Paper: ASAT-16-165-CM

16th International Conference on
AEROSPACE SCIENCES & AVIATION TECHNOLOGY,
ASAT - 16 – May 26 - 28, 2015, E-Mail: asat@mtc.edu.eg
Military Technical College, Kobry Elkobbah, Cairo, Egypt
Tel : +(202) 24025292 – 24036138, Fax: +(202) 22621908

Security Enhancement for LTE Authentication Protocol (EPS-AKA)

Mohammed Aly Abdrabou*, Dr. Essam Abd El-Wanis‡ and Assoc. Prof. Dr. Ashraf Diaa Eldien Elbayoumy§

Abstract: In Long Term Evolution (LTE) networks Extensible Authentication Protocol (EAP) is an authentication framework, not a specific authentication mechanism. EAP-AKA is one of the methods of EAP which uses the Authentication and Key Agreement (AKA) mechanism based on challenge-response mechanisms, EAP-AKA is used in the 3rd generation mobile networks then modified and inherited to 4th generation mobile networks (LTE) as Evolved Packet System Authentication and Key Agreement (EPS-AKA) mechanism. EPS-AKA vulnerabilities are disclosure of the user identity, Man in the Middle attack and Denial of Services (DoS) attacks so a robust authentication mechanism must replace EPS-AKA to avoid such attacks.
In this paper, Modified Evolved Packet System Authentication and Key Agreement (MEPS-AKA) protocol based on Simple Password Exponential Key Exchange (SPEKE) is proposed to solve these problems. Scyther tool is used to verify the efficiency of the proposed protocol against the mentioned attacks. EPS-AKA and MEPS-AKA are simulated using C programming language to calculate the execution time for both algorithms.

Keywords: EAP-AKA, LTE, AKA, SPEKE, EPS-AKA, Scyther.

I. LTE Network and Security Architecture

Radio-Access Network (RAN) and Core Network (CN) was redesigned and this known as System Architecture Evolution (SAE) (which is evolution of the overall network architecture). The RAN which and the EPC are referred to as the Evolved Packet System (EPS). It was decided to separate the user data (UP) and the signaling (CP) to make operators can operate their network easily independent as shown in Fig. 1 [1].

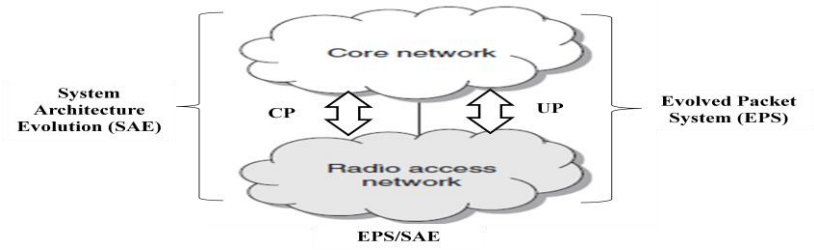

Fig. 1. Overall system architecture.

* Technical Research Center, Egyptian Armed Force, Egypt
‡ Military Technical College, Egyptian Armed Force, Egypt.
§ Military Technical College, Egyptian Armed Force, Egypt.

The RAN in LTE is called E-UTRAN and the CN is called EPC as shown in Fig. 2, it consists of several different types of nodes as follow [2]:

1 Mobility Management Entity (MME): Control-plane node of the EPC, handles the signaling related to mobility and security for E-UTRAN access handling of security keys.
2 Home Subscriber Service (HSS): database that contains subscriber information user authentication.
3 The Serving Gateway (S-GW): User-plane node transports the IP data traffic between the UE and the external networks.
4 The Packet Data Network Gateway (P-GW): Connects the EPC to the internet, Allocation of the IP address for a terminal, the mobility anchor for non-3GPP RAN, as CDMA2000.
5 ENodeB: One eNodeB can be connected to multiple MMEs/S-GWs for the purpose of load sharing and redundancy.

UE reach the EPC using E-UTRAN which is not the only access technology supported: 1 - 3GPP RAN, by interworking between E-UTRAN (LTE and LTE-Advanced), GERAN (GSM) and UTRAN (UMTS). 2 - Non-3GPP RAN (e.g. cdma2000) [1].

