IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Issue-3 E-ISSN: 2347-2693

Investigating Various Possible Attacks and Vulnerabilties in LTE

A. Ahlawat[1*], S. Kumar[2]

[1*]Electronics and Communication, University Institute of Engineering and Technology, MDU, Rohtak, India
[2]Electronics and Communication, University Institute of Engineering and Technology, MDU, Rohtak, India

[*]*Corresponding Author: ahlawat.anu@gmail.com*

Available online at: www.ijcseonline.org

Received: 20/Feb//2018, Revised: 26/Feb2018, Accepted: 19/Mar/2018, Published: 30/Mar/2018

***Abstract*—** This paper provides a comprehensive study of vulnerabilities and various possible attacks associated with LTE. According to reports released by GSMA, association of mobile operators, the number of cell phone users globally will surpass five billion by the middle of this year. With this rapid increase in the number of users, security of cellular network is of utmost importance. In order to ruggedize the security mechanism of cellular networks it is first essential to deeply analyse the vulnerabilities and threats. This paper surveys the attacks and vulnerabilities and provide classification and categorization of attacks in LTE.

***Keywords*—** UMTS (Universal Mobile Terrestrial System), LTE (Long Term Evolution), DoS (Denial of Service), MITM (Man In The Middle), IP address (Internet Protocol), MAC address (Medium Access Control), AKA (Authentication and Key Agreement), ICMP (Internet Control Message Protocol), EPS (Evolved Packet System), 3GPP (3rd Generation Partnership Projects), WLAN (Wireless Local Area Network), QoS (Quality of Service), OSI (Open System Interface), GSM (Global System for Mobile Communication), WPA (Wi-Fi Protected Access), TCP (Transmission Control Protocol), UDP (User Datagram Protocol), IMSI (International Mobile Subscriber Identity), HSS (Home Subscriber System), AuC (AuthenticationCenter).

I. INTRODUCTION

The cellular networks have shown a tremendous growth in the past decades from its First Generation (1G) to 4th Generation which is still evolving hence termed as Long-Term Evolution (LTE). Apart from the advancement shown in the switching mechanism i.e. from circuit switched networks to packet switched networks, there also have been advancement in AKA mechanism. Authentication has moved from single authentication (in GSM) to mutual authentication (in 3G and LTE). This evolution introduced complexity in the network as well as new vulnerabilities and threats. Since the cell phones are being used for various e-commerce applications and sharing of confidential information, hence these threats stand as a major concern for security as well as performance of network. [1]

Cellular Networks are based on OSI protocol architecture comprising layers namely: application, transport, network, MAC and physical. Different security mechanisms and protocols are applied at these layers to enhance the security of cellular networks. For example, to prevent the discloser of information to any unauthorized user cryptography technique is used. Although cryptography helps to achieve confidentiality yet it imposes various constraints of computational power and time. In order to achieve authenticity of a user, multiple authentication approaches are employed at different protocol layers. Particularly, MAC-layer uses MAC address, network layer uses WPA and WPA2 and transport layer uses SSL and TLS protocols for authentication. However, these protocols are vulnerable to various threats including DoS, Jamming, Eavesdropping, MIMT, Flooding, Replay, Impersonate and Sybil attacks etc.

In this paper we are motivated to investigate the possible threats and vulnerabilities in the cellular networks and explore open security issues in cellular networks. Section II reviews various possible attacks categorized on the basis of different layers. Section III focuses on various vulnerabilities in LTE. Section IV discusses issues that are still unaddressed. Finally, the last section provides the conclusion.

II. CATEGORIEZATION OF ATTACKS

A. PHYSICAL-LAYER ATTACKS

The broadcast nature of cellular transmission and flat-IP based architecture of LTE has made the physical layer more vulnerable to eavesdropping and jamming attacks compared to GSM or UMTS. The eavesdropping attacks are carried with sole aim of gathering confidential information of legitimate users [2]. However, when a malicious user prevents any authorized user from using the services, then such types of attacks are termed as Jamming [3] or DoS. The two types of physical layer attacks are tabulated below.

