Security Improvements of EPS-AKA Protocol

Mourad Abdeljebbar and Rachid El Kouch
(Corresponding author: Mourad Abdeljebbar)
Department of Multimedia, Signal and Communications System, National Institute of Posts and Telecommunications
Avenue Allal El Fassi, Madinat Al Irfane, Rabat, Morocco
(Email: abj.mourad@gmail.com)
(Received Apr. 18, 2017; revised and accepted July 30 & Sept. 2, 2017)

Abstract

Nowadays, the users' authentication is a main aspect of any security system in which network access should be completed by only accepted users. For this purpose, the EPS network uses EPS-AKA procedure to authenticate the mobile users. In this paper, we present and analyze this procedure and we propose a new solution in order to manage its weaknesses and vulnerabilities. This solution, called Improved EPS-AKA, is a combination between the simplicity of deployment, the full mutual authentication and the secured communication between all network entities. Finally, our solution is checked and validated by the AVISPA model.

Keywords: 4G Security; Authentication; AVISPA; EPS-AKA; LTE-SAE

1 Introduction

During the last three decades, many new mobile networks have been developed after the first generation. The EPS (Evolved Packet System) network is one of the fourth-generation networks, which was modeled to increase not only the user data rate and mobile communications security, but also the network reliability. The EPS system is the result of combination between Long Term Evolution network (LTE) and System Architecture Evolution network (SAE) in which the LTE plays the role of an access network and the SAE as a core network [11]. In fact, the LTE is an evolved UTRAN connected directly to mobile users via base stations called eNodeB, while the SAE is an IP-based network, which contains many network elements to connect mobile users with outside networks. The main elements of SAE network are as follows [2, 11]:

1) Home Subscriber Server (HSS): A main subscribers database, which contains authentication parameters and subscription information of mobile users;

2) Mobility Management Entity (MME): The control node which handles control functionalities, such as security functionalities;

3) Packet Data Network Gateway (PGW): A bridge between SAE network and external IP-based networks in order to manage mobile users' data;

4) Serving Gateway (SGW): A bridge between E-UTRAN and PGWs in order to manage mobile users' data and mobility.

Regarding mobile user authentication, the 3GPP group has chosen the EPS-AKA (Evolved Packet System - Authentication and Key Agreement) as a procedure of mobile users' authentication in the EPS networks [1]. However, the procedure does not provide a real secure authentication protocol [3]. Many researches have been carried out to address this weakness by improving or modifying totally or partially the initial procedure. Currently, the most proposed solutions are designed to improve the initial procedure as it will not make a considerable change to the network. Cao *et al.* in [10] have made a survey on the security weaknesses of the 4G LTE network and the proposed solutions in the literature. Indeed, the EPS-AKA authentication mechanism was found vulnerable to several kinds of passive and active attacks, breakthrough of the privacy, Denial of Service attacks and some IP attacks. However, many solutions have been proposed to cover these issues but still doest not provide a real secure full authentication procedure like in [4–7, 15, 17].

With a wide range of potential applications, Machine Type Communication (MTC) is gaining a tremendous interest among mobile network operators, equipment vendors and research bodies. Regarding mobile networks, the MTC becomes an important part of the 4G and 5G network infrastructure in which the communication is established between different devices sharing similar features and the core network [12, 14]. Traditionally, each device must authenticate separately to others, which increase the signaling and communication latency between the serving network and the home network. To cover this issue, Giustolisi *et al.* have proposed a group-based AKA to authenticate a group of devices [14]. Despite the solution protects the permanent identity of the mobile users in the air links as the mobile user never send his IMSI, this identity is always in danger on the wired links as the

transmission is done in plaintext format. As well, the network privacy is in danger as it is vulnerable to traffic redirection attacks.

With the rapid development of the smart-cards, the smart-card-based password authentication as a two-factor authentication mechanism (2FA) becomes the subject of many research in the last two decades in which hundreds of this type of schemes have been proposed [27–29]. By the way, the 2FA is a mechanism for confirming the identity claimed by a mobile user by utilizing a combination of two different factors, which means that the user who owns the smart card and its corresponding password is the one who can connect to the server [29]. Indeed, password protection is the main challenge of the 2FA mechanism as it can be leaked from a compromised server or from the user itself. For this reason, several schemes have been proposed to cover these issues like Yi *et al.*s in [32] where they have proposed to distribute the password files and the users' data into several servers to prevent the password leakage from a compromised server, while Yan *et al.* in [31] have proposed to use a trusted device by users to avoid the password leakage from users' side. Although significant efforts have been made to develop safe and effective 2FA schemes, a small effort has been made to design systematic systems to evaluate the 2FA schemes. Hence, Wang *et al.* have proposed a systematic framework that contains a practical adversary model as well as a well-refined criteria set, which was used to evaluate and analyze 67 proposed schemes in the literature. Thus, the proposed schemes do not satisfy truly the security goals of the 2FA mechanism. Therefore, a new scheme has been proposed [29].

