing it with the MAC carried in AUTN. If matched, the ME computes and sends the corresponding response RES back to the MME in an authentication response message.
i) Once the MME receives and verifies RES correctly, it chooses the corresponding KASME as the session key to protect its communication with the ME. In addition, the ME calculates its KASME accordingly.

3.2. Threat and Trust Model

The violation of the wireless network systems is a common target of hackers, thus, in this subsection; we consider two type of attacks that may violate the security of the LTE-A system such as the cyber-attack and the side channel attack [12].

Cyber-attack is any type of offensive maneuver employed by hackers that targets computer information systems, infrastructures, and computer networks by various means of malicious actions usually originating from an anonymous source that steals, alters, or destroys a specified target by hacking into a susceptible system. Cyber-attacks can range from installing spyware on computer systems to attempts to destroy the infrastructure of entire nations. Cyber-attacks have become increasingly sophisticated. In the LTE-A system a cyber-attack may be employed as a malicious such as, MME, UE, Home eNB (HeNB), and non-3GPP access point, in order to break down the system [12].

A side channel attack may be violate the security of the LTE-A system, since it relies on the relationship between information emitted through the side-channel and the secret data depending on information gained from the physical implementation of a cryptosystem. In the LTE-A network, femto and micro cells are good environments for side channel attack to be efficient where a technical knowledge of the internal operation of the system and powerful statistical methods are defined [12].

The trusted model is a TTP in the PKI that creates the public/private keys [12]. However, a meaningful trust model for a PKI must consider the semantic assumption and human cognition of trust relationship, such as the legal constricted agreements between participants and how identity information is displayed and represented. In our proposed scheme, we use the Pretty Good Privacy (PGP) to authenticate UE to the HSS. PGP [12] is a free version commercial encryption entity used to authenticate parities, the PGP allows every user to play a role of relaying parity where each one can sent certificate to each other. Therefore, PGP defines three methods for users

and relaying party to obtain a public key of other users; 1) a secure out-of-band channel, such as physical meeting, 2) online trust decision based on introductions of new certificate from previously trusted users, and 3) based on discretionary trust decision when receiving a public key [12].

4. PRELIMINARIES

In this section, both the public key infrastructure and the RSA scheme are presented as our preliminaries, since the SEPS-AKA is based on both of them.

4.1. Public Key (PK) Cryptography

It is asymmetric cryptography involving the use of two separate keys, unlike symmetric encryption, that uses only one key [13][14]. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication. Public-Key Cryptography was developed to address two key issues. First, key distribution, in how to have secure communications in general without having to trust a KDC with your key. Second, digital signatures, in how to verify a message comes intact from the claimed sender. Public-key cryptography involves the use of two keys. First, Public-key is known to everybody in order to use for encrypting messages, and verifying signatures. Second, Private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures. Public key cryptography applications are classified into three categories: 1) Encryption/decryption; the sender encrypts a message with the recipient's public key, 2) Digital signature; the sender signs a message with its private key, either to the whole message or to a small block of data that is a function of the message, and 3) Key exchange, two sides cooperate to exchange a session key. The main advantage of public key cryptography is the asymmetricity since who encrypts message or verifies signature cannot decrypt same messages or create same signatures, therefore, it is infeasible to determine private key from public [13][14].

4.2. The RSA Scheme

The security principle of the RSA scheme is based on hardness of the factorization problem due to the cost of factorizes large numbers [13][14]. Each user generates a public/private key pair by selecting two large prime numbers at random: p, q. compute $n = p * q$ and $\phi(n)=(p-1)(q-1)$. Randomly, the RSA scheme selects an odd number e, where $1< e < \phi(n)$, $\gcd(e , \phi(n)) =1$, $e*d=1 \bmod \phi(n)$, and $0\leq d \leq n$. Then publishes their public key $PU=\{e,n\}$ and keeps secret private key $PR=\{d,n\}$. To encrypt a message, M, the sender obtains a public key of the recipient and computes the cipher text, $C = M^e \bmod n$, where $0 \leq M < n$. To decrypt the cipher text C, the owner of the message uses their private key, $PR=\{d,n\}$, and computes $M = C^d \bmod n$ [13][14].