Table 1. PHY-layer Attacks

Physical-Layer Attacks	Characteristics
Eavesdropping	Interception of Confidential Information
Jamming	Interception of legitimate transmission

B. MAC-LAYER ATTACKS

Each node in the network is assigned its own unique MAC address. When any malicious user changes its own MAC address with some wrong intentions, then it is known as MAC spoofing [4]. However, when any malicious user steals away MAC address of a legitimate user by overhearing the network traffic, such attacks are termed as Identity-theft attacks. Apart from the aforementioned attacks MAC layer also suffers from MITM [5] attacks and network injection. MIMT attack is sort of impersonation of two legitimate users with an aim of intercepting their secured session and controlling the entire communication. Network Injection [6] are types of attacks which disrupts the operation of network devices like switches, routers etc. The categorization of attacks is tabulated below.

Table 2. MAC-Layer Attacks

MAC-Layer Attacks	Characteristics
MAC spoofing	Falsification of MAC address
Identity Theft	Stealing Legitimate user's identity
MIMT attack	Impersonation of identity of a pair of legitimate user
Network Injection	Injection of forged network commands

C. NETWORK-LAYER ATTACKS

The network layer attacks are basically categorized into three categories namely IP spoofing, IP hijacking and Smurf attack. IP spoofing [7] is basically a way of concealing identity of the attacker for carrying out illicit activities. IP hijacking [8] is a sort of attack in which attacker takes away legitimate user's IP address. The Smurf attack [9] is a kind of DoS attack. The table given below provides different types of attacks at this layer:

Table 3. Network-Layer Attacks

Network Layer Attacks	Characteristics
IP spoofing	Falsification of IP address
IP hijacking	Impersonation of legitimate user's IP address
Smurf Attack	Blocking of network by sending huge number of ICMP requests

D. TRANSPORT-LAYER ATTACK

The attacks at this layer are basically classified into either as TCP attack [10] s or UDP attacks [11]. The further categorization of TCP and UDP attacks is tabulated by the table given below:

Table 4. Transport-Layer Attacks

Transport-Layer Attacks	Characteristics
TCP flooding	Paralysation of network by sending huge number of ping requests
UDP flooding	Sending a huge number of UDP packets
TCP sequence prediction attack	Legitimate user's data packets are fabricated using TCP sequence index

E. APPLICATION-LAYER ATTACKS

The application layer attacks are classified as HTTP (Hypertext Transfer Protocol) attacks [12], FTP (File Transfer Protocol) attacks [13], SMTP (Simple Mail Transfer Protocol) attacks [14]. The different types of attacks at this layer are enlisted and explained by the table below:

Table 5. Application-Layer Attacks

Application-Layer Attacks	Characteristics
Malware attack	Malicious software in form of code and active content programmed by attackers
SQL Injection	Inserting rogue SQL statements to gain unauthorized access
Cross-site scripting	Injecting client-side scripts into web pages
FTP bounce	Impersonating a legitimate user to gain unauthorized access
SMTP attack	Malicious attacks in e-mail

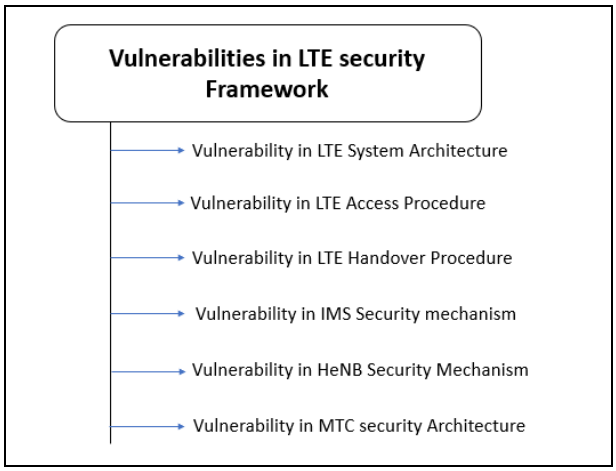
III. VULNERABILITIES IN LTE

In order to launch attacks in LTE there are various possible origin points namely Internal, External and Attacks from mobile devices. The internal attacks can be launched through two different possible entries namely: access network, the backhaul and core network, whereas the external attacks can be launched though other external or 3rd party networks. The figure given below shows various possible scenarios for origin of attacks.

