Survey of security features in LTE Handover Technology

Md Mehedi Masud
Department of Computer Science and Technology
University of Bedfordshire, UK
mdmehedi.masud@study.beds.ac.uk

Abstract— **Improvement in mobile data communication platforms and growing number of data services have motivated 3GPP to evolve current mobile architecture to 4G establishment. To support vast data services, LTE technology was evolved as IP based system which also brings some security threats to the existing network. This paper contributes towards evaluation of security features in LTE network technology. First section presents network security architecture overview; followed by security mechanisms in network handover process. Different security threats and their solutions have been analysed to find out future research development scope in this area.**

Keywords- Long Term Evolution[LTE], LTE-A, LTE handover mechanism, LTE handover security, HeNB security.

I. INTRODUCTION

Since the early 1990s, wireless networking has seen substantial growth due to rapid development of mobile technologies and applications. Latest versions of wireless and mobile technologies have been developed during this period and still researches are going on to improve and accommodate different services. Long term evolution [LTE] and the later version LTE-A are most significant among them along with WIMAX [worldwide interoperability for microwave access] technology due to their latest development to transfer mobile data communication services. Being designed as a packet based system give LTE more advantages than previous 3G network technologies in terms of higher data rate and system integration. It covers more network area and supports bandwidth flexibility to provide data transmission. Improvement of cellular technology allows this network to support different wireless base stations based on femtocell and picocell solutions.

Security threats for UMTS [universal mobile telecommunication systems] networks were increasing highly which led to the development of security enhanced LTE technology. More security features have been added to this technology to eliminate security threats that existed earlier such as DOS [denial of service] attack or MITM [man in the middle] attacks. UMTS- authentication key agreement (AKA) was enhanced and new security approach, evolved packet system (EPS) authentication key agreement was presented. But introduction new features also come with different new challenges to design network and security architecture of the system [1] [2].

This paper focuses on network and security architecture of LTE network system and different security vulnerabilities in handover process. Different approaches and proposed methods are also evaluated to improve security in handover process.

II. LONG TERM EVOLUTION (LTE) TECHNOLOGY

LTE technology is the successor of GSM [global system for mobile] technology and developed as a standard through various research improvements. Earlier mobile technologies were more focused on only cellular technology to transfer voice calls but recent trend of data communication led to evolve different standard mechanisms of those technologies. Circuit switch technology was used for both voice and data communications in GSM technology which pulled the data rate to the lowest. Shifting to packet switching improved data services in mobile communication technologies. Before LTE was evolved several other standards such as UMTS and WCDMA [wideband code division multiple access] were in place where circuit switch were used for voice transfer and data services used packet switching [3].

IP based packet switching is the core technology behind LTE where both voice and data services are transferred through IP. IP address is allocated as any user device is switched on and released when not in service. Frequency division multiple access (FDMA) functionality is used as access method in LTE where downlink layer uses OFDMA [orthogonal frequency division multiplexing] and uplink layer uses SC-FDMA [single carrier FDMA]. This provide higher data rate in LTE devices [4].

III. NETWORK ARCHITECTURE OVERVIEW

Network architecture of LTE is divided into two major parts. Evolved Packet Core (EPC) and E-UTRAN [universal terrestrial radio access network] are the backbone of the LTE network architecture. EPC is fully packet switched technology based on IP based solution. IP multimedia subsystem (IMS) technology is used to carry voice services which earlier was circuit switched based transmission. IMS is used to allocate IP services to the user devices in the networks. Core components of EPC are MME [mobility management entity], SGW [service gateway], PDN GW [PDN gateway] and HSS [home subscriber server]. MME controls mutual authentication when any user connects with the network. eNodeBS (eNB) performs radio transmission in Evolved Universal Terrestrial Radio Access Network. LTE technology features significant improvements in network architecture comparing 3G network entities [5] [6].

1. To improve network coverage in offices and houses LTE network supports new type of base stations HeNB. This is an access point installed indoor to provide high speed voice and data service. HeNB is connected to the EPC through internet.

2. Non-3GPP networks such as CDMA, WiMAX or WLAN are also supported by LTE if they are connected to EPC. Both trusted and un-trusted networks can be connected with EPC if authorised by the network provider. Trusted gateway ePDG is connected to EPC through which user can communicate with un-trusted networks.

