Impact Factor (SJIF): 2.125

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 1, January-2016

Security analysis of Authentication and Key Agreement protocol for LTE network

H T Loriya[1], A. Kulshreshta[2], D R Keraliya[3]

[1]*EC Department, Govt. Engg. College, Rajkot*
[2]*EC Department, KIT, Jamnagar*
[3]*EC Department, Govt. Engg. College, Rajkot*

Abstract —High demand of data traffic in mobile communications and the emergence of new multimedia applications drives the motivation to move towards the development of broadband wireless access technologies. The Long Term Evolution/System Architecture Evolution (LTE/SAE) based next generation 4G technology is on the way towards fourth-generation (4G) mobile technology. LTE/SAE supports flat IP (internet protocol) based connectivity, interworking with heterogeneous wireless network, data traffic with very high speeds in terms of mega bits per seconds. This paper presents analysis of security advances and issues related with LTE/SAE wireless mobile technologies. First, LTE/SAE network architecture is discussed. Second, it studies overview of security based architecture and design for the LTE/SAE. Third, security related vulnerabilities such as user identity privacy, user location tracking and men-in –the middle attack present in LTE/SAE network with the focus of authentication and key access mechanism are discussed. Finally, the proposed solutions to these problems are reviewed and discussed security related research issues for the future works.

Keywords-component; LTE; SAE; EPS; AKA; Security;

I. INTRODUCTION

LTE (Long Term Evolution) is the latest forth generation mobile technological design for wireless telecommunications. LTE has been specified by the 3GPP as the next generation mobile networks. it provides high-speed data for cellular users and other user devices. LTE is an evolution of UMTS system so it is also known as EPS (Evolved Packet System). The radio access network used in the LTE improves access technologies so as to offer high performance in terms of a higher data rate, low latency, and flexible bandwidth. LTE systems support flat IP based connectivity, full interworking with heterogeneous wireless networks and seamless integration with other existing wireless communication systems. Due to the introduction of the new features rise to a number of security challenges in the design of the security architectures of the LTE system. LTE network architecture is comprised of three main components (i) User Equipment (UE) (ii) Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) (iii) Evolved Packet Core (EPC). The most common LTE network architecture is shown in the below figure-1.

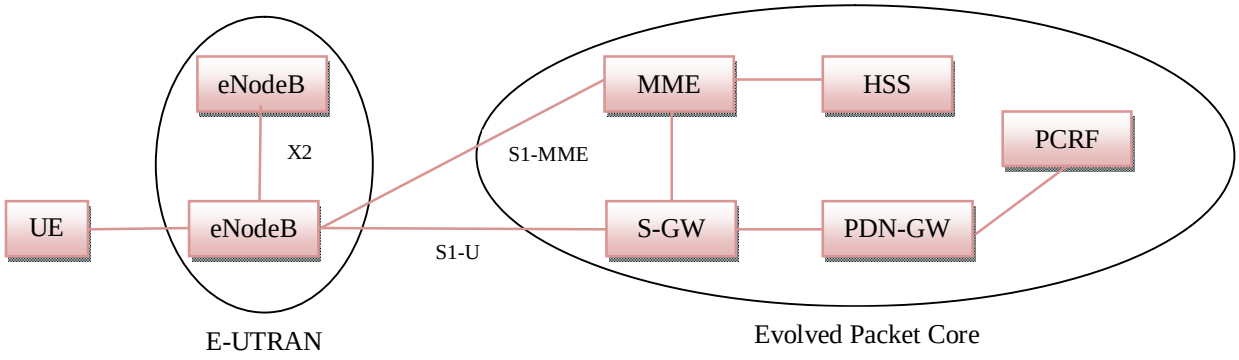

Figure-1 LTE Network architecture

User equipment (UE) is comprised of the Mobile Termination (MT), Terminal Equipment (TE) , Universal Integrated Circuit Card (UICC). UICC is also known as the SIM card for LTE equipments and it runs an application known as the Universal Subscriber Identity Module (USIM). The E-UTRAN handles the radio communications between the mobile and the evolved packet core using the evolved base stations, called eNodeB or eNB. eNodeB provides users with radio interfaces and handles radio resource management functions. The evolved packet core (EPC) communicates with packet data networks in the outside world such as the internet, private networks or the IP multimedia subsystem. EPC is comprised of the MME (Mobility Management Entity), the SGW (Serving Gateway), PDN-GW (Packet Data Network Gateway), HSS (Home Subscriber Server), and PCRF (Policy Charging Rules Function). The mobility_management

