Security Architecture of 3GPP LTE and LTE-A Network: A Review

Warda Ahmed[1], Sidra Anwar[2] and M. Junaid Arshad[3]

[1,2,3]Computer Science and Engineering Department, University of Engineering & Technology, Lahore, Pakistan

[1]balochwarda@gmail.com, [2]sidra.anwar72@yahoo.com

***Abstract*– Mobile wireless communication is improving and getting mature day by day. Due to this, we need the improvement of high broadband wireless technologies. The 3GPP which means that 3rd Generation partnership project is a standard which is developing System Architecture Evolution (SAE)/Long Term Evolution (LTE) architecture for the succeeding mobile communication systems. Many organizations are working to shift 3GPP LTE to LTE-Advanced network, leading to 4th generation (4G) mobile networks. The present study conducted a literature review on security architectures of 3rd Generation partnership project (3GPP), Long Term Evolution (LTE) and Long Term Evolution Advanced (LTE-A) networks. As well as their network security issues are also studied.**

***Keywords*– 3GPP, LTE, LTE-A, Review, Vulnerabilities, EPC, E-UTRAN and MTC Devices**

I. INTRODUCTION

Since last few years, demands of broadband mobile wireless communications and the evolution of new wireless multimedia application have become more and more high, which gives the motivation to the development of broadband wireless access technology. Third Generation Partnership project define LTE/SAE system which then leads to the fourth-generation (4G) mobile keeping 3GPP as dominant cellular communication technologies [1]. Cellular network operators are using such technologies to provide capacity for new multimedia services. Now days, mobile network has become a necessary component of our daily lives. They are providing many services like e-mail, location based applications, video streaming etc. [2].

The LTE system is a packet-based network having less network element. This ability of network improves the size of system and exposure. Its performance is also increased in terms that data rates become high, access latency is decreased, elastic bandwidth operation and also interminable integration with other already present wireless communication systems[3]. 3GPP LTE Release 10 enhances the existing LTE and produce LTE advanced (LTE-A) system which support much increased data usage, less latencies and enhanced spectral efficiency [4].

Some mutual characteristics of both long term evolution and long term evolution advanced networks are given .The first one is complete interworking with heterogeneous WAN(wireless access network), secondly they support flat IP connectivity and thirdly new type of base stations are introduced such as pico/femto and communication nodes in a macro-cellular networks. After the addition of these features long term evolution and long term evolution advanced face novel security challenges in their design of security architecture.

The main purpose of long term evolution security is performing authentication to users and also to provide data integrity and confidentiality. Even though long term evolution have complex and vigorous set of security mechanisms, but still there is a need for improvement [5]. The main security problem found in third generation partnership project long term evolution (3GPP LTE) communication is authentication of identity on both sides. One more security issue is handover process of station equipment. Handover occur when two or more devices communicate with each other [6].

In this paper, a literature review of Long term evolution and Long term evolution advanced network security architectures are presented. Some network security issues are also discussed in this paper. The next section gives an summary of some related work done in this field. Section III discusses the network architectures of third generation partnership project (3GPP), Long term evolution (LTE) and Long term evolution advanced (LTE- A) networks. Section IV presents the overview of 3GPP, LTE and LTE-network security architectures. Weaknesses in LTE and LTE–A network security architectures are discussed in Section V. Some open research topics are mention in Section VI. Finally, Section VII closes the paper with a conclusion.

II. RELATED WORK

Recently, much work has been done on the security functionality of LTE/LTE-A (Long term evolution/Long term evolution advanced) networks. A few studies have already been published to review the present work.