3. MTC [machine type communication] is the method of data communication between different systems without human interaction. MTC is formed of MTC user and MTC server. MTC user is based on outside of the network and use services provided by the MTC server to operate MTC devices. MTC server can be located inside or outside of EPC [10].

IV. Security Architecture of LTE

3GPP proposed layer security architecture for LTE technology. Five different security layer is defined which are as follows [17].

1. Network access: Secured access is ensured for the user devices to EPC. This security level is used to protect integrity and provide ciphering services all the systems and user devices present in the whole network. Main task of this layer is to eliminate threats on access link.
2. Network domain: This layer of security focuses more on the physical establishment in the network. It maintains data security for both signals and users between different nodes. It also eliminates threats on wired networks.
3. User domain: Before accessing any mobile devices USIM passes though user domain security layer. This layer is responsible for secured authentication process of the devices and USIM.
4. Application domain: secure communication between user devices and service provider is ensured through this layer of security. User device applications securely send and receive messages with service providers.
5. Non-3GPP domain: Improved technology allows LTE user devices to connect to EPC through non-3GPP networks. This layer maintains security for this process and also responsible for access link security.

V. LTE Handover Mechanism

Handover mechanism allows any call to transfer between cells in network without being interrupted. This might reduce call or data network performance. Strong handover mechanism is the key to maintain data integrity in any communication service. This process continues in several steps from initiation to completion. In between reservation of network resource and final execution is carried out. Detailed steps of handover process are shown in figure: 1 and also listed below [6] [18].

1. To initiate handover process, user device initiates a measurement report to the source eNB according to the specification. This report also specifies the target cell for handover.

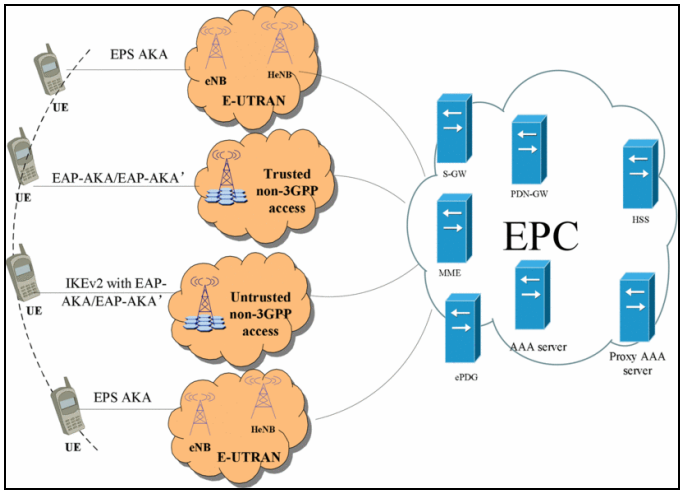

Figure 1: handover between E-UTRAN & non 3GPP[5]

2. After checking measurement report, source eNB decides to perform HO and issues request message to target eNB.

3. Both eNBs perform signal exchanging and to prepare handover and target eNB performs user device admission control before sending acknowledgement to source eNB.

4. Handover command is sent to the user device and after completing handover user device sends a confirmation message back to the eNB.

VI. Handover Process Security Mechanism

Handover procedure and features for security is specified by 3GPP for both within intra UTRAN and GSM networks along with non-3GPP networks.

LTE network uses latest security key management methods to perform secured handover process in intra E-UTRAN network. This mechanism provides several ways to transfer eNB keys either in vertical or horizontal direction. After finishing authentication at initial stage, user equipment (UE) and MME generates K_{ASME} key. Another key K_{eNB} is derived by UE and MME that is used for secured communication along with next hop (NH) parameter from $K_{ASME.}$ K_{eNB} and the NH are then associated with NH chaining counter. Finally either NH parameter or K_{eNB} will generate new session key K^{*}_{eNB} for the handover process [11].

