A Survey on Security Aspects for LTE and LTE-A Networks

Jin Cao, Maode Ma, *Senior Member, IEEE* Hui Li, *Member, IEEE*, Yueyu Zhang, and Zhenxing Luo

***Abstract*—High demands for broadband mobile wireless communications and the emergence of new wireless multimedia applications constitute the motivation to the development of broadband wireless access technologies in recent years. The Long Term Evolution/System Architecture Evolution (LTE/SAE) 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. 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. Since the 3GPP LTE and LTE-A architecture are designed to support flat Internet Protocol (IP) connectivity and full interworking with heterogeneous wireless access networks, the new unique features bring some new challenges in the design of the security mechanisms. This paper makes a number of contributions to the security aspects of the LTE and LTE-A networks. First, we present an overview of the security functionality of the LTE and LTE-A networks. Second, the security vulnerabilities existing in the architecture and the design of the LTE and LTE-A networks are explored. Third, the existing solutions to these problems are classically reviewed. Finally, we show the potential research issues for the future research works.**

***Index Terms*—LTE security, LTE, LTE-A, IMS security, HeNB security, MTC security.**

I. Introduction

With the rapid development of wireless communication and multi-media applications such as Internet browsing, interactive gaming, mobile TV, video and audio streaming, the mobile communication technology needs to meet different requirements of mobile data, mobile calculations and mobile multi-media operations. In order to accommodate the increasing mobile data usage and the new multimedia applications, LTE and LTE-A technologies have been specified by the 3GPP as the emerging mobile communication technologies for the next generation broadband mobile wireless networks. 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 [1]. 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 [2]. In addition, both of the LTE and LTE-A systems support flat IP connectivity, full interworking with heterogeneous wireless access networks and many new types of base stations such as pico/femto base stations and relay nodes in a macro-cellular network. Due to the introduction of the new characteristics, it incurs a lot of new security challenges in the design of the security architectures of the LTE and LTE-A systems.

Since there are a lot of security vulnerabilities in the Universal Mobile Telecommunication System (UMTS) security mechanism such as Man-in-the-Middle (MitM) attacks [3], rogue base station attacks [4] and Deny of Service (DoS) attacks [5], the next generation mobile communication systems need to provide more security functionality than the UMTS systems. To achieve a mutual authentication between the User Equipment (UE) and the Mobility Management Entity (MME) through the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN), the SAE/LTE architecture enhances the UMTS-Authentication and Key Agreement (UMTS-AKA) and presents the new access security approach, Evolved Packet System AKA (EPS AKA) to avoid the attacks existing in the UMTS systems. In addition, a new key hierarchy and handover key management mechanism has been introduced in order to ensure the security of the access and the mobility process in the LTE architecture [6]. In addition to maintain the secure strength of the LTE systems, a LTE-A system has introduced some new entities and applications such as Machine Type Communication (MTC) [7], Home eNodeB (HeNB) [8], Relay nodes [9] and specified the corresponding security vulnerabilities, requirements and solutions [10]–[13]. However, there are still some security vulnerabilities in the current LTE/LTE-A networks, which need to be further analyzed.

Recently, a multitude of research results on the security functionality of LTE/LTE-A networks have been proposed. A few surveys have already been published in order to review the existing works [14]–[18]. A general overview of the security threats on 4G networks has been presented in [14]. In the survey, the security architectures of IP Multimedia Subsystem (IMS) and Next Generation Networks (NGN) have been investigated and a systematic analysis tool based on the Bell Labs Security Model named X.805 standard has been suggested to analyze the security vulnerabilities of the 4G systems. In addition, the survey has presented the possible weaknesses of the current security functionalities in the WiFi,

Manuscript received August 24, 2012; revised January 27, 2013.

J. Cao is with the State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, China (e-mail: caoj897@gmail.com).

M. Ma is with School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: Maode_Ma@pmail.ntu.edu.sg).

H.Li and Y. Zhang are with the State Key Laboratory of Integrated Service Network, Xidian University, Xi'an, China.

Z. Luo is with Department of Electrical and Systems Engineering, Washington University in St. Louis, Saint Louis, MO 63130, USA. (e-mail: mariolzx@seas.wustl.edu).

Digital Object Identifier 10.1109/SURV.2013.041513.00174

Worldwide Interoperability for Microwave Access (WiMAX) and the LTE systems. It has pointed out that 4G systems will inherit all the security problems of underlying access networks and most of the IP-specific security vulnerabilities due to their heterogeneous and IP-based open architecture. The survey in [15] has provided a comprehensive taxonomy of the malicious attacks and countermeasures in WiMAX systems. In the survey, a variety of malicious attacks against the WiMAX systems specified by IEEE 802.16 standards found in the current literatures has been examined and classified based on a few factors. And then, possible countermeasures and remedies proposed for each category of the attacks have been summarized. In addition, the qualitative characteristic of each type of the attacks has been evaluated in terms of both breadth and depth. It has shown that many attacks existing in the WiMAX systems are not severe to the systems while most of them can only cause minor damage to the networks. A brief summary of LTE security functions and procedures has been provided in [16]. In the survey, the overall evolved packet system (EPS) architecture, EPS security threats and security requirements have been discussed. And then, the EPS security architecture and the detailed security procedures designed by the 3GPP specifications have been described. It has indicated that there are still a lot of problems existing in the current EPS security architecture to be addressed because of the wholly heterogeneous nature of the EPS, such as negotiation of Key Derivation Function (KDF), key handling, user activation of User Plane (UP) ciphering, and so on. A study of security advances and challenges in the 4G wireless networks has been presented in [17]. In the survey, the security architectures of WiMAX and LTE networks have been specified with concentration on the specific MAC layer security issues and possible vulnerabilities associating with the LTE and the WiMAX systems. It has shown that a WiMAX system has some MAC layer vulnerabilities under DoS attacks, eavesdropping attacks, and replay attacks, and service degradation due to the faulty key management. In addition, the LTE networks are also susceptible to DoS attacks, data integrity attacks, illegal use of user and mobile equipments, and location tracking at the MAC layer. The survey in [18] has mainly discussed the security aspects of the 4G wireless systems at the application layer. In the 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 explored. In addition, some constructive security defending strategies have been proposed in [18] for the 4G mobile communication systems with the IPv6 networks. The previous surveys have mainly focused on the security architecture, security vulnerabilities, and security requirements in the LTE systems without the introduction of the current research efforts and solutions in progresses to the research topics. Moreover, the new features introduced in the LTE/LTE-A networks such as MTC and HeNB have not been investigated.

In this paper, we present a comprehensive survey of security aspects in LTE/LTE-A networks. Our efforts and contributions made in this work include (1) an overview of the security architectures and functionalities in the LTE/LTE-A networks, (2) an analysis of the security issues and vulnerabilities in the LTE networks and the security aspects of the new features introduced in the LTE-A networks, (3) a discussion on the existing solutions to overcome these vulnerabilities, and (4) an exploration of the potential areas and research directions for the future research work.

The reminder of this paper is organized as follows. In Section II, the overview of the security architecture of the LTE/LTE-A networks is presented. In Section III, the security features and functionalities of the LTE/LTE-A networks are summarized. In Section IV, the vulnerabilities of the security functionality of the LTE/LTE-A networks are explored. The existing solutions are discussed in Section V. Finally, the open research issues are identified and the conclusion of the paper is presented in Section VI and Section VII.

II. Security Architecture Overview

A. LTE Network Architecture

As shown in Fig. 1, a LTE network is comprised of the Evolved Packet Core (EPC) and the E-UTRAN. The EPC is an all-IP and fully packet-switched (PS) backbone network in the LTE systems. Voice service, which is traditionally a circuit-switched (CS) network service, will be handled by the IP multimedia subsystem (IMS) network [19]. The EPC consists of a MME and a Serving Gateway (SGW) , a Packet Data Network Gateway (PDN GW) together with Home Subscriber Server (HSS). When a UE connects to the EPC, the MME represents the EPC to perform a mutual authentication with the UE. E-UTRAN includes the Evolved Universal Terrestrial Radio Access Network Base Stations, called eNodeBs (eNB), which communicates with UEs.

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 EPC 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 EPC [20]. There are two types of non-3GPP access networks, which are trusted non-3GPP access networks and untrusted non-3GPP access networks [21]. 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, an UE needs to pass 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, named as MTC [7], which can exchange and share data without any requirement on any form of human intervention. There are two new entities existing in the MTC, the MTC user and the MTC server. A MTC user, who is a person or a control centre outside the network operator domain, can use the services provided by one or more MTC servers to operate a large number of MTC devices. The MTC server is

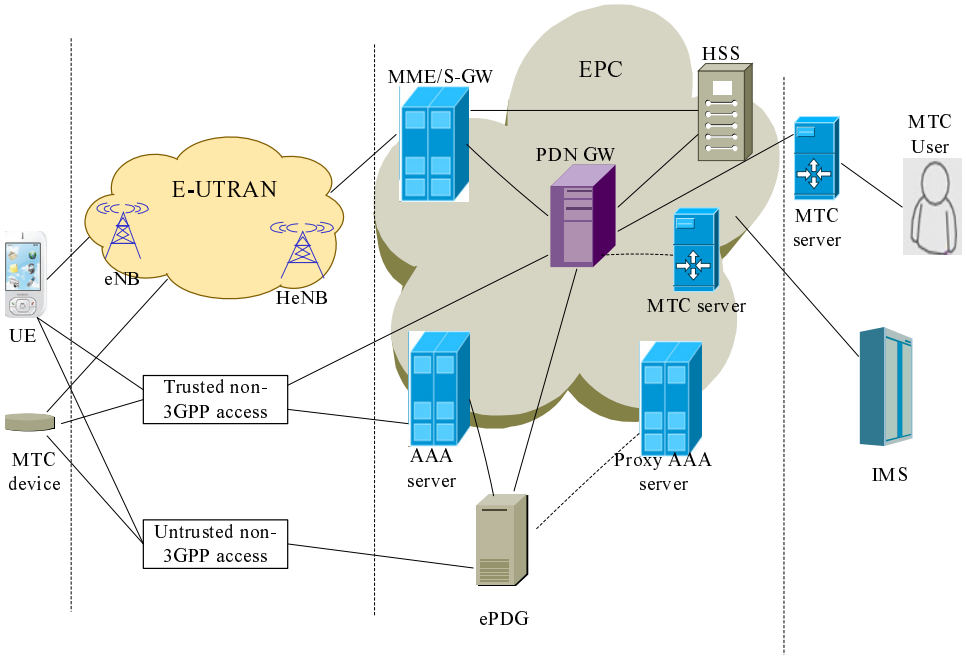

Fig. 1. Network Architecture of LTE

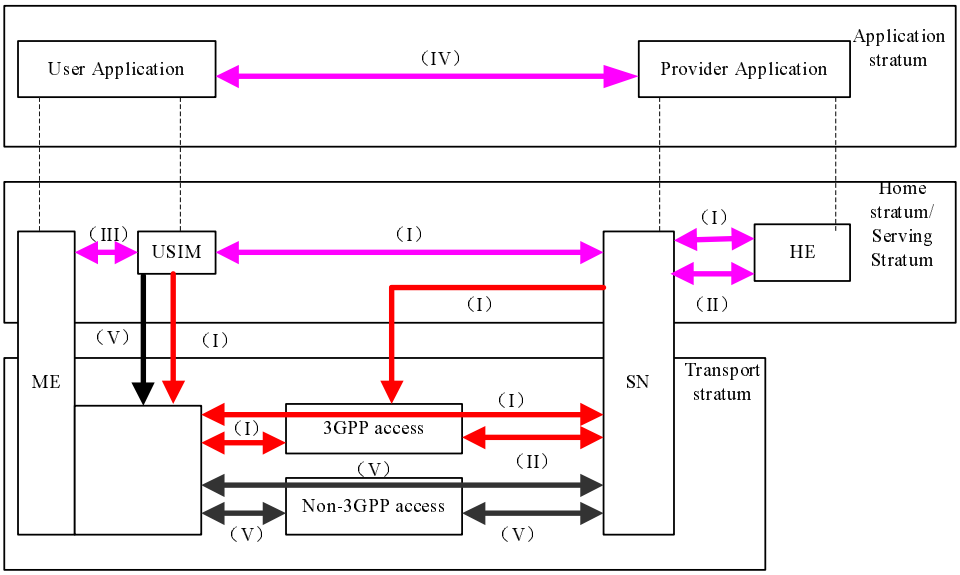

Fig. 2. Overview of Security Architecture

connected to the LTE network to communicate with MTCDs. The MTC server may be an entity outside or inside an operator domain. When a MTC device connects to the LTE network, the MTC device can communicate with the MTC server and be controlled by the MTC user via the MTC servers.