The LTE (Long term evolution) architecture consists of Evolved Packet System (EPS) and Authentication and Key Agreement (AKA) process which is used for mutual authentication among the consumer and the network. Still there are some weaknesses in Evolved Packet system and authentication and key agreement system such as expose of user identity, man in the middle attack, etc. A study conducted by Li Xiehua and Wang Yongjun find out the

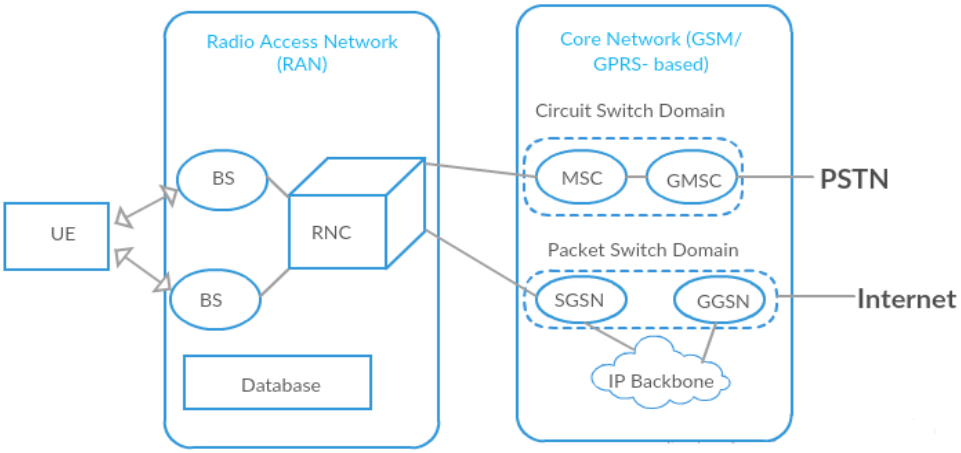

Fig. 1. 3GPP IP Architecture [7]

drawbacks of the Evolved packet system and authentication and key agreement (EPS AKA) protocol, and then propose a Security Enhanced Authentication and Key agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure [8].

Another research provides an overview of the proposed security apparatus in third generation partnership long term evolution (3GPP LTE). It first gives a brief introduction of the long term evolution security mechanisms, and then studies the security architecture of System architecture evolution (SAE)/long term evolution (LTE). Further this paper describes the security layers of LTE/SAE. It also describes domain security and the key architecture of LTE/SAE. It also discusses the some security problems in LTE security [6].

Another study about Long term evolution networks describes the LTE access security architecture and also proposes a new authentication protocol between the ESIM and the MME/HSS. The new Enhanced authentication and key agreement (EAKA) protocol provides full mutual person authentication between ESIM and HSS which removes the need of proxy authentication mechanism. This is attained by making minor changes in the system architecture [9].

III. 3GPP, LTE AND LTE-A NETWORK ARCHITECTURE

Many researchers are looking forward to avoid vulnerabilities occurring today .Now a days everyone is on internet and cyber intrusion is very common by spreading a malware or by fishing attack. User Equipment (UE) in any network is very easy to be hacked. For prevention from all these attacks a lot of work has to be done. Now first take a look at the network architecture of 3GPP, LTE and LTE- A systems.

A. 3GPP Network Architecture

3GPP essentially began with GPRS as the center parcel organize and overlaid it with call control and entryway capacities required for supporting VoIP and other interactive media administrations. The 3GPP network architecture is divided in to different domains (as shown in figure. 1) such as User Equipment i.e., Mobile Terminal and Terminal Equipment , Radio Access Network (RAN), IPT core network that is based on Global System of Mobile communication(GSM)/ General Packet Radio Service (GPRS) Network, Gateways, Databases and Public Switch Telecommunication Network (PSTN). UEs are connected to the different Base Stations (BS) which in turns connected to Radio Network Controller (RNC). The RAN and GPRS arrange together give IP bearers from the UE to the IPT center. In center system, the primary system components are Serving GPRS Support Node (SGSN), Gateway GPRS Support Node (GGSN), Mobile Switching Center (MSC) and Gateway Mobile Switching Center (GMSC).The MSC and GMSC together form a circuit domain, thus it connects to PSTN domain. The SGSN and GGSN together form packet switch domain, thus GGSN in turns connects to the internet cloud. The GPRS system is likewise in charge of controlling IP carrier administration. The fundamental assignments incorporate client validation, approval, bookkeeping, portability administration inside GPRS arrange, and controlling Radio Access Bearers (RAB) [10].