According to the 3GPP specified protocol, handover between E-UTRAN and UTRAN starts with initial key generation from $K_{ASME.}$ CK' and IK' keys are derived by UE and MME respectively. After receiving $CK^{1} \parallel IK^{1}$ along with KSI' from MME, target SGSN and UE use CK' and IK' to generate GPRS key Kc. Target MME generates K^{1}_{ASME} from CK and IK or SGSN generates GPRS Kc for the handover between UTRAN and E-UTRAN. To generate K^{1}_{ASME} key as MME, same key generation procedure is followed by UE. Then K_{eNB} and NAS keys are generated by UE and target MME

following the LTE key hierarchy mechanism defined by 3GPP [6].

Several mobility mechanisms are defined by 3GPP for mobility between non-3GPP and E-UTRAN networks to perform secured handover mechanism showed in Fig:1. According to 3GGP full access authentication is implemented by user device, target networks and EPC for any UE to move between different radio access networks. In different network handover scenario different access authentication mechanism is performed. Handover to E-UTRAN is authenticated by EPS-AKA mechanism while handover to trusted non-3GPP network is authenticated by either EAP-AKA or EAP-AKA'. Again handover procedure performed to un-trusted non-3GPP network access will require IKEv2 along with EAP-AKA or EAP-AKA' authentication mechanism similar like trusted non-3GPP network access [7].

VII. VULNERABILITY OF HANDOVER PROCESS

Although 3GPP has specified most of the security features and requirements along with identifying security threats and vulnerabilities of LTE architecture, yet some more threats remained un-noticed. One of the most vulnerable parts of LTE system architecture is handover process mechanism due to the complex cross platform authentication process.

Handover process in LTE takes place in different network scenario as there are so many network entities such newly introduced base station and HeNB along with traditional eNB. Handover security features between HeNB and eNB is defined by 3GPP, however different authentication process is needed for different scenarios. Inter-network handover scenarios among eNB, HeNB, base stations and MME increase complexity of the network authentication mechanism. Again heterogeneous access system supported by LTE network is another complex scenario for authentication mechanism and poses security threat to the network. This process is shown in figure: 2. Roaming among different network system can increase handover delay due to multiple message transfer in authentication process. Key generation process for LTE includes multiple key derivations which is also increasing network delay and complexity. Smooth connectivity of the network is being affected by this loophole and making network more vulnerable for exploitation by attacker [8] [12].

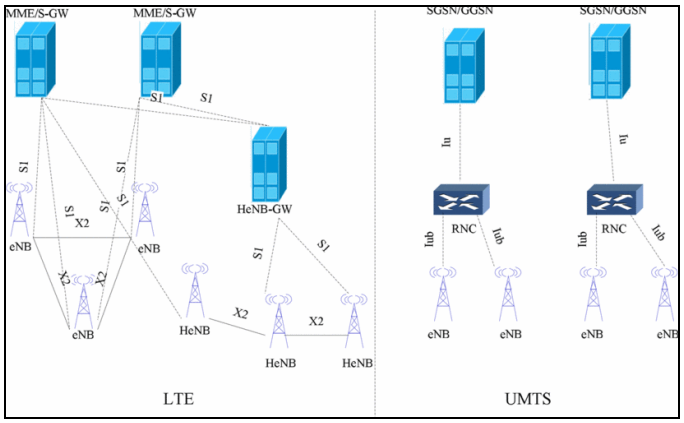

Figure 2 : comparison access network [5]

Lacking of backward security policy is another threat posing towards LTE vulnerability. Inter eNB handover process is shown in figure: 3. LTE key chaining mechanism allows eNB to generate different keys for several target eNBs. New session key K_{eNB} can be derived between user device and target eNB by using previous K^*_{eNB}. So if the UE or source key is compromised that can be used to generate session keys [13].

