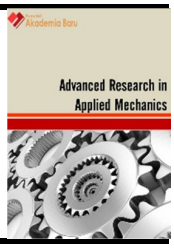
Penerbit Akademia Baru

Journal of Advanced Research in Applied Mechanics

Journal homepage: www.akademiabaru.com/aram.html
ISSN: 2289-7895



Design and Simulation of New Anonymous Intelligent Authentication for 4G (LTE) Mobile Communication Network

Open Access

Mahmoud El Omda[1,*], Mohamed Helmy Megahed[2], Mohamed Hassan Abdel Azeem[1]

[1] Arab Academy for Science and Technology and Maritime Transport Cairo, Egypt
[2] Canadian International College, Cairo, Egypt

ARTICLE INFO

Article history:
Received 5 June 2017
Received in revised form 10 July 2017
Accepted 4 December 2017
Available online 12 March 2018

ABSTRACT

LTE becomes the most widely used mobile communication network and it covers 97% of U.S users. However, LTE security protocol fails to achieve full protection to LTE network. Therefore, LTE needs to provide more security for networks and users. In this paper, we analyze several attacks. First, Disclosure attack which is resulted from sending permanent International Mobile Subscriber Identity (IMSI) in plaintext and this is solved by using anonymous intelligent authentication second, the problem of using the User Equipment (UE) master key for all users which is used in the authentication standard protocol and this problem is solved using a new algorithm to derive a temporary key for each session. The proposed security architecture enhances the LTE security level.

Keywords:
Disclosure attack, user anonymity, zero knowledge proof, 4G security, LTE

Copyright © 2018 PENERBIT AKADEMIA BARU - All rights reserved

1. Introduction

LTE is the evolution of the 3G (UMTS) mobile communication network [1], which provides higher performance for higher data rates, lower delay, and higher level of security. The LTE has been designed to be all-IP architecture. The standard authentication protocol of the LTE is Authentication and Key Agreement for Evolved Packet System (AKA-EPS) [2,3]. However this protocol enhanced (AKA-UMTS), it suffers from many vulnerabilities and attacks. This paper focuses on solving main attack: The Disclosure attack [4] is resulted from sending IMSI in plaintext from the UE to the core-network. This allows adversary to acquire the user identity or track the location of the user and his movements or may listen to all of user's conversation. This problem is solved using a New Anonymous and Intelligent Authentication protocol. The protocol is divided into two phases. We achieve User anonymity [5], which means authenticating the UE with the core-network by variable IMSI for every session. We proposed the anonymous algorithm based on the Zero-Knowledge-Proof (ZKP) concept [6], which stops the disclosure attack. For Changing the IMSI, we proposed an Intelligent Authentication (IA) [7], which means a part of encrypted new IMSI is to

* *Corresponding author.*
E-mail address: El3omDa999@hotmail.com (Mahmoud El Omda)

known to the UE and the other part is sent from the core-network. Our proposed protocol solves the two problems and has higher security level than EPS-AKA.

1.1 Contributions

We designed a new anonymous authentication protocol, which achieves user anonymity by changing permanent IMSI for every session to solve the disclosure attack. This protocol is based on a key list generated from a master key, which is preconfigured securely on the UE and the HSS.

1.2 New anonymous authentication

We designed new anonymous authentication protocol to solve the disclosure attack by means of changing the user identity every session. This is achieved by Zero Knowledge Proof concept.

1.3 Intelligent authentication

Intelligent authentication is based on the symmetric key authentication; this authentication is based on changing the user identity by means of participation between the UE and the MME where part of encrypted new IMSI is known to the UE.

1.4 Outline the paper

Section 2 presents related work. Section 3 describes the network model. Section 4 describes the threat model. Section 5 describes proposed protocol. Section 6 describes the security analysis. Section 7 presents performance analysis. Section 8 concludes the paper.

2. Related Work

Recently, there were many implementations of authentication protocols for 4G LTE. Some of them achieved the user anonymity but with very large computational overhead. Some others achieved lower computational overhead but they could not achieve user anonymity. In this paper, we present protocols for mobile communication network [8-10]. Lu [8] proposed an authentication protocol to solve all known attacks but it still suffers from sending the identity of the user in plaintext, which leads to disclosure attack. He and Chan [9] solved the disclosure attack by using one-way hash function, which achieves the goal of user anonymity, but they still also suffer from very large computational overhead and replay attack. In 2013, Li *et al*., [10] proposed a protocol, which is based on generating an infinite number of one-way hash function for all users in the network until achieving the value sent in plaintext, which raises the computations overhead. It builds a certificate for each user, which needs a very large database. And this protocol is not practical for such a very huge network. In [11], the authors demonstrated the key distribution between the eNBs during the handover, which helped us in using the IPsec between the network entities. All these authentication protocols have vulnerabilities that motivated us to propose a new anonymous intelligent authentication protocol for 4G (LTE) to enhance the weakness in the listed above protocols.