A. Long Term Evolution Network Architecture

The LTE system building design comprises of two fundamental parts; i.e., the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet Core (EPC) as appeared in Fig. 2. The EPC is a completely packet-switched (PS) spine network in LTE network architecture. The EPC is utilized to give an IP association between an outer bundle information system by utilizing E-UTRAN and the UE. Circuit switched (CS) network services, such as voice services, are controlled by IMS (IP multimedia subsystem) network [11].

Diverse parts of EPC are as per the following; a Serving Gateway (SGW), a Packet Data Network Gateway (PDN GW) and Mobility Management Entity (MME), together with Home Subscriber Server (HSS). At the point when a UE join with the EPC through E-UTRAN, then MME performs a shared confirmation with the user equipment. E-UTRAN contains Evolved Universal Terrestrial Radio Access Network

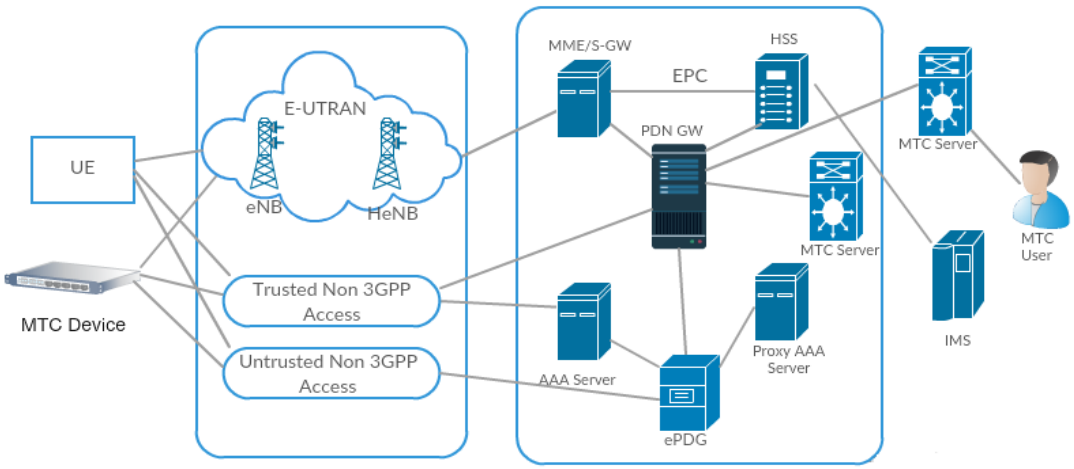

Fig. 2. LTE Network Architecture [1]

Base Station, known as eNodeB (eNB) and Home eNodeBs (HeNB), which communicates with users. HeNB is introduced to improve the network capacity and the indoor coverage [1].

The extra element of the LTE framework is the backing for the non 3GPP access systems. Two types of non 3GPP access system exist , named as trusted and untrusted non 3GPP access systems [12]. A new type of data communication is also introduced in LTE system, named as Machine Type Communication (MTC). MTC can exchange and share data between different devices without human involvement. The two main components of the machine type communication are MTC users and the MTC servers. The MTC servers are joined with LTE network and are utilized to communicate with two or more MTC devices. MTC user uses the services provided by the different MTC servers [13].

C. LTE Advanced Network architecture

System Architecture Evolution (SAE) /Long term evolution (LTE) provides the description of EPC, Evolved Universal Terrestrial Radio Access (E-UTRA) network and E-UTRAN. These parts are individually one by one compare with radio access system, system center and framework air interface. In the LTE Advance frameworks, the E-UTRAN and E-UTRA is tiny bit enhanced, while the structural planning of center system (i.e., EPC) is not experiencing vast adjustments the LTE framework construction modeling. The principle distinction in the structural planning of E-UTRAN from the construction modeling of LTE E-UTRAN is the enhanced Node B (eNB or eNodeB). The eNodeBs give the air interface between the control plane convention terminations and the client plane towards the client gear (UE). Both of the eNodeBs are the sensible components that give administration to one or more E-UTRAN cells and the interfacing between the eNodeBs is known as the X2 interface. These system interfaces are based on IP conventions. The eNodeBs are joined with the MME/GW (Mobility Management Entity/Gateway) by using S1 interface as represented in Fig. 3.