entity (MME) is main entity of EPC. MME controls the high-level operation of the mobile by means of signalling messages and Home Subscriber Server (HSS). It communicates with HSS for user authentication, NAS signalling, Mobility management, handover management and EPS bearer management. Home Subscriber Server (HSS) component is a central database that contains information about user profiles. It provides user authentication information to MME. The Packet Data Network (PDN) Gateway (P-GW) communicates with the outside world ie. packet data networks PDN. The PDN gateway has the same role as the GPRS support node (GGSN) and the serving GPRS support node (SGSN) with UMTS and GSM. The serving gateway (S-GW) forwards data between the base station and the PDN gateway. The Policy Control and Charging Rules Function (PCRF) is a entity which is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW.

When UE is in the range of LTE network it send signal to connects to eNodeB. UE sends an attach request message to eNodeB to connect to the network. eNodeB sends attach request to the MME via the S1-MME interface. The MME check the validity of the UE request against the HSS central data base, then selects required SGW that has access to the PLMN. Finally the request reaches the PGW where IP is assigned to the connection. After IP assignment connection is established between the UE and the network [1].

II. LTE SECURITY ARCHITECTURE

LTE security architecture is specified by 3GPP committee [2]. The five main security levels are specified as shown in the figure-2. (1) Network access security: In this level it provides the UEs with secure access to the core network and secure against attacks on the radio link. (2) Network domain security: In this level it enable nodes to securely exchange signalling data, user data (between AN and SN, and within AN), and it provides security against various attacks on wireline network. (3) User domain security: In this level it provides a mutual authentication between USIM and ME. (4) Application domain security: In this level it enables applications in the user and in the provider domain to securely exchange messages. (5) Visibility and configurability: In this level it allow user to check whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

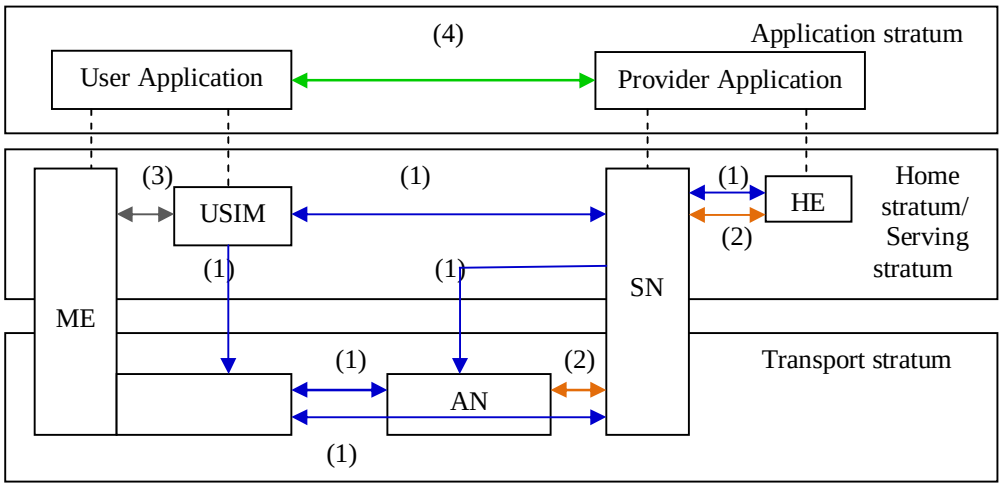

Figure-2 LTE security architecture

2.1 User Identity Confidentiality

When UE register for the first time, it sends permanent identity (IMSI) over the radio link. during network access, the Serving Mobility Management Entity (MME) allocate a Globally Unique Temporary Identity (GUTI) to the UE during network access, which is used in the system to avoid frequent exchange of permanant identity over the radio link. The GUTI is divided in two components: a Globally Unique MME Identity (GUMMEI), which is the identity of the serving MME, and the M-TMSI, which is the identity of the UE within serving MME.

2.2 User Device Confidentiality

The International Mobile Equipment Identity (IMEI) is sent when network request from user using non access stratum (NAS) procedures. It is protected with typical confidentiality.

