International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.17-24
http://dx.doi.org/10.14257/ijsia.2014.8.4.02

Issues toward Networks Architecture Security for LTE and LTE-A Networks

Jin Wang[1], Zhongqi Zhang[2], Yongjun Ren[2], Bin Li[1] and Jeong-Uk Kim[3]

[1] *College of Information Engineering, Yangzhou University, Yangzhou 225009, China*
[2] *School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing 210044, China*
[3] *Deptartment of Energy Grid, Sangmyung University, Seoul 110-743, Korea*

Abstract

With all these years' rapid development in wireless communication, high demands for broadband mobile wireless communications and the emergence of new wireless multimedia applications have constituted the motivation to the development of broadband wireless access technologies. The Long Term Evolution (LTE) system has been specified by the Third Generation Partnership Project (3GPP) on the way towards fourth-generation (4G) mobile to ensure 3GPP keeping the dominance of the cellular communication technologies. In this paper, several security issues of the LTE and LTE-A networks have been discussed. First, we illustrate an overview of the LTE Network Architecture. Second, LTE security architecture is shown as well. Third, some drawbacks in LTE security framework are discussed in Section 4. Finally, some open issues will be talked, and hopefully this will be a guideline for the new learners.

Keywords: *LTE security, EPC, LTE, LTE-A*

1. Introduction

The term Long Term Evolution (LTE) stands for the process to generate a novel air interface by the 3rd Generation Partnership Project (3GPP), and for the specified technology. Through the design and optimization of new radio access techniques and a further evolution of the LTE systems, the 3GPP is developing the future LTE-Advanced (LTE-A) wireless networks as the 4G standard of the 3GPP [1]. Earlier, the 3G Wideband Code Division Multiple Access (WCDMA) provided a new, high capacity, air interface including transport of packet traffic, and the Radio Access Network (RAN) designed to be compatible with the second generation GSM and GPRS core networks. WCDMA allows multiplexing of voice and variable rate data services, and its evolution to High Speed Packet Access (HSPA) [2, 3] further enhances the high rate packet capabilities as a set of new transport channels.

The LTE system is designed to be a packet-based system containing less network elements, which improves the system capacity and coverage, and provides high performance in terms of high data rates, low access latency, flexible bandwidth operation and seamless integration with other existing wireless communication systems [4]. The LTE-A system specified by the 3GPP LTE Release 10 enhances the existing LTE systems to support much higher data usage, lower latencies and better spectral efficiency [5].

Organization of the paper: The main content of this paper is constructed in 6 sections as follows: Section 2 gives an overview about LTE Network Architecture. Section 3 describes the LTE Security Architecture. Section 4 describes Drawbacks in LTE Security Framework. Section 5 discusses some Open Issues. Section 6 concludes our work.

ISSN: 1738-9976 IJSIA

2. LTE Network Architecture

As shown in Figure 1, a LTE network is comprised of the evolved packet core and the E-UTRAN [1]. The evolved packet core is an all-IP and fully packet-switched backbone network in the LTE systems. Voice service is a digital circuit switched network service, and is handled by the IP multimedia subsystem network [6]. The evolved packet core consists of a MME and a Serving Gateway (SGW), a Packet Data Network Gateway (PDN GW) together with Home Subscriber Server (HSS). When user equipment connects to the evolved packet core, the MME represents the evolved packet core to perform a mutual authentication with the user equipment. E-UTRAN includes the Evolved Universal Terrestrial Radio Access Network Base Stations, called eNodeBs (eNB), which communicates with user equipment

Compared with the 3G wireless networks, the LTE/LTE-A networks introduce some new functions and entities. (1) A new type of base station, named HeNB, is suggested by the 3GPP committee to improve the indoor coverage and network capacity. HeNB is a low-power access point and is typically installed by a subscriber in the residence or a small office to increase the indoor coverage for the voice and high speed data service. It connects to the evolved packet core over the Internet via a broadband backhaul [8]. (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 evolved packet core [13]. There are two types of non-3GPP access networks, which are trusted non-3GPP access networks and untrusted non-3GPP access networks [14].Whether a non- 3GPP access network is trusted or not is not a characteristic of the access networks, which depends on the decision of the network operators. For an untrusted non-3GPP access network, user equipment needs to pass a trusted evolved packet data gateway (ePDG) connected to the evolved packet core. (3) A LTE-A system also supports a new type of data communications between entities, named as Machine Type Communication [7], which can exchange and share data without any requirement on any form of human intervention. There are two new entities existing in the Machine Type Communication, the Machine Type Communication user and the Machine Type Communication server. A Machine Type Communication user, who is a person or a control centre outside the network operator domain, can use the services provided by one or more Machine Type Communication servers to operate a large number of Machine Type Communication devices. The Machine Type Communication server is connected to the LTE network to communicate with Machine Type Communications. The Machine Type Communication server may be an entity outside or inside an operator domain. When a Machine Type Communication device connects to the LTE network, the Machine Type Communication device can communicate with the Machine Type Communication server and be controlled by the Machine Type Communication user via the Machine Type Communication servers.

