Analysis of Authentication and Key Agreement (AKA) Protocols in Long-Term Evolution (LTE) Access Network

Mariya Ouaissa, A. Rhattoy and M. Lahmer

Abstract Mobile communications systems have evolved considerably in recent years. Fourth generation networks (4G) allow to expand cellular coverage while improving accessibility to Internet services. Network access security includes security features that provide the subscriber with secure access to services of the EPS, and protects particularly against several attacks on the radio link. This area is the largest and most vulnerable among all EPS security domains since it ensures the security of the radio link, the weakest link of all mobile telephone networks. In the LTE architecture, Evolved Packet System Authentication and Key Agreement (EPS-AKA) procedure is used to realize mutual authentication between the subscriber and the network. However, the current authentication and key agreement protocol 3GPP LTE-AKA has some issues, including bandwidth consumption, traffic overload due to control message and vulnerabilities. Several protocols have been proposed to solve these problems. In this paper, we will analyze and compare several existing protocols: EPS-AKA, SE-AKA, EC-AKA, and EC-AKA2 according to different factors in order to estimate the performances in terms of security, cost, and delay of each one of these protocols.

Keywords LTE/SAE · AKA · Network security · Authentication

M. Ouaissa (✉)
ISIC, High School of Technology, LMMI Laboratory, ENSAM,
Moulay-Ismail University, Meknes, Morocco
e-mail: mariya.ouaissa@edu.umi.ac.ma

A. Rhattoy · M. Lahmer
Department of Computer Engineering, High School of Technology,
Moulay-Ismail University, Meknes, Morocco
e-mail: rhattoy@gmail.com

M. Lahmer
e-mail: mohammed.lahmer@gmail.com

A. Kalam et al. (eds.), *Advances in Electronics, Communication and Computing*, Lecture Notes in Electrical Engineering 443,
https://doi.org/10.1007/978-981-10-4765-7_1

1 Introduction

Mobile communications systems have evolved considerably in recent years. Fourth generation networks (4G) allow to expand cellular coverage while improving accessibility to Internet services. The new mobile network system called Evolved Packet System (EPS) comprises a new access network called LTE (Long-Term Evolution) and a new core network called Evolved Packet Core (EPC) or System Architecture Evolution (SAE). All services are offered by a packet domain. The mobile must first connect and authenticate to the EPS network before being able to send or receive Internet Protocol (IP) packets [1, 2]. The element that allows authentication is called Mobility Management Entity (MME), the Home Location Register/Authentication Center (HLR/AuC) is characterized by Home Subscriber Service (HSS) in the EPS architecture (Fig. 1). Security in the fourth generation mobile networks EPS includes security of the radio access network infrastructure, terminals, and applications running on it. Network access security includes security features that provide the subscriber with secure access to services of the EPS, and protects particularly against the attacks on the radio link. One of the most important security services is authentication, 3GPP LTE-AKA protocol has some problems, including the consumption of bandwidth, the traffic generated: control and authentication messages and several vulnerabilities such as disclosure of user identity, man-in-middle attack, etc. In recent years, many articles have been published on the subject of security, focusing mainly on the applicative field. Some recent works on cellular communications have nevertheless made significant advances and demonstrated realism of attacks previously reputed theoretical. These studies identify certain inertness in the consideration of threats. This article is primarily concerned with these works and presents an overview of the security of communications in LTE Network. The second section of this article presents first a brief description of the elements composing the 4G network. These elements are necessary for understanding the principles underlying the security of mobile networks and their vulnerabilities, and then explain the principle steps of Evolved Packet System Authentication and Key Agreement (EPS-AKA) procedure.