In LTE-A network architecture, MME/GW is split into two separate parts. The logical gateway (GW) is again isolated into two different entities; one is the Serving Gateway (S-GW) and the other is Packet Data Network Gateway (P-GW). The Serving gateway acts as a limited anchor for the mobility service to send and receive the packet data rates to and from the eNodeB to serve the UE, while the packet data network (P-GW) is interface with the outside Packet Data Networks (PDNs), for example the IMS (Internet multimedia server) and the Internet. P-GW gives other IP capacities, for example, packet filtering, directing, arrangement explanation, and location distribution [14].

Table 1 shows the comparison of the LTE and LTE advanced system specifications.

IV. 3GPP LTE SECURITY ARCHITECTURE

In 1996, when the third Generation framework known as UMTS was being created in the European Telecommunications Standards Organization (ETSI), the open door was taken to survey the premise for security in existing versatile frameworks and to grow new security construction modeling particularly to be utilized as a part of UMTS. This early work was along these lines taken forward into the Third Generation Partnership Project (3GPP) and this will be the premise for the Release 99 organization of 3G frameworks [16]. There is no big difference between the security architecture of 3GPP and LTE. It consists of five security levels which are given as follows and shown in Fig. 4.

Network entrance security (I): This layer characterizes the arrangement of security parameters which furnish clients with protected access to EPC and ensure beside numerous assaults on the access interfaces. This level provides the security systems, for example, trustworthiness insurance and ciphering between the Mobile Equipment (ME), Universal Subscriber Identity Module (USIM), the E-UTRAN and substances in the EPC.

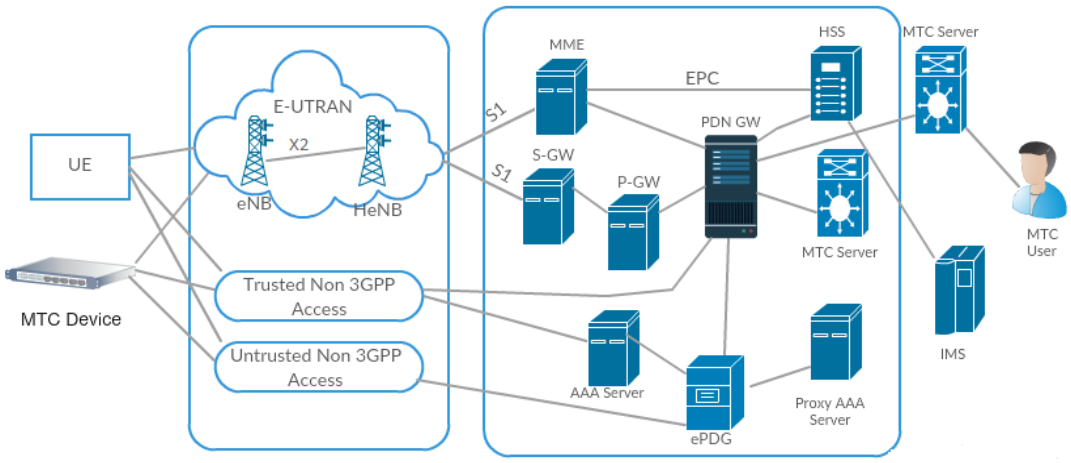

Fig. 3. LTE Advance Network architecture [14]

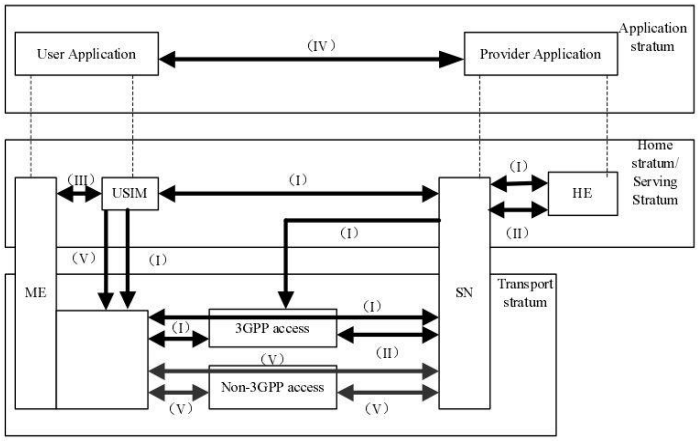

Fig. 4. Security Architecture of LTE [15]