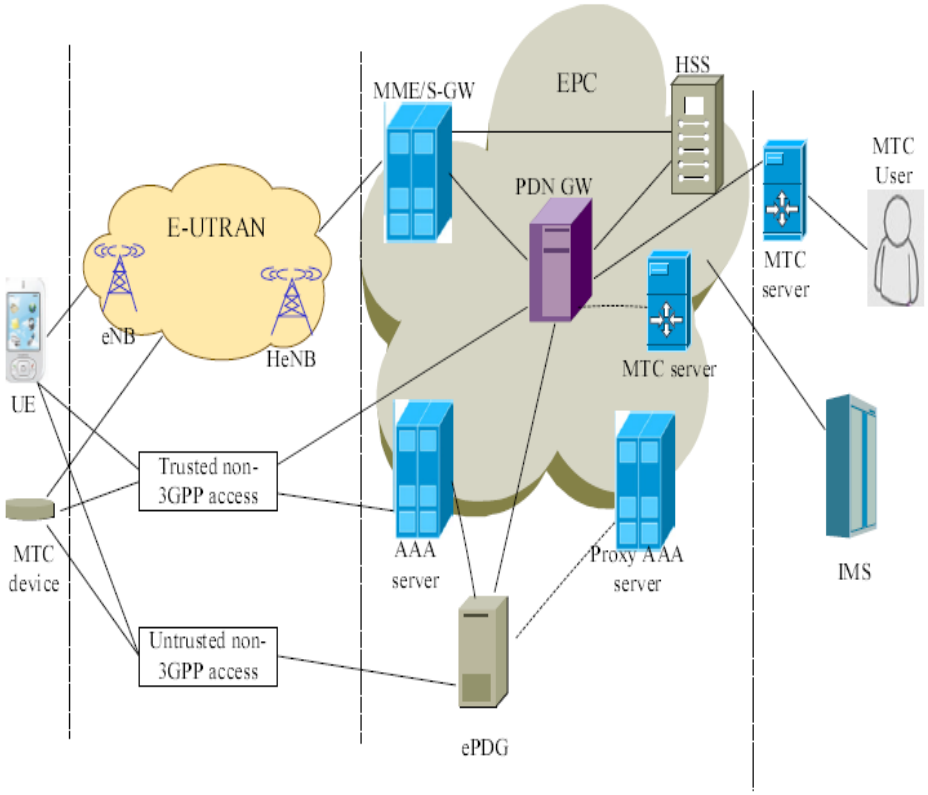


Figure 1. Network Architecture of LTE

3. LTE Security Architecture

As shown in Figure 2 [1], five security modules are defined by 3GPP committee, which are known as network access security, Network domain security, User domain security, Application domain security, and Non 3GPP domain security [7]. For detail, I: The set of security features that provides the user equipment with secure access to the evolved packet core and protect against various attacks on the (radio) access link. This level has security mechanisms such as integrity protection and ciphering between the USIM, Mobile Equipment, the E-UTRAN, and the entities in the evolved packet core. II: The set of security features that protects against attacks in the wire line networks and enable nodes to exchange signaling data and user data in a secure manner. III: The set of security features that provides a mutual authentication between the USIM and the Mobile Equipment before the USIM access to the Mobile Equipment. IV: The set of security features that enables applications in the user equipment and in the service provider domain to securely exchange messages. V: The set of features that enables the user equipment to securely access to the evolved packet core via non-3GPP.