The reminder of this paper is organized as follows. In Sections 2 and 3, we describe and analyze the EPS-AKA procedure, while in Sections 4 and 5 we present and analyze the new solution. In Section 6, we describe the AVISPA tool that is used to test the new solution and Section 7 present the tests results. Finally, we draw our conclusions and interpretations.

2 EPS-AKA Protocol

The EPS-AKA procedure is an authentication protocol defined by 3GPP group for mobile users' authentication when they access to EPS network via E-UTRAN. The procedure is an improvement of UMTS-AKA used in 3G network in order to have a strong authentication protocol. The authentication procedure as shown in Figure 1 is described as follows [13]:

1) UE ⟶ MME: The user equipment (UE) starts the authentication procedure by sending its permanent identity IMSI to the serving MME in an attach request message;

2) MME ⟶ HSS: In the authentication information request message, the serving MME forwards the received IMSI and its network identity SNID to the home HSS;

3) HSS ⟶ MME: Consequently, the HSS checks the IMSI and the SNID in order to generate an authentication vectors array when the verification is done successfully. In the authentication information response, the HSS shares these authentication vectors with the serving MME. In fact, each authentication vector contains a random number (RAND), a local master key (KASME), an expected response (XRES) and an authentication token (AUTN);

4) MME ⟶ UE: The serving MME stores then the received authentication vectors and selects one to answer to UE's request. In the authentication request message, the serving MME sends the value of RAND and AUTN to the UE. For future authentication, the serving MME will select an unused authentication vector from its database or from previous serving MME;

5) UE ⟶ MME: Consequently, the UE calculates its AUTN and compares it with the received one in order to authenticate the home HSS. After a successful authentication, the UE calculates the value of RES and then sends it to the serving MME;

6) MME: Finally, the serving MME compares the value of RES and XRES to authenticate the UE.

3 Security Analysis of EPS-AKA Protocol

Currently, the EPS-AKA protocol presents many threats and weaknesses, which can affect the privacy and secrecy of the network and mobile users. We explain and analyze below some threats and possible attacks [3]:

- IMSI leakage: In the attach request message, the UE sends its permanent identity (IMSI) to the serving MME in plaintext without confirming, in advance, the honesty of this MME. Therefore, an attacker who can catch and read this message can easily identify this UE and then affect his privacy;

- SNID leakage: According to 3GPP specifications [1], the serving network identity (SNID) is a combination of mobile country code (MCC) and mobile network code (MNC). In the authentication information request message, the serving MME sends its identity to the home HSS in plaintext. Therefore, an attacker who can catch and read this message can easily identify this MME and then impersonate the serving network;

- GUTI Tracking: The radio interface is a weak space against attacks. Therefore, the knowledge of the UE's temporary identity (GUTI) may affect the privacy of that user in which a fake eNodeB or MME