3. Network Model

Figure 1 shows the network model, which is called Evolved Packet system (EPS). It is consisted of two main parts. The first part is the Evolved Universal Terrestrial Radio Network (E-UTRAN), which is responsible for radio interfacing between the User Equipment (UE), the eNodeB (eNB) and the Mobility Management entity (MME.) while the second part is the Evolved Packet Core (EPC). This is responsible for directing the user either to use the internet passing through the Service Gateway (S-GW) and the Packet data Gateway (P-GW), or to voice call passing through the Home Network (HN) [2]. Figure 2 shows the LTE security standard protocol, which is EPS-AKA.

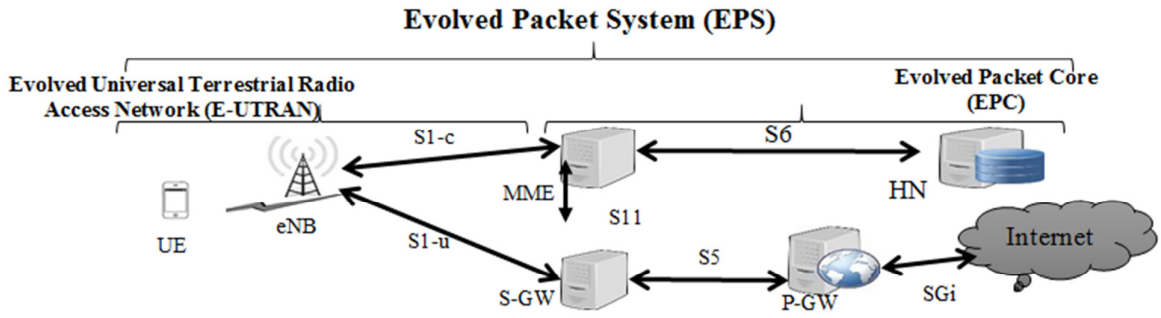


Fig. 1. LTE Network Model

Table 1
Notations

Notation	Description	Notation	Description
UE	User Equipment	SQN	Sequence Number
MME	Mobility Management Equipment	XRES	Expected Response
eNB	eNodeB	AUTN	Authentication Token
HSS	Home Subscriber Server	AV	Authentication Vector
R	Random Number	F	Encryption Function
IMSI	International Mobile Subscriber Identity	CK	Cipher Key
T_M	Timestamp	IK	Integrity Key
H	One Way Hash Function	AK	Anonymity Key
Ver.	Version number of the key list	MAC	Message of Authentication Challenge
I	Key index of the key from the key list	AMF	Authentication Message Field
K_{si}	One key from the key list	K_{ASME}	Authentication and Security Master key
ID_{eNB}	eNodeB Identity	KDF	Key Distribution Function
m	Message	ZKP	Zero Knowledge Proof

4. Threat Model

The EPS-AKA is vulnerable to many attacks. In this paper, we faced some attacks such as disclosure attack, fixed UE security key attack. During the explanation of the EPS-AKA, we have underlined two problems.
(1) The first problem resulted from sending permanent IMSI in plaintext, which caused disclosure attack.
(2) The second problem: is resulted from depending on a fixed key for each user.