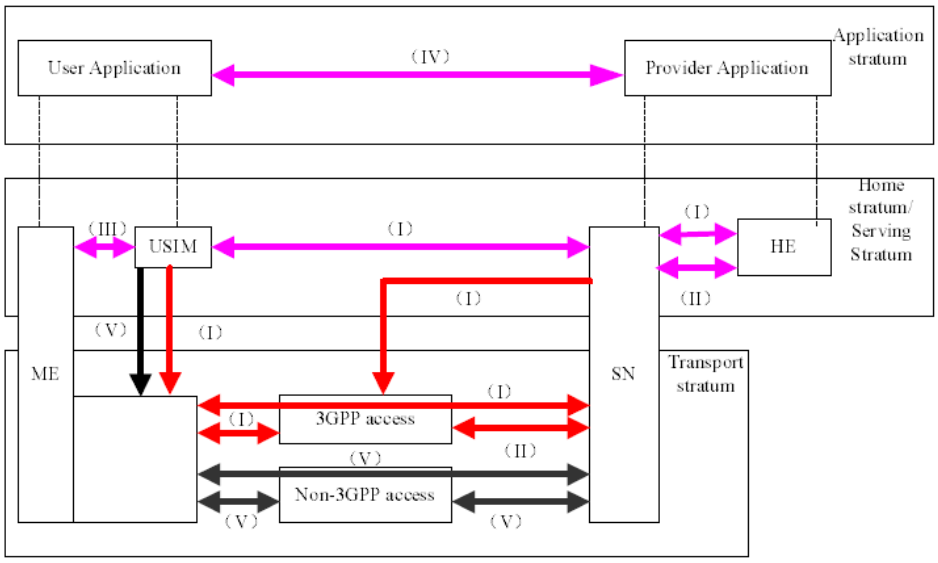


Figure 2. Overview of Security Architecture

A mutual authentication between the user equipment and the EPC is the most important security feature in the LTE security framework. The LTE system utilizes the AKA procedure to achieve the mutual authentication between the user equipment and the EPC and generate a ciphering key (CK) and an integrity key (IK), which are used to derive different session keys for the encryption and the integrity protection. Owing to the support of non-3GPP access, several different AKA procedures are implemented in the LTE security architecture when the user equipment access to the EPC via distinct access networks.

When an user equipment connects to the EPC over the E-UTRAN, the MME represents the EPC to perform a mutual authentication with the user equipment by the EPS AKA protocol [6] as shown in Figure 3. In addition, the new key hierarchy has been introduced to protect the signaling and user data traffic. When an user equipment connects to the EPC via non-3GPP access networks, the non-3GPP access authentication will be executed between the user equipment and the AAA server. The authentication signaling will pass through the Proxy AAA server in the roaming scenarios. The trusted non-3GPP access networks [15] can be pre-configured at the user equipment. If there is no preconfigured information at the user equipment, the user equipment shall consider the non-3GPP access network untrusted. For a trusted non-3GPP access network, the user equipment and the AAA server will implement the Extensible Authentication Protocol-AKA (EAP-AKA) or Improved EAP-AKA (EAP-AKA') to accomplish the access authentication. As an user equipment connects to the EPC over an untrusted non-3GP access network, the user equipment and the ePDG need to perform the IPsec tunnel establishment. The user equipment and the ePDG shall use the Internet Key Exchange Protocol Version 2 (IKEv2) with EAP-AKA or EAP-AKA' to establish the IPSec security associations.

4. Drawbacks in LTE Security Framework

There are some security risks due to the IP-based architecture of LTE/LTE-A networks, like the vulnerability to the injection, modification, eavesdropping attacks and more privacy risks than those in the GSM and the UMTS networks [8, 9]. It is found that IP address

spoofing, DoS attacks, viruses, worms, spam mails and calls are more likely to threaten the LTE architecture, as its traditional malicious attacks presenting in the Internet [10].

Besides, there are some other potential weaknesses caused by then base stations existing in the LTE systems. The all-IP network provides a direct path to the base stations for malicious attackers. Since an MME manages numerous eNBs in the flat LTE architecture, the base stations in the LTE networks are more susceptible to the attacks compared with those in the UMTS architecture, where the serving network in the UMTS only manages a couple of Radio Network Controls (RNCs) in a hierarchical way. Once an adversary compromises a base station, it can further endanger the entire network due to the all-IP nature of the LTE networks. Moreover, due to the introduction of small and low-cost base stations, HeNBs, which are easily obtained by an attacker, the attacker can thus create its own rogue version equipped with the functionality of a base station and a user simultaneously. By using a rogue base station, the attacker can impersonate as a genuine base station to entice a legitimate user. And, it can also disguise a legitimate user to establish a connection with a genuine base station. Furthermore, since the HeNB can be placed in unsecure regions of the Internet, which will be susceptible to a large number of threats of physical intrusions [11].

The LTE architecture may produce some new problems in the handover authentication procedures. Due to the introduction of the simple base station, HeNB, there are several different mobility scenarios in the LTE networks when an user equipment moves away from an eNB/HeNB to a new HeNB/eNB as shown in Figure 3 [1]. The 3GPP committee has proposed a few mobility scenarios possibly occurring between a HeNB and an eNB, and has described the relevant handover call flows in details [7, 12].