Table 1: Comparison of LTE & LTE-A

Specifications	LTE	LTE-A
Standard	3 GPP Release 9	3 GPP Release 10
Peak Data Rate	300 MBps	1 GBps
Download Rate	10-100 MBps	100-300 MBps
Upload Rate	5-50 MBps	10-70 MBps
Bandwidth	Supports 20MHZ, 15MHZ, 10MHZ, 5MHZ and <5MHZ	70 MHZ in downlink, 40 MHZ in uplink
Latency (Delay)	In user plan < 5 ms, in control plane < 50 ms	From idle to connected in less than 50 ms and then shorter than 5 ms
Throughput	About 100 MBps for single chain	2 times less than LTE
Peak Spectrun Efficiency	5 bps in downlink, 2.5 bps in uplink	30 bps in downlink, 15 bps in uplink
Career Aggregaton	Not supported	Supported
Relay Node	Not Supported	Supported
Multiple Access technology	OFDMA for downlink, DFTS- OFDM for uplink	Hybrid OFDMA for downlink, SC-FDMA for uplink

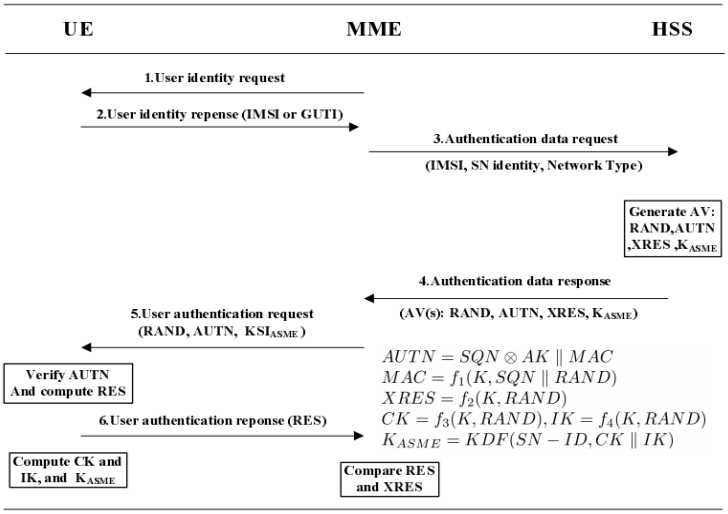

Fig. 5. EPS AKA [17]

Network domain security (II): This layer defines the set of security parameters that allow nodes to securely exchange signaling data and the user data. This layer also provides the protection against the wire line attacks in network.

User domain security (III): This layer characterizes the arrangement of security parameters with a specific end goal to give a mutual authentication and a protected access to the mobile station.

Application realm security (IV): This layer characterizes the rules that permit the provider domain and user application to exchange message in secure manner.

Non 3GPP realm security (V): This layer defines the rules that allow the user equipment to get right of entry to the EPC by means of non-3GPP system in secure manners and also provide protection to the access link [18].

A. Security in cellular system

AKA mechanism is used to achieve the security of cellular system. AKA is used for mutual authentication between EPC and UE in 3GPP [19]. While LTE uses Extensible Authentication Protocol-AKA (EAP-AKA) or Improved EAP-AKA to achieve the authentication between user equipment and non 3GPP access network. This is implemented by AAA server.

AKA generates two type of keys i.e. cypher (CK) and integrity (IK) keys. These keys are utilized to determine different session keys the integrity protection and the encryption. When an UE establishes a connection with the EPC via the E-UTRAN, then EPS AKA protocol is used to perform mutual authentication between EPC and UE [17] as appeared in Fig. 5.