Figure 1. Origin Points for various security attacks

Whenever security aspects of LTE network are considered then each of the aforementioned sections requires a different

set of security requirements. Hence the vulnerabilities existing in LTE network can be broadly categorized into six categories depending upon the LTE security framework. The six aspects of LTE vulnerability are depicted by figure given below.



Each of these vulnerabilities are explained in detail in the sections below.

A. Vulnerability of LTE System Architecture

To achieve full internetworking, the LTE network has flat all-IP based architecture. This advancement towards IP architecture has introduced new vulnerabilities in security mechanism of LTE.

- The flat IP-based architecture of LTE networks has made it more vulnerable to risks such as eavesdropping attacks, modification, injection as compared to that of GSM and the UMTS networks [15], [16]. Apart from the aforementioned risks LTE networks are even prone to malicious attacks present in Internet like worms, spams, IP spoofing etc. [17].
- The base stations of LTE systems cause some other potential weaknesses in the security architecture of LTE. The all-IP network provides a direct path to the base stations for malicious attackers. The Base stations in LTE network are more vulnerable to attacks as compared to those of UMTS networks, where only a couple of RNCs are managed by serving node however in LTE network architecture numerous eNBs are managed by MME as clearly depicted from the figure given below, which shows a comparison between network architecture of UMTS and LTE. Moreover, HeNBs are easily obtained by attackers since they are small and low cost. The attacker then creates its own rogue base station and impersonates a genuine base station and makes the network susceptible to large number of threats. [18].

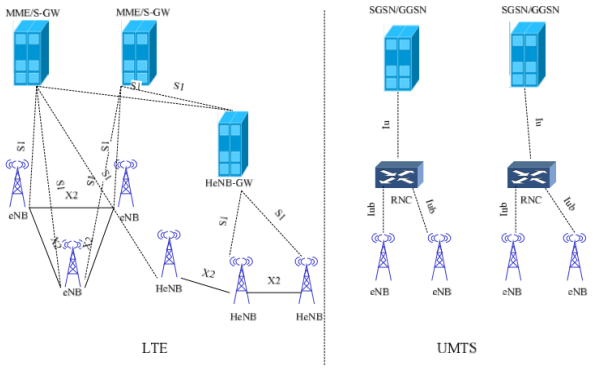


Figure 2. Comparison of Network architecture of LTE and UMTS

- The IP-based architecture also introduced new problems in handover authentication procedure. Because of small and low cost HeNB, several mobility scenarios are introduced in LTE networks as shown in Fig 3. Different handover scenarios require different handover procedures for example handovers between HeNBs, between eNB and HeNB and thereby increasing system complexity