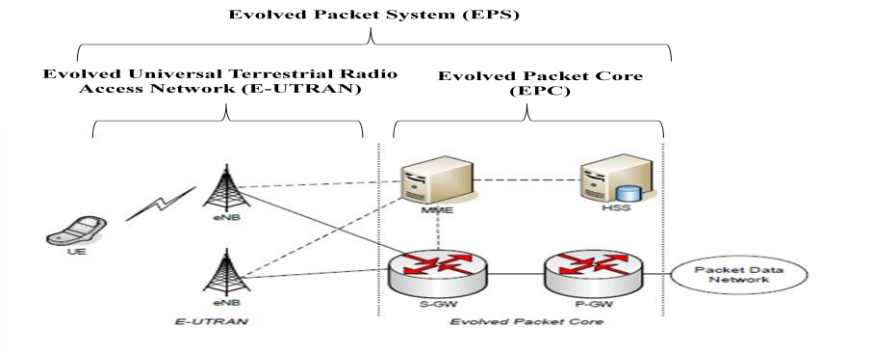

Fig. 2. LTE network nodes architecture.

A security feature is a service capability that meets one or several security requirements. A security mechanism is an element that is used to realize a security feature. All security features and security mechanisms form the security architecture as shown in Fig. 3. Example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher [3].

The 3GPP classify security feature in the LTE network into five groups as follow:

I. Network access security: the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link
II. Network domain security: the set of security features that enable nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wireline network
III. User domain security: the set of security features that secure access to mobile stations
IV. Application domain security: the set of security features that enable applications in the user and in the provider domain to securely exchange messages
V. Visibility and configurability of security: the set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

Our work will be in the network access security; where Entity authentication comprises two steps and should occur at each connection setup between the user and the network. First, user authentication ensures that the serving network corroborates the user identity of the user. Next, network authentication ensures that the user's connection is to a serving network with an up-to-date authorization from the user's home environment (HE) to provide services; to achieve mutual authentication between the user and the network [3].

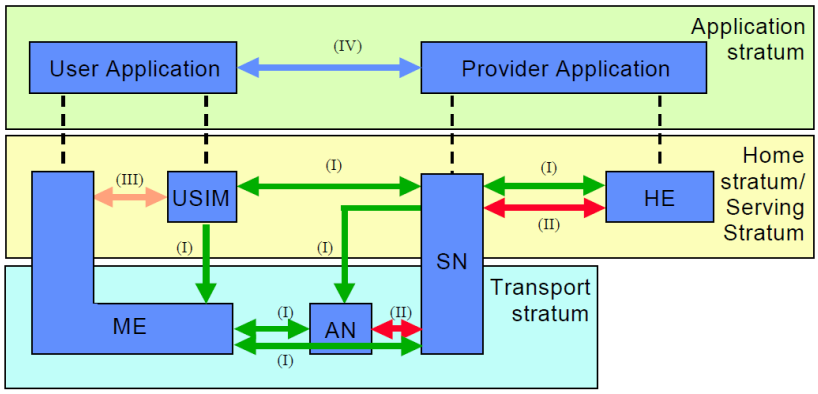

Fig. 3. Overview of the security architecture

II. EPS-AKA protocol

In LTE network, EPS-AKA protocol is used as an authentication mechanism, where Extensible Authentication Protocol (EAP) is an authentication framework, not a specific authentication mechanism, providing for the transport and usage of keying material and parameters generated by EAP methods [4], EAP-AKA is one of the methods of EAP uses the Authentication and Key Agreement (AKA) mechanism based on challenge-response mechanisms and symmetric cryptography.

The authentication procedure starts after connection establishment as shown in Fig. 4 between UE and MME as follow [3-6]:

1 MME send an ID request to the UE via eNB.
2 UE respond by IMSI.
3 MME request an EPS authentication vector (AV) from the HSS, Based on the IMSI, the HSS looks up the key K and a sequence number associated with that IMSI, the AuC increases the SQN and generates a random challenge (RAND) beside master key K as input to cryptographic functions, and generates AV, this AV consists of: XRES, AUTN, K_{ASME} and RAND.
4 HSS/AuC send the AV to MME, the MME keeps the K_{ASME} and XRES but forwards RAND and AUTN to UE.
5 Both RAND and AUTN are sent to the UE to calculate its own version of AUTN using its own key K and SQN and compare it with the AUTN received from the MME, To make user authenticate the network, if matched UE compute RES using cryptographic functions with the key K and the RAND. Also computes CK and IK.
6 Sends the RES back to the MME, MME authenticates the terminal by verifying that the RES is equal to XRES. This completes the mutual authentication. The UE then uses the CK and IK to compute K_{ASME} in the same way as HSS. Then both UE and MME now have the same key K_{ASME}.
7 Then MME send to UE the success or failure authentication process.