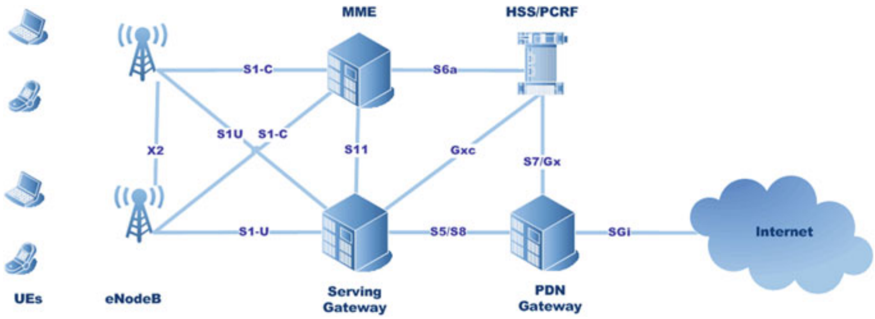

Fig. 1 LTE network architecture

Section 3 addresses in one hand the security analysis of AKA protocols of 4G and presents in the other hand, a comparison of performances between various existing security protocols in terms of communication overhead and delay, and finally conclusions are retained for Sect. 4.

2 LTE System Architecture and Security Mechanisms

This section presents an overview of the main elements of LTE network. We separate this description into two parts: the first is devoted to the infrastructure of the 4G network and the second to the mechanisms of security and the EPS-AKA procedure used to realize mutual authentication between the user and the network.

2.1 System Architecture

LTE is also referred to as the Evolved Packet System (EPS). The EPS is divided between the radio access network Evolved UMTS Terrestrial Radio Access Network (EUTRAN) and the EPC. In EUTRAN, mobile devices are called User Equipment (UE). The operation of base stations has been defined from the Universal Mobile Telecommunications System (UMTS) network architecture. That is why they bear the same designation than UMTS, Evolved Node B (eNodeB). As in Fig. 1, each eNodeB connects with the EPC via the S1 interface and can also be connected to the neighboring base stations by the X2 interface [3, 4].

EPC uses IP as a transport medium. The MME is used to connect users to the network and to localize them on the LTE network. For this, the MME accesses the HSS. If the terminal has a valid SIM card, the account of the participant is assigned to a Serving Gateway (SGW). From there, a connection is established with the Packet Data Network Gateway (PDN-GW), which assigns an IP address to the terminal and establishes a connection with the IP network of the operator. The EPC also includes the Policy and Charging Rules Function (PCRF).

2.2 EPS-AKA Procedure

Before you can transfer or receive IP packets, the mobile must first connect and authenticate to the EPS network [5]. The element that allows authentication is called MME. The HLR/AuC is replaced by an HSS in the EPS architecture. Authentication vectors (AV) are generated by the MME from the HSS, as displayed in Fig. 2, through the interface S6 (based on DIAMETER) when the MME receives from the UE the Attach Request or Service Request messages. The MME launches along with the UE the EPS-AKA.