5. PROPOSED SCHEME (SEPS-AKA)

Figure 2 describes the SEPS-AKA proposed scheme, the workflow of the SEPS-AKA is the similar to the framework of the original EPS-AKA scheme. The methodology of our proposed system uses the two methods explained in the previous section to enhance and adapt the privacy of the original LTE-A authentication procedure. First, the infrastructure of the public key cryptography is used to encrypt the exchanged data between LTE-A network entities. Second, the RSA scheme computation is used to compute the used parameters in the previous section. A pre-shared secret key K is used as the original LTE-A network where the key was industrially preset to the devices and stored physically in the USIM and to the HSS. The workflow of the SEPS-AKA scheme is described as follows:

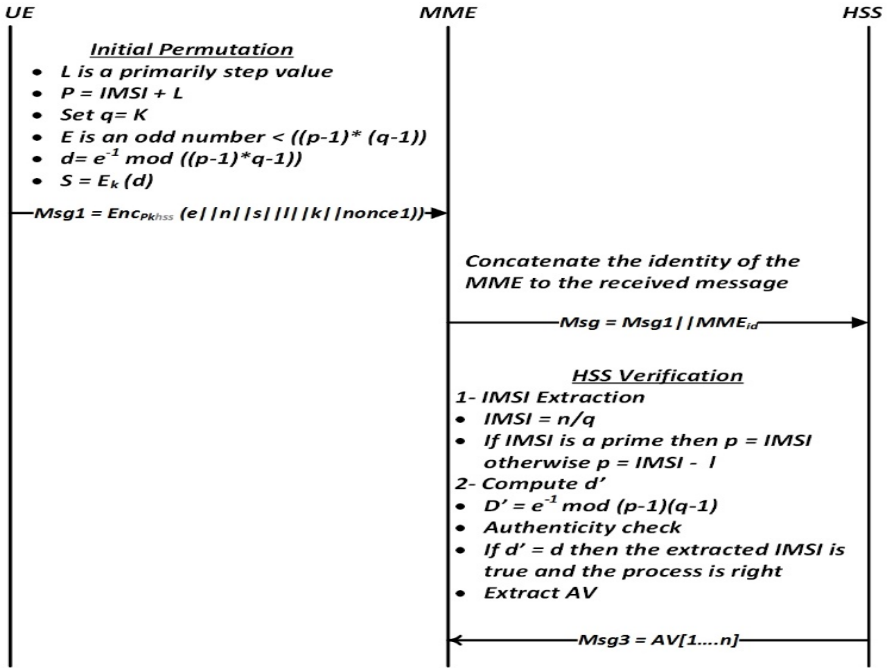

Figure 2: The SEPS-AKA Scheme

5.1. UE ⟶ MME

In this stage, UE initiates five parameters; *p, q, n, d*, and *L*. these parameters are computed based on the RSA scheme computations using the IMSI and k as follows:

a) Parameter Initiation

○ Select large prime number p.

$$p = IMSI + L \quad (1)$$

Where *L* is an integer number computed when the IMSI is not prime as L = 0, if IMSI is prime, otherwise L is the step value of the next prime after IMSI.