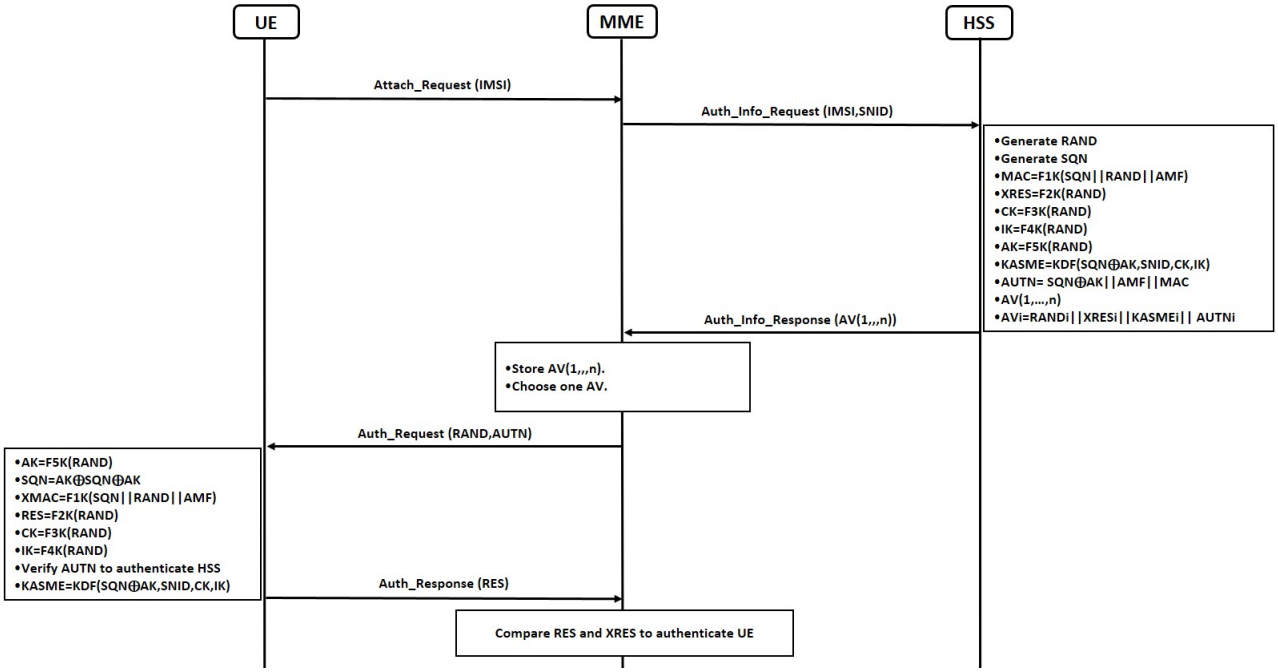

Figure 1: EPS-AKA procedure

can use this information to ask the UE to send its permanent identity and then affect the UE's privacy;

- Key leaked: Usually, the transmission over wired links is performed in plaintext, so an attacker can easily catch the authentication vectors shared with the serving MME and then gets the value of session keys. Therefore, the attacker can affect the secrecy of UE's communications;
- Link leakage: The transmission between EPC network entities is not protected against attacks because the transmission is performed in plaintext. Therefore, an attacker can easily catch the shared information and then affect the network privacy and secrecy;
- Traffic redirection: According to 3GPP specifications [1], the UE uses the value of AUTN to authenticate the HSS and the serving MME uses the value of RES to authenticate the UE, while the UE does not authenticate the MME and the MME does not authenticate the HSS. Therefore, the traffic redirection from an honest network to a fake network can be done by attackers.

4 Improved EPS-AKA Protocol

As described above, the EPS-AKA protocol still has some weaknesses related to the privacy and secrecy of the network and mobile users. To avoid such situation, the communication between UE and network in one side and between network elements in the other side should be protected. As well, the involved entities in the authentication procedure should be authenticated by each other's and the identity of the UE and network should be kept away from the third parties. Therefore, we propose the following changes to the original procedure:

- The communication between the involved entities in the authentication procedure is protected by the asymmetric cryptography system [20];
- The UE's permanent identity (IMSI) is hidden from the serving MME;
- The UE uses new symmetric key (NK) calculated by applying the XOR (exclusive or) operator to a generated random key (RK) and the original symmetric key (K) that is installed on its USIM card. The purpose of this new symmetric key is to protect the procedure from the replay attacks [18];
- The UE and HSS use a new secret parameter, called User Validation Parameter (UVP), to authenticate the UE by the HSS. The purpose of this new parameter is to protect the UE to be impersonated by an attacker when the UE's permanent identity is leaked;
- The serving MME and the home HSS use two new secret parameters, called Serving Network Validation Parameter (SVP) and Home Network Validation Parameter (HVP). The SVP is used to authenticate the serving MME by the home HSS while the HVP is used to authenticate the home HSS by the serving MME. Indeed, the two new parameters are an agreement between the home network and the serving network.

The improved EPS-AKA procedure is illustrated and explained below (Figure 2):

1) UE ⟶ MME: Firstly, the UE generates a random key RK to calculate a new symmetric key NK by applying the XOR operator to this random key and the original symmetric key K: $NK = RK \oplus K$. After that, it executes the hash function H on the new symmetric key and the UVP parameter: $UA = H(NK.UVP)$. By using the HSS's public key (Pkh), it encrypts the values of UA, RK and IMSI in which the result is sent to the serving MME in the attach request message with the value of the hybrid IMSI (HIMSI). In fact, the HIMSI is the first five digits of IMSI, which are related to country and network codes;

2) MME ⟶ HSS: The serving MME uses the HIMSI to get the HSS's public key from its database to encrypt its network identity (SNID), its SVP parameter and the encrypted value sent by the UE. Then, the result is sent to the home HSS;

3) HSS ⟶ MME: The HSS uses its private key (Prh) to decrypt the received messages and gets the values of UA, IMSI, RK, SNID and SVP. In order to authenticate the serving MME, the HSS uses the SNID to get the value of SVP parameter and then compares it with the received one. After a successful authentication, it uses the IMSI to get the value of the UVP parameter and the symmetric key K in which the latter is used to calculate the new symmetric key by the same way as UE: $XNK = RK \oplus K$. In order to authenticate the UE, it calculates the value of $XUA = H(XNK.UVP))$ and compares it with the value of UA. After a successful authentication of MME and UE, the HSS executes the hash function H on the SNID and the XNK: $MA = H(XNK.SNID))$ in which the result is encrypted by the UE's public key (Pku). Moreover, it generates an authentication vectors array, which is encrypted by the MME's public key (Pkm) with the UE's public key (Pku), the home network identity (HNID), the HVP parameter and the value of MA encrypted by the Pku key. Finally, the result is sent to the serving MME in the authentication response message;

4) MME ⟶ UE: The serving MME uses its private key (Prm) to decrypt the received message and then authenticates the HSS by verifying the HVP parameter. After a successful authentication of the HSS, it stores all data and choose one authentication vector (AV) to answer to UE's request. By the received UE's public key (Pku), it encrypts its identity SNID, its public key Pkm, the value of encrypted MA and the values of RAND and AUTN obtained from the selected vector, which are sent to UE in the authentication request message;