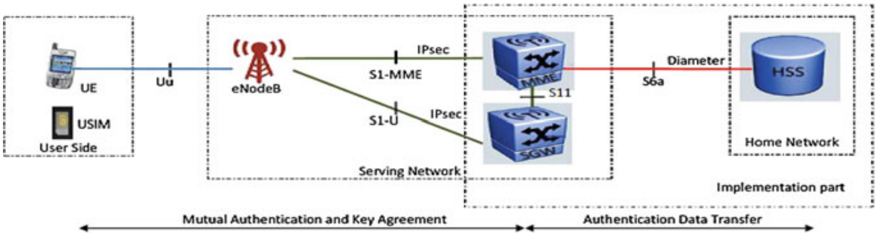

Fig. 2 EPS security architecture

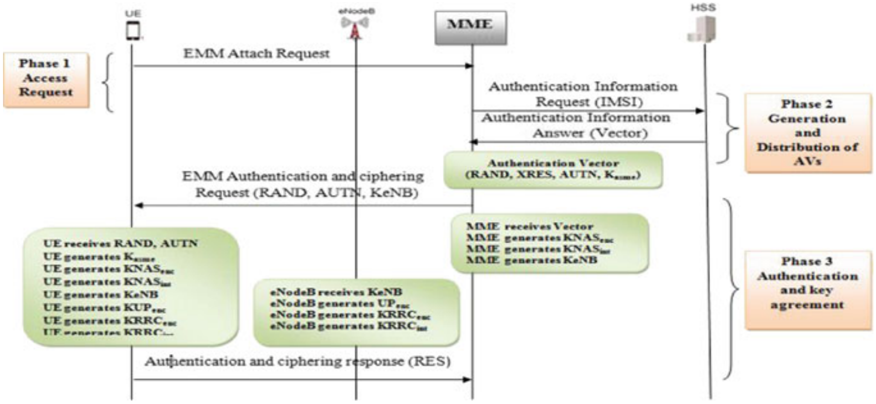
UE
eNodeB
MME
HSS
Phase 1 Access Request
EMM Attach Request
Authentication Information Request (IMSI)
Authentication Information Answer (Vector)
Phase 2 Generation and Distribution of AVs
Authentication Vector (RAND, XRES, AUTN, K_{asme})
EMM Authentication and ciphering Request (RAND, AUTN, KeNB)
MME receives Vector
MME generates $KNAS_{enc}$
MME generates $KNAS_{int}$
MME generates KeNB
UE receives RAND, AUTN
UE generates K_{asme}
UE generates $KNAS_{enc}$
UE generates $KNAS_{int}$
UE generates KeNB
UE generates KUP_{enc}
UE generates $KRRC_{enc}$
UE generates $KRRC_{int}$
eNodeB receives KeNB
eNodeB generates UP_{enc}
eNodeB generates $KRRC_{enc}$
eNodeB generates $KRRC_{int}$
Phase 3 Authentication and key agreement
Authentication and ciphering response (RES)

Fig. 3 EPS-AKA procedure

Figure 3 shows the progress of the EPS-AKA procedure which is initiated by the identification of the user through his IMSI or Globally Unique Temporary Identifier (GUTI) [6].

3 Performance Analysis and Simulations Results

In this section, we analyze and compare the performance of several authentication protocols: EPS-AKA, Security Enhanced Authentication and Key Agreement (SE-AKA) [7], Ensured Confidentiality Authentication and Key Agreement (EC-AKA) [8], and EC-AKA2 [9] protocols according to different parameters to estimate the performance and quality of service (QoS) in terms of security, cost, and delay of each one of these protocols. According to the survey we can see that in most existing 4G protocols, a high level of security can have a high processing cost and great added data rate (additional overhead).

To evaluate the performance of each protocol, we can consider the following parameters:

- Security: the security of a protocol is defined as its ability to resist attacks, while the risk is the probability that an attack could succeed in violating the protocol.
- Overhead: This is the added traffic on transmission interfaces in order to apply the relevant protocol.
- Computational delays: To calculate this delay, we consider the number and type of some operations required in each protocol.

3.1 Protocols Security

The security of a protocol is defined as its ability to resist attacks and the risk is the probability that an attack could succeed in violating the protocol. The more the cost and efforts to exploit vulnerability are high (increases), the more the probability of an attack's success decreases. In order to compare the security protocols' performance, EPS-AKA, SE-AKA, EC-AKA and EC-AKA2, we have compiled in Table 1, all of these studies are found in the literature.

After modeling the EPS-AKA protocol in High-Level Protocol Specification Language (HLPSL) in order to be able to verify its security using Automated Validation of Internet Security Protocols and Applications (AVISPA) [10], the result indicates that it becomes insecure if the MME-HSS interface is not considered secure. When roaming, HSS and MME belong to different networks, so we believe it is open to attack if no closed network is used.

The SE-AKA protocol was analyzed using the authentication test method and it has been proved to be insecure, but the effort to exploit it exceeds one of the EPS-AKA. EC-AKA and EC-AKA2 protocols have been verified using AVISPA

Table 1 Comparison of different protocol security

Vulnerability	EPS-AKA	SE-AKA	EC-AKA and EC-AKA2
Ensure confidentiality of IMSI	No	Yes	Yes
Resistance against replay attack	No	No	No
Resistance against the DoS attack of UE	No	No	Yes
Resistance against the blocking of services by a man-in-the-middle (MITM)	No	No	Yes
Confidentiality of MME-HSS interface	No	Yes	Yes
Resistance against attacks on the responses of authentication data	No	Yes	No
Resistance against the DoS attack of HSS	No	No	No
Resistance against the usurpation of identity of MME	No	No	No

and transformed to be sure. The more protocol is secure, the lower the vulnerability it gets. The security level is inversely proportional to the level of vulnerability. From Table 1, we see that the two versions of EC-AKA protocol are the least vulnerable, and as such, they are the most secured.