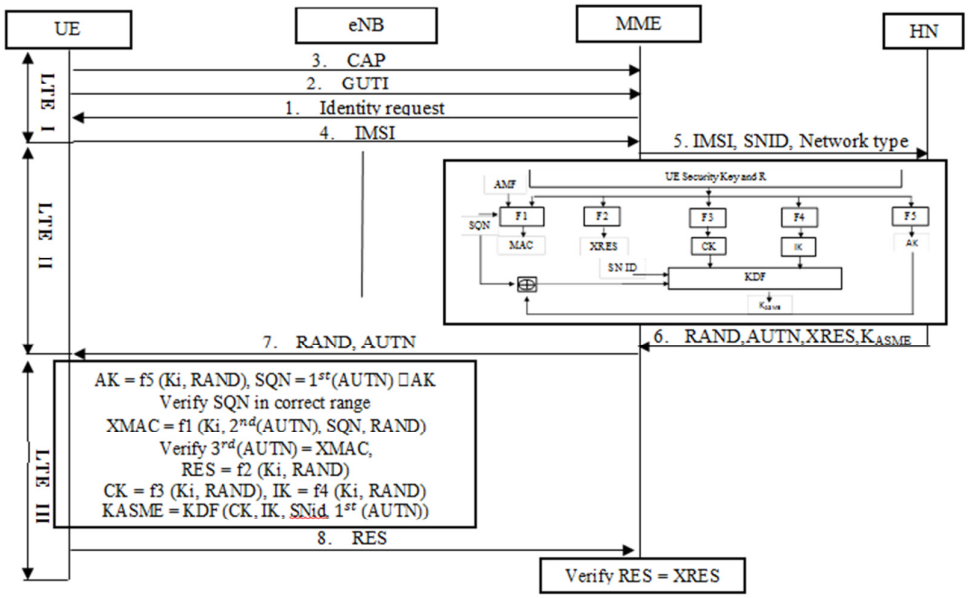


Fig. 2. AKA-EPS

5. Proposed Protocol

The proposed security architecture is composed of two components which are new anonymous and intelligent authentication and unfixed UE master key. Figure3 shows the proposed protocol, which is based on the concept of the ZKP authentication to achieve user anonymity. In addition, we use the intelligent authentication to achieve the new IMSI between the UE and the HSS. Our protocol based on a securely preconfigured master key per user, which generates variable key list of ten keys each of 256 bits for every user. This key list has a version number and it should be changed periodically by the Home Subscriber Server (HSS). This key list should be encrypted on the User Equipment (UE). Our proposed protocol consisted of 2 phases which will be demonstrated in this section setup phase, and the call phase.

Assumptions:

We have proposed our protocol based on assuming a pre-shared key among all entities of the core network using IPsec protocol. Also, every user has a key list with ten keys of 256 bits at the user equipment and the core network. The key list is changed periodically and it has version number indicating the user. Multiple handover for the proposed protocol is secure due to IPSec protocol between eNB. Mobility will apply extra messages due to errors during mobility. QoS will not be affected.

By using anonymous intelligent authentication, we achieved user anonymity. In addition, we changed the permanent UE security key K to be variable key for each user using a key from the key list.

6. Security analysis

We have enhanced the security level of the designed new anonymous intelligent authentication protocol by solving the main problems we have faced in EPS-AKA.

We achieved the user anonymity by using anonymous intelligent authentication, which is based on ZKP concept, by means of sending an encrypted challenge from the UE to the HSS.

We changed the permanent key K, which is used for the user to a variable key for every user using a key from the key list. This enhances the security level of the proposed protocol.