B. LTE Security Architecture

As shown in Fig. 2, there are five security levels defined by 3GPP committee [6], which are specified as follows.

Network access security (I): The set of security features that provides the UEs with secure access to the EPC 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 (ME), the E-UTRAN, and the entities in the EPC.

Network domain security (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.

User domain security (III): The set of security features that provides a mutual authentication between the USIM and the ME before the USIM access to the ME.

Application domain security (IV): The set of security features that enables applications in the UE and in the service provider domain to securely exchange messages.

Non 3GPP domain security (V): The set of features that enables the UEs to securely access to the EPC via non-3GPP

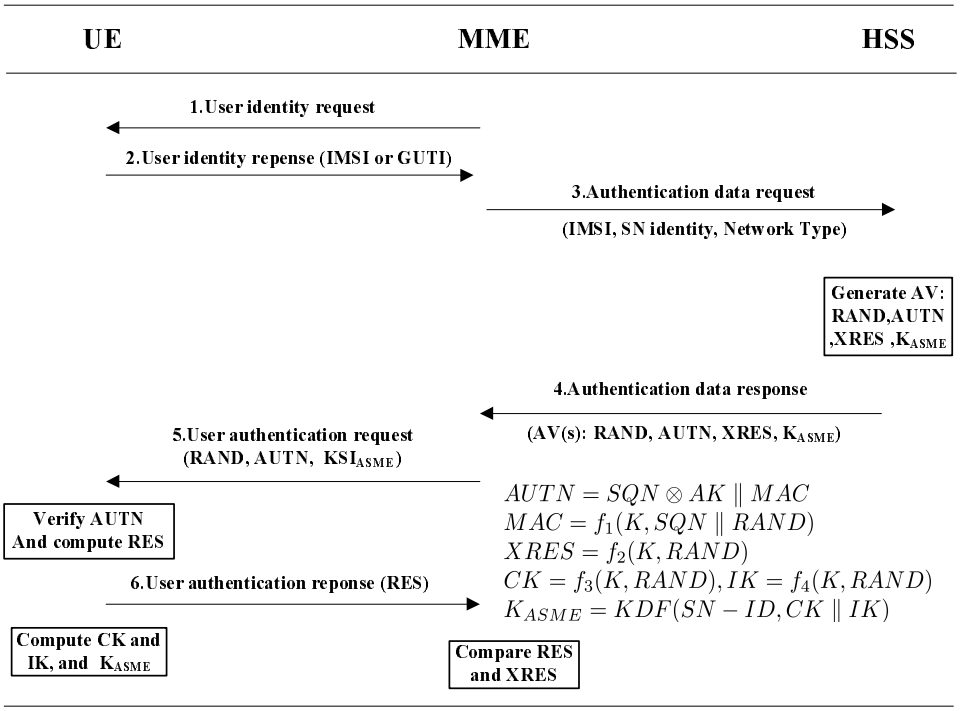

Fig. 3. EPS AKA

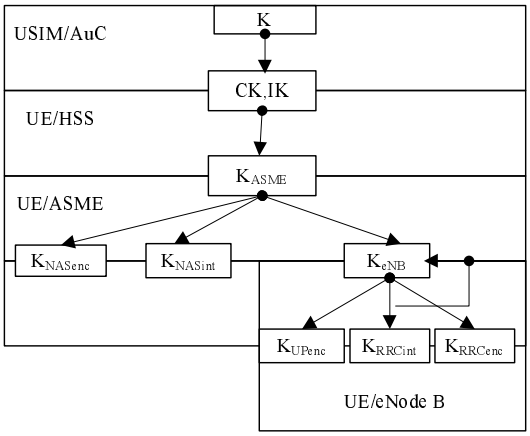

Fig. 4. Key Hierarchy of 3GPP LTE

access networks and provide security protection on the (radio) access link.

III. LTE Security Feature and Mechanisms

In this section, we primarily detail the LTE security features and procedures that can meet the security requirements at network access security level, and specify the security aspects of the new features introduced in LTE-A networks. Based on the research progresses on the LTE/LTE-A security features in recent years, we concentrate on the following five aspects for the LTE security.

1) LTE cellular security.
2) LTE handover security.
3) IMS security.
4) HeNB security.
5) MTC security.

A. Security in A LTE Cellular System

A mutual authentication between the UE 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 UE 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 UEs access to the EPC via distinct access networks.

When an UE connects to the EPC over the E-UTRAN, the MME represents the EPC to perform a mutual authentication with the UE by the EPS AKA protocol [6] as shown in Fig. 3. In addition, the new key hierarchy has been introduced to protect the signaling and user data traffic as shown in Fig. 4. When an UE connects to the EPC via non-3GPP access networks, the non-3GPP access authentication will be executed between the UE and the AAA server. The authentication signaling will pass through the Proxy AAA server in the roaming scenarios. The trusted non-3GPP access networks [22] can be pre-configured at the UE. If there is no pre-configured information at the UE, the UE shall consider the non-3GPP access network untrusted. For a trusted non-3GPP access network, the UE 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 UE connects to the EPC over an untrusted non-3GP access network, the UE and the ePDG need to perform the IPsec tunnel establishment. The UE 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.

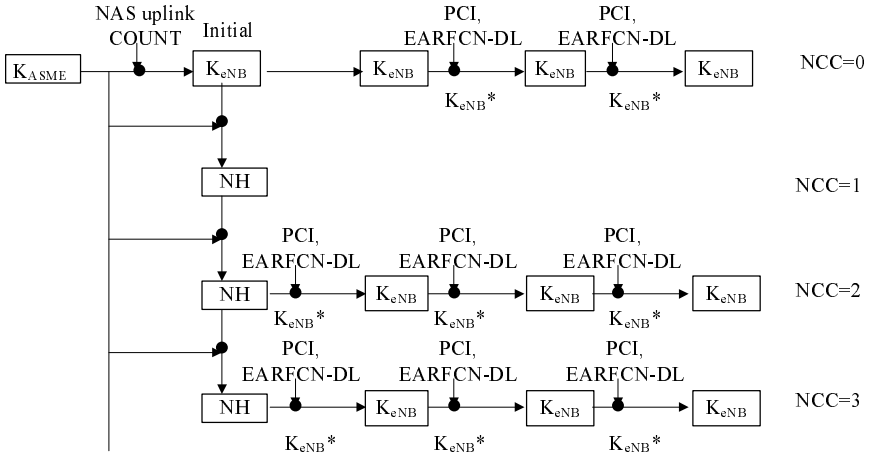

Fig. 5. Handover Key Management

B. Security in Handover Processes

3GPP committee has specified the security features and procedures on the mobility within E-UTRAN as well as between the E-UTRAN and the UMTS Terrestrial Radio Access Network (UTRAN)/ GSM EDGE Radio Access Network (GERAN)/non-3GPP access networks [6], [22]–[25], which are described in detail as follows.

(1)Intra E-UTRAN mobility [22], [23]. In order to achieve a secure handover within E-UTRAN, the LTE networks employ a new key management mechanism, which contains different ways to derive the new eNB keys based on vertical or horizontal key derivations [6] as shown in Fig. 5. To achieve a secure communication between an UE and an eNB, a MME and the UE shall derive a K_{eNB} and a Next Hop parameter (NH) from the K_{ASME}, which is derived by the UE and the MME after an initial authentication procedure. A NH Chaining Counter (NCC) is associated with each K_{eNB} and the NH parameter. In handovers, the new session keys that will be used between the UE and the target eNB, called K^*_{eNB}, will be derived from either the currently active K_{eNB} or from the NH parameter.

(2) Mobility between the E-UTRAN and UTRAN/GERAN [23], [24]. For the handover from the E-UTRAN to the UTRAN or the GERAN, the UE and the MME shall derive a CK' and IK' from the K_{ASME} [6]. Upon receiving $CK' \parallel IK'$ with KSI' from the MME, the target Service GPRS Supporting Node (SGSN) and the UE shall use CK' and IK' to derive the General Packet Radio Service (GPRS) Kc [22]. For the handover from the UTRAN/GERAN to the E-UTRAN, the target MME shall derive K'_{ASME} from CK and IK or GPRS Kc received from the SGSN. The UE shall also execute the above same procedure as the MME to derive K'_{ASME}. Then, the target MME and the UE shall derive K_{eNB} and the corresponding NAS keys according to the key hierarchy of LTE as shown in Fig. 4.

(3) Mobility between the E-UTRAN and non-3GPP access networks [25]. 3GPP committee [25] has proposed several mobility approaches for the EPC to achieve secure seamless handovers between the E-UTRAN and non-3GPP access networks. According to the 3GPP specification [22], when an UE moves from one radio access network to another, the UE, the target access network and the EPC will implement a full access authentication. The different access authentication procedures will be executed in distinct mobility scenarios, such as EPS-AKA when handover to the E-UTRAN, the EAP-AKA or the EAP-AKA' when handover to trusted non-3GPP access networks and IKEv2 with EAP-AKA or EAP-AKA' when handover to untrusted non-3GPP access networks.

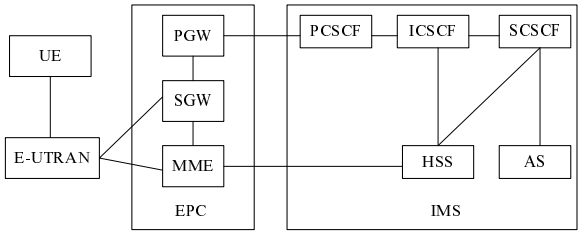

Fig. 6. LTE and IMS Integrated System Architecture

C. Security in IMS

The LTE/LTE-A networks are evolving towards all-IP and fully PS networks. The IMS, which is an access-independent, IP based service control architecture, has been developed by the 3GPP [19], [26]. IMS is an overlay architecture to provide the LTE/LTE-A networks with multimedia services such as Voice over IP (VoIP), video conferencing etc.

