Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Full length article

Anonymous authentication and location privacy preserving schemes for LTE-A networks

Zaher Jabr Haddad [a],[*], Sanaa Taha [b], Imane Aly Saroit [b]

[a] *Department of Computer Science, Al-Aqsa University, Gaza, Palestine*
[b] *Department of Information Technology, Cairo University, Cairo, Egypt*

ARTICLE INFO

Article history:
Received 31 July 2016
Revised 15 December 2016
Accepted 17 January 2017
Available online xxxx

Keywords:
LTE-A
Anonymous authentication
Pseudonymes
Schnorr Zero knowledge protocol
IMSI
Privacy
Tracking attack
HSS
MME
BS

ABSTRACT

Long Term Evaluation Advanced (LTE-A) is the third generation partnership project for cellular network that allows subscribers to roam into networks (i.e., the Internet and wireless connections) using spacial purpose base-stations, such as wireless access points and home node B. In such LTE-A based networks, neither base-stations, nor the Internet and wireless connections are trusted because base-stations are operated by un-trusted subscribers. Attackers may exploit these vulnerabilities to violate the privacy of the LTE-A subscribers. On the other hand, the tradeoff between privacy and authentication is another challenge in such networks. Therefore, in this paper, we propose two anonymous authentication schemes based on one-time pseudonymes and Schnorr Zero Knowledge Protocols. Instead of the international mobile subscriber identity, these schemes enable the user equipment, base-stations and mobility management entity to mutually authenticate each others and update the location of the user equipment without evolving the home subscriber server. The security analysis demonstrate that the proposed schemes thwart security and privacy attacks, such as malicious, international mobile subscriber identity catching, and tracking attacks. Additionally, our proposed schemes preserve the location privacy of user equipment since no entity except the mobility management entity and Gate-Way Mobile Location Center can link between the pseudonymes and the international mobile subscriber identity. Also attackers have no knowledge about international mobile subscriber identity. Hence, the proposed schemes achieve backward/forward secrecy. Furthermore, the performance evaluation shows that the proposed handover schemes impose a small overhead on the mobile nodes and it has smaller computation and communication overheads than those in other schemes.

1. Introduction

As a promising packet-based system, and envisioned toward forth generation cellular networks, the Long Term Evaluation Advanced (LTE-A) system is developed through the Third Generation Partner Project (3GPP) to enhance network's Quality of Service, including [1]: (1) increasing bandwidth up to 100 MHz; (2) enhancing performance using Multiple Input Multiple Output (MIMO) and coordinate scheduling; (3) supporting heterogeneous networks; and (4) providing sufficient services for the cell edge [2]. Moreover, LTE-A systems are open nature networks where a User Equipment (UE) employs different types of connectivity, such wireless and Internet, and of Base Stations (BSs), such as the Home node B (HeNB). Subscribers in LTE-A systems may own HeNBs as well as employ traditional Access Points (APs) used in wireless local area network to roam through different LTE-A networks [3].

Like other cellular systems, LTE-A has different mobility procedures, such as Evolved Packet system Authentication and Key Agreement (EPS-AKA) and location update procedures, to perform system functionalities, include, authentication, call originating, handover, location update, and paging [4]. Despite quality of service enhancement, UE Location in LTE-A network suffers security and privacy issues such as tracking, tracing and impersonating since the International Mobile subscriber Identity (IMSI) is exchanged in clear text between the LTE-A network entities. Therefore, security and privacy adversaries, such as impersonating, IMSI catching, and tracking, may exploit the open nature of the LTE-A connectivity and BSs [5]. In addition, the tradeoff between the UE

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

[*] Corresponding author.
E-mail addresses: zj.haddad@alaqsa.edu.ps (Z.J. Haddad), staha@fci-cu.edu.eg (S. Taha), i.saroit@fci-cu.edu.eg (I.A. Saroit).

http://dx.doi.org/10.1016/j.eij.2017.01.002
1110-8665/© 2017 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University.

privacy and authentication make it a challenge to secure such networks.

In this paper, we propose two novel anonymous authentication and location privacy preserving scheme for LTE-A network to thwart potential attacks violating the privacy of LTE-A networks. Both schemes keep the original LTE-A infrastructure.

The reasons behind introducing two anonymous authentication schemes as following: the first scheme, the pseudo random-based authentication scheme, is suitable for call establishment procedure which requires fast authentication to solve the call termination problem. The second scheme, the Zero knowledge authentication scheme, is suitable for the handover procedure where there are two evolving entities, eNBs, that need to verify each other as a prover and verifier [6].

In the first scheme, we use pseudonymes based public key cryptography, named pseud-auth, to perform the authentication procedure. In pseud-auth scheme, only the Mobility and Management Entity (MME) can link the pseudonymes and IMSI, therefore, pseudonymes are used to perform a mutual authentication between the UE, BS and the MME. BSs can verify pseudonymes without knowing the IMSI. pseud-auth scheme allows UE, BS and MME to share a symmetric key to be use for achieving the LTE-A security requirements, such as integrity, confidentiality, and non-repudiation.