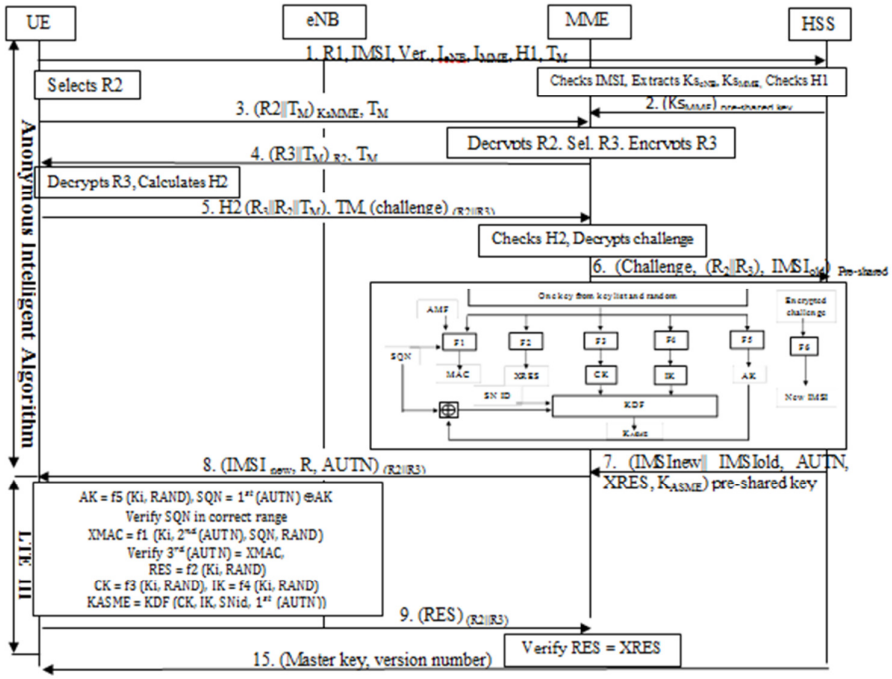


Fig. 3. Proposed Protocol

Table 2
Proposed Protocol

Phase 1 : Setup phase
Algorithm : Anonymous Intelligent Authentication
1 : UE ⟶ HSS : m1 = (R1, IMSI, ver., I_{MME}, I_{eNB}, H1,T_M) The UE broadcasts m1. This message passes through eNB and MME to HSS. m1 is grouped of seven parts as following: 128 bits random number, the temporary IMSI, version number of the key list, two key indexes (one for eNB and the other is for the MME) of the used keys for that session, the hash value of the random concatenated with the keys from the key list concatenated with the time stamp TM, and timestamp in plaintext T_M. This part of the message reveals nothing because the initial IMSI would be changed at the end of this session. Also, the random number reveals nothing. There is no problem about sending this initial IMSI of the user in plaintext. **2 : HSS ⟶ MME : Extracts (Ks_{MME}), (Ks_{eNB}) Sends m2= { $(Ks_{MME})_{Pre\text{-}shared\ key}$}** The HSS extracts the Ks_{MME} and Ks_{eNB} using the index of that key from the key list that has a version number. Checks the hash value H1 to authenticate that user. Then the HSS sends m2 to the MME, which is the session key (Ks_{MME}) between the MME and the UE encrypted using a pre-shared key between the HSS and the MME. **3:UE ⟶ MME: Selects R_2, m3 = {$(R_2||T_M)_{KsMME}$}**

The UE generates R_2 and sends m3 to the MME, which is a random number concatenated with timestamp encrypted using the session key (Ks_{MME}) between the UE and the MME.

4: MME ⟶ UE : Decrypts R_2, Sel. R_3, Sends m4 = $(R_3||T_M)_{R2}$

The MME decrypts R_2 using the session key (Ks_{MME}). And selects a new random number R3. Then the MME Sends m4 to the UE, which is the new random number (R_3) and timestamp encrypted using R_2.

5: UE ⟶ MME : Decrypts R_3, Generates H_2, Sends m5 = $\{H_2(R_3||R_2||T_M), T_M, (challenge)_{(R2||R3)}\}$

The UE decrypts R3 and generates H2, which is the two random numbers and timestamp. Then the UE sends m5 to the MME, which is the hash value, timestamp in plaintext and a challenge encrypted using the new session key ($R_2||R_3$).

6: MME ⟶ HSS :{checks $((H_2), T_M)$, Sends m6 = $\{(IMSI_{old}$, challenge$)_{pre\text{-}shared\ key}\}$

The MME checks H2 and extracts ($R_2||R_3$).Then decrypts the challenge using ($R_2||R_3$). And the MME sends m6 to the HSS, which is the old IMSI, challenge and ($R_2||R_3$). This message would be encrypted using a pre-shared key between the MME and HSS.

7: HSS ⟶ MME : Generates$\{(IMSI_{new}), SQN, AUTN, XRES, CK, IK, MAC, K_{ASME}\}$, Sends m7 = $\{ IMSI_{new}||$ $IMSI_{old}$, AUTN, XRES, $K_{ASME}\}_{pre\text{-}shared\ key}$

The HSS uses the same cryptographic function of the standard security protocol except using a new cryptographic function (F6) to generate the IMSInew depending on the encrypted challenge, then the HSS sends m7 to the MME, which is the new IMSI, old IMSI, authentication token, the expected response of the UE and KASME to the MME encrypted using the pre-shared key.

8: MME ⟶ UE : m8 = $\{IMSI_{new}$, R, AUTN$\}_{(R2||R3)}$

The MME sends m8, which this new IMSI to achieve user anonymity, random and authentication token to establish the key management algorithm, which is proposed in the EPS-AKA. This message is encrypted using the new session key ($R_2||R_3$).

9: UE ⟶ MME : m9 = (RES)

As the UE receives m8 from the MME. It can generate all cryptographic functions and the RES. Then the UE sends this RES in encrypted message using the new session key ($R_2||R_3$) to the MME to complete the mutual authentication with the MME.

10: HSS ⟶ UE: {Sends m15 = (Master key, Ver.) $_{(R2||R3)}$}

Every certain time, HSS generates a new key list for the UE, then sends m15 to the UE, which is the new master key and the version number. This message is encrypted using new session key (R2||R3).

Phase 2: Call Phase

In this phase, the anonymous and intelligent authentication algorithms are used to achieve user anonymity. This phase will be the same as used in the phase 1 until message number 8. Every call, the user would achieve a new IMSI before the end of the call, and use it for the next call.