Fig. 6 describes the architecture of the LTE and the IMS integrated system [27]. In order to access multimedia services, the UE needs a new IMS Subscriber Identity Module (ISIM) located within the Universal Integrated Circuit Card (UICC). Similar to the UMTS SIM (USIM), which is used to connect to the LTE networks, the IMS authentication keys and functions at the user side shall be stored at the ISIM. Due to the use of Session Initiation Protocol (SIP) for the control and signaling of sessions, the main architectural elements in the IMS are the SIP proxies, known as the Call Service Control Functions (CSCF). All the SIP session signaling can be handled by the CSCFs, which can be divided into three entities, Proxies-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF) and Serving-CSCF (S-CSCF). When an IM user wants to communicate with the IMS, the S-CSCF represents the HSS to authenticate

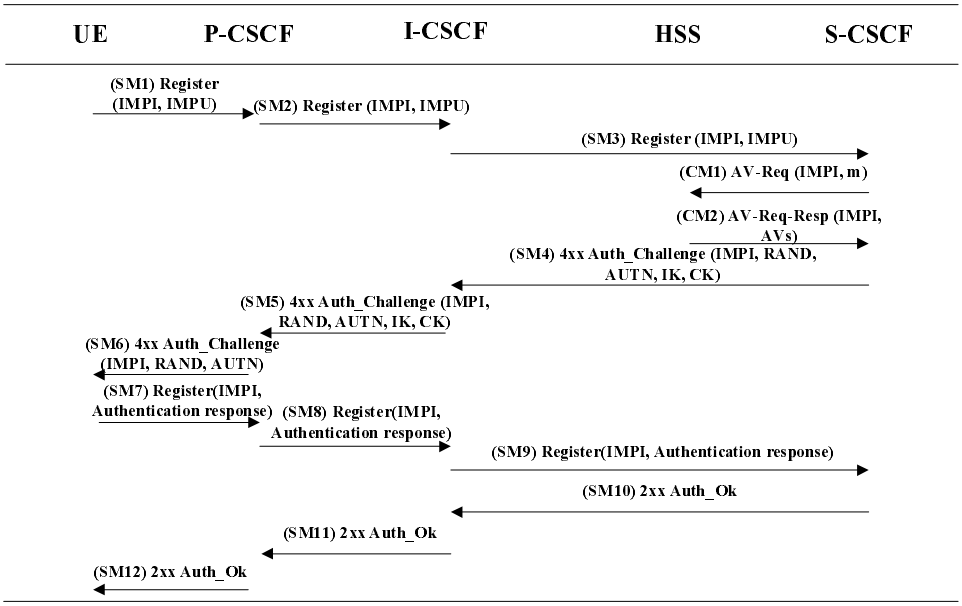

Fig. 7. IMS AKA

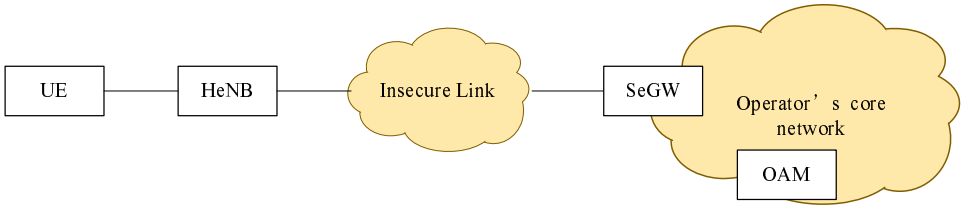

Fig. 8. HeNB System Architecture

the IM user and provides the session control of the multimedia services for it.

The multimedia services will not be provided until the UE has successfully established the security association with the network. In addition, a separate security association is required between the IM UE and the IMS before an access is granted to multimedia services. According to the 3GPP specification [27], in order to access the multimedia services, IM UEs have to be authenticated in both the LTE network layer and the IMS service layer. An IM UE firstly needs to accomplish the mutual authentication with the LTE network by the EPS-AKA before the access to multimedia services. Then, an IMS AKA is executed between the ISIM and the Home Network (HN) for authentication and key agreement for the IMS as shown in Fig. 7. Once the network authentication and the IMS authentication are successful, the IM subscriber will be granted access to the IM services.

D. Security at HeNB

A HeNB known as a femtocell is a low-power access point. It is typically installed by a subscriber in residences or small offices to increase indoor coverage for voice and high speed data service. The HeNB is an attractive device for operators to offer extended services with the advantages of low costs and high quality of services. There are three types of access for the HeNB, i.e. closed access, hybrid access and open access [8], [12].

As shown in Fig. 8, a HeNB connects to the EPC over the Internet via the broadband backhaul. The backhaul between the HeNB and security gateway (SeGW) may be insecure. The SeGW represents the EPC to perform a mutual authentication with the HeNB by the IKEv2 with the EAP-AKA or certificates-based scheme. A HeNB needs to be configured and authorized by the operation, administration and maintenance (OAM). When an UE wants to access to the network via a HeNB, the MME will firstly check whether the UE is allowed to access the target HeNB based on the allowed Closed Subscriber Group (CSG) list. Then, a secure access authentication between the UE and the MME will be performed by the EPS AKA.

E. Security in MTC

The MTC, also called Machine to Machine (M2M) communication, is viewed as one of the next sophisticated techniques for future wireless communications. Different from the traditional human to human (H2H) communications designed by the current wireless networks, the MTC is defined as a form of data communication between entities that do not necessarily need human interaction. It is mainly used for automatically collecting and delivering the information of measurement. As shown in Fig.9, the 3GPP committee has suggested three scenarios for the MTC [7]. Fig.9 (a) shows that the MTC devices can communicate with one or more MTC servers via the LTE network. The MTC servers can be located in or

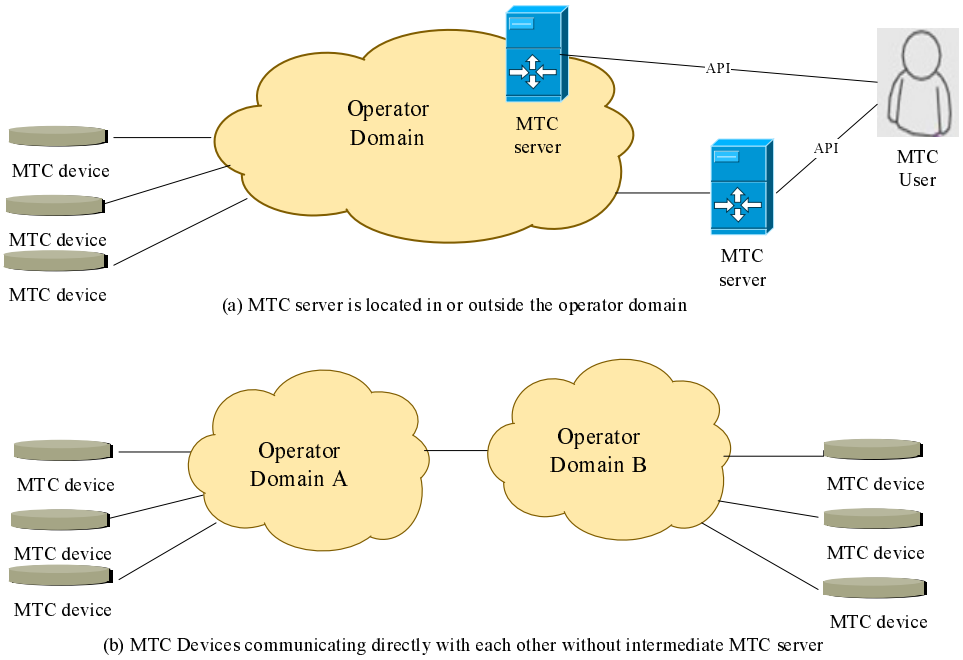

Fig. 9. MTC Communication Scenarios

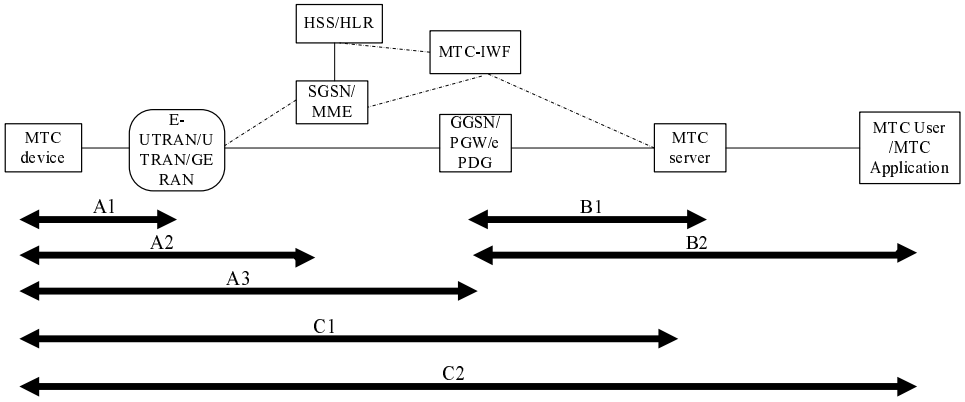

Fig. 10. MTC Security Architecture

outside the operator domain. In addition, the MTC devices can communicate directly with each other without an involvement of the MTC servers as shown in Fig.9 (b). For the communication scenario in Fig.9 (a), the MME represents the network to implement mutual authentications with the MTC devices by the EPS AKA to enable the secure communication between the MTC devices and the MTC server. For the communication scenarios in Fig.9 (b), there is no specific approach to ensure the secure communication between MTC devices proposed in the current 3GPP standard. The 3GPP committee has described a potential high level security architecture for the MTC [10], which includes three different security areas described in Fig. 10.

A) Security for the MTC between the MTC device and 3GPP network, which can be divided into three subareas. (A1) Security for the MTC between the MTC device and the Radio Access Network, E-UTRAN/UTRAN/GERAN, (A2) Security for the MTC between the MTC device and the MME, (A3) Security for the MTC between the MTC device and the MTC-IWF for 3GPP access/ ePDG for non-3GPP access.
B) Security for the MTC between the 3GPP network and the MTC server/MTC user, MTC application, which can be divided into two subareas, (B1) Security for the MTC between the MTC server and the 3GPP network, which can be further divided into security aspects when the MTC server is within and outside the 3GPP network, (B2) Security for the MTC between the MTC user, MTC application, and the 3GPP network.
C) Security for the MTC between the MTC server/MTC user, the MTC application, and the MTC device, which can be further divided into two subareas, (C1) Security for the MTC between the MTC server and the MTC device, (C2) Security for the MTC between the MTC user, MTC application, and the MTC device.

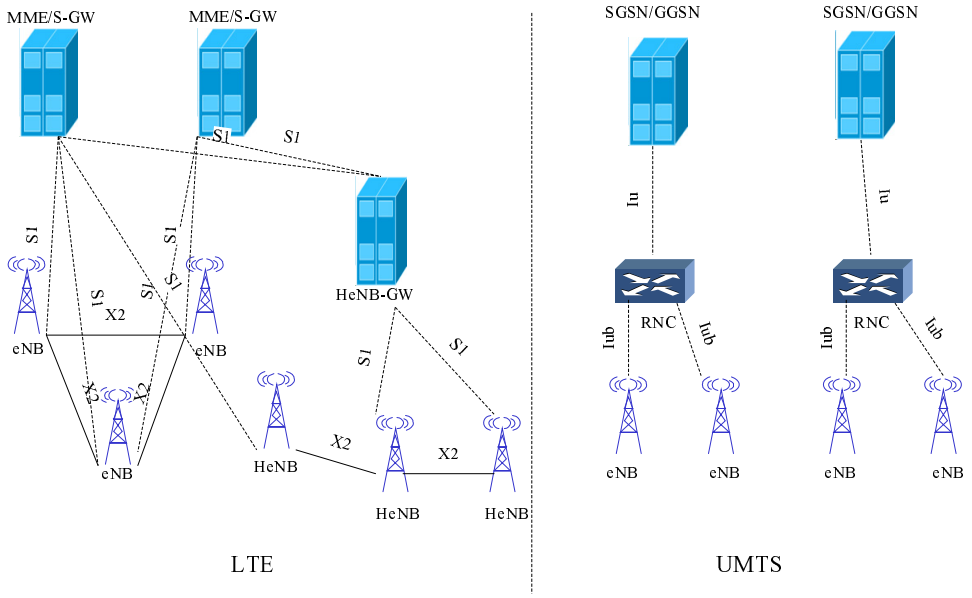

Fig. 11. Comparison of Access Network Architecture

IV. Vulnerabilities in LTE Security Framework

As mentioned above, 3GPP has specified the security requirements, features, threats and the solutions for the corresponding security problems. However, there are still some vulnerabilities and security problems existing in the current LTE security architecture. In this section, we explore these weaknesses in detail on the LTE security framework, specifically at the MAC layer.

A. Vulnerability of LTE System Architecture

The LTE network is designed for the flat all-IP based architecture to support full interworking with heterogeneous radio access networks. The unique features of the LTE networks bring some new security challenges in the design of the security mechanisms.

(1) The flat IP-based architecture of the 3GPP LTE networks results in more security risks such as the vulnerability to the injection, modification, eavesdropping attacks and more privacy risks than those in the GSM and the UMTS networks [28], [29]. It is found that the LTE architecture is more vulnerable to the traditional malicious attacks presenting in the Internet such as IP address spoofing, DoS attacks, viruses, worms, spam mails and calls, and so on [14].

(2) There are some other potential weaknesses caused by the base stations existing in the LTE systems. The all-IP network provides a direct path to the base stations for malicious attackers. As shown in Fig.11, 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 [30].