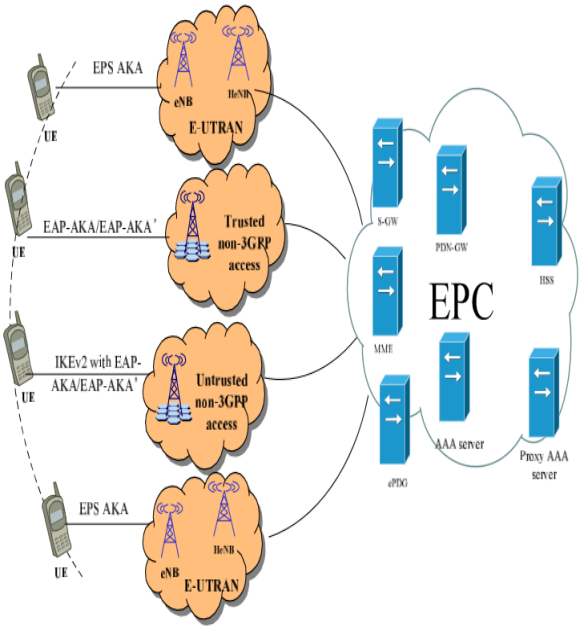


Figure 3. Handover Mechanism

B. Vulnerability in the LTE Access Procedure

To prevent malicious attacks such as MIMT attacks, redirection attacks, identity catching attacks, some improvements in authentication mechanism of UMTS i.e. AKA were made and a new authentication mechanism EPS AKA was introduced for LTE networks. However, some vulnerabilities still exist in EPS AKA. Some of the vulnerabilities are enlisted below:

- Disclosure of User Identity

The EPS AKA mechanism does not provide privacy protection i.e. it does not prevent disclosure of IMSI. When the user registers for the first time to the network, MME requests the IMSI of the user, the user transmits the IMSI without any encryption. Once the identity of the user is disclosed it can lead to several other security issues. In [19], authors have proposed an active attack model for stealing IMSI and concluded that the current security mechanism could not prevent such attacks.

- DoS Attacks

In case of EPS AKA protocol DoS attacks cannot be prevented [19], [20]. Firstly, as it is clear from figure 5 MME have to forward UE's requests to HSS or Authentication Center before the authentication of UE and secondly, MME authenticates UE only after receiving RES. These two aforementioned conditions provide a platform for an adversary to launch DoS attacks [19], [21]. Hence the malicious user sends a huge number of fake IMSI's to HSS/AuC which results in consumption of computational power for generation of authentication vectors for the UE. On the other side, memory buffer of MME is consumed as it has to wait for a long period of time for a response from malicious user.

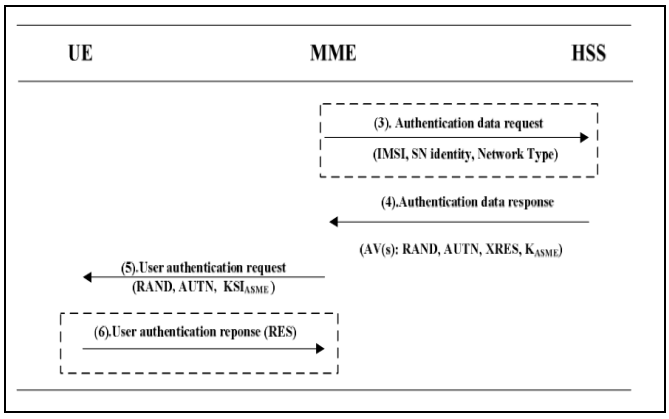


Figure 5. Authentication Procedure

- Increased Bandwidth Consumption and Signalling Overhead

During the authentication procedure whenever any user stays in the SN for a long period of time and its authentication vector gets exhausted then the SN rely upon the HN for a set of another authentication vector which causes huge amount of bandwidth consumption and storage consumption in SN [22].

- Lack of online authentication

In case of EPS-AKA the HN is offline as the LTE authentication lacks the ability of online authentication. As a result of offline mode of operation of HN it can be traced back.

- EAP-AKA shortcomings

The LTE architecture reuses EAP-AKA whenever the UE accesses to EPC through a trusted non-3GPP access network. The authors in [23] pointed out several loopholes in EAP-AKA protocol namely MIMT attacks, user identity disclosure, additional bandwidth consumption and lack of sequence number synchronization.