However, distinct handover authentication procedures are required in different scenarios, such as the handovers between eNBs, between HeNBs, between a HeNB and an eNB, and the inter-MME handovers when the base stations are managed by different MMEs, which will increase the overall system complexity. Moreover, since a few heterogeneous access systems could coexist in the LTE networks, it brings more threats to the network security, especially when the mobility is supported among the heterogeneous access systems. 3GPP committee has proposed several handover authentication approaches to achieve secured seamless handovers between the E-UTRAN and the non-3GPP access networks [15]. But they need to go through a full access authentication procedure between a user equipment and the target access network before the user equipment handover to the new access network, which will bring a longer handover delay due to multiple rounds of message exchanges with contacting the authentication, authorizing, and accounting (AAA) server or a proxy AAA server when a roaming happens. In addition, different mobility scenarios need distinct handover authentication procedures, which will increase the complexity of the entire system.

Furthermore, Forsberg [16] has analyzed all of the key derivation procedures for the handovers and pointed out that the key management system employed by the LTE networks includes multiple key management mechanisms, which will also increase the overall system complexity. These vulnerabilities will not only bring a lot of difficulty to support the continuous connectivity in the LTE networks, but also may be exploited by attackers to attack other access networks or the core network to deplete the network resources, even to paralyze the entire networks.

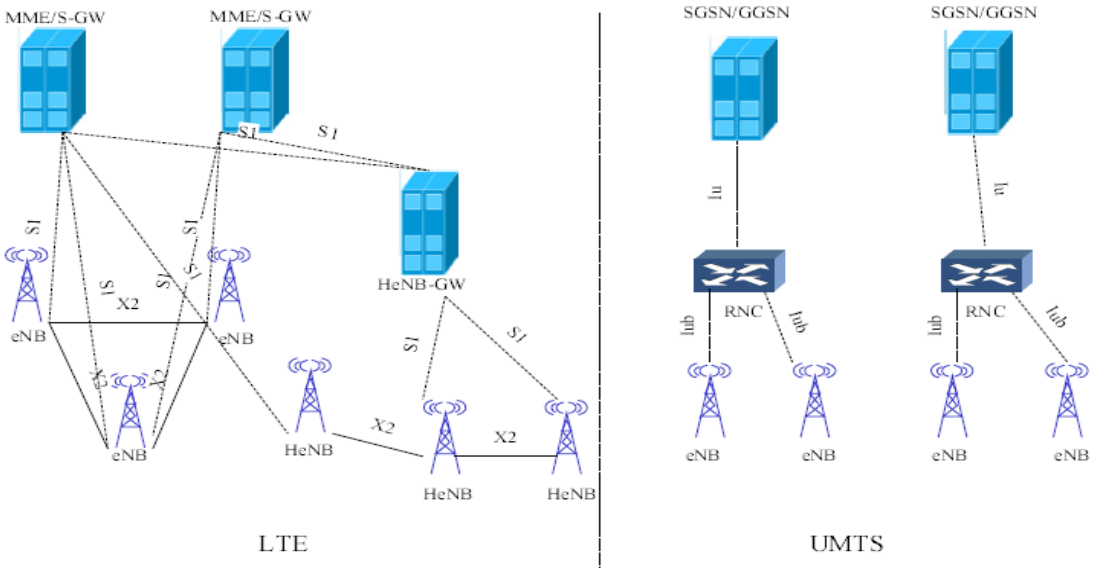


Figure 3. Comparison of Access Network Architecture

5. Open Issues

At the end of this paper, we suggest a few promising research directions on the LTE security as the potential future works, which are described as follows.

The security mechanisms to ensure reliable high-speed connectivity for sensitive data are required. For example, in the healthcare industry, remote patient monitoring and care provisioning is an important service area. Usually, bio-sensors can be mounted to a patient to monitor the patients' vital signs of health, such as heart/pulse, blood pressure and respiratory rate. Sensors working as Machine Type Communication devices send the collected information to a Machine Type Communication application server via the 3GPP network. In emergency situations, a Machine Type Communication device can directly send a patient's medical status information to the hospital to allow physicians to prepare for the necessary treatment in advance. In this important scenario, reliable high-speed connectivity is highly demanded. Similar scenarios also exist in military area, environmental monitoring and fire rescue. In those scenarios, the security mechanism for the sensory data should not cause massive operational overheads and delays in order to operate efficiently.

6. Conclusions

In this paper, we have first illustrated the security architectures by the 3GPP standard. We further discussed the drawbacks existing in the security architecture of the LTE wireless networks. Our survey has explored that there are still a lot of security issues in the current LTE networks. Finally, we have summarized potential open research issues as the suggestion for the future research activities on the security of LTE wireless networks.