○ Set q as a random large prime number

○ Compute *n* :

$$n = p * q \quad (2)$$

○ Compute large number d:

$$d = e^{-1} \bmod (p-1)(q-1) \quad (3)$$

Where *e* is an odd number < *((p-1) *(q-1))*

b) Parameter Encryption: Encrypts d using a standard encryption algorithm (AES) to provide an encrypted parameter, *s*.

$$s = E_k (d) \quad (4)$$

c) Message Building and originating: Concatenates the last parameters p, n, q, s, L and a nonce1 together, encrypts the result using the public key of the HSS (PK_{HSS}) and originating the encrypted message to the HSS.

$$msg1 = E_{PK_{HSS}}(e \,||\, n \,||\, s \,||\, q \,||\, L \,||\, nonce1) \quad (5)$$

5.2. MME ⟶ HSS

Once MME receives msg1, it builds msg2 as illustrated in (6), which is the received message from the UE msg1 plus its identity MME_{id} and originates the message to the HSS

$$msg2 = msg1 \,||\, MME_{id} \quad (6)$$

Where MME_{id} is the identity of the MME

5.3. HSS ⟶ MME

Once the HSS receives *msg2* from the MME, it decrypts the message and executes the following:

- **IMSI extraction**

$$IMSI = (n / q) \quad (7)$$

- Check the primarility of the extracted IMSI,
  If IMSI is prime then

$$p = IMSI \quad (8)$$

Otherwise

$$p = IMSI - L \quad (9)$$

Where L is an integer number transmitted from the UE, and was computed when the IMSI is not prime in equation (1) as; $L = 0$, if IMSI is prime, otherwise L is the step value of the next prime after IMSI

- **IMSI Verification:**

Compute d' as illustrated in (10); a large number computed based on the RSA scheme computation, in order to verify the IMSI in the HSS side. The IMSI verification in the HSS is done as follows; check $d' = d$, if true then the IMSI is true; this process is not supported in the original EPS-AKA scheme, while the IMSI is verified in the HSS using database query.

$$d' = (e^{-1}) \bmod (p-1)(q-1) \quad (10)$$

After the IMSI verification is done correctly the remained steps are doing normally as the original EPS-AKA scheme.

6. SECURITY AND PRIVACY ANALYSIS

In this section, we analyze the security of our scheme to demonstrate that it meets the security requirements of the LTE-A systems. In our scheme, three levels of security are used: PKI, the RSA scheme computations and nonces. Nonces are random numbers generated by UE, MME and HSS to use in generating challenge messages toward the opposite side. A different Nonces are used in each authentication procedure, therefore, the reusing of these Nonces are not efficient. An out-of-sync situation will lead to authentication failure.

Consider a cyber-attack, in which a malicious UE aims to register to the LTE-A network, the malicious UE need to gain the computation of the RSA scheme parameters (p, q, s, and n) and to

gain the encryption information, which is required to prepare the message before sending from the UE. For the malicious MME, at the first registration time, the MME is considered as a gateway to route encrypted messages from the UE to HSS, while the MME must concatenate its certificate with the routed message in order to prove its authenticity to the HSS. Therefore, we consider the presence of the cyber-attack is impossible.

Consider a legal UE is worked through a femto and micro cells, which are two authorized environments uncontrolled by the LTE-A network, IMSI is not sent through the authentication message but is computed by the RSA scheme parameters (p and q), which is an NP problem, while the side channel attacks need a technical knowledge of the internal operation of the system and powerful statistical methods to be efficient.

In addition, our scheme prevent replay, impersonate attacks, the Man in the Middle, and DoS attacks. The replay attack is prevented by using the nonces in the transmitted messages, therefore, it is no possibility to use this message again. In addition of using the PK cryptography to encrypts the transmitted messages, the IMSI, the legal identity of the UE, is not transmitted in clear text over the transmitted messages, therefore, the attack cannot able to impersonate the identity of the UE. The MitM and DoS attacks are prevented as; if a member is able to sniff PKI, it still cannot computes the IMSI using the RSA scheme computations, although these messages are sent with PKI protection therefore, the attacker may not be able to hack this data since PKI is having the residency of DoS and MitM attacks. Therefore, the SEPS-AKA scheme attained the security requirements such as privacy, confidentiality, authentication, and data integrity.