Moreover, the different key hierarchy has been presented to secure user data traffic and the signaling as appeared Figure. 6. In this situation, when a UE associate with the EPC through non-3GPP entree systems, then the non-3GPP authentication will be performed between the AAA server and the UE. In roaming conditions, authentication signaling will pass through the Proxy AAA. The trusted non-3GPP systems can be pre-designed at the UE [20]. In the event that there is no pre-configured data at the UE, the UE should consider the non-3GPP system untrusted, for a trusted non-3GPP access organize the client equipment and the AAA server will actualize the Extensible Authentication Protocol-AKA (EAP-AKA) or Improved EAP-AKA (EAP-AKA) to perform the access verification. As client hardware associate with the EPC over an untrusted non-3GP access organize, the ePDG and the client equipment need to perform the IPsec tunneling technique. The ePDG and the user equipment shall use the Internet Key Exchange Protocol Version 2 (IKEv2) with EAP AKA or EAP-AKA' to build up IPSec security affiliations [1].

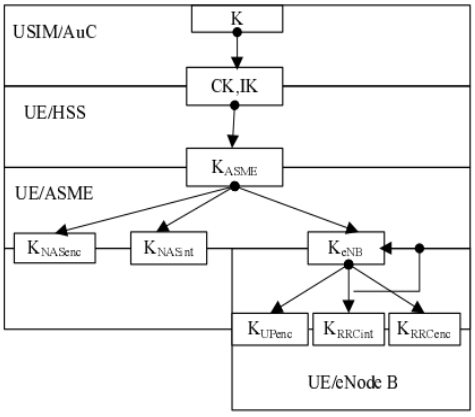

Fig. 6. Key Hierarchy of 3GPP LTE [20]

V. VULNERABILITIES IN 3GPP LTE AND LTE-A

With the passage of time, security movements are changing. In first generation mobile networks, there is not so much security because at that time the attacks like eavesdropping, man-in-the-middle attack etc. are not common. By the time to overcome these attacks new

advancements are made and the concept of AKA mechanism was introduced, this mechanism proved to be very good. However its security is week since Its validation is stand out directional; the client can't verify the serving network. To build the security, 3GPP AKA instrument is presented which comprises of two way confirmation and Key agreement to incorporated key between the mobile terminal and the serving system .It likewise give freshness certification of cipher key and trustworthiness key.

In spite of the fact that the 3GPP AKA has been acknowledged as dependable and utilized, there still exist shortcomings in 3GPP AKA. The shortcomings incorporate (1) diverting client movement utilizing false BS and versatile terminals, (2) given the way that the counter estimation of set to a high value by foe, the mobile terminal's life time may be reduced, (3) on the grounds that a home system keeps a counter and powerfully synchronized for each versatile terminal, a flaw in counter database might influence every single versatile terminal [6].

After that in LTE/LTE-A Extensible Authentication Protocol-AKA (EAP-AKA) or Improved EAP-AKA (EAP-AKA') is utilized to perform the access confirmation. In any case, there are a few issues happen because of IP based building design of LTE/LTE-A system. These attacks are injection, eavesdropping, modification and more privacy risks than those mentions above [1].Traditional attacks already present in the internet like IP location mocking, DoS assaults, infections, worms, spam sends and calls will probably influence the LTE structural engineering [21].

There are some other problems exist in LTE system are cause by base station. As LTE is IP base network so attackers have direct path to the base station. And once they get into the base station they can damage the entire network. In addition, HeNBs are very easy to attain by an attacker, due to this foe can thus generate its own reprobate versions which gives functionality of a base stations and users at the same time. By using this type of base stations, the enemy can pretend as genuine base stations to the whole network to become legitimate users. And, it can also masquerade legitimate users to create connections with genuine base stations. Furthermore, the HeNB can be placed in that regions of the Internet which are not secure, by doing this they will be susceptible to a lot of physical intrusion threats [22].

