Volume : 4 | Issue : 12 | December 2015 • ISSN No 2277 - 8179

Research Paper

A Survey on Different Security Solutions For Lte and Lte-A Networks

Engineering

KEYWORDS : LTE security, LTE, LTE-A, EPC security architecture, IMS security, HeNB security, MTC security.

Amruta Kokate | Pune University ,NMIET,Talegoan Dabhade, Pune, Maharashtra, India.

ABSTRACT

In recent years, huge requirements for broadband mobile wireless communications and the upcoming new wireless multimedia applications become the inspiration to the research of broadband wireless access technologies. The Long Term Evolution (LTE) system has been introduced by the Third Generation Partnership Project (3GPP) on the direction towards fourth-generation (4G) mobile to conform 3GPP keeping the dominance of the cellular communication technologies with the design of new radio access techniques and a further evolution of the LTE systems, the 3GPP is presenting the future LTE-Advanced (LTE-A) wireless networks as the standard for 4G network. hence the 3GPP LTE and LTE-Advance architecture are formed to support at Internet Protocol (IP) connectivity and full interworking with wireless access networks, the new unique features containing some new challenges in the design of the security mechanisms. This solution makes help to research in the security aspects of the LTE and LTE-A networks.

1. Introduction

The current security functions in the Wi-Fi and the LTE systems. It has been analyzed that 4G systems will carry forward all the security challenges of underlying access networks and most of the IP-specific security vulnerabilities due to their heterogeneous and at IP-based open architecture. The survey has provided details of the harmful attacks in WiMAX systems. In the survey, different malicious attacks against the WiMAX systems specified by IEEE 802.16 standards added in the current literature has been analyzed and classified based on a some factors..

In this survey, the characteristics of 4G mobile communication systems with the IPv6 networks have been described and the challenges and security issues existing in 4G IPv6 wireless networks have been explained. In addition, some constructive security defending strategies have been proposed in for the 4G mobile communication systems with the IPv6 networks. The previous surveys have mainly focused on the security architecture, security vulnerabilities, securities in different components of LTE architecture and security requirements in the LTE systems without the introduction of the current research issues and solutions in progresses to the research topics. Here, the survey present a comprehensive survey of security aspects in LTE/LTE-A networks.

2. Existing Framework

2.1 LTE Network Architecture

A LTE network contain the Evolved Packet Core (EPC) ,MTC and the E-UTRAN.The EPC is an Flat-IP and fully packet-switched (PS) backbone network in the LTE systems also there is Voice service for voice communication , which is traditionally a circuit switched (CS) network service, so it will be handled by the IP multimedia subsystem (IMS) network.

(1) A new type of base station, named HeNB base station, is referenced by the 3GPP committee to improve the indoor coverage and network capacity. HeNB is a low-power access point and is installed by a user in the home or a small office to improve the indoor coverage for the voice and high speed data service. It communicates to the EPC over the Internet via a broadband backhaul.

(2) In addition to the E-UTRAN, the LTE-A system supports non-3GPP access networks such as wireless local area networks (WLAN), WiMAX systems, and code division multiple access (CDMA) 2000 systems, connected to the EPC. There are mainly two types of non-3GPP access networks, which are trusted non-3GPP access networks and non trusted non-3GPP access networks. Whether a non- 3GPP access network is trusted or not is not a important consideration of the access networks, that is depends on the decision of the network operators. For an non trusted non-3GPP access network, an UE needs to go through a trusted evolved packet data gateway (ePDG) connected to the EPC.

(3) A LTE-A system also supports a new type of data communications between entities, which is called as MTC, which can exchange data without any requirement on any form of human interaction. There are two new components existing in the MTC, the MTC server and the MTC user server. An MTC user is a person or a control centre placed outside the network operator domain, can the services provided by one or more MTC servers to manage a large number of MTC devices. The MTC server is attached to the LTE network to communicate with MTCDs. The MTC server may be an outside or inside an operator. When a MTC device connects to the LTE network, the MTC device can connect with the MTC server and be controlled by the MTC.

3. Propose Solution

In this section, we will review existing solutions to address the above vulnerabilities in the current literatures.

3.1 LTE System Architecture

On the LTE system architecture, a new simple and robust handover authorization scheme based on updated proxy signature , which can be applied to all of the mobility scenarios including the handovers between the HeNBs, By the scheme, a UE and the target eNB or HeNB can accomplish a mutual authentication and establish a session key with their long term secret keys generated by the proxy signatures when the UE injected to the coverage of the target eNB or HeNB. Therefore, it has a simple authentication process without a complex key management.

3.2 LTE Cellular Security

LTE cellular system containing a hybrid authentication and key agreement and authorization scheme based on Trust Model Platform (TMP) and Public Key Infrastructure (PKI) for 4G mobile networks. By the scheme, due to the adoption of the new concept of trusted computing and PKI, it can provide robustness for mobile users to access sensitive service and data in 4G systems.