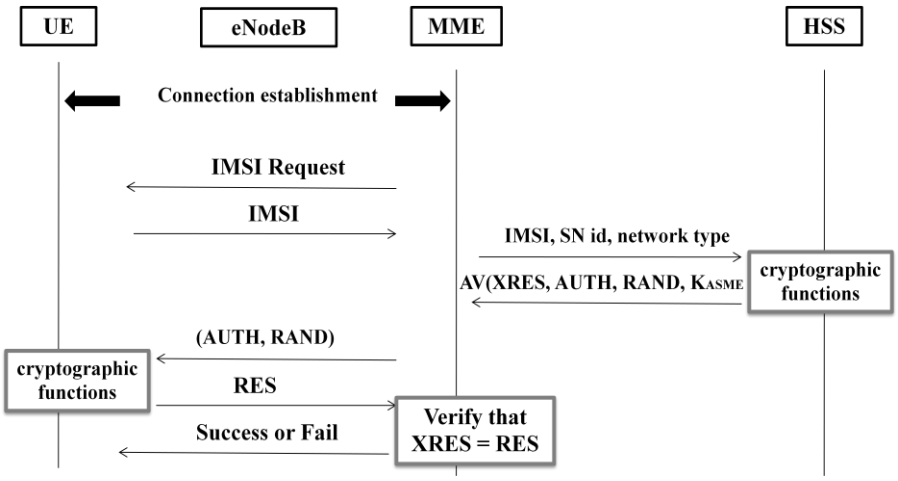

Fig. 4. EPS-AKA procedure.

III. Weakness in the EPS-AKA Protocol

The first weakness is; Disclosure of the user identity which caused when the UE registers to the network for the first time, So UE transmits IMSI in plaintext. So attacker can capture the IMSI as shown in Fig. 5. The attacker can impersonates the UE afterwards and send the IMSI to the MME to gain some information. Once the IMSI has been obtained, the adversary could acquire subscriber information, location information, and even conversation information, and then hide the real UE and launch the other attacks such as DoS attacks to destroy the network [3],[7].

Fig. 5. Disclosure of the user identity.

The second is; Man In The Middle attack (MITM) where the attacker obtain the UE's IMSI, then tries to register with genuine BS by this IMSI then network sends RAND and AUTN. Attacker disconnects when these parameters are received. Afterwards the genuine UE register with a false BS by sending the original the RAND and AUTN and getting it to calculate RES. The false base station re-initiates an authentication request to the network. This time the false station has the correct RES as shown in Fig. 6.

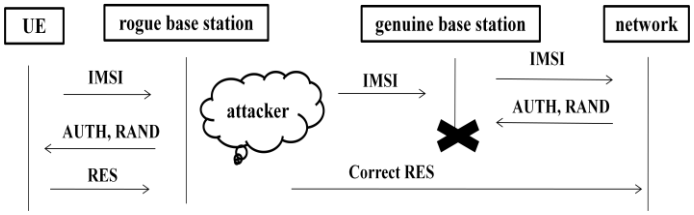

Fig. 6. MITM attack.

The third is; Denial of Services (DoS) attack, since MME manages numerous eNBs in the flat LTE architecture, the base stations in the LTE networks are more susceptible to the attacks compared with those in the UMTS architecture, where the serving network in the UMTS only manages a couple of RNCs in a hierarchical way. Once an adversary compromises base station, it can further endanger the entire network due to the all-IP nature of the LTE

networks; Adversary can launch DoS attacks to the HSS and the MME as shown in Fig. 7. The adversary can hide a legitimate UE to constantly send fake IMSIs to Fool the HSS. Thus, the HSS has to consume its computational power to generate excessive authentication vectors for the UE. On the other hand, the MME has to consume its memory buffer to wait overly long period of time for a legitimate or false response from the corresponding UE [7].