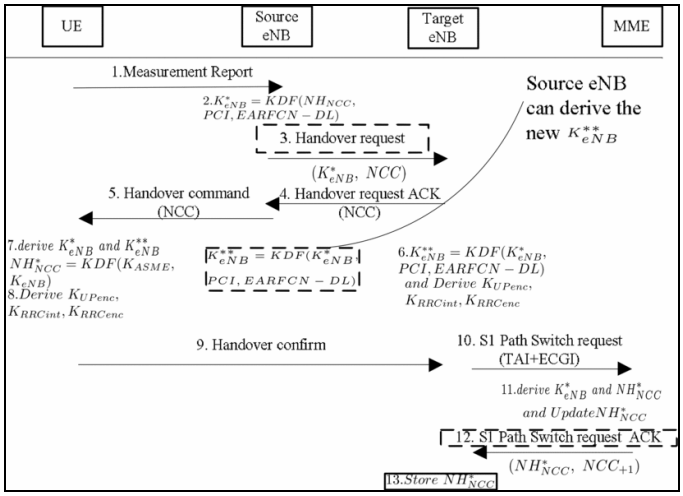

Figure 3 : inter eNB handover [5]

If any eNB is compromised and attacker deploys rogue eNB, he will be able to manipulate HO messages. NCC value will not be refreshed which will result in target eNBs to perform horizontal key generation. Resynchronisation of NCC value will make future keys vulnerable as shown in figure: 4.

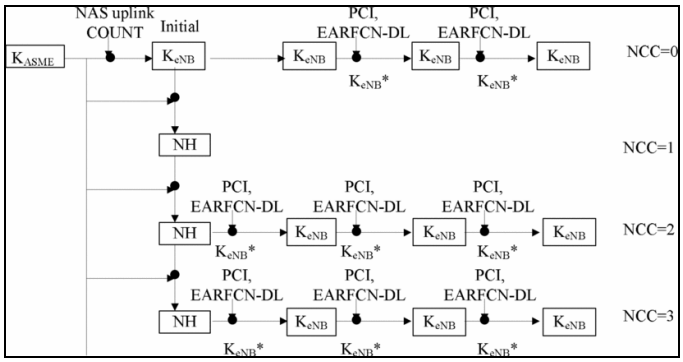

Figure 4 : handover key management [5]

Replay attacks can destroy security features of the synchronised link between target eNB and user equipment.
At first HO request message is being intercepted by the attacker and this message is sent to the target eNB when UE moves to the target eNB. Target eNB replies back to the UE with NCC value. Upon receiving this value UE performs and check with the stored value. But as messages is being intercepted and previous keys been sent to the target eNB those values are different. Thus secured connection between the user device and target eNB is not established and HO process needs to be initiated again [14].

VIII. SECURE SOLUTIONS FOR HANDOVER PROCESS

Simpler mutual authentication system can be the best solution to secure handover process vulnerability as this mechanism is mostly vulnerable due to complex authentication process. Several proposals have been made by the researchers to eliminate threats against handover security mechanism. When UE enters any target eNB or HeNB coverage they can perform authentication process directly in between themselves to generate session keys. This process will make authentication mechanism more efficient as simpler key management solution will be in place based on proxy signature to generate session keys. Authentication will be performed faster and securely in heterogeneous LTE architecture [9].

Other researches has proposed key generation centre (KGC) to derive session keys. When any UE moves to new target coverage based on previous secret keys, new session keys will be generated for both UE and target ENBs through KGC. This process follows three way handshake mechanisms without contacting other third parties. This process supports both eUTRAN and non-3GPP networks [6].

Yet both of the security mechanism works well to eliminate significant threats but it also increases compatibility problems among LTE networks. Alongside proxy signature based authentication and IBC are not cost effective to implement in mobile networks as user device's battery depletion is another reason for none of this mechanisms to become as standalone standard.

Hybrid authentication is another solution for secreting key management in handover process. Public key is assigned with dynamic password for each entity. Broadcasting public key allows cross platform network devices to perform mutual authentication securely. Yet this mechanism is not also cost effective due to public cryptography.

Earlier GSM technology based security mechanism is also provided by different network provider yet they do not fully feature LTE functionality. Fast handover method can reduce latency in the process by implementing pre-authenticated keys. This mechanism also supports both trusted and non-trusted 3GPP access networks. Extra security parameters are included along with EAP-AKA protocol to perform handover process between WLAN and WIMAX access networks. Interoperability problems can be solved through this method as this mechanism provides forward and backward secret method. Drawback of this method is it only supports single-hop UE to access point communication [10].