Table 1. EPS-AKA Security Requirements

	Entity mutual authentication	Privacy	Confidentiality	Data Integrity
SEPS-AKA	Yes	Yes	Yes	Yes
EC AKA	Yes	Yes	Yes	No
SP AKA	Yes	No	Yes	No
HSK AKA	Yes	No	No	No
EPS-AKA	Yes	No	No	No

Table 1 is a comparison between SEPS-AKA scheme and the other previous EPS-AKA schemes in addition to the original EPS-AKA. The SEPS-AKA scheme adopts the same secured architecture as the EPS-AKA protocol. Therefore, it has the same security threshold in most situations. As illustrated in Table 1, the SEPS-AKA scheme can attain the security requirements as follows:

6.1. Entity mutual authentication

All schemes attain the entity mutual authentication since a UE is identified to the HSS by its IMSI. However, comparing with the SEPS-AKA scheme, where an UE is identified mathematically by its IMSI, as mentioned in equations (1), (7), (8), and (9), and the mathematical computation were based on the RSA scheme. The original and the EC-AKA schemes, the transmission of the IMSI gains the probability to different previous attack. In the SP-AKA and the HSK-AKA, the first step is begin from the MME that maintain a high probability of the presence of cyber-attack and the side channel attack.

6.2 Privacy

To ensure user privacy, the IMSI should be confidentiality protected. It should never be transmitted without protection. The EC-AKA achieves the privacy since an encrypted IMSI is transmitted. But the remainder schemes has no privacy since the IMSI is transmitted in clear text. But the SEPS-AKA scheme attains a high level of privacy where the IMSI is protected using the public key of the HSS.

6.3 Confidentiality

Confidentiality includes cipher algorithm agreement, cipher key agreement, confidentiality of user data and confidentiality of signaling data. The SEPS-AKA scheme follows the mechanism of the EPS-AKA protocol and hence is successful with these demands.

6.4 Data Integrity

Data integrity includes integrity algorithm agreement, integrity key agreement, data integrity and original authentication of signaling data. As illustrated in table I, No one of the scheme presented in table 1 except the SEPS-AKA scheme attain these purposes since no one of these schemes provide a level of verification of the IMSI, while in the SEPS-AKA scheme a high level of IMSI verification is performed using the IMSI extraction as illustrated in equation (9).

7. PERFORMANCE EVALUATION

The evaluation of the performance of the SEPS-AKA scheme is compared to HSK-AKA [7], EC-AKA [8], SP-AKA [9] and the original EPS-AKA. Therefore, two comparison criteria's will be discussed; bandwidth consumption and computation overhead.

7.1.Bandwidth consumption

Measuring the bandwidth consumption requires defining the employed cryptographic algorithm. Suppose the RSA scheme with 1024-bit key, therefore, the measuring of cipher text size as following [14]:

o Compute n:

$$n = \sum plaintext\ length\ in\ bytes \tag{11}$$

Where n is the length of the transmitted plaintext in bytes.

o Divides plaintext into equal blocks (16 byte)

$$s = ceil(\frac{n}{16}) \tag{12}$$

Where *S* is the integer number of blocks of the plaintext.

o Compute Ciphertext length c_len as :

$$c\_len = \left(1 + \frac{floor(RSAkeysize-1)}{8}\right) * s \tag{13}$$

Where S is the number of blocks

As shown in the table 2 and figure 3, the SEPS-AKA scheme consumes a bandwidth less than the EC-AKA, but comparing with SP-AKA, HSK-AKA and original EPS-AKA schemes, SEPS-AKA consumes a greater bandwidth. Since SP-AKA is not follow the same framework of the original EPS-AKA. HSK-AKA secures the original AKA based on the pseudonyms approach without PKI, and there is no security consideration on the original EPS-AKA

Table 2. Bandwidth Consumption

Scheme	Total bandwidth in bytes
SEPS-AKA	676
EC-AKA	816
SP-AKA	240
HSK-AKA	336
EPS-AKA	276