5) UE ⟶ MME: The UE decrypts the received messages by its private key (Pru). In order to authenticate the serving MME, the UE calculates the value of XMA by using the value of its new symmetric key NK and compares it with the received MA. After a successful authentication of the serving MME, it calculates the value of AUTN and compares it with the received one in order to authenticate the HSS. After a successful authentication of the serving MME and the home HSS, it calculates the value of RES and encrypts it with the received Pkm. Finally, the result is sent to the serving MME;

6) MME: Finally, the serving MME compares the values of RES and XRES to authenticate the UE.

5 Security Analysis of Improved EPS-AKA Protocol

The improved EPS-AKA protocol is designed to be a full mutual authentication protocol and solve the problem of the privacy and secrecy of the original protocol. A security analysis of this protocol is explained below according to the threats mentioned in Section 3:

- IMSI leakage: The UE encrypts its permanent identity (IMSI) by the HSS's public key before sending it to the serving MME. Therefore, the UE's identity is protected even if the serving MME is an attacker because it will need the HSS's private key to decrypt the message;

- SNID leakage: Using the SVP parameter by the HSS to authenticate the serving MME can protect the serving network from being impersonated by an attacker even if the SNID is disclosed. In addition, the transmission of this parameter is encrypted by the HSS's public key, which means that the attacker needs to know the HSS's private key to know the value of SVP parameter;

- GUTI Tracking: The transmission of the UE's permanent identity is protected by the HSS's public key. Therefore, an attacker cannot get the value of this identity even if he knows the value of his temporary identity, because he will need the HSS's private key to decrypt the message;

- Key leaked: The transmission of the UE's authentication vectors is protected by the MME's public key. Moreover, the serving MME must be authenticated successfully by the HSS before having these vectors. Therefore, a fake MME needs to be authenticated successfully by the HSS and needs to know the private key of the true MME to have these vectors and thus the session keys;

- Link leakage: The transmission of the authentication messages is protected by the asymmetric cryptogra-

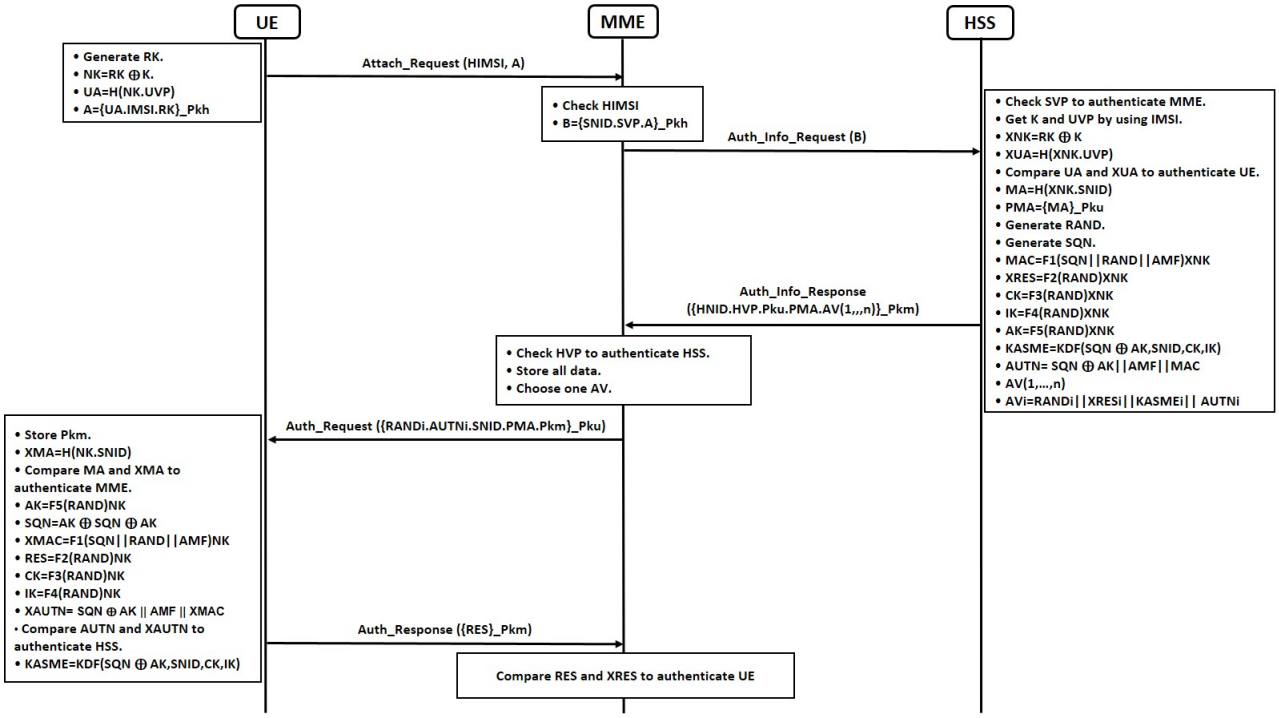

Figure 2: Improved EPS-AKA procedure

phy, which protects the network links against the disclosure of the shared information;