(3). 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 UE moves away from an eNB/HeNB to a new HeNB/eNB as shown in Fig.11. 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 [6], [23]. 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 [22]. But they need to go through a full access authentication procedure between a UE and the target access network before the UE 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 as shown in Fig. 12. In addition, different mobility scenarios need distinct handover authentication procedures, which will

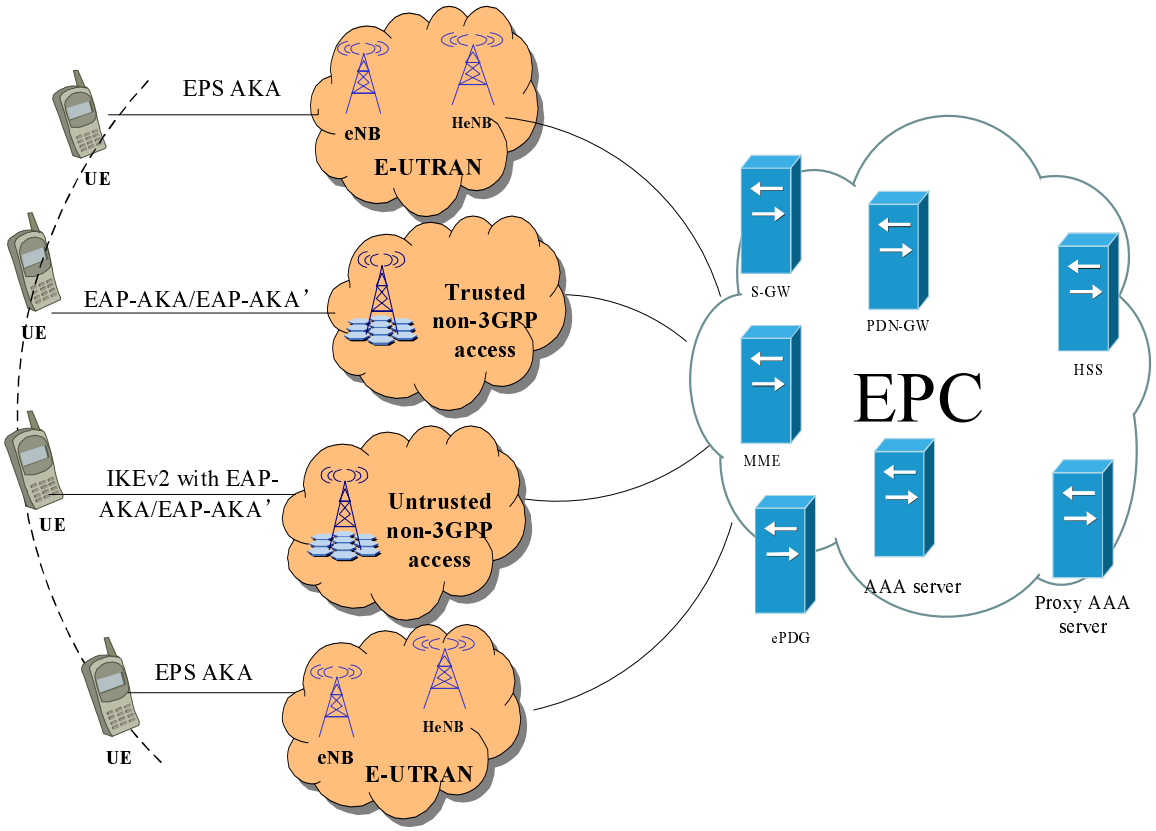

Fig. 12. Handover between E-UTRAN and Non-3GPP Access Network

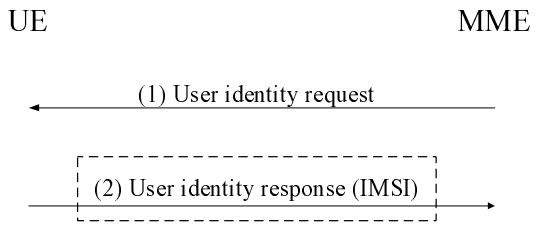

Fig. 13. IMSI Request Process in EPS AKA

increase the complexity of the entire system. Furthermore, Forsberg [31] 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.

B. Vulnerability in the LTE Access Procedure

The EPS AKA has some improvements over the UMTS AKA so that it can prevent some malicious attacks such as redirection attacks, rogue base station attacks and MitM attacks. However, there are still some weaknesses in the current LTE access security mechanism.

(1) The EPS AKA scheme lacks a privacy protection [32]. There are many instances resulted in disclosure of the IMSI. For example, when a UE registers to the network for the first time, or the current MME cannot be contacted or the IMSI cannot be retrieved due to a possible synchronization failure when it roams to a new MME, the current MME or the new MME requests the IMSI of the UE, and thus, the UE must transmit the IMSI in plaintext as shown in the message (2) in Fig. 13. Disclosure of the IMSI may incur severe security problems. Once the IMSI has been obtained, the adversary could acquire subscriber information, location information, and even conversation information, and then disguise the real UE and launch the other attacks such as DoS attacks to destroy the network. An active attack model for stealing the IMSI have been proposed in [32] by which, the IMSI can be easily disclosed by an active attacker and the current security mechanism could not prevent such active attacks.

(2) The EPS AKA scheme cannot prevent DoS attacks [32]–[34]. The MME must forward the UE's requests to the HSS/AuC even before the UE has been authenticated by the MME as shown in message (3) in Fig. 14. In addition, the MME can only authenticate the UE after an RES has been received as shown in message (6) Fig. 14. Based on the above two conditions, an adversary can launch DoS attacks to the HSS/AuC and the MME [32], [33]. The adversary can disguise a legitimate UE to constantly send fake IMSIs to overwhelm the HSS/AuC. Thus, the HSS has to consume its computational power to generate excessive authentication vectors for the UE. On the other hand, the MME has to consume its memory buffer to wait overly long period of time for a legitimate or false response from the corresponding UE.

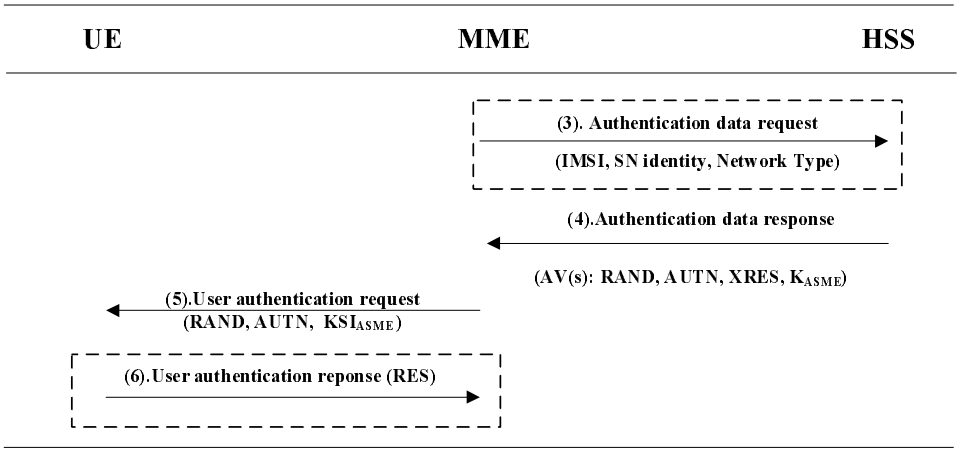

Fig. 14. Authentication Data Request and Mutual Authentication Process

In addition, it has been indicated in [34] that the NAS security procedure is vulnerable to DoS attacks and several DoS attacks have been found in the NAS procedure to overload the entities in E-UTRAN.

(3). Similar to the UMTS AKA, in the EPS-AKA as shown in message (3) and (4) in Fig. 14, the SN must turn back to the HN for a request of another set of authentication vectors when the UE stays in the SN for a long period and exhausts its set of AVs for the authentication, which causes the bandwidth consumption and authentication signaling overhead between the SN and the HN and the storage consumption in the SN [35].

(4). The EPS AKA protocol, same as the GSM AKA and the UMTS AKA, is a delegated protocol [36]. Almost all authentication authorities are delegated from the home network to the visited network, which requires strong trust assumptions between these operators. With the increasing number of roaming partners and the introduction of other access systems, the original trust assumptions seem outdated among heterogeneous networks. In addition, the EPS-AKA protocol lacks the ability of online authentications because the HN is off-line with respect to the authentication process between the UE and the SN, which can be traced back to its evolved history.

(5) When a UE accesses to the EPC via a trusted non-3GPP access network, the LTE architecture reuses the EAP-AKA or EAP-AKA' to provide a secure access authentication. It has been pointed out in [37] that the EAP-AKA protocol has several shortcomings such as the disclosure of user identity, vulnerability to MitM attacks, lack of sequence number (SQN) synchronization, and additional bandwidth consumption.

C. Vulnerability in LTE Handover Procedure

To mitigate the security threats posed by malicious base stations, the LTE security mechanism provides a new handover key management scheme to refresh the key materials between an UE and an eNB whenever the UE moves from one eNB to another. In addition, the 3GPP committee has specified the security requirements, threats and solutions to the security problems to support secure mobility between heterogeneous access systems. However, a lot of vulnerabilities have still been found in the LTE mobility management procedure and the handover key mechanism.

(1) Lack of backward security [38]. Since the LTE key management mechanism utilizes the key chaining architecture, the current eNB may derive new keys for multiple target eNBs by chaining the current key with the eNB specific parameters [38]. For example, as shown in Fig. 15, the source eNB can derive the new session key K_{eNB} between the target eNB and the UE from the known key K^*_{eNB} and the respective target parameters. Once an attacker compromises the source eNB, the subsequent session keys will be obtained. Thus, the handover key management fails to achieve backward security in the current LTE networks.

(2) Vulnerability to de-synchronization attacks [39]. Assume that an adversary compromises a legal eNB or deploys a personal eNB. By the rogue eNB, the attacker can disrupt refreshing of the NCC value by either manipulating the handover request message, shown in Fig.15, between the eNBs or the S1 path switch acknowledgement message, shown in Fig.15, from an MME to a target eNB. In this occasion, the target eNBs desynchronize the NCC value and can only perform horizontal handover key derivation, and thus the future session keys will be vulnerable to be compromised.

(3) Vulnerability to the replay attacks [39]. The purpose of this attack is to destroy the establishment of the secure link between an UE and a target eNB. Firstly, an attacker intercepts an encrypted handover request message, shown in Fig.15, between an UE and a legitimate eNB. When the UE wants to move into a target eNB, the adversary sends the collected previous handover request messages instead of the legitimate one to the target eNB. Then, the target eNB regards the received key K_{eNB} in the previous message as the link key, and sends back the NCC value in previous message to the UE. Upon receiving the NCC value from the target eNB, the UE checks if the received NCC is equal to the value stored in the UE. Since the received NCC value comes from the previous message, the check is failure. Thus, the security connection between the UE and the target eNB will not be established and the UE has to launch a new handover procedure.