7. Performance Analysis

7.1 Communication overhead

A) AKA-EPS uses eight messages to achieve mutual authentication without anonymity.

B) Huxian Li uses six messages to achieve user anonymity authentication.

C) Our proposed protocol uses nine messages to achieve the mutual authentication with user anonymity.

7.2 Computation overhead

A) EPS-AKA uses 20 of KDFs, 14 blocks of AES and 10 rotators, which are 128 bits shift registers.

B) Huxian Li uses uncountable one-way hash function. It generates a hash value for all users in the network by the concept of try and error until reaching the appropriate user, which achieves the value of SID XOR h(x). It uses two pseudo random number generators (PRNG). And it builds a temporary certificate for each user per each session.

C) Our proposed protocol uses four one-way hash function (SHA-3). We used twenty blocks of AES encryption algorithm. Finally, we build our protocol on 10 keys of 256 bits key list.

7.3 Setup time

We used C++ program to implement LTE standard protocol and our proposed protocol and we calculated the setup time for both protocols as follows: The new anonymous intelligent authentication protocol has 820-millisecond setup time, which is higher than EPS-AKA's setup-time, which is 512 milliseconds.

Table 3
Comparison with Others Works

	EPS-AKA	**Huxian Li**	**proposed protocol**
Communication Overhead	8 messages	6 Messages	11 messages
Computation Overhead	Lower	un-countable	Higher
Setup Time	512 m-sec	un-computable	820 m-sec
Anonymity	×	√	√
Confidentiality	×	×	√
Network Scalability	Scalable	Not-Scalable	Scalable
Security Level	Low	Low	High

8. Conclusion

We proposed a new anonymous intelligent authentication protocol to achieve anonymity by driving a new IMSI each session. The concept of permanent key for users is changed to a variable key for each user by using key list. Finally, we achieved confidentiality by encrypting all messages even during authentication.

References

[1] Dahlman, Erik, Stefan Parkvall, and Johan Skold. *4G: LTE/LTE-advanced for mobile broadband*. Academic press, 2013.

[2] Tang, Chunyu, David A. Naumann, and Susanne 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), 2013 IEEE 10th International Conference on*, pp. 1605-1614. IEEE, 2013.

[3] Cao, Jin, Maode Ma, Hui Li, Yueyu Zhang, and Zhenxing Luo. "A survey on security aspects for LTE and LTE-A networks." *IEEE Communications Surveys & Tutorials* 16, no. 1 (2014): 283-302.

[4] Oya, Simon, Carmela Troncosoy, and Fernando Pérez-González. "Understanding the effects of real-world behavior in statistical disclosure attacks." In *Information Forensics and Security (WIFS), 2014 IEEE International Workshop on*, pp. 72-77. IEEE, 2014.

[5] Li, Xinghua, Hai Liu, Fushan Wei, Jianfeng Ma, and Weidong Yang. "A Lightweight Anonymous Authentication Protocol Using k-Pseudonym Set in Wireless Networks." In *Global Communications Conference (GLOBECOM), 2015 IEEE*, pp. 1-6. IEEE, 2015.

[6] Catalano, Dario, Mario Di Raimondo, Dario Fiore, and Mariagrazia Messina. "Zero-knowledge sets with short proofs." *IEEE Transactions on Information Theory* 57, no. 4 (2011): 2488-2502.

[7] Avgerou, Artemis, Panayotis E. Nastou, Dimitra Nastouli, Panos M. Pardalos, and Yannis C. Stamatiou. "Adopting an ABCs Authentication Framework for Collective Intelligent eBusiness Models in Smart Cities." In *Security Technology (SecTech), 2015 8th International Conference on*, pp. 31-34. IEEE, 2015.

[8] Lu, Jian-zhu, and Jipeng Zhou. "On the security of an efficient mobile authentication scheme for wireless networks." In *Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on*, pp. 1-3. IEEE, 2010.

[9] He, Daojing, and Sammy Chan. "A secure and lightweight user authentication scheme with anonymity for the global mobility network." In *Network-Based Information Systems (NBiS), 2010 13th International Conference on*, pp. 305-312. IEEE, 2010.

[10] Li, Huixian, Yafang Yang, and Liaojun Pang. "An efficient authentication protocol with user anonymity for mobile networks." In *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pp. 1842-1847. IEEE, 2013.

[11] Han, Chan-Kyu, and Hyoung-Kee Choi. "Security analysis of handover key management in 4G LTE/SAE networks." *IEEE transactions on mobile computing* 13, no. 2 (2014): 457-468