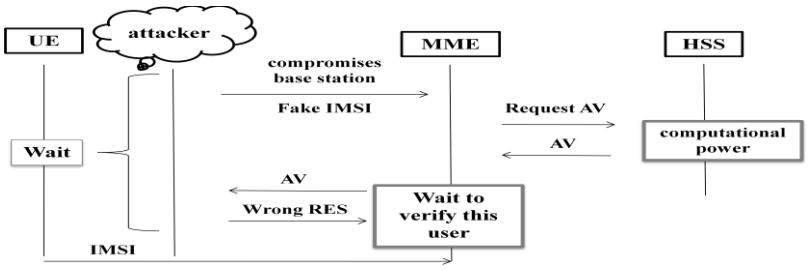

Fig. 7. DoS attack.

IV. Related work

A Security Enhanced Authentication and Key Agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI) has been proposed in [15]. The scheme ensures the security of user identity and the exchanged message with limited energy consumption by using Ellipse Curve Cipher (ECC) encryption. It has been pointed out in [16] that the SE-EPS AKA protocol is vulnerable to brute force and intelligent force attacks and thus it cannot guarantee the security of the user identity. Then, an ensured confidentiality authentication and key agreement (ECAKA) has been proposed to enhance the user's confidentiality. By the scheme, all the AKA messages are fully protected on the integrity by encryption, which can prevent the disclosure of identity of the users and the users being tracked, due to using public-key based protection mechanisms in [16] to overcome the shortcoming of the EPS AKA protocol, and thus can achieve a mutual authentication and ensure the security communication between the UE and HSS/AuC by the use of the UE and/or the HSS/AuC of public key certificates, these will cause a large number of computational costs, storage costs and communication costs for mobile devices with resource limitation. A slightly modified version of the EPS-AKA protocol has been presented in [17]. The scheme introduces a new subscriber module ESIM instead of the USIM and provides a direct online mutual authentication between the ESIM and the MME/HSS to overcome the shortcomings of the EPS-AKA protocol only with minor modifications of the access security architecture. However, it may suffer compatible problems in the LTE networks due to the use of the new ESIM. Since the HSS needs to participate in every authentication procedure for each UE, it may incur a large number of communication delays and thus cause signaling congestion on the HSS. In addition, it cannot overcome the disclosure of user identity.

In [18], the use of the password authentication key exchange by Juggling Password Authenticated Key Exchange (J-PAKE) protocol in the authentication process instead of the EPS AKA protocol to provide a stronger security protection has been proposed. The J-PAKE [19] is a password authentication keying agreement protocol to provide a zero knowledge proof using a shared key that is never sent over the transmission medium. However, it has only addressed the use of J-PAKE in the LTE networks without the introduction of the implementation of it to ensure secure communication and the reasons that the J-PAKE scheme can provide a stronger security than the EPS AKA. In addition, it cannot handle the security issue presented in the EPS AKA protocol, i.e. identity protection.

V. Proposed Modified EPS-AKA protocol (MEPS-AKA)

A Modified EPS-AKA protocol (MEPS-AKA) is proposed to overcome those weakness mentioned above. Based on a Simple Password Exponential Key Exchange (SPEKE) [8], [9] protocol, the cryptographic function includes a little change than a Diffie-Hellman key exchange where a password is hashed at the start.

There is pre-shared password (Psw), prime number (P), a shared key (Kum) and hash algorithm (H ( )) between MME and UE. The authentication procedure starts after connection establishment as shown in Fig. 8 between UE and MME through the following steps:

1 UE compute A and generate two random nonce (Ru1, u); send ({Ru1, A}kum,Ru1) to MME.

$$A = H(psw)^{u} \bmod p$$

2 MME compute B and generate two random nonce (Rm1, m); send ({Rm1, Ru1, B} kum, Rm1) to UE.

$$B = H(psw)^{m} \bmod p$$

3 From step 1 and 2 (UE and MME) compute their new key shared (k (u, m)) which is based on (SPEKE); then UE generate a random nonce (Ru2); then UE send ({IMSI, Ru2, Rm1} k(u , m) , Ru2) to MME. Where IMSI is International Mobile Subscriber Identity.

4 MME retrieve IMSI and Ru2 and then create a random nonce (Rm2); send ({{IMSI, Ru2, Rm2} k (u, m), k (u, m)} k (h, m), Rm2) to HSS. Where K (h, m) is a shared key between MME and HSS.