IX. Open Research Issues

Comparison and analysis demonstrates issues in security vulnerability in LTE handover mechanism. Further development and research is needed to find perfect solution for key generation and mutual authentication process in handover mechanism. Existing systems do provide support and security mechanisms through different public key cryptography process that prevents protocol attacks. But implementation of this mechanism in heterogeneous environment still poses security threats. Lightweight mechanism can be the best solution to secure handover process based on authentication using hash mechanism. HMAC or CMAC can be forwarded to the target base station to check for validity which will lead to no interaction between UE and access network. Target network will check and process handover for UE. This technology is commonly used in WIMAX network scenario as a countermeasure against DoS attack. Similar features can also be implemented in LTE technology as further improvement into the network system [7] [15].

X. Conclusion

LTE is taking over as 4G networks to support current demand of higher data services through mobile communications. Main objective of LTE is to provide efficient service and higher data rate through secured transmission. This paper presents LTE network and security architecture followed by security features of handover mechanisms. It also presents survey of existing security threats and evaluates different present solutions. Comparing the present and proposed solutions it can be concluded that, this method still has open issues for further research. Integration of different network solutions is the main cause of security loophole as they are varied in features in different infrastructures. Further improvements in security features will allow users to get best data communication services through mobile networks.

REFERENCES

[1] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom and S. Parkvall, "LTE: the evolution of mobile broadband," *Communications Magazine, IEEE,* vol. 47, pp. 44-51, 2009.

[2] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe and T. Thomas, "LTE-advanced: next-generation wireless broadband technology [Invited Paper]," *Wireless Communications, IEEE,* vol. 17, pp. 10-22, 2010.

[3] Jin Cao, Maode Ma and Hui Li, "Unified handover authentication between heterogeneous access systems in LTE networks," in *Global Communications Conference (GLOBECOM), 2012 IEEE,* 2012, pp. 5308-5313.

[4] Jin Cao, Maode Ma and Hui Li, "An Uniform Handover Authentication between E-UTRAN and Non-3GPP Access Networks," *Wireless Communications, IEEE Transactions on,* vol. 11, pp. 3644-3650, 2012.

[5] Jin Cao, Maode Ma, Hui Li, Yueyu Zhang and Zhenxing Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *Communications Surveys & Tutorials, IEEE,* vol. 16, pp. 283-302, 2014.

[6] R. P. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on,* 2013, pp. 1-9.

[7] C. Kolias, G. Kambourakis and S. Gritzalis, "Attacks and Countermeasures on 802.16: Analysis and Assessment," *Communications Surveys & Tutorials, IEEE,* vol. 15, pp. 487-514, 2013.

[8] N. Krichene and N. Boudriga, "Securing roaming and vertical handover in fourth generation networks," in *Network and System Security, 2009. NSS '09. Third International Conference on*, 2009, pp. 225-231.

[9] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *Communications Magazine, IEEE,* vol. 47, pp. 84-91, 2009.

[10] Bai Xiang-yu and Hu Jing, "The design and application of LTE core network equipment," in *Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2013 Third International Conference on*, 2013, pp. 222-227.

[11] A. N. Bikos and N. Sklavos, "LTE/SAE Security Issues on 4G Wireless Networks," *Security & Privacy, IEEE,* vol. 11, pp. 55-62, 2013.

[12] Li Xiao-Wen and Wang Jing, "The optimized method of reducing unnecessary handover in LTE system," in *Instrumentation, Measurement, Computer, Communication and Control (IMCCC), 2013 Third International Conference on*, 2013, pp. 1224-1227.

[13] B. Matt and Chengcheng Li, "A survey of the security and threats of the IMT-advanced requirements for 4G standards," in *Conference Anthology, IEEE*, 2013, pp. 1-5.

[14] N. Seddigh, B. Nandy, R. Makkar and J. -. Beaumont, "Security advances and challenges in 4G wireless networks," in *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, 2010, pp. 62-71.

[15] G. Siwach and A. Esmailpour, "LTE security potential vulnerability and algorithm enhancements," in *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on*, 2014, pp. 1-7.

[16] Wang Zizhou, Fan Chen, Wang Yafeng and Yang Dacheng, "A novel network architecture for 3G evolution," in *Personal, Indoor and Mobile Radio Communications, 2006 IEEE 17th International Symposium on*, 2006, pp. 1-5.

[17] 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.

[18] 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.