- Traffic redirection: The HSS needs to authenticate successfully the UE and the serving MME before sharing any information related to this UE's authentication. In addition, the serving MME needs to authenticate successfully this HSS before sending an authentication request message to the UE. Similarly, the UE needs to authenticate successfully the home HSS and the serving MME before confirming its access to the network in which the serving MME accepts this access if the authentication of that UE is succeeded. Therefore, the improved EPS-AKA is resistant against redirection attacks because each involved entity in the authentication procedure is authenticated by the others.

Furthermore, many schemes have recently been proposed to also secure the authentication procedure and solve the privacy problem in EPS networks. We present below three proposed schemes in order to compare them with our solution. The result of this comparison is shown in Table 1.

Hamandi *et al.* have proposed a privacy-enhanced to the initial EPS-AKA in which the aim is to minimize the transmission of IMSI and remove the linkability between the IMSI and GUTI [16]. In fact, the idea is to replace the permanent identity by a dynamic identity based on the RAND value and redefine the temporary identity by removing the MCC and MNC from the GUMMEI and calculating the M-TMSI by using the encryption and integrity keys of the NAS traffic. These keys are shared between the UE and the serving MME. In addition, the transmission of IMSI in the first attach is protected by the home HSS's public key and randomized by a timestamp. However, the transmission delay can affect the whole procedure if the request doest not arrive to the home HSS in the acceptable delay, hence the HSS will reject the request. This case is mostly happened when the serving MME and the home HSS are belongs to different networks (roaming case). As well, the transmission over the wired links is achieved in plaintext, which can affect the transferred information.

Wang *et al.* have proposed in [30] an improved privacy-preserving to Li *et al.* scheme [19] as it is found vulnerable to user anonymity violation attack and offline password guessing attack. Indeed, the both schemes are based on the use of a password-based smart card when a mobile user tries to access a foreign network and this password is used in the authentication parameters. However, the human action can affect the whole procedure as the human being can forgot the password of his or her smart-card or make multiple times a wrong password, which will block the smart-card and then the network access will not be possible. In addition, the human user can use the same password to access other applications and servers, such as e-mails, credit cards and so on, hence if the password is leaked from a non-secure access to these application and/or devices, the mobile user privacy can be affected.

Ramadan *et al.* have proposed in [22] a new scheme to solve the problem of radio attacks such as base station attacks in order to provide user-to-user mutual authentication and key agreement security in which the authentica-

Table 1: EPS network authentication schemes comparison result

	Our scheme	K. Hamandi scheme	D. Wang scheme	M. Ramadan scheme
IMSI leakage	**Safe**	**Safe**: The IMSI is encrypted before being sent.	**Safe**: The identity used instead of the IMSI is protected before being sent.	**Safe**: The hash value of the IMSI is used instead of the IMSI.
SNID leakage	**Safe**	**Unsafe**: The SNID is sent in plaintext.	**Unsafe**e: The identity (IDFA) used instead of the SNID is sent in plaintext.	**Safe**: The hash value of the SNID is used instead of the SNID.
GUTI Tracking	**Safe**	**Safe**: The new identity is calculated separately in both sides (UE and MME).	Not specified.	**Safe**: The hash value of the IMSI/GUTI is used instead of the IMSI/GUTI.
Key leaked	**Safe**	**Unsafe**: The AVs are sent in plaintext.	**Safe**: The session keys are calculated separately in both sides (foreign agent and mobile user).	**Safe**: The session keys are calculated separately in both sides (user A and user B).
Link leakage	**Safe**	**Unsafe**: The transmission over the wired links is done in plaintext.	**Safe**: A pre-shared symmetric key is used between foreign agent and home agent.	**Unsafe**: The transmission between HSS and MME is not secured.
Traffic redirection	**Safe**	**Unsafe**: The property of full mutual authentication is not applied.	**Unsafe**: The property of full mutual authentication is not applied.	**Unsafe**: The property of full mutual authentication is not applied.

tion is done between mobile users and the serving MME, while the HSS is used only to generate the system parameters from the security parameters. In fact, the proposed scheme is based on the Designated Verifier Proxy Signature (DVPS) in which the network is operate as a proxy and a non-trusted party. However, the idea of doing a user-to-user mutual authentication is interesting but the solution doest not provide any network privacy protection as the communication between the home network and the serving network is not discussed.

6 AVISPA Description and Architecture

The validation of security protocols is more difficult than normal communication protocols. Recently, many researches have been done to design validation tools by using the formal verification mechanism. R. Patel *et al.* in [21] have made a comparative study on the existing security verification tools in which they have concluded that the Scyther and AVISPA tools are the most efficient to verify and falsify security protocols. Therefore, we have chosen AVISPA to validate our solution.