5 HSS retrieve the IMSI and get the corresponding key for this IMSI (k), calculate the shared key between UE and HSS (K (u, h)), generate nonce (Rh), calculate the expected response to authenticate the UE; then send ({{Rh, Ru2} k(u , h) , Rm2, Rh} k(h , m), Rh) to the MME.

$$K(u, h) = k(u, m) \oplus k$$
$$XRES = \{Rh\}\ k(u, h)$$

6 MME generate random nonce (Rm3); send ({{Rh, Ru2} k (u, h), Rm3} k (u, m), Rm3, Rh) to UE.

7 UE authenticate MME by checking the values of retrieved Rm3 and Rm3 received, authenticate HSS by checking the values of retrieved Rh and Rh received, if they are matched then calculate the response and generate a random nonce (Ru3); send ({{Rh} k(u , h) , Ru3} k(u , m) , Ru3) to MME.

$$RES = \{Rh\}\ k(u, h)$$

8 MME generate a random nonce (Rm3); then send ({{Rh} k(u , h) , Rm3} k(h , m) , Rm3) to HSS

9 HSS authenticate UE by checking the values of response to the value of the expected response.

$$RES = \{Rh\}\ k(u, h)$$

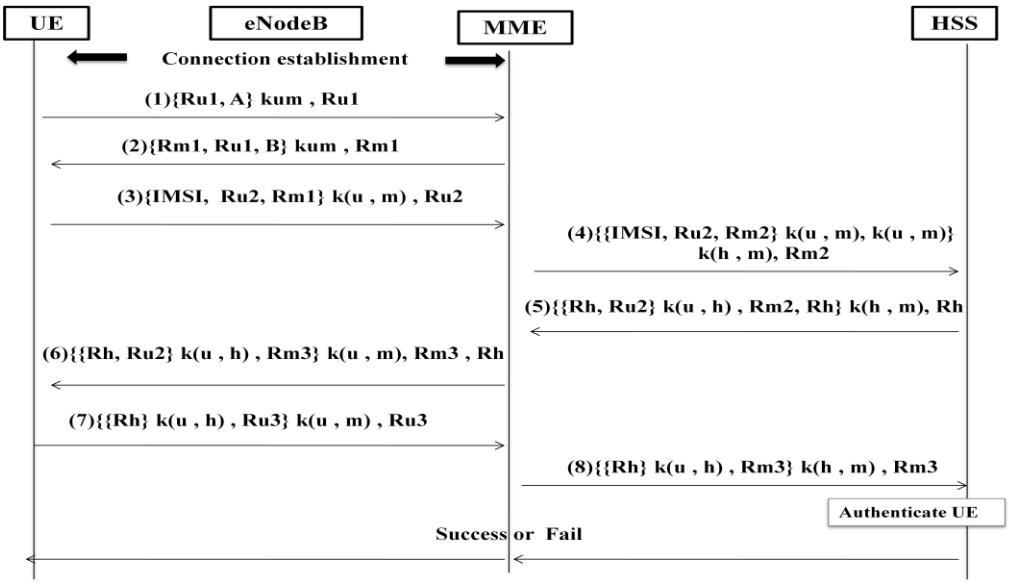

Fig. 8. MEPS-AKA procedure.

VI. MEPS-AKA Protocol Verification Results

The proposed protocol (MEPS-AKA) is verified using Scyther tool which used for the formal analysis of the security protocols to find problems that arise from the way the protocols are constructed. Many protocols can be either proven correct or attacks can be found [10].

Fig. 9 show an overview for MEPS-AKA protocol verification flow chart, where the following claims on the messages translated are checked:

Claim1; "Secrecy" expresses that certain information is not revealed to an adversary.

Claim2; "SKR" is used with the Diffie–Hellman to test the secrecy of the exchanged key.

Claim3; "Alive" if an agent A executes a role of the protocol, thinking she ran it with B, and then B has indeed performed an action (alive).

Claim4; "Weakagree" additionally B assumes that he is communicating with A, and hence they both "agree" on the agents involved in the protocol.

Claim5; "Niagree" focuses on agreement on the data exchanged between the agents.

Claim6; "Nisynch" synchronization only considers the contents and ordering of the messages.