The second scheme, relies on schonner zero knowledge protocol and public key cryptography (SZN-auth) to perform the authentication procedure. In SZN-auth, only the Gate-Way Mobile Location Center (GMLC) can extract IMSI, therefore, random numbers are used to perform a mutual authentication between the UE, BS and the MME without revealing the secret information regarding to the UE. SZN-auth scheme allows each entity of the network to verify the correctness of the message without need to reveal secret information of that entity. Table 1 shows the full definition of the abbreviations used throughout the paper.

The remainder of the paper is organized as follows.The related work is outlined in Section 2. Section 3 discusses the network and threat models. Section 4 describes the schnorr zero knowledge protocols. The proposed schemes are explained in Section 5. The security, privacy and performance evaluations are provided in Sections 6 and 7, respectively. Section 8 describes the experimental results of the proposed scheme. Finally, Section 9 concludes the paper and suggests some future works.

Table 1
List of abbreviations.

Acronym	Definition
LTE-A	Long Term Evaluation – Advanced
3GPP	Third Generation Partnership Project
UE	User Equipement
BS	Base Station
eNB	Evolved Node B
HeNB	Home Evolved Node B
EPS-AKA	Evolved Packet System authentication and Key Agreement Protocol
HSS	Home Subscriber Server
MME	Mobility and Management Enitity
E-UTRAN	Evolved universal terrestrial Radio Access Network
2G GSM	Second Generation Global System for mobile
3G UTRAN	Third Generation Universal Terrestrial Radio Access Network
eNB	Evolved Node B
GMLC	Gateway Mobile Location center
SGW	Serving Gateway
SGSW	Serving Gateway Support Node
PDN SW	Packet Data Network Serving Gateway
ME	Mobile Element
PSTN	Public Switching Telephony Network

2. Related work

The importance of the UE privacy preserving in the LTE-A networks attracts the researchers providing work for handling its problems [7]8. The ideas of anonymous authentication and location privacy schemes are divided into three main categories: encrypting IMSI, using dynamic identity, and using pseudonymes.

For encrypting IMSI, in [9], Abdo et al. address the IMSI capturing as privacy problem in LTE network authentication protocol. Therefore, they proposes a self-certified scheme called (SP-AKA) based on the public key cryptography to encrypt the IMSI during their transmission. However, the linkability between two transmitted identity is still a privacy problem. In [10], Sanaa Taha and Xuemin Shen consider the anonymity and location privacy of mobile node in the case of heterogenous networks. They consider the location privacy preserving of mobile node as a problem faced the seamless roaming via heterogenous networks. Therefore, authors introduce anonymous home building update scheme for mobile IPv6 wireless networking. In this scheme, authors achieve mutual authentication and share a symmetric key between two anonymous network entities. In [11], So-In figured that the IP-based architecture of the 4G networks bring several problems such as mobility, multi-homing and location privacy. Therefore, they introduce a proxy protocol as a modification of the standard mobile IPv6 protocol. In this scheme, authors uses virtual identity to achieve location privacy. However, proxy protocols allow home entity to delegate a privilege to other entity in order to sign on behalf of the home entity. Therefore, the presence of impersonating attacks still a big problem faced the delegation authority. In [12], Tuan Ta and John Baras prove that the paging procedure of LTE network suffers a lack of location privacy problem. Therefore, they suggest to embed the user identity information of the mobile into the transmitted signal properties that carry the paging information. However, this scheme requires a modification of the signal recognition in the physical layer, which is not desirable in the network.

For dynamic identity-based privacy schemes, in [13], Hamandi et. al. consider the AP and the Internet connection as untrusted entities. Therefore, attackers, such as active and passive attackers, may disseminate through those untrusted APs and Internet connections to violate the privacy of the UEs. For the purpose of UE privacy preserving, [13] employs a dynamic identity instead of using the traditional IMSI to create the pseudonyms (W-AKA). However, in this scheme, the Home subscriber Server (HSS) entities should initially or periodically be met in each authentication process causing a big overhead on the network. Furthermore, Despite this scheme achieves the forward secrecy, the backward secrecy is not achieved since the next pseudonyms generated by the previous one. Moreover, the IMSI should be transmitted in clear text at the registration process, which makes the IMSI linkable. Additionally, In [14], Gier M. Koien, proposes a privacy enhanced mutual authentication scheme for LTE networks using identity based cryptography. Author considered the privacy of the UE may violated by the tracing attack since these attacks could link the sequence of temporary identities of UE. Therefore, authors used the public key encryption technique using dummy IMSI to make the temporary identity unlinkable and withstands the tracing attack. However, this scheme increases the number of messages required to perform the authentication, therefore, it consumes the bandwidth of the network. In [15], Jo et. al. consider the requirement of achieving location privacy of mobile node causes a big performance problems such as high communication, computation cost and huge revocation list. Therefore, authors introduce a privacy preserving scheme based on the identity based sign-encryption. However, authors claimed that the computation cost is a big problem and back to use the bilinear pairing which is well-known