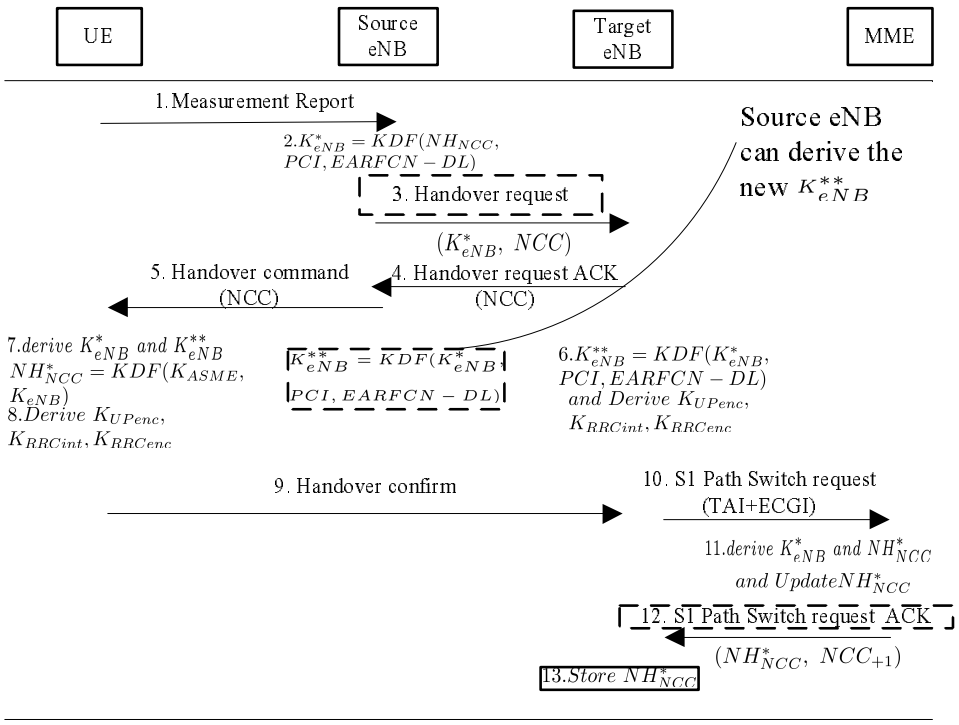

Fig. 15. Inter-eNB Handover

D. Vulnerability in IMS Security Mechanism

The IMS introduced by the 3GPP committee, works based on the SIP and IP. Due to its connection to the Internet directly, the IMS is vulnerable to several types of attacks. 3GPP committee has employed the IMS AKA scheme to ensure the IMS security. However, IMS security mechanism specified by the 3GPP has some vulnerability found.

(1) The authentication procedure in the IMS has increased the energy consumption of a UE and the system complexity [40]. An IMS UE needs to execute two AKA protocols, the EPS AKA in the LTE access authentication and the IMS AKA in the IMS authentication, which brings high energy consumption for the energy limited UEs and thus reduces the battery life of the UEs. In addition, these two AKA procedures share many similar operations, which increase the overall system complexity and results in quality of service (QoS) degradation.

(2) The IMS AKA works based on the EAP AKA scheme [41]. Thus, similar to the EAP AKA, the IMS AKA has several shortcomings such as vulnerability to the MitM attacks, lack of SQN synchronization, and extra bandwidth consumption.

(3) The IMS security mechanism is vulnerable to several types of DoS attacks [42]. For example, after receiving a register request from an IMS UE, as shown in Fig. 7, the P-CSCF/MME sends the request to the core network (I-CSCF/S-CSCF/HSS) to implement an access authentication. In this procedure, an adversary could flood the I-CSCF/S-CSCF/HSS by sending correct packets with invalid IMSI/IMPI.

E. Vulnerability in HeNB Security Mechanism

The 3GPP committee has decribed the threats to the HeNBs and the requirements of the HeNB security [12]. Most of the security vulnerabilities defined in [12] arise from the insecure wireless links between the UE and the HeNB and the backhaul between the HeNB and the EPC, which are susceptible to many kinds of attacks because the data and conversations are vulnerable to interception and eavesdropping over these links. To overcome these vulnerabilities, the corresponding counter-measures have been discussed by the 3GPP committee [12]. However, it is explored that the current 3GPP specification has still not addressed some requirements of the HeNB security.

(1) Lack of a mutual authentication between the UE and the HeNB. It is pointed out in [43] that the current HeNB security mechanism cannot prevent various protocol attacks including eavesdropping attacks, MitM attacks, masquerading attacks and compromising subscriber access list because it does not have vigorous mutual authentications between the UE and the HeNB. In addition, the HeNB is not sufficiently a trust party if the core network and OAM authenticate it independently because the honesty between them is not valid in the IP based network.

(2) Vulnerability to DoS attacks. The HeNB architecture in the LTE network is subject to DoS attacks [44]. Due to the characteristics of a small size with low cost, it is a good alternative for mobile operators to make a large scale deployment of the HeNBs, which can avoid expensive upgrades to the backbone connections and meet the increasing need for data rates. However, because of the exposure of the entrance points of core network to the public Internet, it is vulnerable to several Internet-based attacks, especially, DoS attacks.

F. Vulnerability in MTC Security Architecture

The introduction of the MTC into the LTE systems remains in its infancy. Different from the H2H communication de-

signed in the current 3GPP networks, the MTC involves a lot of unique features such as massive number of devices, small and infrequent data transmissions, distinct service scenarios and fewer opportunities for recharging the devices, which bring unprecedented challenges for the 3GPP to achieving its standardization. Thus, the current LTE network needs to overcome a lot of technical obstacles in the system architecture, air interface, radio resource and QoS management in order to promote the rapid development of the MTC. In recent years, a lot of solutions [45]–[47] have been proposed to address above issues. The 3GPP committee has also described the MTC architecture, service requirements and many system improvements for the MTC [7], [48]. However, the security issues inherent in the MTC have not been well explored by the 3GPP committee and other researchers.

The 3GPP committee has provided the overview of the MTC security architecture as shown in Fig. 10 and discussed some secure threats, requirements and the corresponding solutions for the MTC security [10]. However, there are still many issues for the MTC security architecture to be further improved. For example, it lacks security mechanisms for the MTC between the MTC device and the ePDG for non-3GPP access, the MTC between the MTC applications and the 3GPP networks and the MTC between the MTC applications and the MTC Devices (i.e. A3, B2, and C2 in Fig. 10). In addition, there is no any specific mechanism to ensure the secure communication among MTC devices. Furthermore, in order to support diverse MTC features, the LTE system architecture will be improved, which may incur some new security issues. Thus, the 3GPP committee needs to further investigate the security aspects of the MTC.

There are few literatures on the MTC security addressed in [49], [50]. The security threats in the MTC have been analyzed in [49] and found that the MTC devices are extremely vulnerable to several types of attacks such as physical attacks, compromise of credentials, protocol attacks and the attacks to the core network because the MTC devices are typically required to be low capabilities in terms of both energy and computing resources, deployed without human supervision for a long time. It is indicated in [50] that simultaneous authentication of a multitude of MTC devices can incur signaling overload between an HSS and the MME when they simultaneously request to access to the network.

V. Solutions to the Related Security Issues

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

A. LTE System Architecture

On the LTE system architecture, a new simple and robust handover authentication scheme based on improved proxy signature has been proposed in [38], which can be applied to all of the mobility scenarios including the handovers between the HeNBs, the handovers between the eNBs and the HeNBs, the handovers between the eNBs and the inter-MME handovers. By the scheme, a UE and the target eNB or HeNB can directly accomplish a mutual authentication and establish a session key with their long term secret keys generated by the proxy signatures when the UE enters to the coverage of the target eNB or HeNB. Therefore, it has a simple authentication process without a complex key management and can achieve desirable efficiency. Subsequently, a fast and secure handover authentication scheme has been proposed to achieve seamless handovers between heterogeneous access systems in the LTE networks [51]. By the scheme, the E-UTRAN, the trusted non-3GPP access networks and the ePDG for untrusted non-3GPP access networks are collectively referred to as access points (APs). When a UE moves into the coverage of a new AP, the UE and the new AP can implement an authenticated key agreement using their long-term keys generated by Key Generate Centre (KGC) to derive their shared session key only with 3-handshake without contacting any other third party. The scheme in [51] can provide a robust security protection and ideal efficiency and can be applied to all of the mobility scenarios between the E-UTRAN and the non 3GPP access networks in the LTE networks. However, due to the use of the technique of proxy signature and Identity-based cryptography (IBC), both of these two schemes may incur a lot of computational costs and battery depletion, which is not feasible to the mobile devices with resource constraints. In addition, they may suffer compatible problems in the LTE networks.

B. LTE Cellular Security

In the LTE cellular system, a hybrid authentication and key agreement and authorization scheme based on Trust Model Platform (TMP) and Public Key Infrastructure (PKI) for 4G mobile networks has been proposed in [52]. By the scheme, due to the adoption of the concept of trusted computing and PKI, it can provide considerable 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 based on self-certified public key (SPAKA) has been proposed for 4G wireless systems in [53]. The scheme generates a public key broadcast protocol based on a probabilistic method for a UE to identify the genuine base station, and thus overcomes the shortcomings of 3G AKA scheme. In addition, three authentication protocols including register authentication, re-authentication and handover authentication have been presented respectively for different authentication scenarios. A Security Enhanced Authentication and Key Agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI) has been proposed in [54]. The scheme ensures the security of user identity and the exchanged message with limited energy consumption by using Ellipse Curve Cipher (ECC) encryption. The schemes in [37], [55] have analyzed the threats and attacks in the 3G-WLAN interworking and have proposed new access authentication and key agreement protocols based on the EAP-AKA. Both of the two schemes employ the Elliptic Curve Diffie-Hellman (ECDH) with symmetric key cryptosystem to overcome the vulnerabilities presented in the EAP-AKA protocol. It has been pointed out in [56] that the SE-EPS AKA protocol is vulnerable to brute force and intelligent force attacks and thus

it cannot guarantee the security of the user identity. Then, an ensured confidentiality authentication and key agreement (EC-AKA) has been proposed to enhance the user's confidentiality. By the scheme, all the AKA messages are fully protected on the integrity by encryption, which can prevent the disclosure of identity of the users and the users being tracked. All of these above schemes in [37], [52]–[54], [56] employ the public-key based protection mechanisms to overcome the shortcoming of the EPS AKA protocol, and thus can achieve a mutual authentication and ensure the security communication between the UE and HSS/AuC by the use of the UE and/or the HSS/AuC of public key certificates. However, it will cause a large number of computational costs, storage costs and communication costs for mobile devices with resource limitation. In addition, in an open nature environment of the LTE network, the public key infrastructure should be spanning across all operators with mutual roaming agreements. Therefore, the LTE network needs to take a large number of deployment overheads to establish the public key infrastructure. Indeed, the 3GPP seems reluctant to mandate such an expensive infrastructure [57]. An EAP-Archie method [58] has been introduced to ensure the access layer security in the LTE networks. By using the AES ciphering, the scheme in [58] can achieve a mutual authentication and key agreement between the users and the network access layer. However, this scheme faces the same vulnerabilities as the EPS AKA protocol, which cannot prevent the LTE network against the disclosure of the user identity and spoofing attacks. A slightly modified version of the EPS-AKA protocol has been presented in [36]. The scheme introduces a new subscriber module ESIM instead of the USIM and provides a direct online mutual authentication between the ESIM and the MME/HSS to overcome the shortcomings of the EPS-AKA protocol only with minor modifications of the access security architecture. However, it may suffer compatible problems in the LTE networks due to the use of the new ESIM. Since the HSS needs to participate in every authentication procedure for each UE, it may incur a large number of communication delays and thus cause signaling congestion on the HSS. In addition, it cannot overcome the disclosure of user identity. An enhanced EPS AKA protocol has been proposed in [35] to improve the performance of the current authentication procedure by increasing a little computation in the SN. By the scheme, the SN/MME generates and stores a lot of authentication vectors (AVs) from the original AVs at the HN/HSS. The scheme in [35] can largely reduce the authentication signaling exchange between the SN and the HN, and thus saves the bandwidth consumption at the HSS/HN. However, this scheme is able to increase the burden of the MME because a lot of AVs will be generated at the MME. In addition, it can only enhance the efficiency of the authentication procedure, while security problems existing in the EPS-AKA procedure cannot be overcome. In [59], the use of the password authentication key exchange by Juggling Password Authenticated Key Exchange (J-PAKE) protocol in the authentication process instead of the EPS AKA protocol to provide a stronger security protection has been proposed. The J-PAKE [60] is a password authentication keying agreement protocol to provide a zero-knowledge proof using a shared key that is never sent over the transmission medium. However, it has only addressed the use of J-PAKE in the LTE networks without the introduction of the implementation of it to ensure secure communication and the reasons that the J-PAKE scheme can provide a stronger security than the EPS AKA. In addition, it cannot handle the security issue presented in the EPS AKA protocol, i.e. identity protection.