The AVISPA project has been funded by European Community under the Information Society Technologies Program in which the High-Level Protocol Specification Language (HLSPL) was chosen as the programming language for the formulation of security protocols [23]. In fact, the HLPSL program is translated to intermediate format (IF) in order to be used by the four following back-ends tools: OFMC, CL-AtSe, SATMC and TA4SP (Figure 3) [26].

The HLPSL specification is defined by roles instead of messages, so it is sometimes difficult to confirm the correspondence between the HLPSL program and what the protocol designer wants to design. For this reason, an animator tool, called Security Protocol Animator (SPAN), has been developed to write, animate and understand the HLPSL specifications and build a Message Sequence Charts (MSC) of the protocol. In addition, the SPAN tool can simulate the possible attacks by constituting an active intruder [9].

7 Specification and Validation

The validation tests of the Improved EPS-AKA have been performed by the SPAN tool in which the security features to be simulated are mentioned in the HLPSL program goals section. By the way, our HLPSL program is divided into six sections in which the first three ones define the

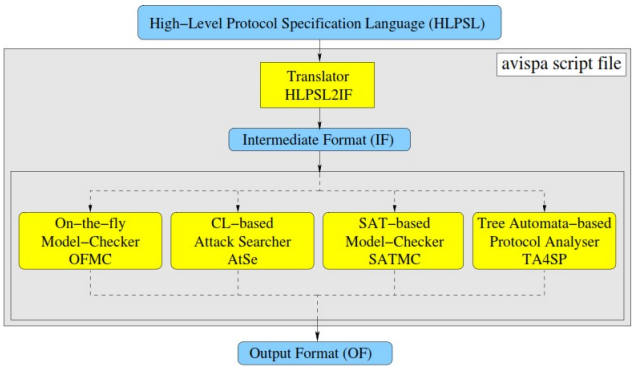

Figure 3: AVISPA Architecture

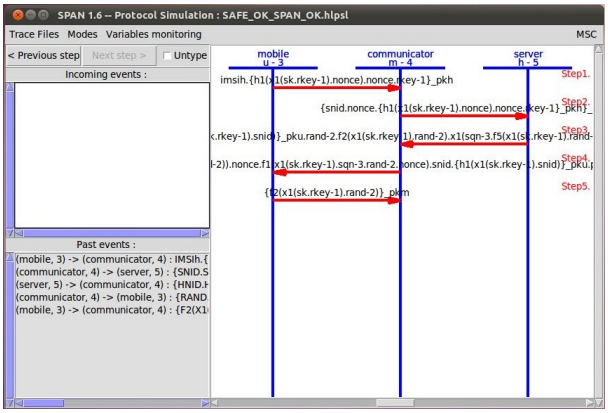

Figure 4: Improved EPS-AKA protocol simulation

role of UE, MME and HSS while the last three ones define the sessions, environment and goals of the protocol [24]. The improved EPS-AKA protocol simulation is illustrated in the Figure 4.

In order to check the robustness of the protocol, the following security features have been verified:

Secrecy: The expression secret(K,k,{A,B}) in the HLPSL program means that the value K produced or selected by a role played by the agent A is a shared secret between this agent and the agent B in which k is used to identify the secrecy goal in the goals section. In our case, the values of IMSI, K and UVP should be kept secret between the UE and the HSS while the values of SVP and HVP should be kept secret between the HSS and the MME;

Full mutual authentication: The full mutual authentication is obtained when the involved entities in the authentication procedure authenticate each other's. The verification of such goal is done by declaring the authentication request in the agent to be authenticated and the authentication witness in the authenticator. In our case, the UE authenticates the HSS by checking the AUTN value and the HSS authenticates the UE by checking the UA value. As well, the UE authenticates the MME by checking the MA value and the MME authenticates the UE by checking the RES value. Finally, the HSS authenticates the MME by verifying the SVP parameter and the MME authenticates the HSS by verifying the HVP parameter.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/SAFE_OK_SPAN_OK.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 1 nodes
  depth: 0 plies
```

Figure 5: Improved EPS-AKA simulation results by OFMC

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/SAFE_OK_SPAN_OK.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 0 states
  Reachable  : 0 states
  Translation: 0.01 seconds
  Computation: 0.00 seconds
```

Figure 6: Improved EPS-AKA simulation results by Cl-AtSe

In addition, the protocol robustness is also simulated by introducing in the intruder knowledge any information that can be known by the attackers. In fact, the Figures 5 and 6 show the results of the simulation by OFMC and Cl-AtSe verification tools [8,25]. As we can see, the summary of the simulation shows that the protocol is safe and that no attack has been detected. Therefore, all security goals mentioned above have been satisfied.