2.3 Entity Authentication

Authentication and Key Agreement (AKA) protocol is used to provide mutual authentication between the user and the network. During mutual authentication both user and network agree to use K_{ASME} (the Key Access Security Management Entity) as secure session key. K_{ASME} is base key to generate Access Stratum (AS) and Non Access Stratum (NAS) ciphering and integrity keys. Core network (NAS) signalling, integrity and confidentiality protection terminates in MME (Mobile Management Entity) and Radio network (AS) signalling, integrity and confidentiality protection terminates in eNodeB.

III. LTE Authentication and Key agreement protocol (AKA)

LTE Authentication and Key agreement protocol (AKA) is built on UMTS (Universal Mobile Telecommunication System) AKA with improved security features such as Serving Network identity (SNID), Separation of security functions for Non Access Stratum (NAS) and Access Stratum (AS) and new key hierarchy to protect the signalling and user data traffic. LTE AKA protocol is shown in the figure-3.

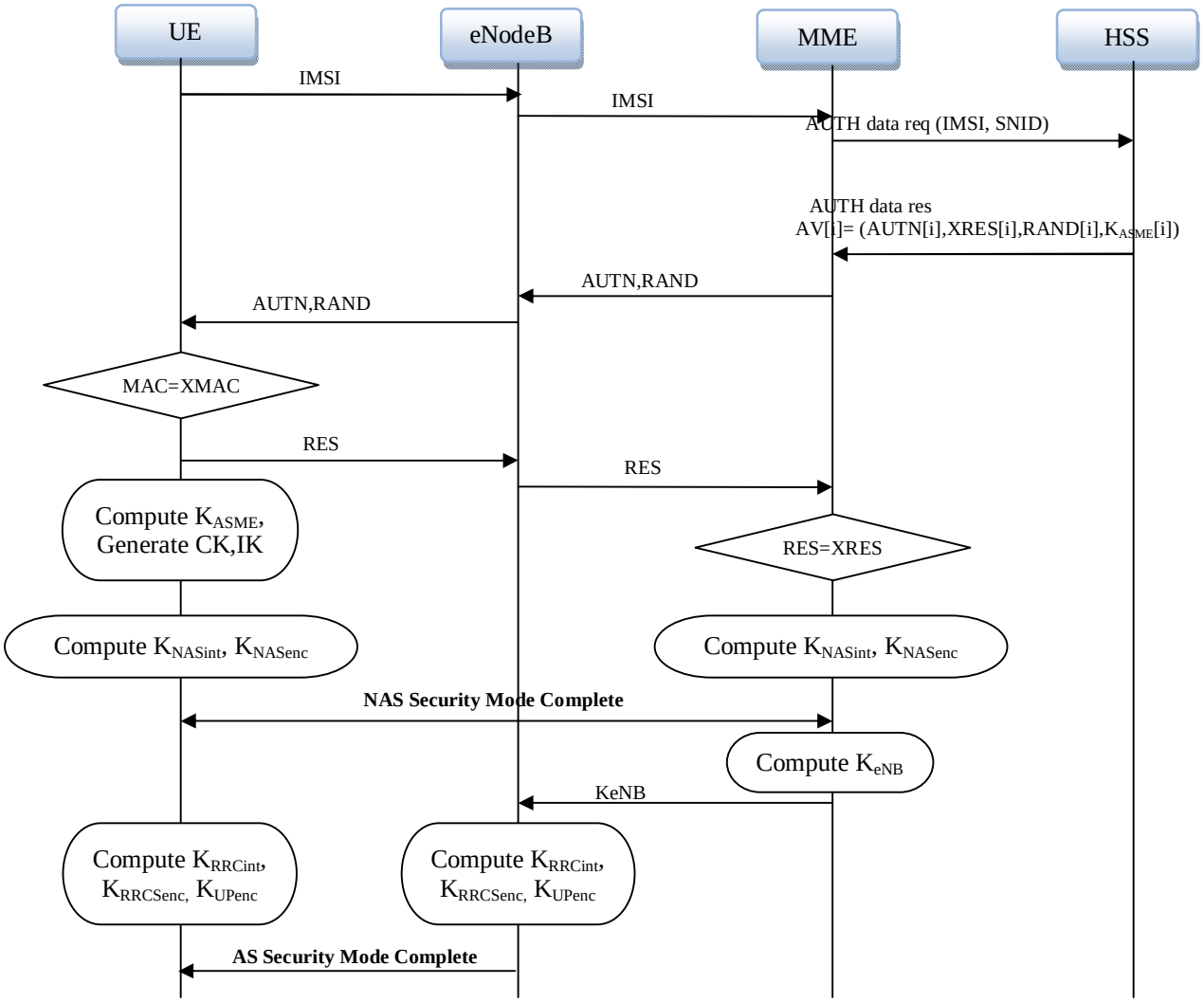

Figure-3 LTE Authentication and Key Agreement protocol

LTE-AKA protocol works as follows.