C. LTE Handover Security

For the secure LTE handovers, a hybrid authentication and key agreement scheme has been proposed to support globe mobility and secure communications in 4G wireless systems [61]. The scheme in [61] associates a dynamic password with a public-key to provide a lightweight authentication and a non-repudiation service. In addition, by adopting the public key broadcast protocol designed as a part of the scheme, a mutual authentication between the UE and foreign network (FN) can be achieved without the use of certificate. However, it may incur a lot of computational costs and storage costs due to the use of public cryptography, and thus brings a lot of difficulty to support the seamless handovers in 4G wireless systems. A security roaming and vertical handover scheme among several different access technologies in 4G wireless networks has been proposed in [62]. The scheme in [62] designs a global authentication protocol to enable a vertical handover between heterogeneous access systems including GSM, UMTS, WiFi and WiMAX without requiring a prior subscription to the visited networks. However, this scheme focuses only on the handovers between WiMAX/ WiFi and GSM/ UMTS and covers the security issues existing in the GSM systems. The handovers between the LTE/LTE-A systems and other access networks have not been addressed, where the LTE/LTE-A systems are much different from the GSM and the UMTS in the handover procedures and security vulnerabilities. A new re-authentication protocol to secure interworking and roaming from the 3GPP LTE to the WLAN has been proposed in [63]. The scheme improves the EAP-AKA protocol and adopts hybrid unit to provide the secure 3GPP LTE-WLAN interworking. However, by this scheme, a new entity, Hybrid Interconnection Unit (HIU), needs to deployed to serve as a relay station between the LTE network and the WLAN, which may require a lot of deployment costs and changes of the existing architecture and thus increase the complexity of the entire system. In addition, handovers from WLAN to 3GPP LTE have not been presented. An optimized fast handover mechanism has been presented in [64] to handle handovers between the 3GPP and the non-3GPP networks. By the scheme, it employs a security context transfer mechanism for the handovers between the 3GPP networks and the trusted non-3GPP networks and a pre-authentication mechanism for the handovers between the 3GPP and the untrusted non-3GPP networks to reduce the handover latency without compromising the security level. By adopting the current approaches including security context transfer and pre-authentication mechanism, the scheme in [64] proposes a good idea to achieve seamless mobility between the 3GPP networks and the non-3GPP networks. However, there are still a lot of issues to be addressed, such as security, performance and compatible problems, etc. Five fast and secure

re-authentications protocols for the LTE subscribers to perform handovers between the WiMAX systems and the WLANs have been proposed in [65], which avoid contacting authentication servers in the LTE networks during the handovers. By these schemes, the EAP-AKA protocol for the handovers from a WiMAX system to a WLAN and Initial Network Entry Authentication (INEA) protocol for the handovers from a WLAN to a WiMAX system can be improved by including extra security parameters and keys to speed up the re-authentications in the future WiMAX-WLAN handovers. The modified version of the EAP-AKA and INEA has the same messaging sequences as that in the standard EAP-AKA and INEA, which can avoid interoperability problems with other services without a loss of capabilities due to the modifications. The scheme in [65] can achieve an outstanding performance in terms of the re-authentication signaling traffic and the re-authentication delay compared with the current 3GPP standard protocols and can provide several security features including forward and backward secrecy. However, the scheme can only support single-hop communications between a UE and AP/Base Station (BS). Multi-hop wireless communications and security mechanisms to protect the multi-hop messages need to be investigated.

D. IMS Security

On the IMS security, many one-pass authentication schemes in the UMTS have been proposed in order to reduce the authentication signaling costs [66]–[69]. An improved one-pass AKA procedure for the next generation networks (NGNs) has been presented in [70]. By the scheme, the security key binding between the initial authentication and the second authentication can be implemented so that the user can be authenticated by using the (IMPI, IMSI) pair at the IMS service layer authentication without the security protection between the UE and the P-CSCF, and thus it can reduce significantly the authentication overhead compared with the multi-pass authentication procedure. However, this approach is very vulnerable to the fraudulent use of IMS services, eavesdropping attacks, fake server attacks, and temporary cheat attacks. An Improved AKA (I-AKA) authentication protocol has been addressed in [40] for the LTE networks to reduce energy consumption. By the scheme, the network layer and the IMS layer authentication can be executed by using the IMPI only without the IMSI of the users. After the network layer authentication is successful, the P-CSCF can directly obtain user's AV from the MME to generate the valid encryption and integrity keys with the user in the IMS layer authentication procedure without contacting the HSS. Therefore, the scheme can avoid double execution of the AKA protocol and thus largely reduce the signaling overhead. However, the scheme may bring some problems in the use of normal network services because the only IMPI has been used to achieve the network layer authentication. A new IMS service authentication scheme has been proposed in [71] using IBC to enhance the security of the IMS authentication process. By adopting the concept of the IBC and the Elliptic Curve Cryptography (ECC), the scheme allows the personalization of the IMS services by authenticating the users in a personal manner during the services access and provides a robust security protection. However, the scheme may incur a lot of computational costs and storage costs due to the use of IBC and ECC, which is not feasible to the mobile devices with resource limitations. An improved IMS authentication mechanism for the 3G-WLAN networks by promoting an efficient key re-use for a mobile user has been proposed in [72]. By the scheme, the authentication vectors and encryption keys obtained in the initial network authentication procedure will be re-used in the IMS authentication by securely transporting them from the Home AAA (HAAA) to the S-CSCF via the HSS. Therefore, the scheme can largely reduce the time required to derive authentication vectors and thus avoid extra overheads and QoS degradation when the user moves from one WLAN domain into another without the change of the existing architecture. However, it cannot provide a mutual authentication between the UE and the S-CSCF in the proposed IMS authentication procedure.

E. HeNB Security

For the HeNB systems, the issues of the authentication and access control of the HeNB users have been addressed in [73]. The paper provides an overview of the ongoing work on the HeNB standardization in the 3GPP, especially on the access control strategy. When a UE wants to access to the network via a HeNB, the CN is additionally responsible for performing the access control for the UE. In order to perform access control, the CN is required to maintain and update a list of CSG identities named as a allowed CSG list to which the UE is subscribed. Each entry in the list associates the CSG identity with a PLMN identity. The information contained in the UE allowed CSG list is stored as subscription data for the UE in the HSS and provided to the MME for access control. Before the mutual authentication with the UE, the MME needs to check whether the UE is allowed to access the HeNB based on the allowed CSG list. A vigorous mutual authentication and access control mechanism has been proposed to guarantee secure communication for the HeNB by adapting a proxy-signature [43]. By the scheme, the OAM and the core network (CN) have a contractual agreement on the installation, operation and management of the HeNB by issuing a proxy-signature to each other. Then, the OAM re-delegates its proxy-signing capability to a HeNB. The CN also re-delegates its proxy-signing capability to the HeNB and issues its own signature to a UE. Finally, the mutual authentication between the UE and the HeNB can be achieved with the proxy signature on behalf of the OAM and the CN. The scheme can prevent various protocol attacks such as masquerading a valid HeNB, MitM attacks and DoS attacks. However, it incurs a large amount of computational costs and storage costs and requires several changes to the existing architecture due to the use of proxy signature, which makes the system more infeasible in real scenarios. Significant threats to the security and the privacy of the HeNB-enabled LTE networks have been reviewed in [44] with novel research directions tackling some of these threats. The paper has presented a solution to the issue of identity and location tracking at the air interface by assigning and changing identifiers based on the context. This approach provides a

new identity protection strategy named as user-triggered ID change strategy instead of network controlled strategy, where the mobile devices can dynamically decide when to change identifiers based on their own observation of the surroundings, such as node density, device speed and mobility pattern. In addition, a protection mechanism against DoS attacks with a HeNB deployment in the LTE architecture has also been suggested. It has been pointed out that the solutions relied on the cooperation among several participating entities such as Internet Service Provider (ISPs) could be as an efficient protection against DoS attacks.

F. MTC Security

In the MTC, the threats, the security requirements, and the corresponding solutions of the MTC security have been discussed in [74]. It is advised in [74] that the Trust Environment (TrE) can be embedded within the MTC devices to protect the security of the MTC devices, which can provide more robust protected functions for the access authentication and support several cryptographic capabilities including the symmetric and asymmetric encryption and decryption compared with the current UICC. A group-based authentication and key agreement approach for a group of UEs roaming from the same HN to a SN has been presented in [50]. By the scheme, multiple UEs, which belong to the same HN, can form a group. When the first UE in a group moves to the SN, the SN obtains the authentication information for the UE and other members from the concerned HN by performing a full authentication. Thus, when other group members visit, the SN can authenticate them locally without the involvement of the HN. The scheme can reduce the communication cost between the HN and the SN. However, there are still some problems such as signaling network congestions at the SN nodes when multiple devices move to the SN simultaneously because each device still requires 4 signaling messages to accomplish an access authentication. A new mass device access authentication scheme based on an aggregate signature has been proposed in [75]. By the scheme, a large number of MTCDs is initialized to form an MTC group to choose a group leader. When multiple MTCDs in the MTC group request to access to the network simultaneously, the MME authenticates the MTC group by verifying the aggregate signature generated by the group leader on behalf of all the group members. Then each MTCD trusts the MME by verifying the Elliptic Curve Digital Signature Algorithm (ECDSA) signature from the MME via the group leader. Finally, a distinct session key between each MTCD and the MME will be established according to the different key agreement parameters sent from the requesting MTCDs. The scheme cannot only achieve a mutual authentication and a key agreement between each MTCD in a group and the MME at the same time, but also can greatly reduce the signaling traffic and thus avoid network congestions. However, it may bring a lot of computational costs due to the use of the ECDSA signature and the aggregate signature. In addition, the scheme requires the devices to support both LTE and WiFi communications, which is unlikely that all MTCDs are required to equip with both network interfaces. A Machine-to-Machine communication model based on 4G cellular systems has been introduced in [76], [77], where secure communication between two MTC devices can be achieved through the establishment of ad hoc networks within the coverage of the LTE systems. By the proposed model, the MTCDs are capable of communicating in both cellular and ad hoc modes. If a MTCD is located in the coverage of the LTE/LTE-A network but far from other devices, it will use LTE/LTE-A network resources. Otherwise, it tends to communicate with nearby devices, where they form an ad hoc network wherever possible. However, the case where a device is in the range of both of other devices and the coverage of the LTE/LTE-A network has not been addressed in the proposed model. In addition, the introduction of ad hoc networks may incur much more security issues which will have much impact on the integration of the ad hoc architecture into the LTE/LTE-A networks. It requires further network modifications and optimization to best integrate the M2M communications into the LTE/LTE-A networks.

VI. Open Research Issues

According to the above analysis, a lot of security issues for the LTE/LTE-A networks are still open research issues without perfect resolutions. 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.

(1) The design of the MTC security mechanisms in the LTE/LTE-A networks will be the major work of the future research for the LTE security because the introduction of the MTC into the 3GPP networks remains in its early stage of the development. There are still many issues as open challenges for the practical enforcement of the MTC security. The following unexplored MTC features are important issues for the future research work.

1) 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 MTC devices send the collected information to a MTC application server via the 3GPP network. In emergency situations, an MTC device can directly send a patients 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.

2) The ratio of encryption overhead and the amount of information to be transmitted must be considered. According to the current LTE security schemes, both of the control signaling and the payloads need to be encrypted with integrity checking operations. However, for the MTC devices holding the features of small data transmission, the cost of encryption and integrity checking operations might be relatively higher comparing to that of the transmitting small-sized payload.

Thus, the LTE networks need to reduce the overhead of the cryptographic operations to achieve a trade-off between the security functionality and the system performance or system cost.