Acknowledgments

This paper is a revised and expanded version of a paper entitled "A Survey about Location-Based Routing Protocols for Wireless Sensor Network" presented at CIA 2014, Angeles City (Clark), Philippines, April 24 -26, 2014. This work was supported by the Industrial Strategic

Technology Development Program (10041740) funded by the Ministry of Trade, Industry and Energy (MOTIE) Korea. It was also supported by the Natural Science Foundation of Jiangsu Province (No. BK2012461). Prof. Jeong-Uk Kim is the corresponding author.

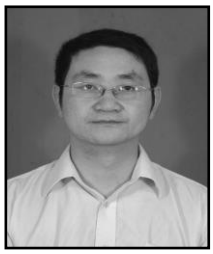
References

[1] J. Cao, M. Ma and H. Li, "A survey on security aspects for LTE and LTE-A networks", Communications Surveys & Tutorials, vol. 16, no. 1, **(2013)**.
[2] 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, **(2009)**.
[3] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe and T. Thomas, "LTE-advanced: Next-generation Wireless Broadband Technology", IEEE Wireless Commun., vol. 17, no. 3, **(2010)**.
[4] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks", Proc. IEEE Globecom Workshops, **(2007)** November.
[5] D. Forsberg, "LTE Key Management Analysis with Session Keys Context", Computer Communications, vol. 33, no. 16, **(2010)**.
[6] "3GPP", available: <http://www.3gpp.org/ftp/Specs/latest/Rel-8/36_series/>.
[7] H. Holma and A. Toskala, "WCDMA for UMTS: HSPA Evolution and LTE", fourth ed., John Wiley, **(2007)**.
[8] "3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, IP Multimedia Subsystem (IMS)", (Rel 11), 3GPP TS 23.228 V11.6.0, **(2012)** September.
[9] "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE)", Security architecture (Rel 12) 3GPP TS 33.401 V12.5.0, **(2012)** September.
[10] M. Al-Humaigani, D. Dunn and D. Brown, "Security Transition Roadmap to 4G and Future Generations Wireless Networks", Proc. 41st Southeastern Symposium on System Theory, **(2009)** March.
[11] M. Aiash, G. Mapp, A. Lasebae and R. Phan, "Providing Security in 4G Systems: Unveiling the Challenges", Proc. Sixth Advanced International Conference on Telecommunications, **(2010)** May.
[12] "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, **(2009)** June.
[13] "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network; Overall description", (Rel 11), 3GPP TS 36.300 V11.3.0, **(2012)** September.
[14] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for the Evolved Packet System (EPS) (Rel 12)", 3GPP TS 22.278 V12.1.0, **(2012)** June.
[15] "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks (Rel 11)", 3GPP TS 24.302 V11.4.0, **(2012)** September.
[16] "3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Rel 11)", 3GPP TS 33.402 V11.4.0, **(2012)** June.

Authors

Jin Wang, he received the B.S. and M.S. degree in the Electronical Engineering from Nanjing University of Posts and Telecommunications, China in 2002 and 2005, respectively. He received Ph.D. degree from Kyung Hee University Korea in 2010. Now, he is a professor in the Computer and Software Institute, Nanjing University of Information Science and Technology. His research interests mainly include routing protocol and algorithm design, performance evaluation and optimization for wireless ad hoc and sensor networks. He is a member of the IEEE and ACM.

Zhongqi Zhang, he obtained his B.S. degree in the Eletronic and Information Engineering from Nanjing University of Information Science and technology, China in 2012. Now, he is working toward the M.S. degree in the Computer and Software Institute. His current research interests are in performance evaluation for wireless sensor networks, and healthcare with wireless body area networks. He is a student member of ACM and CCF.



Yongjun Ren, he obtained his Masters in Computer received the M.S. degree in computer science from HoHai University, China, in 2004 and PhD degree at Nanjing University of Aeronautics and Astronautics in 2008. Now he is serving as a full time faculty at Nanjing University of Information Science and Technology. His research interests include network security and privacy and applied cryptography with current focus on security and privacy in cloud computing, lower layer attack and defense mechanisms for wireless networks, and sensor network security.

Jeong-Uk Kim, he received his B.S. degree in Control and Instrumentation Engineering from Seoul National University in 1987, M.S. and Ph.D. degrees in Electrical Engineering from Korea Advanced Institute of Science and Technology in 1989, and 1993, respectively. He is a professor in Sangmyung University in Seoul. His research interests include smart grid demand response, building automation system, and renewable energy.