The LTE construction modeling delivers some new issues in the handover confirmation procedures. When user equipment changes its position from one eNB/HeNB to new HeNB/eNB as appeared in Fig. 7, there exist different mobility issues. Handover mechanism allows any calls to transfer in the network without any interruption. Many problems occur in handover mechanism which is listed below. Diverse handover confirmation strategies are required in various circumstances, for example, the handovers between eNBs, between HeNBs, between a HeNB and an eNB, and the between MME handovers when the base stations are overseen by various MMEs, which will expand overall system complexity. Likewise, in LTE system few mixed access systems could co-occur, due to this, network is vulnerable to more security threats especially when the mobility is maintained among the heterogeneous networks. Handover delay increases during the roaming when multiple network transfer multiple massages and for this purpose authentication is required. Key generation process of LTE is also complicated that is multiple key derivations which increase the network delay and complexity .This make network more vulnerable to attacker. Simple solution for handover mechanism is mutual authentication. Another method is that when user equipment enters in eNB or HeNB exposure they can perform authentication process directly in between themselves to create session keys [23].

Other problems that occur in LTE/LTE-A are on physical layer. These are of two types first is noise which is generated by using white Gaussian noise (WGN).The second one is Multi-carrier interface which is generated by identifying carries that are used by the system and injecting a very narrow band signal to them. This technique is easy to implement who have knowledge equipment to carry out this type of attacks. Although this problem is easy to detect and address [21].

These vulnerabilities won't just convey a considerable measure of trouble to sustain the persistent availability in the LTE systems, additionally might be misused by foes to assault different access systems or the central system to exhaust the system resource, even to incapacitate the whole systems.

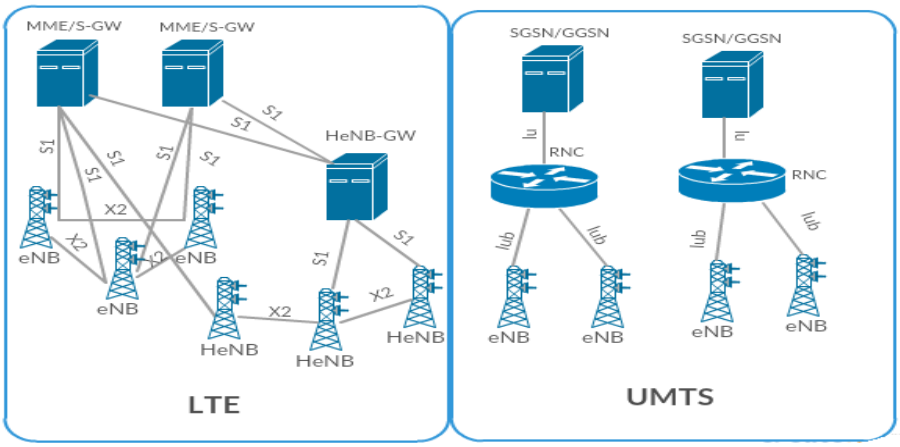

Fig. 7. Comparison of Access Network Architecture [15]

V. OPEN RESEARCH ISSUES

Although much work has been done for the improvement of LTE/LTE-A network security architectures, but many security problems for the LTE/LTE-A networks still exist without proper solutions. In this section, some research directions on the Long term evolution security are suggested as the possible future works. These research directions are given below:

(1) The real future examination for the LTE security will be the configuration of MTC security systems in LTE/LTE-A systems on the grounds that the presentation of the MTC into the 3GPP system construction modeling stays in its starting period of the advancement. (2)Such security instruments are required that ensure the solid rapid availability for sensitive information (3) The proportion of encryption overhead and the measure of data to be exchanged must be considered. Since the MTC gadgets are little in size however they require high information rates. (4) Diverse Novel access verification plans for clog evasion are required to accomplish the concurrent validation of various devices. (5) Such secure mechanisms are required that guarantee the safe communication among MTC devices. Future LTE network needs to develop end-to-end safe devices for machine-to-machine communications between two MTC devices. (6) Such secure mechanisms are required that support the high speed mobility and the restricted mobility of the MTC devices.