In addition, passwords are associated with the fingerprint and public key to achieve mutual authentication between UEs and the HN over the TMP. An authentication and key agreement scheme on self-certified public key (SPAKA) has been suggested for 4G wireless systems . The scheme generates a public key broadcast protocol simply based on a probabilistic method for a UE to identify the genuine base station, and thus to overcomes the shortcomings of 3G AKA scheme. A Security Enhanced Authentication and Key Agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI) ..

3.3 LTE Handover Security

For the secure LTE handovers, a hybrid authentication and key agreement scheme has been suggested to support globe mobility and secure communications within 4G wireless systems. The scheme in designs a global authentication protocol to allow a vertical handover between access systems including GSM, UMTS, WiFi and WiMAX without requiring a prior subscription to the visited networks. However, this scheme concentrate only on the handovers between WiMAX/ Wi-Fi also on GSM/ UMTS and covers the security problems existing in the GSM systems. The handovers between the LTE/LTE-A systems and other accessing networks have not been located, where the LTE/LTE-A systems are much different the GSM and the UMTS in the handover procedures and security vulnerabilities.

3.4 IMS Security

An improved one pass AKA procedure for the next generation networks (NGNs) Authentication without the security protection between the UE and the P-CSCF, and thus it can decrease significantly the authentication overhead compared with the multipass authentication mechanism. However, this approach is very risky to the fraudulent use of IMS services, containing eaves dropping attacks, fake server attacks, also the temporary cheat attacks. An Improved AKA (I-AKA) authentication protocol for the LTE networks to reduce energy consumption problem. By the scheme, the network layer and the IMS authentication layer can be executed by using the IMPI only without the IMSI of the users. After the network layer authentication is secure.

3.5 HeNB Security

For the HeNB systems, problem of the authentication and access control of the HeNB users . The paper describe the overview of the ongoing work on the HeNB standardization in the 3GPP,especially on the form of access control strategy. When a UE wants to connect to the network via a HeNB, the CN is responsible for performing the access control for the UE. In order to do the access control, the CN is required to manage and update a list of CSG identities called as allowed CSG list which can be subscribed by UE. Each entry in the list related to the CSG identity with a PLMN identity. The information in the UE allowed CSG list is stored data for the UE in the HSS and provided to the MME for access control. Before the mutual authentication with the UE, the MME require to check whether the UE is allowed to access the HeNB based on the allowed CSG list.

3.6 MTC Security

In the MTC, the threats, the security requirements, and related solutions of the MTC security. It is advised that the Trust Environment (TrE) can be embedded in the MTC devices to protect the security of the MTC devices, which can provide more secure protected functions for the access authentication and support different cryptographic capabilities containing the symmetric and asymmetric encryption and decryption compared with the current UICC. A group-based authentication with the support of key agreement approach for a group of UEs roaming from the same HN to a SN . By the scheme, lots of UEs, which related to the same HN, can form a group..

4. Conclusion

The 3GPP committee has motivated the LTE research in order to meet the requirements of increasing mobile data traffic and new multimedia applications. In this paper, we have overviewed the security problems in the LTE/LTE-A 4G wireless networks. We have first describe the security architectures and mechanisms specified by the 3GPP standard. We have further extensively discussed the vulnerabilities located in the security architecture of the LTE/LTE-A wireless networks and reviewed the corresponding the state-of-the-art solutions proposed to mitigate those security laws in the literatures. Our survey has explored that there are still a lot of security problems in the current LTE/LTE-A networks. Finally, we have summarized potential open research issues as the recommendation for the future research activities on the security of LTE/LTE-A wireless networks. It is expected that our work could attract much more attentions from the academia and industry to support the corresponding research activities and could provide helpful indications for the deployment of the LTE/LTE-A 4G wireless networks.

REFERENCE

[1] Jin Cao, Maode Ma, Senior Member, IEEE Hui Li, Member, IEEE, Yueyu Zhang, and Zhenxing Luo, A Survey on Security Aspects for LTE and LTE-A Networks,IEEE Com- munications Surveys Tutorials, Vol. 16, No. 1, First Quarter 2014. [2] Roger Piqueras Jover, Joshua Lackey and Arvind Raghavan,Enhancing the security of LTE networks against jamming attacks Research Article October - December 2014: 7, doi:10.1186/1687-417X-2014-7.2014 Piqueras Jover et al.; licensee Springer. [3] Naim Qachri, Olivier Markowitch and Jean-Michel Dricot A Formally Verified Protocol for Secure Vertical Handovers in 4G Heterogeneous Networks International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.309-326. [4] D. Forsberg, LTE Key Management Analysis with Session Keys Context, Computer Communications, Vol. 33, No.16, Octomber 2010,Gpp 1907-1915 [5] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, and S. Parkvall, LTE: The Evolution of Mobile Broadband, IEEE Commun. Mag., Vol.47, No.4, April 2009, pp.44-51. [6] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE), (Rel 9), 3GPP TR 33.821 V9.0.0 June 2009. [7] Oleg Dementev, Machine-Type Communications as Part of LTE-Advanced Technology in Beyond-4G Networks, The 14th Conference Of FRUCT Association ISSN 2305-7254.