(1) An UE sends an access request message to MME through eNodeB. MME initiates an authentication procedure by asking the UE's identity

(2) In response to UE's identity request. UE send IMSI to MME. if UE is new to the area. If UE is not new in the area then the UE send GUTI

(3) MME sends an authentication data request containing UE's identity and SNID to the HSS.

(4) HSS uses long term secret key K shared with UE. HSS uses message authentication functions and key generation functions to computes the LTE authentication vectors. First it generate Random Nonce (RAND) and increse sequence number (SQN) for every vector. Using K, IMSI, RAND and SQN it computes following values.
Message Authentication Code (MAC) =$f1_K$(K, SQN||RAND||AMF),
Expected Response (XRES) = $f2_K$(K, RAND),
Cipher Key (CK) = $f3_K$(K, RAND),
Integrity Key (IK) = $f4_K$(K, RAND),
Anonymity Key AK=$f5_K$(K, RAND)
K_{ASME}= KDF (SQN⊕AK,SN ID , CK,IK)
AUTN= SQN⊕AK|| AMF || MAC
AV[i]= RAND[i] ||XRES[i] || KASME[i] || AUTN[i]
Whether AV belongs to EPS or UMTS can be identify using AMF.
(5) The HSS sends authentication data response message with array of authentication vectors (AVs) to MME so that MME is authorized to authenticate the requesting UE.
(6) MME stores received array of authentication vectors AVs and send RAND and AUTN from chosen AV to the UE.
(7) UE computes XMAC and compares it with the MAC carried in AUTN. If both are equal then UE computes and sends the RES back to MME. UE also calculates CK and IK same way as derived in HSS.
(8) After receiving RES from UE, MME verify it with XRES which is available in the AV. MME choose the corresponding K_{ASME} as the session key to protect wireless communication with the UE. UE also calculates its K_{ASME}. In this way UE and MME both agree on common session key K_{ASME}.
(9) Secure Mode Command (SMC) procedure is initiated whose purpose is to provide security for signalling and user data using derived keys and security algorithms.

New key hierarchy has been introduced to derived sub keys in LTE as shown in figure-4.