VI. CONCLUSION

In this paper, we have initially delineated the system architectures of 3GPP, LTE and LTE advanced. We then talked about the security architectures of 3GPP, LTE and LTE-A systems. We encourage examined the disadvantages existing in the security building design of the 3GPP, LTE and LTE-A remote systems. Our review has investigated that there are still a considerable measure of security problems in the existing LTE systems. At last, we have summarized possible open examination issues as the recommendation for the future exploration exercises on the security of LTE and LTE-A remote systems.

REFERENCES

[1] C. Jin, M. Maode, L. Hui, Z. Yueyu, And L. Zhenxing, "A Survey On Security Aspects For Lte And Lte-A Networks," Communications Surveys & Tutorials, Ieee, Vol. 16, Pp. 283-302, 2014.

[2] J. Jermyn, R. P. Jover, M. Istomin, And I. Murynets, "Firecycle: A Scalable Test Bed For Large-Scale Lte Security Research," In Communications (Icc), 2014 Ieee International Conference On, 2014, Pp. 907-913.

[3] 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.

[4] 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.

[5] 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.

[6] Z. Li, Q. Hang, M. Huaqing, And H. Zhiwen, "Research On 3gpp Lte Security Architecture," In Wireless Communications, Networking And Mobile Computing (Wicom), 2012 8th International Conference On, 2012, Pp. 1-4.

[7] I. T. V. Mancuso. (2. December 2015). Umts Core Network. Available: Http://Www.Tti.Unipa.It/~Ilenia/Course/13-Umts-Core.Pdf

[8] L. Xiehua And W. Yongjun, "Security Enhanced Authentication And Key Agreement Protocol For Lte/Sae Network," In Wireless Communications, Networking And Mobile Computing (Wicom), 2011 7th International Conference On, 2011, Pp. 1-4.

[9] G. M. Koien, "Mutual Entity Authentication For Lte," In Wireless Communications And Mobile Computing Conference (Iwcmc), 2011 7th International, 2011, Pp. 689-694.

[10] S. Uskela, "All Ip Architectures For Cellular Networks," Presented At The 3g Mobile Communication Technologies, Second International Conference On (Conf. Pub. No. 477), London, 2001.

[11] 3gpp, "3rd Generation Partnership Project; Technical Specification Group Services And System Aspects; Ip Multimedia Subsystem (Ims); (Rel 11), 3gpp Ts 23.228 V11.6.0 ", Ed, Sep. 2012.

[12] 3gpp, "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," Ed, Sep. 2012.

[13] 3gpp, "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 ", Ed, Sep. 2012.

[14] G. A. Abed, M. Ismail, And K. Jumari, "The Evolution To 4g Cellular Systems: Architecture And Key Features Of Lte-Advanced Networks," Spectrum, Vol. 2, 2012.

[15] J. Wang, Z. Zhang, Y. Ren, B. Li, And J.-U. Kim, "Issues Toward Networks Architecture Security For Lte And Lte-A Networks," International Journal Of Security And Its Applications, Vol. 8, Pp. 17-24, 2014.

[16] C. Blanchard. (2. December 2015). Security For The Third Generation (3g) Mobile System. Available: Http://Www.Isrc.Rhul.Ac.Uk/Useca/Otherpublications/3g_Umts%20security.Pdf

[17] 3gpp, "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," Ed, Sep. 2012.

[18] C. Xenakis And L. Merakos, "Security In Third Generation Mobile Networks," Computer Communications, Vol. 27, Pp. 638-650, 5/1/ 2004.

[19] Y. Park And T. Park, "A Survey Of Security Threats On 4g Networks," In Globecom Workshops, 2007 Ieee, 2007, Pp. 1-6.

[20] 3gpp, "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," Ed, June 2012.

[21] S. K. Mohapatra, B. R. Swain, And P. Das, "Comprehensive Survey Of Possible Security Issues On 4g Networks," International Journal of Network Security & Its Applications, vol. 7, p. 61, 2015.

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

[23] M. M. Masud, "Survey of security features in LTE Handover Technology," system, vol. 1, p. 2, 2015.