3.2 Communication Overhead

In this section, we calculate the size of the transmitted messages, in order to estimate their communication overhead with regard to the EPS-AKA and other AKA protocols. The size of parameters in bit is shown in Table 2. On the basis of each parameter passed in the message, we can calculate the total number of bits in all messages during each protocol (where n is the number of authentication requests) [11].

Number of bits in step 1 = Σ messages (phase 1 + phase 2)
Number of bits in step 2 = Σ message (phase 3 * n)
Total number of transmitted bits = Σ messages (phase 1 + phase 2) + Σ message (phase 3 * n)

Figure 4 illustrates the overhead according to the number of AVs for different AKA protocols. According to this figure, it can be seen that EPS-AKA protocol generates the least overhead compared to other protocols.

Table 2 Size of parameters

Parameter	Size (bits)
IMSI/TMSI/GUTI	128
K/CK/EK/IK/TIK	128
AK	48
K_{ASME}	256
KSI_{ASME}	64
XRES/RES	128
AV	Variable
RAND/RANDIK/RANDEK/AUTN	128
SQN/XSQN/PSQN/NSQN	48/32
AMF	48
LAI	40
MACi/XMAC/MACue	64
SN id/IDhss	20
RandUESecCapab	6
UESecCapab	12

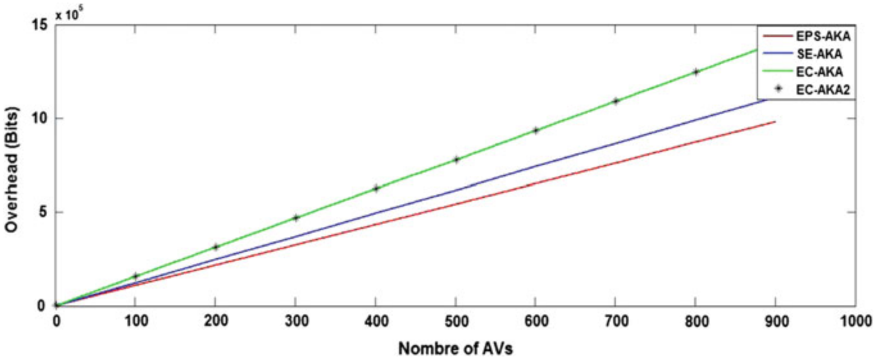

Fig. 4 Communication overhead for different AKA protocols

3.3 Computational Delays

The computation delays of all protocols are evaluated and compared to similar schemes. Corresponding calculations of the delays are due to calculations made at each of the following elements: UE, MME, and HSS. According to 3GPP, the functions f0, f1, f2, f3, f4, and f5 are Hash-based Message Authentication Code—Secure Hash Algorithm 256 (HMAC-SHA256). For digital signatures, we will study the overhead associated with Digital Signature Algorithm (DSA). For public key encryption, we will investigate the use of Rivest, Shamir, Adleman (RSA) and for symmetric encryption we will use the Advanced Encryption Standard (AES) algorithm.

The delay of calculation for each of the functions mentioned above is presented in Table 3. Delay values, available in [12], were obtained by measurements using Microsoft Visual C++ 2005 SP1 running on a processor Intel Core 21.83GHz Windows Vista32-bit.

To calculate the delay, we consider the number and type of some operations required in each protocol. The number and type of operations for each protocol are described in Table 4 [13].

Figure 5 shows the different protocol delays. From the figure we see that SE-AKA protocol that uses public key cryptography has a great delay of calculation followed by EC-AKA hybrid protocol.