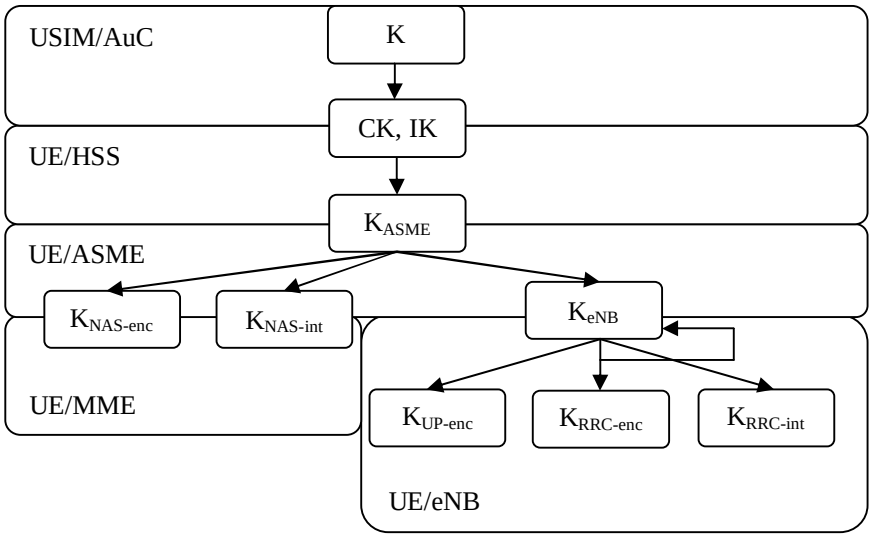

Figure-4 Key hierarchy

In the LTE, Access Stratum (AS) and Non Access Stratum (NAS) are two types of security context exits to protect the signalling and user data traffic. After the successful completion of LTE AKA, the UE and HSS agree on common session key K_{ASME}. The purpose of NAS security is to securely deliver NAS signalling messages between a UE and an MME in the control plane using NAS security keys. The purpose of AS security is to securely deliver RRC messages between a UE and an eNB in the control plane and IP packets in the user plane using AS security keys. K_{ASME} can be used to derive three second level keys in MME such as K_{NASint} , K_{NASenc} and K_{eNB}. K_{NASint} and K_{NASenc} are used for the protection of Non Access Stratum (NAS). K_{NASint} key is used for integrity protection between UE and MME. K_{NASenc} key is used to encrypt messages between UE and MME. MME computes K_{eNB} key and send this key to evolved eNodeB. K_{eNB} can be used to three third level keys such as K_{UPenc}, K_{RRCint} and K_{RRCenc}. These three keys are used for protection of Access stratum (AS). K_{UPenc} is used to encrypt user data traffic between UE and eNodeB. K_{RRCint} and K_{RRCenc} are used for integrity and encryption for radio resource control traffic between UE and eNodeB. Key hierarchy in LTE is more complicated than UMTS. Key is derived from top to bottom in downward derivation by one-way function. It is impossible to get high key from low key. It protect root keys and also reduces the need of periodic updates, re-generation

and transmission of the root keys. It improves the speed of the re-authentication mechanism and refreshing process of the keys. It also protect system from effect of compromised low key.

IV. LTE SECURITY ISSUES AND PROPOSED SOLTUTIONS

The LTE AKA has improvements over the UMTS AKA but still there are some security vulnerabilities present in the LTE network such as user privacy, location privacy, rogue base station attack, Denial of Service (DoS) attack and man in the middle (MitM) attack. Normally, LTE send temporary identity GUTI over the air instead of the permanent identity IMSI. There are many cases where IMSI is disclosed. For example, when a UE attach to network for first time, or when serving MME cannot be contacted or IMSI can not be retrieved due to synchronization problem when it roams to a new MME, the serving MME or the new MME requests the IMSI of the UE at that time UE must transmit the IMSI in plain text as shown in the figure-3. Attackers can collect this permanent identity in special areas (e.g. airport), where all new users switch on their mobiles, thus triggering the identification process in LTE AKA. Once the IMSI is captured, the attackers can collect subscriber information, location information some times even conversation information, and then possible to disguise UE and may launch DoS attacks. It also opens the door for a man-in-the-middle attack. (1) LTE AKA vulnerable to privacy protection [4, 8]. An active attack model for capturing IMSI have been proposed in [3] by which, the IMSI can be easily disclosed by an active attacker and the current LTE AKA mechanism can not prevent such active attacks.

.

The LTE AKA mechanism can not prevent DoS attacks [9]–[11]. The MME must forward the requests of UEs to the HSS even before the UE has been authenticated by the MME as shown in figure-3. Moreover, MME can only authenticate the user after an RES has been received from UE. Based on these two conditions, attackers can launch DoS attacks to HSS and MME [10], [11]. Attackers can disguise a legitimate user to constantly send fake IMSIs to overwhelm the HSS. HSS has to use its computational power to generate excessive authentication vectors for the UE. On the other hand, the MME has to use its memory storage to wait overly long period of time for a legitimate or false response from the corresponding UE. LTE AKA is vulnerable to DoS attacks and several DoS attacks have been found in the NAS procedure to overload the entities in E-UTRAN [11].

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 eNodeBs in to LTE network with the functionality of a base station. Rogue eNodeBs can impersonate the operator's node and intercept voice and data transmission from the UE. By using a rogue base station, the attacker can also passively eavesdrop or redirect user traffic to a different network [7]. This allows attackers to track the user mobile location or launch man in the middle attack.

It has been pointed in [6] that LTE security is vulnerable to IMSI catching, bandwidth stealing, open architecture problem and DoS attacks.

A minor modified version of the LTE-AKA protocol has been presented in [12]. It requires a new user module ESIM instead of USIM to provide a direct online mutual authentication between the ESIM and the MME/HSS to overcome the shortcomings of the LTE-AKA protocol. This is a considerable operational drawback in LTE network due to the use of the new ESIM.

An enhanced LTE-AKA protocol has been proposed in [13] to improve the performance of LTE-AKA mechanism by increasing a little computation in the MME. MME generates and stores many authentication vectors (AVs) from the original AVs at the HSS. It can reduce the authentication signalling exchange between MME and HSS to saves the bandwidth consumption at the HSS. However, this scheme increases the burden of the MME because a lot of AVs required to generate at the MME.