3) Novel access authentication schemes for congestion avoidance for the simultaneous authentication of multiple devices are required. In the 3GPP systems, a lot of MTC applications should be supported simultaneously. For example, many mobile payment terminals could become active on a public holiday or a large number of metering or monitoring devices become active at the same time almost after a period of power outage or at precisely synchronous time intervals. In these cases, since a mass of devices sends messages to the network at the same time, a signaling overload and congestion can be triggered over the network at the MME and the HSS to cause the network be blocked to provide services for these MTC devices. In order to combat the congestions, there are two approaches suggested by the 3GPP committee [10]. Firstly, relevant network nodes should be able to reject or prevent connection requests. The method will bring a new problem that non-MTC traffic or traffic from other MTC devices may be suffered. The rejected connections from a particular MTC device may contain some significant messages, which cannot be timely delivered by the network and thus QoS for the MTC users will be impacted seriously. Another way is to make a large number of MTC devices to form a MTC group and then the LTE network can handle the MTC group orderly instead of messy individual devices. A MTC group can be constructed by multiple devices in the neighborhood, or holding the same features or from the same MTC users. The 3GPP committee has specified a mechanism to form a MTC group. However, it has only addressed the issues of communications between MTC devices and the MTC server such as group based policing and group based addressing without consideration of security schemes between them. Since it is the most important for a group of MTCDs to implement an access authentication with the network before any communication, new access authentication and key agreement schemes are required to avoid a signaling congestion when a large number of MTCDs connect to the network at the same time. The current schemes in [50], [75] have employed a group-based approach to simplify the access authentication process. However, there are still vulnerabilities due to their inherent features. In [50], since each device still needs to send an independent authentication request message to the network by the solution, the network congestion at the SN nodes cannot be avoided when many MTC devices simultaneously attach to the network. In [75], due to adopting the technique of public cryptography including the ECDSA signature and the aggregate signature, the network has to perform a lot of computation to authenticate the MTC group, and thus the burden of the network cannot be alleviated. Therefore, to design efficient and secure group-based access authentication schemes for mass device connection is still a key issue for MTC in the LTE-A networks.

4) End-to-end secure mechanisms for MTC are required. In the future, secure communication among MTC devices without an MTC server is likely to become a dominant communication paradigm. Thus, the LTE networks need to establish end-to-end secure mechanisms for machine-to-machine (M2M) communications between two MTC devices. The current schemes in [76], [77] have designed an M2M communication model by combining the LTE networks with ad hoc networks. However, it may bring much more threats existing in the integration architecture due to the introduction of the ad hoc architecture into the LTE/LTE-A networks. Therefore, further network modifications and optimization are required to tackle new threats in the integration and to optimize the protocols and interconnections to best integrate M2M communications into the LTE/LTE-A networks.

5) Secure mechanisms for supporting restricted mobility and the high speed mobility of the MTC devices are required. The service requirements and solutions for the MTC devices with low-mobility features in the LTE networks have been discussed in [48]. However, the service requirements of the restricted mobility and the high speed mobility of the MTC devices have not been described. In the restricted mobility case, e.g., a building surveillance system with asset management, a secure protection mechanism to monitor the location change of the MTC devices and avoid malicious mobility of the MTC devices in a LTE network needs to be designed. In the high speed mobility case, tracking some MTC devices such as an animal tracking by MTC devices in the natural world with high mobility requires extra low power consumption because it is almost impossible to replace the battery or recharge the battery for the MTC devices. Thus, extra low power consumption for the MTC devices is required in the design of security mechanisms.

(2) On other aspects of LTE security, there are still a lot of issues to be addressed, which need further research work for the improvements.

1) On the LTE security architecture, more security mechanisms need to be designed to protect the communications between the UEs, eNBs (HeNB) and the EPC from traditional protocol attacks and physical intrusions in the LTE networks. In addition, more efficient handover authentication architectures need to be designed to achieve the secure seamless handovers between the HeNBs and the eNBs and the handovers between 3GPP networks and non-3GPP networks. Although some handover authentication protocols between the HeNBs and the eNBs and between heterogeneous access systems in the LTE networks have been proposed in [38], [51], there are some weaknesses such as inefficiency and incompatibility due to the use of public cryptography such as proxy signature and IBC.

2) On the LTE cellular security, the EPS AKA scheme in the LTE networks needs to be further enhanced to be able to prevent the disclosure of user identity, the DoS attacks and other malicious attacks with the improved performance of the authentications. The most of the current solutions in [36], [51]–[55] have adopted the public key mechanism to avoid various vulnerabilities, which bring a lot of computation consumption. The other improved schemes in [35], [36], [58], [59] are not suitable for the access scenarios in the LTE networks due to their inherent vulnerabilities. Moreover, more secure access authentication mechanisms need to be designed when a UE accesses to the EPC via non-3GPP networks.

3) On the LTE handover security, the key management

mechanisms and handover authentication procedures need to be further enhanced in the LTE networks to prevent several protocol attacks including the de-synchronization attacks and reply attacks. The current scheme in [61] is not suitable for the mobility scenarios in the LTE networks due to the employment of the public cryptography technique. In addition, some other handover authentication protocols in [62]–[65] have been proposed for some specific mobility scenarios between heterogeneous access systems, such as handovers between WiMAX/ WiFi and GSM/ UMTS in [62], handovers from LTE to WLAN in [63], handovers between 3GPP networks and non-3GPP networks in [64], and handovers between WiMAX and WLAN in [65]. However, there are still a lot of issues need to be further investigated. The survey in [15] has discussed an interesting way to overcome the vulnerabilities of the mobile WiMAX systems that may lead to distributed DoS (DDoS) attacks. By the approach, some discarded information such as the upper 64 bits of the Hash Message Authentication Code (HMAC)/Cipher-based MAC (CMAC) could be used as a proof that a UE has already registered to the networks. When the UE roams into a new BS, an Access Services Network Gateway (ASN GW) sends the preceding HMAC/CMAC to the new BS, and then the new BS checks its validity. This approach can achieve a lightweight handover authentication and withstand the DDoS attacks in the WiMAX systems, which may bring us some inspiration for the future design of secured handover authentication schemes in the LTE networks.

4) On the IMS security, fast and robust IMS access authentication mechanisms need to be designed to simplify the authentication process and prevent DoS attacks and other malicious attacks in the LTE networks. A lot of solutions [40], [70]–[72] have been proposed to enhance the IMS security. However, there are still some security issues unsolved by these schemes and vulnerabilities exist such as the fraudulent use of IMS services, temporary cheat attacks, lack of mutual authentications, and so on.

5) On the HeNB security, simple and robust mutual authentication mechanisms between the UEs and the HeNBs need to be designed to prevent various protocol attacks. Due to the use of the proxy signature, the current solution in [43] needs a lot computational consumption and is not compatible to the LTE architecture specified by the current 3GPP standard.

VII. Conclusion

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

Acknowledgment

This work is supported by 973 National Basic Research Program of China grant 2012CB316100. And it is also supported by the National Natural Science Foundation of China grant 61102056, the Fundamental Research Funds for the Central Universities K50511010001, National 111 Project B08038 and Program for Changjiang Scholars and Innovative Research Team in University (PCSIRT 1078).

Appendix A
Abbreviation

AAA	Authentication, Authorizing, and Accounting
AP	Access Point
AV	Authentication Vector
AS	Access Stratum
CDMA	Code Division Multiple Access
CK	Ciphering Key
CS	Circuit-Switched
CSCF	Call Service Control Function
CSG	Closed Subscriber Group
EAP-AKA	Extensible Authentication Protocol-Authentication and Key Agreement
EAP-AKA'	Improved EAP-AKA
ECC	Ellipse Curve Cipher
EDGE	Enhanced Data Rate for GSM Evolution
eNB	eNodeB
EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
EPS AKA	Evolved Packet System Authentication and Key Agreement
E-UTRAN	Evolved-Universal Terrestrial Radio Access Network
FN	Foreign Network
GERAN	GSM EDGE Radio Access Network
GPRS	General Packet Radio Service
GUTI	Globally Unique Temporary Identity
GSM	Global System of Mobile communication
HeNB	Home eNodeB
HN	Home Network
H2H	Human to Human
IBC	Identity Based Cryptography
I-CSCF	Interrogating-CSCF
IMPI	IM Private Identity
IMS	IP multimedia subsystem

IK	Integrity Key
IKEv2	Internet Key Exchange Protocol Version 2
ISIM	IMS Subscriber Identity Module
KGC	Key Generate Centre
LTE/SAE	Long Term Evolution/System Architecture Evolution
LTE-A	LTE-Advanced
ME	Mobile Equipment
MME	Mobility Management Entity
MTC	Machine Type Communication
M2M	Machine to Machine
NAS	None Access Stratum
NCC	NH chaining counter
NDS	Network Domain Security
NGN	Next Generation Network
NH	Next Hop
P-CSCF	Proxies-CSCF
PDN GW	Packet Data Network Gateway
PKI	Public Key Infrastructure
PS	Packet-Switched
RNC	Radio Network Control
S-CSCF	Serving-CSCF
SGW	Serving Gateway
SeGW	Security Gateway
SGSN	Service GPRS Supporting Node
SIP	Session Initiation Protocol
SN	Serving Network
SN ID	Serving Network Identity
SQN	Sequence Number
TrE	Trust Environment
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UMTS-AKA	UMTS-Authentication and Key Agreement
USIM	Universal Subscriber Identity Module
UTRAN	UMTS Terrestrial Radio Access Network
VoIP	Voice over IP
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
OAM	Operation, Administration and Maintenance
QoS	Quality of Service

REFERENCES

[1] 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.

[2] 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, June 2010, pp.10-22.

[3] U. Meyer and S. Wetzel, "A Man-in-the-Middle Attack on UMTS," Proc. 3rd ACM Workshop on Wireless Security, Octomber 2004, pp. 90-97.

[4] M. Zhang and Y. Fang, "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Commun., Vol.4, No.2, Mar. 2005, pp. 734- 742.

[5] C. Tang and D.O. Wu, "An Efficient Mobile Authentication Scheme for Wireless Networks," IEEE Trans. Wireless Commun., Vol.7, No.4, April 2008, pp.1408-1416.

[6] 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, Sep. 2012.

[7] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC) (Rel 12), 3GPP TS 22.368 V12.0.0 Sep. 2012.

[8] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB) (Rel 11), 3GPP TS 22.220 V11.6.0 Sep. 2012.

[9] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network;Evolved Universal Terrestrial Radio Access (E-UTRA); Further advancements for E-UTRA physical layer aspects (Rel 9), 3GPP TR 36.814 V9.0.0 March 2010.

[10] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of Machine-Type Communications (Rel 12), 3GPP TR 33.868 V0.10.0, Sep. 2012.

[11] 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Security of H(e)NB; (Rel 8), 3GPP TR 33.820 V8.3.0 November 2009

[12] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (Rel 11), 3GPP TS 33.320 V11.6.0 June 2012.

[13] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on LTE relay node security (Rel 10), 3GPP TR 33.816 V10.0.0 March 2011.

[14] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," Proc. IEEE Globecom Workshops, November 2007, pp.1-6.

[15] C. Kolias, G. Kambourakis, and S. Gritzalis, "Attacks and Countermeasures on 802.16: Analysis and Assessment", IEEE Communications Surveys and Tutorials, 2013, IEEE Press.

[16] C.B. Sankaran, "Network Access Security in Next-generation 3GPP Systems: A Tutorial," IEEE Commun. Mag., Vol.47, No.2, February 2009, pp.84-91.

[17] N. Seddigh, B. Nandy, R. Makkar, and J.F. Beaumont, "Security Advances and Challenges in 4G Wireless Networks," Proc. Eighth Annual International Conference on Privacy Security and Trust (PST), August 2010, pp.62-71.

[18] J. Zheng, "Research on the Security of 4G Mobile System in the IPv6 Network," Recent Advances in Computer Science and Information Engineering, Vol. 126, 2012, pp. 829-834.

[19] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); (Rel 11), 3GPP TS 23.228 V11.6.0 ,Sep. 2012.

[20] 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 June 2012.

[21] 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 Sep. 2012.

[22] 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, June 2012.

[23] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; (Rel 11), 3GPP TS 36.300 V11.3.0 Sep. 2012.

[24] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Rel 11), 3GPP TS 23.401 V11.3.0 Sep. 2012.

[25] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Rel11), 3GPP TS 23.402 V11.4.0 Sep. 2012.

[26] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); (Rel 11), 3GPP TS 24.229 V11.5.0 Sep. 2012.

[27] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;3G Security; Access security for IP-based services; (Rel 12), 3GPP TS 33.203 V12.1.0 Sep. 2012.

[28] 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 (SSST 2009), March 2009, pp.94-97.