C. Vulnerability in the LTE Handover Procedure

The various vulnerabilities associated with handover key mechanism are enlisted below:

- Absence of backward security

The LTE key management mechanism is based on chaining architecture i.e. the current eNB derives new keys by chaining the current key with eNB specific parameter. Once the current eNB is compromised by the attacker, then subsequent key sessions can be traced easily. Hence the backward security is not achieved by LTE handover key management. [24]

- Vulnerability to de-synchronization attacks

The attacker uses rogue eNB to disrupt the NCC from being refreshed. In the de-synchronization attacks, the targeted eNBs desynchronizes the NCC value as a result of which horizontal handover key derivation can only be performed thereby making future session keys vulnerable to attacks. [25]

- Vulnerability to the replay attacks

Replay attacks prevents establishment of secure connection between an UE and a target eNB. The attacker firstly intercepts handover request message and whenever the UE wants to move to target eNB, then the attacker re-transmits the intercepted handover request messages instead of original ones. As a result of this a new handover procedure has to be launched by UE. [25]

D. Vulnerability in IMS Security Mechanism

The working of IMS is based on SIP and IP and is vulnerable to various attacks given below:

- Increased energy consumption and system complexity

An IMS UE has to execute two AKA protocols i.e. EPS AKA for LTE authentication and IMS AKA for IMS authentication that increases energy consumption and reduces battery life.

- Vulnerable to MIMT and Lack of SQL synchronization

The working of IMS AKA is based on EAP AKA scheme thus making it vulnerable to MIMT attacks and lack of SQL synchronization.

- Vulnerability to DoS attacks

E. Vulnerability in HeNB Security Mechanism

The authors in [26] presented various vulnerabilities existing in HeNB security mechanism are due to insecure wireless links between UE and HeNB making it susceptible to various attacks.

- Lack of a mutual authentication between the UE and the HeNB

Lack of mutual authentication in HeNB security mechanism has made it prone to various security attacks namely MIMT attacks, eavesdropping and masquerading attacks. [27]

- Vulnerability to DoS attacks

The authors in [28] presented that HeNB security architecture is vulnerable to various Internet-based attacks, specifically DoS attacks.

F. Vulnerability in MTC Security Architecture

MTC security architecture of LTE is still in its initial stage. The MTC devices are prone to various types of attacks including protocol attacks, physical attacks, leakage of confidential information and many more. Such attacks occur due to low energy and computing capabilities of MTC devices. Furthermore, MTC has massive number of devices so when they simultaneously try to access the network then simultaneous authentication can cause signaling overhead between HSS and MME.

IV. OPEN CHALLENGES

This section presents security issues that are still not mitigated and the issues that needs further research investigation.

A. Addressing LTE Availability and Security Attacks

As aforementioned that DoS and DDoS can be performed by exploiting vulnerabilities of LTE networks, these attacks are still an open issue. Physical and MAC layer are still open to various attacks as pointed in [29], [30]. There is need to further enhance the encryption mechanisms at physical layer. DoS attacks are also resulted because of amalgamation of WLAN and LTE networks [31], [32]. Various solutions have been proposed however efficiency of the proposed solutions has not been demonstrated on cellular networks. There are some more issues in LTE security architecture worth investigating. The security architecture needs to be further ruggedize to prevent traditional protocol attacks and physical intrusions in LTE. The EPS AKA authentication mechanism needs additional enhancements in order to prevent disclosure of identity, DoS and other malicious attacks. Several papers have been published related to EPS AKA weakness such as bandwidth consumption and signaling overhead [33]-[35]. Apart from the improvements mentioned above key management mechanism and handover authentication procedure needs further enhancements in order to prevent the aforementioned attacks in LTE handover mechanism.

B. Addressing Backhaul Attacks

IP-based attacks mainly target control elements and interfaces. In order to address IP-based attacks in backhaul networks several solutions have been proposed by different authors such as IP-based traffic encryption and certificate authority. However, the proposed solutions need further improvements. E-UTRAN is vulnerable to various attacks including redirection attacks, eavesdropping, false base station, MIMT and DoS attacks. In order to mitigate these issues various countermeasures have been proposed. However, the proposed solutions are not fully efficient and hence it is necessary to further ruggedized security mechanism to deliver better services to the users. Also, physical layer of E-UTRAN is vulnerable to a major threat i.e. Jamming that needs more research investigation.