J-PAKE based protocol has been proposed in [1], it uses password authentication key exchange by Juggling (J-PAKE) protocol in authentication process instead of the LTE-AKA protocol to provide strong security protection. However, it only discussed the use of J-PAKE in the LTE networks without introduction of the implementation.

A security surveys have already been published in order to review the existing works. A general overview of the security threats on 4G networks has been presented in many research papers [15] [16] [17] [18][19][20].

V. CONCLUSION AND FUTURE WORK

In this paper, we have reviewed security issues in the LTE wireless networks with the focus of authentication and key access mechanism in fourth generation mobile telecommunication system. We have discussed the vulnerabilities existing in the security architecture of the LTE-AKA and reviewed existing proposed solutions to overcome security problems. One possible solution would be the use of public key based mechanism for authentication and key agreement in 5G. User

permanant identity confidentiality could be protected against active attacks using public key based authentication and key agreement[24].

However, there are still some security vulnerabilities present in the current LTE networks. It is beyond the scope of this paper to discuss all security vulnerabilities. Lots of research is going on to enhance security of LTE network. Further on, research continues to protect permanent identity IMSI to proposes complete identity protection solution to protect against various attacks. we have also pointed out open research issues for future research activities to enhance authentication and key agreement mechanism for the future wireless communication network.

References

[1] C. Vintila, V. Patriciu, and I. Bica, “Security Analysis of LTE Access Network”, Proceedings of The Tenth International Conference on Networks (ICN 2011), January 2011, pp. 29-34.
[2] 3GPP TS 33.401 V8.2.1 (2008-12) 3GPP System Architecture Evolution (SAE); Security architecture
[3] D. Forsberg, L. Huang, K. Tsuyoshi, and S. Alanara, ”Enhancing Security and Privacy in 3GPP E-UTRAN Radio Interface,” Proc. Personal,
[4] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, “A survey on security aspects for LTE and LTE-A networks,” Communications Surveys Tutorials, IEEE, vol. 16, no. 1, pp. 283–302, First 2013. Indoor and Mobile Radio Communications (PIMRC), Septmber 2007, pp.1-5.
[5] Chan-kya Han and hyoung-kee choi, “Security Analysis Of Handover Key Management In 4G LTE/SAE Networks”, IEEE Transactions on Mobile Computing ,VOL.13 , NO.2, FEB 2014.
[6] N. Seddigh, B. Nandy, R. Makkar, J. F. Beaumont, “Security advances and challenges in 4G wireless networks,” PST, 2010.
[7] Y. Park, T. Park, “A Survey of Security Threats on 4G Networks,” in GLOBECOM-07.
[8] L. Xiehua, W. Yongjun, “Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network,” WiCOM, 2011.
[9] 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.
[10] 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.
[11] D. Yu and W. Wen, ”Non-access-stratum Request Attack in E-UTRAN,” Proc. Computing, Communications and Applications Conference (Com-ComAp), January 2012, pp.48-53.
[12] G. M. Koien, "Mutual Entity Authentication for LTE," Proceedings of 7th International Wireless Communications and Mobile Computing Conference (IWCMC), July 2011, pp.689-694.
[13] M. Purkhiabani and A. Salahi, "Enhanced Authentication and Key Agreement Procedure of Next Generation Evolved Mobile Networks," Proceedings of IEEE 3rd International Conference on Communication Software and Networks (ICCSN), May 2011, pp.557-563.
[14] 3GPP TS 24.301 V8.0.0 (2008-12) Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS).
[15] Y. Park and T. Park, ”A Survey of Security Threats on 4G Networks,” Proc. IEEE Globecom Workshops, November 2007, pp.1-6.
[16] C. Kolias, G. Kambourakis, and S. Gritzalis, ”Attacks and Countermeasures on 802.16: Analysis and Assessment”, IEEE Communications Surveys and Tutorials, 2013, IEEE Press.
[17] 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.
[18] 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.
[19] 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.
[20] Li Zhu, Hang Qin, Huaqing Mao, Zhiwen Hu, “Research on 3GPP LTE Security Architecture”, International Conference on WiCOM, IEEE Conference publications-2012
[21] G. Escudero-Andreu, R. C-W. Phan and D. J. Parish, "Analysis and Design of Security for Next Generation 4G Cellular Networks," PGNet, Loughborough, U.K., 2012.
[22] 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.
[23] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi,” LTE Security”. John Wiley and Sons, Ltd, 2010.
[24] Gunther Horn, Peter Schneider, “Towards 5G Security” IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, 20-22 August, 2015