[29] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Security in 4G Systems: Unveiling the Challenges," Proc. Sixth Advanced International Conference on Telecommunications (AICT), May 2010, pp.439-444.

[30] 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.

[31] D. Forsberg, "LTE Key Management Analysis with Session Keys Context", Computer Communications, Vol. 33, No.16, Octomber 2010, pp 1907-1915.

[32] D. Forsberg, L. Huang, K. Tsuyoshi, and S. Alanara, "Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface," Proc. Personal, Indoor and Mobile Radio Communications (PIMRC), Septmber 2007, pp.1-5.

[33] T. Ahmed, D. Barankanira, S. Antoine, X. Huang, and H. Duvocelle, "Inter-system Mobility in Evolved Packet System (EPS): Connecting Non-3GPP Accesses," Proc. Intelligence in Next Generation Networks (ICIN), Octomber 2010, pp.1-6.

[34] D. Yu and W. Wen, "Non-access-stratum Request Attack in E-UTRAN," Proc. Computing, Communications and Applications Conference (ComComAp), January 2012, pp.48-53.

[35] M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks," Proc. IEEE 3rd International Conference on Communication Software and Networks (ICCSN), May 2011, pp.557-563.

[36] G.M. Koien, "Mutual Entity Authentication for LTE," Proc. 7th International Wireless Communications and Mobile Computing Conference (IWCMC), July 2011, pp.689-694.

[37] H. Mun, K. Han, and K. Kim, "3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement Based on EAP-AKA," Proc. Wireless Telecommunications Symposium (WTS), April 2009, pp.1-8.

[38] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A Simple and Robust Handover Authentication between HeNB and eNB in LTE Networks," Computer Networks, Vol. 56, No. 8, May 2012, pp. 2119-2131.

[39] C-H. Han, "Security Analysis and Enhancements in LTE-Advanced Networks", Ph.D. Dissertation, Department of Mobile Systems Engineering, The Graduate School, Sungkyunkwan University, 2011, http://hit.skku.edu/ hedwig/pds/dissertation.pdf.

[40] L. Gu and M.A. Gregory, "A Green and Secure Authentication for the 4th Generation Mobile Network," Proc. Australasian Telecommunication Networks and Applications Conference (ATNAC), November 2011, pp.1-7.

[41] G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, "Advanced SSL/TLS-based Authentication for Secure WLAN-3G Interworking," Proc. IEE Communications, Vol.151, No.5, October 2004, pp. 501- 506.

[42] G. Kambourakis, C. Kolias, S. Gritzalis, and J. Park, "DoS Attacks Exploiting Signaling in UMTS and IMS," Computer Communications, Vol. 34, No. 3, March 2011, pp. 226-235.

[43] C. K. Han, H. K. Choi and I. H. Kim, "Building Femtocell More Secure with Improved Proxy Signature", Proc. IEEE GLOBECOM 2009, USA, December 2009, pp. 1-6.

[44] I. Bilogrevic, M. Jadliwala and J-P. Hubaux, "Security and Privacy in Next Generation Mobile Networks: LTE and Femtocells," Femtocell Workshop, June 2010.

[45] Y. Chen and W. Wang, "Machine-to-Machine Communication in LTE-A," Proc. Vehicular Technology Conference Fall (VTC 2010-Fall), Septmber 2010, pp.1-4.

[46] Z.M. Fadlullah, M.M Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward Intelligent Machine-to-Machine Communications in Smart Grid," IEEE Commun. Mag., Vol.49, No.4, April 2011, pp.60-65.

[47] Y. Zhang, R. Yu; S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M Networks: Architectures, Standards, and QoS Improvement," IEEE Commun. Mag., Vol.49, No.4, April 2011, pp.44-52.

[48] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Improvements for Machine-Type Communications (Rel 11), 3GPP TR 23.888 V11.0.0, Sep. 2012.

[49] I. Cha, Y. Shah, A.U. Schmidt, A. Leicher, and M.V. Meyerstein, "Trust in M2M Communication," IEEE Veh. Technol. Mag.,Vol.4, No.3, Septmber 2009, pp.69-75.

[50] Y. W. Chen, J. T. Wang, K. H. Chi, and C. C. Tseng, "Group-Based Authentication and Key Agreement", Wireless Personal Communications, 2010, pp. 1-15.

[51] J. Cao, M. Ma, and H. Li, "An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks," IEEE Trans. Wireless Commun., Vol. 11, No. 10, Oct. 2012, pp 3644-3650.

[52] Y. Zheng, D. He, X. Tang, and H. Wang, "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform," Proc. Fifth International Conference on Information, Communications and Signal Processing, 2005, pp.976-980.

[53] D. He, J. Wang, and Y. Zheng, "User Authentication Scheme based on Self-certified Public-key for Next Generation Wireless Network," Proc. Biometrics and Security Technologies (ISBAST 2008), April 2008, pp.1-8.

[54] X. Li, and Y. Wang, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," Proc. Wireless Communications, Networking and Mobile Computing (WiCOM), Septmber 2011, pp.1-4.

[55] J.V. Franklin and K. Paramasivam, "Enhanced Authentication Protocol for Improving Security in 3GPP LTE Networks," Proc. International Conference on Information and Network Technology (ICINT 2011), 2011.

[56] J. Abdo, H. Chaouchi, and M. Aoude, "Ensured Confidentiality Authentication and Key Agreement Protocol for EPS," Proc. Broadband Networks and Fast Internet (RELABIRA 2012), May 2012, pp.73-77.

[57] G. M. Kien, "Entity Authentication and Personal Privacy in Future Cellular Systems," River Publisher, Oct. 2009.

[58] Z. Shi, Z. Ji, Z. Gao, and L. Huang, "Layered Security Approach in LTE and Simulation," Proc. Anti-counterfeiting, Security, and Identification in Communication (ASID 2009), August 2009, pp.171-173.

[59] C.Vintila, V. Patriciu, and I. Bica, "Security Analysis of LTE Access Network", Proc. The Tenth International Conference on Networks (ICN 2011), January 2011, pp. 29-34.

[60] F. Hao and P. Ryan, "J-PAKE: Authenticated Key Exchange without PKI," Trans. Computational Science XI, LNCS, Vol. 6480, 2010, pp. 192-206.

[61] Y. Zheng, D. He, L. Xu, and X. Tang, "Security Scheme for 4G Wireless Systems," Proc. Communications, Circuits and Systems, May 2005, pp. 397- 401.

[62] N. Krichene and N. Boudriga, "Securing Roaming and Vertical Handover in Fourth Generation Networks," Proc. Network and System Security (NSS '09), Octomber 2009, pp.225-231.

[63] I. Bouabidi, I. Daly, and F. Zarai, "Secure Handoff Protocol in 3GPP LTE Networks," Proc. Third International Conference on Communications and Networking (ComNet), March 2012, pp.1-6.

[64] R. Rajavelsamy and S. Choi, "Security Aspects of Inter-access System Mobility between 3GPP and Non-3GPP networks," Proc. Communication Systems Software and Middleware and Workshops (COMSWARE), January 2008, pp.209-213.

[65] A.A. Al Shidhani and V.C.M. Leung, "Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers," IEEE Trans. Dependable Secure Comput., Vol.8, No.5, Septmber-Octomber 2011, pp.699-713.

[66] Y. Lin, M. Chang, M. Hsu, and L. Wu, "One-pass GPRS and IMS Authentication Procedure for UMTS," IEEE J. Sel. Areas Commun., Vol.23, No.6, June 2005, pp. 1233- 1239.

[67] J. Fu, C. Wu, J. Chen, R. Fan, and L. Ping, "Lightweight Efficient and Feasible IP Multimedia Subsystem Authentication," Proc. Networking and Information Technology (ICNIT), June 2010, pp.139-144.

[68] X. Long and J. Joshi, "Enhanced One-Pass IP Multimedia Subsystem Authentication Protocol for UMTS," Proc. Communications (ICC), May 2010, pp.1-6.

[69] G. Sharma, A. Vidhate, and S. Devane, "Improved One-pass IMS Authentication in UMTS," Proc. Communication Software and Networks (ICCSN), May 2011, pp.244-248.

[70] C. Ntantogian, C. Xenakis, and I. Stavrakakis, "Efficient Authentication for Users Autonomy in Next Generation All-IP Networks," Proc. Bio-Inspired Models of Network, Information and Computing Systems, December 2007, pp.295-300.
[71] M. Abid, S. Song, H. Moustafa, and H. Afifi, "Efficient Identity-based Authentication for IMS based Services Access," Proc. 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM '09), 2009, pp. 260-266.
[72] M.J. Sharma and V.C.M. Leung, "Improved IP Multimedia Subsystem Authentication Mechanism for 3G-WLAN Networks," Proc. Computer Communications Workshops (INFOCOM WKSHPS), April 2011, pp.1000-1005.
[73] A. Golaup, M. Mustapha, and L.B. Patanapongpibul, "Femtocell Access Control Strategy in UMTS and LTE," IEEE Commun. Mag., Vol.47, No.9, Septmber 2009, pp.117-123.
[74] M. Meyerstein, I. Cha, and Y. Shah, "Security Aspects of Smart Cards vs. Embedded Security in Machine-to-Machine (M2M) Advanced Mobile Network Applications", Security and Privacy in Mobile Information and Communication Systems, Vol. 17, 2009, pp. 214-225.
[75] Jin Cao, Maode Ma, and Hui Li, "A Group-based Authentication and Key Agreement for MTC in LTE Networks", Proc. IEEE GLOBECOM 2012, Dec. 2012, accepted for publication.
[76] M. Saedy and V. Mojtahed, "Ad Hoc M2M Communications and Security based on 4G Cellular System," Proc. Wireless Telecommunications Symposium (WTS), April 2011, pp.1-5.
[77] M. Saedy and V. Mojtahed, "Machine-to-Machine Communications and Security Solution in Cellular Systems," International Journal of Interdisciplinary Telecommunications and Networking (IJITN), Vol. 3, No. 2, 2011, pp. 66-75.

Jin Cao Received the B.Sc. degree from Xidian University, China, in 2008. He is currently working toward the Ph.D. degree in Cryptography, Xidian University, China. His interests are in wireless network security and LTE networks.

Maode Ma received his BE degree in computer engineering from Tsinghua University in 1982, ME degree in computer engineering from Tianjin University in 1991 and Ph.D. degree in computer science from Hong Kong University of Science and Technology in 1999. He is a tenured Associate Professor in the School of Electrical and Electronic Engineering at Nanyang Technological University in Singapore. He has extensive research interests including wireless networking, wireless network security and optical networking, etc. He has been a member of the technical program committee for more than 110 international conferences. He has been a technical track chair, tutorial chair, publication chair, and session chair for more than 50 international conferences. He has published more than 130 international academic research papers on wireless networks and optical networks. He currently serves as an Associate Editor for IEEE Communications Letters, an Editor for IEEE Communications Surveys and Tutorials, and an Associate Editor for International Journal of Wireless Communications and Mobile Computing, Journal of Network and Computer Applications, Security and Communication Networks, International Journal of Vehicular Technology, Journal of Computer Systems, Networks, and Communications, and International Journal of Computing and Information Technology.

Hui Li Received B.Sc. degree from Fudan University in 1990, M.A.Sc. and Ph.D. degrees from Xidian University in 1993 and 1998. Since June 2005, he has been the professor in the school of Telecommunications Engineering, Xidian University, Xi'an Shaanxi, China. His research interests are in the areas of cryptography, wireless network security, information theory and network coding. He is a co-author of two books. He served as technique committee co-chairs of ISPEC 2009 and IAS 2009.

Yueyu Zhang received B.Sc. degree from Xidian University in 2005, M.A.Sc. and Ph.D. degrees from Xidian University in 2005 and 2008. He is an Associate Professor in the School of Telecommunications Engineering. His current research is in information security and next generation mobile communication network security.

Zhenxing Luo received Ph.D degree from the University of Alabama at Birmingham, Birmingham, AL 35294, USA. Currently, he is a Postdoctoral research associate at Washington University in St. Louis, St. Louis, MO, USA. His research interests include computer networks, wireless sensor networks, and estimation theory.