Several solutions based on physical layer secret key generation, information-theoretic security, diversity assisted security and many more approaches have been proposed by the researchers but these approaches are at their infancy and further enhancements are needed to get a practical design that is easy to implement.

V. CONCLUSIONS

This paper provides a comprehensive review of various vulnerabilities in LTE cellular networks taking into consideration different security aspects. It deeply analyzed various possible threats experienced at different layers from application to physical layer. Dos and DDoS attacks need further investigation as they are still an open issue and need

to be addressed to enhance efficiency of cellular networks for seamless delivery of services.

There are some more issues in LTE security architecture that are worth investigating including the vulnerabilities existing in EPS-AKA protocol as aforementioned. Handover authentication procedure and key management mechanism needs to be ruggedized to reduce de-synchronization and replay attacks. Hence it is of paramount importance to enhance the security of cellular networks either by increasing length of secret keys, and by ruggedizing the encryption algorithms to improve the confidentially and integrity of the cellular network. This paper will provide researchers a complete overview of possible threats in LTE and vulnerabilities that are still unaddressed and needs further investigation by security architecture designers.

REFERENCES

[1] A. Ahlawat and S. Kumar "*Analysis of Different Security and Vulnerability in Cellular Networks*", Journal of Engineering and Applied Sciences, vol 12, no.22, pp. 6252-6259, 2017.

[2] A. Perrig, J. Stankovic, and D. Wagner "*Security in wireless sensor networks*", Commun. ACM, vol. 47, no. 6, pp. 53–57, 2004.

[3] A. Mpitziopoulos "*A survey on jamming attacks and countermeasures in WSNs*", IEEE Commun. Surv. Tut., vol. 11, no. 4, pp. 42–56, 2009.

[4] V. Nagarajan and D. Huang "*Using power hopping to counter MAC spoof attacks in WLAN*", in Proc. IEEE Consumer Communication Network Conf., Las Vegas, NV, USA, pp. 1–5, 2010.

[5] W. Zhou, A. Marshall , and Q. Gu "*A novel classification scheme for 802.11 WLAN active attacking traffic patterns*", in Proc. IEEE Wireless Commun. Netw. Conf., Las Vegas, NV, pp. 623–628, 2006.

[6] J. Park and S. Kasera "*Securing Ad Hoc wireless networks against data injection attacks using firewalls*", in Proc. IEEE Wireless Communication Network Conf., Hongkong, China, pp. 2843–2848, 2007.

[7] Computer Emergency Response Team (CERT) CERT Advisory "*IP Spoofing Attacks and Hijacked Terminal Connections*", 1995.

[8] N. Hastings and P. McLean , "*TCP/IP spoofing fundamentals*," in Proc. IEEE 15th Annu. Int. Conf. Comput. Communication, Phoenix, AZ, USA, pp. 218–224, 1996.

[9] B. Harrisa and R. Hunt "*TCP/IP security threats and attack methods*", Computational Communication, vol. 22, no. 10, pp. 885–897, 1999.

[10] C. Schuba et al. "*Analysis of a denial of service attack on TCP*", in Proc. IEEE Symp. Security Privacy, Oakland, USA, pp. 208–223, 1997.

[11] A. Kuzmanovic and EW. Knightly" Low-*rate TCP-targeted denial of service attacks and counter strategies*", IEEE/ACM Trans. Netw., vol. 14, no. 4, pp. 683–696, 2006.

[12] B. Haibo, L. Sohraby, and C. Wan "*Future internet services and applications*", IEEE Network, vol. 24, no. 4, pp. 4–5, 2010.

[13] RFC 2577 FTP security considerations. [Online]. Available: http://tools. ietf.org/html/rfc2577, 1997.