8 Conclusions

The EPS-AKA protocol objectives are quite similar to those for UMTS-AKA, used in 3G networks. The enhancement of EPS-AKA is that it provides implicit serving network authentication, which is achieved by binding an appropriate key, KASME, to the serving network identity. However, the existing EPS-AKA protocol does not offer a real secure authentication. Therefore, in this paper we proposed a new method called Improved EPS-AKA, which offers a secure authentication procedure by protecting any message exchange by the asymmetric cryptography system. Moreover, it protects the confidentiality of the UE and network even if the serving MME and the HSS are belong to the same network. The AVISPA tool was used to validate this new solution in which the result shows that it is resistant against attacks such as a replay attacks. The choice of AVISPA tool to validate our solution is due to the validation tools that it contains, which are used to validate the security protocols such as the authentication protocols. However, the security goals defined in a formal model may be different from the others, hence the simulation results may be different also. In addition, new attacks may be appeared in the future and may be difficult to model on a formal verification model. Therefore, if the security model used is currently the right one, the correctness of a security proof generally depends on the attacking experience.

References

[1] 3rd Generation Partnership Project (3GPP), *3rd generation partnership project; technical specification group services and system aspects: 3GPP system architecture evolution (SAE)/security architecture*, Technical Report 3GPP TS 33.401, V15.0.0, June 2017.

[2] 3rd Generation Partnership Project (3GPP), *3rd generation partnership project; technical specification group services and system aspects: Network architecture*, Technical Report 3GPP TS 23.002, V14.1.0, Mar. 2017.

[3] M. Abdeljebbar and R. E. Kouch, "Security analysis of LTE/sae networks over e-utran," in *Proceedings of The Second International Conference on Information Technology for Organizations Development (IT4OD'16)*, Fez, Morocco, 2016.

[4] J. B. Abdo, J. Demerjian, H. Chaouchi and G. Pujolle, "Ec-aka2 a revolutionary aka protocol," in *Proceedings of The International Conference on Computer Applications Technology (ICCAT'13)*, Sousse, Tunisia, Jan. 2013.

[5] M. A. Abdrabou, A. D. E. Elbayoumy and E. A. El-Wanis, "LTE authentication protocol (EPS-AKA) weaknesses solution," in *Proceedings of The IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15)*, Cairo, Egypt, Dec. 2015.

[6] K. A. Alezabi, F. Hashim, S. J. Hashim and B. M. Ali, "An efficient authentication and key agreement protocol for 4g (LTE) networks," in *Proceedings of The IEEE Region 10 Symposium*, Kuala Lumpur, Malaysia, Apr. 2014.

[7] C. G. Apostol and C. Racuciu, "Improving LTE EPS-AKA using the security request vector," in *Proceedings of The Seventh International Conference on Electronics, Computers and Artificial Intelligence (ECAI'15)*, Bucharest, Romania, June 2015.

[8] D. Basin, S. Modersheim and L. Vigano, "OFMC: A symbolic model-checker for security protocols," *International Journal of Information Security*, vol. 4, no. 3, pp. 181–208, 2005.

[9] Y. Boichut, T. Genet, Y. Glouche and O. Heen, "Using animation to improve formal specifications of security protocols," in *Proceedings of the Second National Conference on Security in Network Architectures and Information Systems*, Annecy, France, 2007.

[10] J. Cao, M. Ma, H.Li, Y. Zhang and Z. Luo, "A survey on security aspects for LTE and LTE-A networks," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 283–302, 2014.

[11] C. Cox, *An introduction to LTE, LTE-advanced, SAE and 4G mobile communications (1st, in English)*, pp. 352, 2012.

[12] O. Dementev, "Machine-type communications as part of LTE-advanced technology in beyond-4g networks," in *Proceedings of The Fourteenth Conference of Open Innovations Association (FRUCT'13)*, Espoo, Finland, Nov. 2013.

[13] D. Forsberg, G. Horn, W. D. Moeller and V. Niemi, *LTE Security (2ed, in English)*, pp. 368, 2013.

[14] R. Giustolisi, C. Gehrmann, M. Ahlstrm and S. Holmberg, "A secure group-based AKA protocol for machine-type communications," in *Proceedings of The International Conference on Information Security and Cryptology (ICISC'16)*, Seoul, South Korea, 2016.

[15] Z. J. Haddad, S. Taha and I. A. S. Ismail, "SEPS-AKA: A secure evolved packet system authentication and key agreement scheme for LTE-A networks," in *Proceedings of The Sixth International Conference on Wireless and Mobile Networks (WiMONe'14)*, Sydney, Australia, Dec. 2014.

[16] K. Hamandi, J. B. Abdo, I. H. Elhajj, A. Kayssi and A. Chehab, "A privacy-enhanced computationally-efficient and comprehensive LTE-AKA," *Computer Communications*, vol. 98, pp. 20–30, 2017.

[17] K. Hamandi, I. Sarji, A. Chehab, I.H. Elhajj and A. Kayssi, "Privacy enhanced and computationally efficient hsk-AKA LTE scheme," in *Proceedings of The Twenty-seventh International Conference on Advanced Information Networking and Applications Workshops (WAINA'13)*, Barcelona, Spain, Mar. 2013.