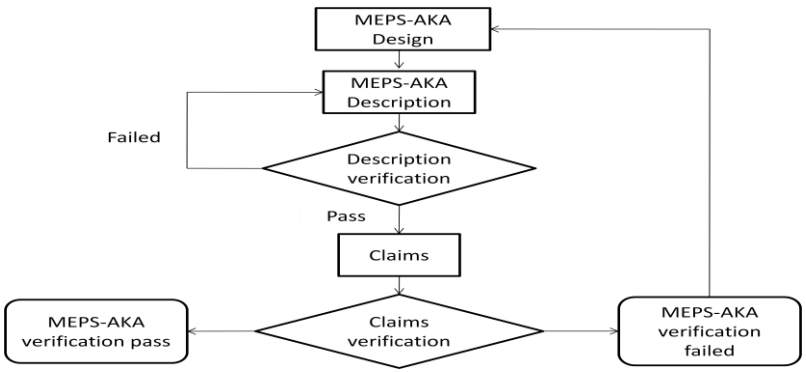

Fig. 9. Protocol Verification Flow Chart

MEPS-AKA protocol is verified in two steps. In the first step the messages between (UE) and (MME) is verified separately from the messages between (HSS) and (MME) which is the second step:

Step1; verification of the messages between (UE) and (MME): for messages (1, 2, 3, 6 and 7), the verification result shown in Fig. 10 and the claims are written as follow and:

1 - from the UE point of view as follow:

send_1 (ue, mme, {Ru1, exp (hash (psw), u)} kum, Ru1);
recv_2 (mme, ue, {Rm1, Ru1, z} kum, Rm1);
send_3 (ue, mme, {IMSI, Ru2, Rm1} k (ue, mme), Ru2);
recv_4(mme, ue, {{Rh, Ru2} kuh, Rm3, Rh} k (ue, mme), Rm3, Rh);
send_5 (ue, mme, {{Rh} kuh, Rm3} k (ue, mme), Rm3);
claim_ue (ue, SKR, exp (z, u));
claim_ue (ue, Secret, IMSI);
claim_ue (ue, Alive);
claim_ue (ue, Weakagree);
claim_ue (ue, Niagree);
claim_ue (ue, Nisynch);

2 - from MME point of view as follow:

recv_1 (ue, mme, {Ru1, z} kum, Ru1);
send_2 (mme, ue, {Rm1, Ru1, exp (hash (psw), m)} kum, Rm1);
recv_3 (ue, mme, {IMSI, Ru2, Rm1} k (ue, mme), Ru2);
send_4 (mme, ue, {{Rh, Ru2} kuh, Rm3, Rh} k (ue, mme), Rm3, Rh);
recv_5 (ue, mme, {{Rh1} kuh, Rm3} k (ue, mme), Rm3);
claim_mme (mme, SKR, exp (z, m));
claim_mme (mme, Secret, IMSI);
claim_mme (mme, Alive);
claim_mme (mme, Weakagree);
claim_mme (mme, Niagree);
claim_mme (mme, Nisynch);

Step2; verification of the messages between (MME) and (HSS): for the messages (4, 5 and 8), the verification result is shown in Fig. 11 and the claims are written as follow:

1 – from the MME point of view as follow:

send_1 (mme, hss, {{IMSI, Ru2} kum, Rm2, kum} k (hss, mme), Rm2);
recv_2 (hss, mme, {{Rh, Ru2} kuh, Rm2, Rh} k (hss, mme), Rh);
send_3 (mme, hss, {{Rh} kuh, Rm4} k (mme, hss), Rm4);
claim_mme (mme, Secret, IMSI);
claim_mme (mme, Alive);
claim_mme (mme, Weakagree);
claim_mme (mme, Niagree);
claim_mme (mme, Nisynch);

2 - from HSS point of view as follow:

recv_1 (mme, hss, {{IMSI, Ru2} kum, Rm2, kum} k (hss, mme), Rm2);
send_2 (hss, mme, {{Rh, Ru2} kuh, Rm2, Rh} k (hss, mme), Rh);
recv_3 (mme, hss, {{Rh} kuh, Rm4}k (mme, hss), Rm4);
claim_hss (hss, Secret, IMSI);
claim_hss (hss, Alive);
claim_hss (hss, Weakagree);
claim_hss (hss, Niagree);
claim_hss (hss, Nisynch);