[14] T. Bass, A. Freyre, D. Gruber, and G. Watt "*E-mail bombs and countermeasures. Cyber-attacks on availability and brand integrity*", IEEE Network, vol. 12, no. 2, pp. 10–17, 1998.

[15] M. 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), pp.94-97, 2009.

[16] 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), pp.439-444, 2010

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

[18] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE), (Rel 9), 3GPP TR 33.821 V9.0.0, 2009.

[19] 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), pp.1-5,2007.

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

[21] 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), pp.1-6, 2010.

[22] 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), pp.557-563, 2011.

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

[24] 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, pp. 2119-2131, 2012.

[25] H. Han Security "*Analysis and Enhancements in LTE-Advanced Networks*", Ph.D. Dissertation, Department of Mobile Systems Engineering, The Graduate School, Sungkyunkwan University, 2011.

[26] 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, 2012.

[27] CK. Han, HK. Choi and IH. Kim "*Building Femtocell More Secure with Improved Proxy Signature*", Proc. IEEE GLOBECOM 2009, USA, pp. 1-6, 2009.

[28] I. Bilogrevic, M. Jadliwala and JP. Hubaux "*Security and Privacy in Next Generation Mobile Networks LTE and Femtocells*", Femtocell Workshop, 2010.

[29] B. Matt and C. Li "*A survey of the security and threats of the IMT advanced requirements for 4G standards*", in Proc. IEEE Conf. Anthol., pp. 1–5, 2013.

[30] M. Habib and M. Ahmad "*A review of some security aspects of WiMAX and converged network*" In Proc.2ndInt.Conf.Commun.Softw. Netw. (ICCSN), pp. 372–376, 2010.

[31] N. Qachri and JM. Dricot "*On the security of WLAN access points integrated /LTE architectures*", in Proc.19thIEEE Workshop Local Metropolitan Area Netw. (LANMAN), pp. 1–6, 2013.

[32] TQ. Thanh, Y. Rebahi, and TA. Magedanz "*DIAMETER based security framework for mobile networks*", in Proc. Int. Conf. Telecommun. Multimedia (TEMU), pp. 7–12, 2014.

[33] X. Li and Y. Wang "*Security enhanced authentication and key agreement protocol for LTE/SAE network*", in Proc. 7th Int. Conf. Wireless Commun., Netw. Mobile Comput. (WiCOM), pp. 1–4, 2011.

[34] M. Purkhiabani and A. Salahi "*Enhanced authentication and key agreement procedure of next generation evolved mobile networks*", in Proc. IEEE 3rd Int. Conf. Commun. Softw. Netw. (ICCSN), pp. 557–563, 2011.

[35] H. Choudhury, B. Roychoudhury, and DK. Saikia "*Enhancing user identity privacy in LTE*", in Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun., pp. 949–957, 2012.

Authors Profile

Mrs. Anu Ahawat pursed Bachelor of Technology from Maharishi Dayanad University, Rohtak in 2013 and Master of Technology from Maharishi Dayanad University in year 2015. She is currently pursuing Ph.D. in Department of Electronics and Communication, Maharishi Dayanad University since 2017..

Col (Dr.) Suresh Kumar has served in Corps of Signals (Indian Army) After taking PMR, joined as teaching faculty in UIET, MDU Rohtak, in Department of ECE in October 2008. He did his B.Tech from CME Pune and MCTE Mhow in 1999 from JNU New Delhi in Electronics and Communication Engineering. He did his PhD. In ECE in 2011 on the title "CONTROL SPILL OVER OF TRANSMITTED POWER IN CDMA CELLULAR COMMUNICATION NETWORKS IN BORDER AREAS FOR DEFENCE FORCES". His area of specialization is wireless and Optical communication. He has guided 06 PhD. Thesis (04 awarded and 02 pursuing) and 24 M Tech students dissertations. He has published 85 papers in International Journals and international/national conf proceedings in India and abroad.