Table 3 Computational delay

Function	Delay (μs)
HMAC-SHA-256	0.55
DSA-1024 (signature)	450
DSA-1024 (verification)	520
RSA-1024 (encryption)	80
RSA-1024 (decryption)	1460
AES-256	161

Table 4 Number of operations

Protocol	Operation	UE	MME	HSS
EPS-AKA	HMAC	6	–	6
	Encryption	–	–	–
	Decryption	–	–	–
SE-AKA	HMAC	6	–	6
	Encryption	1	2	1
	Decryption	1	1	1
EC-AKA	HMAC	6	–	6
	Encryption (asymmetric)	1	1	1
	Decryption (asymmetric)	–	1	1
	Encryption (symmetric)	1	2	–
	Decryption (symmetric)	2	1	–

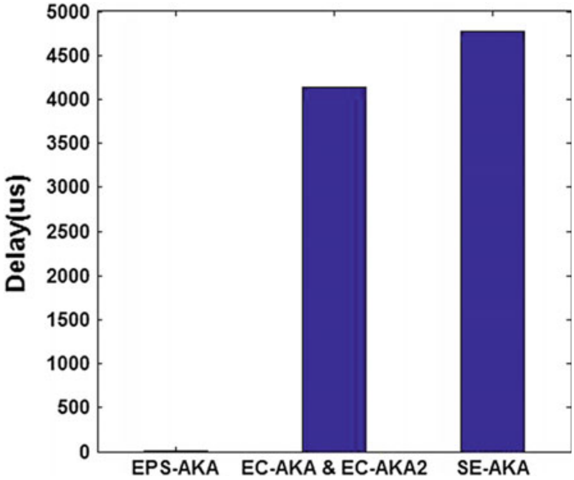

Fig. 5 Computation delays

4 Conclusion

3GPP propose EPS-AKA for supporting authentication in the next generation mobile communication system. However, from the security analysis, the present paper has found divers vulnerabilities in EPS-AKA, several protocols have been proposed to solve these problems. The analysis that we did between existing AKA protocols EPS-AKA, SE-AKA, EC-AKA, and EC-AKA2 to estimate their performances in terms of security, cost, and delay showed the importance of each protocol according to the previous metrics. We conclude that the two versions of

EC-AKA protocol are the least vulnerable, thus the most secured. EPS-AKA protocol generates the least overhead compared to other protocols. SE-AKA protocol that uses public key cryptography has the greatest delay of calculation.

References

1. Fritze, G.: SAE: The Core Network for LTE. Ericsson (2012)
2. Netmanias Technical Document.: LTE Security I: LTE Security Concept and LTE Authentication (2013)
3. Bouguen, Y., Hardouin, E., Xavier Wolff, F.: LTE et les réseaux 4G (Chap 19). Eyrolles. ISBN: 978-2-212-12990-8 (2012)
4. Hu, H., Zhang, J., Zheng, X., Yang, Y., Wu, P.: Self configuration and self-optimization for LTE networks. IEEE Commun. Mag. 94–100 (2010)
5. Han, C., Choi, H.: Security analysis of handover key management in 4G LTE/SAE networks. IEEE Trans. Mob. Comput. **13**(2), 457–468 (2014)
6. 3GPP TS 35.206 V11.0.0. Technical Specification. 3G Security: Specification of the MILENAGE Algorithm Set: An Example Algorithm Set for the 3GPP Authentication and Key Generation Functions f1, f1*, f2, f3, f4, f5 and f5*. Document 2: Algorithm Specification (Release 11) (2012–09)
7. Li, X., Wang, Y.: Security enhanced authentication and key agreement protocol for LTE/SAE network. In: 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1–4 (2011)
8. Bou Abdo, J., Chaouchi, H., Aoude, M.: Ensured confidentiality authentication and key agreement protocol for EPS. In: 3rd Symposium on Broadband Networks and Fast Internet (2012)
9. Bou Abdo, J., Chaouchi, H., Aoude, M., Pujolle, G.: EC-AKA2 a revolutionary AKA protocol. In: 2013 International Conference on Computer Applications Technology (ICCAT), pp. 1–6 (2013)
10. AVISPA Project. http://www.avispa-project.org/
11. Saxena, N., Thomas, J., Chaudhari, N.S.: ES-AKA: An Efficient and Secure Authentication and Key Agreement Protocol for UMTS Networks (2015)
12. Dai, W.: Crypto++5.6.0 Benchmarks (Online). Available: http://www.cryptopp.com/benchmarks.html (2009)
13. Hamandi, K., Sarji, I., Chehab, A., Elhajj, I.H., Kayssi, A.: Privacy enhanced and computationally efficient HSK-AKA LTE scheme. In: 27th International Conference on Advanced Information Networking and Applications Workshops (2013)