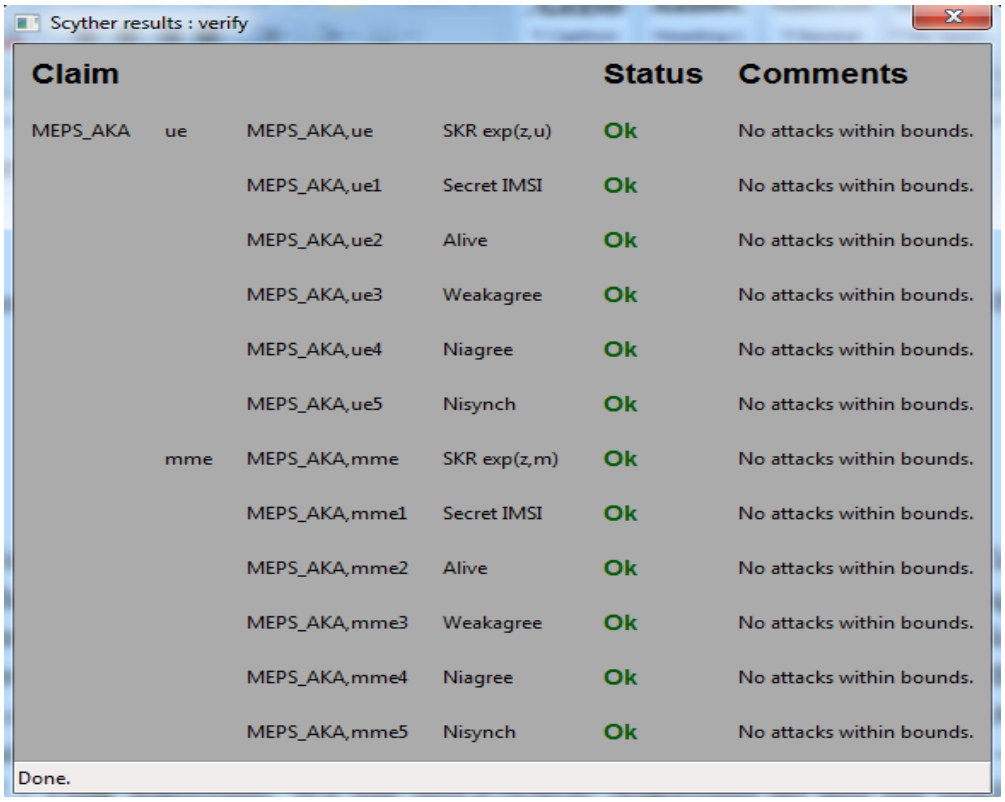

Fig. 10. The output result of first step

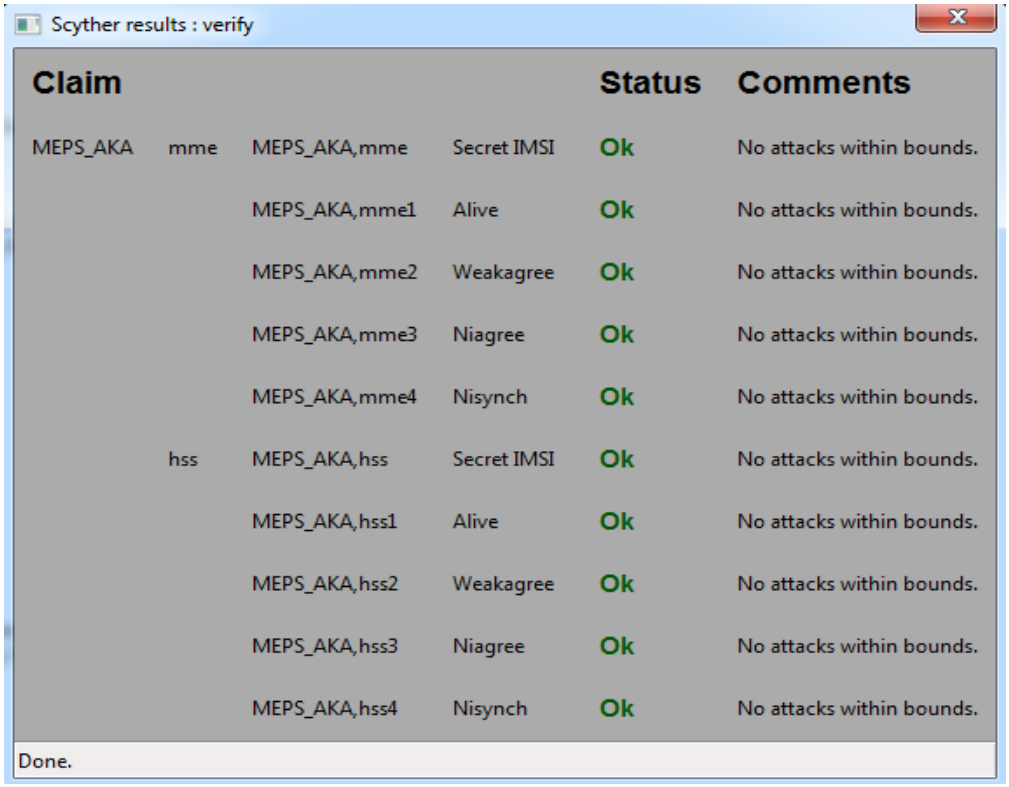

Fig. 11. The output result of second step

Our proposed protocol provides a strong mutual authentication between UE and HSS. Also it protects User identity. Also it is resistant to MITM attack where user identity cannot be retrieved or altered by the attacker, since it is protected by a strong secret key, only UE and HSS can do. Two examples for the cryptographic functions of EPS-AKA introduced by the

3GPP (they are not mandatory to use) and we use MILENAGE Algorithm one to implementation EPS-AKA as specified in [11-14], while implementation of MEPS-AKA is performed using gmp library, the implementation is performed using eclipse environment and C programming language, the simulations have taken place on a Laptop using a 64-bit windows 7 operating system. The Laptop is running with processing speed of 1.8 GHz, to calculate the time consumed for EPS-AKA (1.516 Sec) and MEPS-AKA (2.844 Sec). The consumed time for MEPS-AKA is greater than EPS-AKA but it is more secure than EPS-AKA from the results of the Scyther.

VII. Conclusion

The EAP-AKA protocol used in the 3G mobile networks and inherited to the 4G mobile networks (LTE) with minor modification leading to the Appearance EPS-AKA. This protocol fails to investigation full protection to the LTE network because it is exposed to disclosure of the user identity, MITM attack and DoS attack. MEPS-AKA protocol is proposed to overcome the vulnerabilities of EPS-AKA protocol. The performance evaluation for MEPS-AKA protocol is done using Scyther tool, also simulation of the EPS-AKA protocol and the MEPS-AKA is performed using C programming language. Results show that MEPS-AKA protocol execution time is greater than EPS-AKA protocol but MEPS-AKA protocol is more secure than the EPS-AKA protocol against the mentioned attacks.