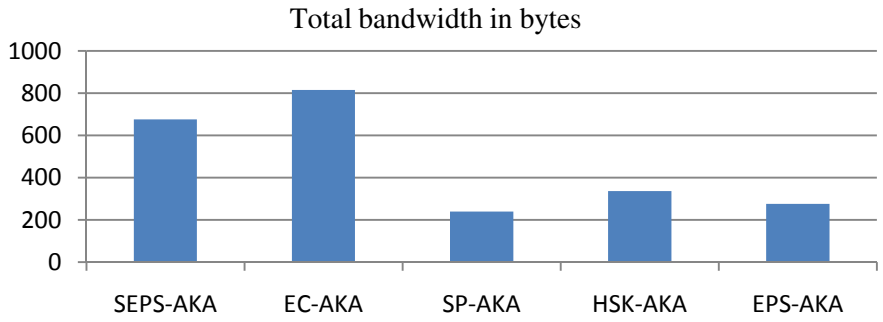

Figure 3: Bandwidth Consumption

7.2.Computation Overhead

To measure the computational overhead, we use crypto++5.6.0 benchmark which is compiled with Microsoft visual C++ 2005 SP1 and runs on Intel core 2 1.83 GHz processor under WINDOWS VISTA in 32 bit mode [15].

As illustrated in table 3 and figure 4, SEPS-AKA preserves the computational overhead compared to the EC-AKA scheme, while SP-AKA scheme provide less than computational overhead since, it is not recognized based on the original framework of the original EPS-AKA scheme. In addition, the original EPS-AKA and HSK-AKA schemes have no security aspects, therefore, there is no computational overhead attached with them.

Table 3. Computational overhead

Scheme	Computational overhead in microsecond
SEPS-AKA	39540
EC-AKA	89540
SP-AKA	2926

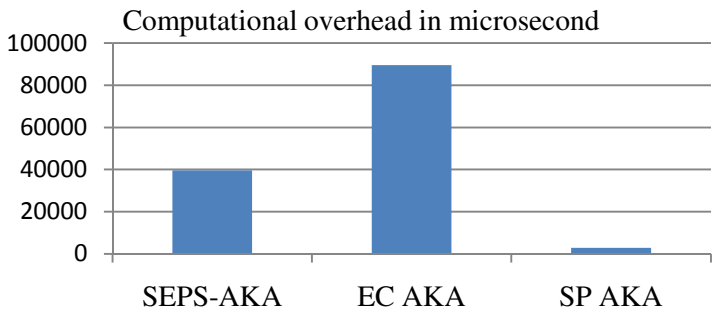

Figure 4: Computational Overhead

8. CONCLUSION

In this paper, we have proposed a secure and efficient EPS-AKA scheme, SEPS-AKA, using PKI and the RSA scheme computations in order to maintain the problems in the LTE-A authentication and key management. Compared with other authentication protocols, our proposed scheme robustly achieves security requirements including; privacy, authentication, confidentiality, and data integrity. Moreover, as the major contributions of the paper, extensive security analysis shows that the SEPS-AKA scheme is secure against various malicious attacks such as cyber and side channel attacks. Furthermore, the SEPS-AKA scheme has a high withstanding to the replay, DoS, MitM, and Impersonation attacks. The performance evaluation shows that the SEPS-AKA scheme achieves good bandwidth consumption and less computation overhead.

ACKNOWLEDGEMENTS

This paper is supported in part by the Zamalah Fellowship Program, Gaza, Palestine.

REFERENCES

[1] P. Bhat, S. Nagata, L. Campoy, I. Berberana, T. Derham, G. Liu, X. Shen, P. Zong, and J. Yang, "LTE-advanced: an operator perspective, "Communications Magazine, IEEE, vol. 50, no. 2, pp. 104–114, February 2012.

[2] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," Communications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 283–302, First 2013.

[3] S. Kanchi, S. Sandilya, D. Bhosale, A. Pitkar, and M. Gondhalekar, "Overview of LTE-A technology," in Global High Tech Congress on Electronics (GHTCE), 2013 IEEE, Nov 2013, pp. 195–200.