[18] A. Jesudoss and N. P. Subramaniam, "A survey on authentication attacks and countermeasures in a distributed environment," *The Indian Journal of Computer Science and Engineering (IJCSE'14)*, vol. 5, no. 2, pp. 71–77, 2014.

[19] H. Li, Y. Yang and L. Pang, "An efcient authentication protocol with user anonymity for mobile networks," in *Proceedings of The Wireless Communications and Networking Conference (WCNC'13)*, Shanghai, China, Apr. 2013.

[20] S. Nithya and D. E. G. D. P. Raj, "Survey on asymmetric key cryptography algorithms," *Journal of Advanced Computing and Communication Technologies (JACOTECH'14)*, vol. 2, no. 1, pp. 1–4, 2014.

[21] R. Patel, B. Borisaniya, A. Patel, D. Patel, M. Rajarajan and A. Zisman, "Comparative analysis of formal model checking tools for security protocol verification," in *Proceedings of The International Conference on Network Security and Applications (CNSA'10)*, Chennai, India, July 2010.

[22] M. Ramadan, F. Li, C.X. Xu, A. Mohamed, H. Abdalla and A. Abdalla, "User-to-user mutual authentication and key agreement scheme for LTE cellular system," *International Journal of Network Security*, vol. 18, no. 4, pp. 769–781, 2016.

[23] The AVISPA Team, *Avispa v1.1 user manual*, Technical Report www.avispa-project.org, June 2006.

[24] The AVISPA Team. *A beginners guide to modelling and analyzing internet security protocols*, Technical Report www.avispa-project.org, June 2006.

[25] M. Turuani, "The cl-atse protocol analyser," in *Proceedings of The Seventeenth International Conference on Term Rewriting and Applications (RTA'06)*, Seattle, USA, Aug. 2006.

[26] L. Vigan, "Automated security protocol analysis with the avispa tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61–86, 2006.

[27] D. Wang, Q. Gu, H. Cheng and P. Wang, "The request for better measurement: A comparative evaluation of two-factor authentication schemes," in *Proceedings of The Eleventh ACM on Asia Conference on Computer and Communications Security (ASIA CCS'16)*, Xi'an, China, 2016.

[28] D. Wang and P. Wang, "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks," *Ad Hoc Networks*, vol. 20, pp. 1–15, 2014.

[29] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 99, no. 99, pp. 1–1, 2016.

[30] D. Wang, P. wang and J. Liu, "Improved privacy-preserving authentication scheme for roaming service in mobile networks," in *Proceedings of The Wireless Communications and Networking Conference (WCNC'14)*, Istanbul, Turkey, Apr. 2014.

[31] Q. Yan, J. Han, Y. Li and R. H. Deng, "On limitations of designing leakage-resilient password systems: Attacks, principles and usability," in *Proceedings of The Nineteenth Network and Distributed System Security Symposium (NDSS'12)*, San Diego, California, Feb. 2012.

[32] X. Yi, S. Ling and H. Wang, "Efficient two-server password-only authenticated key exchange," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 9, pp. 1773–1782, 2013.

Biography

Mourad Abdeljebbar is a doctoral student at the National Institute of Posts and Telecommunications (Rabat, Morocco), where he graduated as a telecommunication engineer in 2008. After that, he joined Nokia Networks Morocco as a R4 circuit switching core consultant where he worked on several projects related to 3G and 4G networks. His research interests include authentication protocols, mobile networks, network security, cryptography and telecommunications networks.

Rachid El Kouch is a professor at the National Post and Telecommunications Institute (Rabat, Morocco). Since 1981, he is responsible for the PABX laboratory attached to the Systems and Communications Department at the INPT. Pr. EL KOUCH began his career as a telecommunications assistant engineer. He worked as an assistant in the INPT's electricity and electronics laboratory. In 1989, he graduated from the University of Colorado with a Master of Science in Telecommunications degree at Boulder, USA. In 2005, he received his PhD in Applied Mathematics from Mohammed Ben Abdellah University - Faculty of Science and Technology of Fez-USMBA. Between 1990 and 1992, he was a specialized tutor for several technical inspectors. It was a technology transfer program under a convention between France and Morocco. He supervised several internships for engineering students in the 2nd year of the engineering cycle and over 100 graduation projects for engineering students at the end of their training at INPT. He has been Deputy Director of Internships and Relationships with Enterprises since 2008. In 2010, he was asked for the position of Deputy Director of Continuing Education. In addition, he is a member of the research team Phare (UFR MDA) of the Laboratory of computer science and mathematics of the USMBA. Since December 2005, when the training project was launched (collaboration between UBC and Lyon1 USMBA), he supervised several modules on the electronic platform Miage (Lyon 1): B202- Bases of telecommunications and B214 - Network protocols. He has more than 30 articles in conferences and national / international journals on telecommunications, networks and security. He has also been a reporter for more than twenty theses (Ph.D).