VIII. Reference

1) Stefan Parkvall, Johan Skold, 4G: LTE/LTE-Advanced for Mobile Broadband Second Edition, Erik Dahlman, 2011.
2) 3GPP TS 23.002 version 11.6.0 Release 11, 2013.
3) 3GPP TS 33.401 version 12.12.0 Release 12, 2014.
4) B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed, Extensible Authentication Protocol (EAP), RFC 3748, 2004.
5) Fang-Yie Leu, IIsun You, Yi-Li Huang, Kangbin Yim, Cheng-Ru Dai1, Improving Security Level of LTE Authentication and Key Agreement Procedure, 2012.
6) Chunyu Tang, David A. Neumann, and Susanne Wetzel, Analysis of authentication and key establishment in inter-generational mobile telephony 2013.
7) Jin Cao, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo, A Survey on Security Aspects for LTE and LTE-A Networks, 2014.
8) Anjani K. Rai, Vimal Kumar, Shivendu Mishra, An Improved Password Based EAP Method for WiMAX with Formal Verification, 2011.
9) Kamal Ali Alezabi, Fazirulhisyam Hashim, Shaiful Jahari Hashim and Borhanuddin M. Ali, An Efficient Authentication and Key Agreement Protocol for 4G (LTE) Networks, 2014.
10) cas.cremers, scyther manual, 2014.
11) 3GPP TS 35.205 version 12.0.0 Release 12, 2014.
12) 3GPP TS 35.206 version 12.0.0 Release 12, 2014.
13) 3GPP TS 35.207 version 12.0.0 Release 12, 2014.
14) 3GPP TS 35.208 version 12.0.0 Release 12, 2014.
15) X. Li, and Y. Wang, ”Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network,” 2011.
16) J. Abdo, H. Chaouchi, and M. Aoude, ”Ensured Confidentiality Authentication and Key Agreement Protocol for EPS,”2012.
17) G.M. Koien, ”Mutual Entity Authentication for LTE” 2011.
18) C.Vintila, V. Patriciu, and I. Bica, ”Security Analysis of LTE Access Network 2011.

F. Hao and P. Ryan, ”J-PAKE: Authenticated Key Exchange without PKI 2010.