[4] J.-K. Tsay and S. F. Mjlsnes, "Computational security analysis of the UMTS and LTE authentication and key agreement protocols," Report arXiv: 1203.3866v2, Norwegian University of Sciences and Technology (NTNU), Department of Telematics, Norway, 2013.

[5] Y. Park and T. Park, "A survey of security threats on 4g networks," in Globecom Workshops, 2007 IEEE, Nov 2007, pp. 1–6.

[6] M. Purkhiabani and A. Salahi, "Enhanced authentication and key agreement procedure of next generation evolved mobile networks," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, May 2011, pp. 557–563.

[7] K. Hamandi, I. Sarji, A. Chehab, I. Elhajj, and A. Kayssi, "Privacy enhanced and computationally efficient HSK-AKA LTE scheme," in Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on, March 2013, pp. 929–934.

[8] J. Abdo, J. Demerjian, H. Chaouchi, and G. Pujolle, "EC-AKA2 a revolutionary aka protocol," in Computer Applications Technology (ICCAT), 2013 International Conference on, Jan 2013, pp. 1–6.

[9] J. B. Abdo, J. Demerjian, K. Ahmad, H. Chaouchi, and G. Pujolle, "EPS mutual authentication and crypt-analyzing SP-AKA," in Computing, Management and Telecommunications (ComManTel), 2013 International Conference on, Jan 2013, pp. 303–308.
[10] C. Lai, H. Li, R. Lu, and X. S. Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," in Computer Networks, Sep 2013, pp. 3492 – 3510.
[11] Y. Zheng, D. He, X. Tang, and H. Wang, "AKA and authorization scheme for 4G mobile networks based on trusted mobile platform," in Information, Communications and Signal Processing, 2005 Fifth International Conference on, 2005, pp. 976–980.
[12] C. Tang, D. Naumann, and S. Wetzel, "Analysis of authentication and key establishment in inter-generational mobile telephony," in High Performance Computing and Communications 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC·EUC), pp. 1605–1614.
[13] Eli, Atilla and R. Shankaran, "Theory and practice of cryptography solutions for secure information systems," in IGI Global, Sep 2013, pp. 1–351.
[14] W. Stallings, "Cryptography and network security: Principles and practice," in Prentice Hall, Jan 2011, p. Fifth Edition.
[15] W. Dai, "Crypto++ 5.6.0 benchmarks," MARCH 2009.
[16] P. Rengaraju, C.-H. Lung, and A. Srinivasan, "Measuring and analyzing WIMAX security and QoS in testbed experiments," in Communications (ICC), 2011 IEEE International Conference on, June 2011, pp. 1–5.

AUTHORS

Zaher Jabr Haddad received the BSc degree from the computer science department, faculty of applied science, Al-Aqsa University, Palestine in 1999 and MSc degree from the Department of Information Technology, Faculty of Computers and Information, Cairo University, Egypt in 2007. He is currently working toward the Ph.D. degree in Information Technology Department, Faculty of Computers and Information, Cairo University, Egypt. His interest in wireless network security and LTE networks

Sanaa Taha received the BSc and MSc degrees from the Department of Information Technology, Faculty of Computers and Information, Cairo University, Egypt, 2001, 2005, respectively, and the PhD degree in the Electrical and Computer Engineering from the University of Waterloo, Canada in 2013. She is currently an associated professor in the Department of Information Technology, Faculty of Computers and Information, Cairo University, Egypt. Her research interest include wireless network security, mobile networks security, mobile management, and applied cryptography.

Imane Aly Saroit Ismail received the B.Sc, MSc, and PhD from Department of Communication, Faculty of Engineering, Cairo University, Egypt, in 1985, 1990, and 1994, respectively. She is currently a full professor in the Department of Information Technology, Faculty of Computers and Information, Cairo University, Egypt. Her research interest include wireless network security, mobile networks security, mobile management, and applied cryptography.