AN OVERVIEW OF THE ATTACKS ON LTE IN 4G: EXPLOITING THE SECURITY

Nidhi
M. Tech Scholar, ECE Deptt.
University Institute of Engineering and Technology,
Maharshi Dayanand University
Rohtak, Haryana, India

Vikas Nandal
Asst. Professor, ECE Deptt.
University Institute of Engineering and Technology,
Maharshi Dayanand University
Rohtak, Haryana, India

Abstract: Communication in wireless provides a number of applications. Wireless communications have grown from last ten decades. Because of increased uses of wireless network and communication in our life, society has faced different problem to cyber security attacks and threats. In this paper we have studied various security threats on LTE system and their analysis and comparison to overcome these attacks has been done.

Keywords: Long term evolution; Wi-max; 4G; wireless; security

I. INTRODUCTION

4G is the 4th generation technology. In 4G, more bandwidth and services are provided as in comparison of 3G [1]. LTE and Wimax are two technologies that increase the levels of 4G [2].

I. Long Term Evolution

3GPP release specifications in 3G partnership project in which introduced the long term evolution. It is approved with download speeds up to 173mb/sec in 2008.It is based on internet protocol and orthogonal frequency division multiple access.

4G wireless is due to give the flexibility of different size, display, battery, computational power [3]. LTE and Wimax remain as the key of wireless technology. Fourth generation is used because it provides high data rates to the large number of users at a time [1]. It gives the higher speed as compare to the other generation. Due to this, it is used on wide scope. In 4G, different security issue arises, these all are due to the attacks on physical and Mac layer. In the next part discuss, different security **issues** as known the open nature of the 4G. So, it needs more security towards it. In 4G architecture, Y-comma frame work and Y-comma favors the heterogonous networking. It is internet protocol based and due to which, it faces the different problems. And, need to protect not only the data but also, the entities from each other and the network infrastructure. [4]

Security requirement in 4G is much more than 3G Network and needs a model to protect its infrastructure. These different security issues on different standards such as Wi-Fi security, wi-max security and3GPP LTE security.

I. Wi-Fi Security

Mainly this arises due to the change in the format of words during coding and decoding. After finding its weakness, we can approach, towards an efficient system.

II. Wi-Max Security

When the system does not support the management and integrity of the system, then this problem arises. After careful observation, its security system can be raise in a better way.

II. 3GPP LTE SECURITY

It is a standard form used for wireless communication. Different reasons, that effects it, one of the major reason is not to synchronize in a proper manner and security issue arise.

1. DIFFERENT ATTACKS IN LONG TERM EVOLUTION

Attacks affect the integrity of the system. There are mainly two types of attacks, one is active attack and other is passive attack. When the attackers only aim is to take the information and then it is passive attack. But its aim is not only take the information, but effect the integrity of the system is active attack. Passive attack is such that traffic problem arise, during communication. Other is unauthorized user, get the information is eavesdropping. Passive attacks are such as denial of service attack, resource consumption, masquerade attack, replay attack, information disclosure; message modification etc. [9]. Sensor network is used in wireless communication on a wide level. Larger number of nodes relates to the sensor networks, due to which different problem arise. Denial of service attackers, aim is to target the destination information, take the information. So, for, its need higher security, because on wireless sensor can be easily attacked. [12]
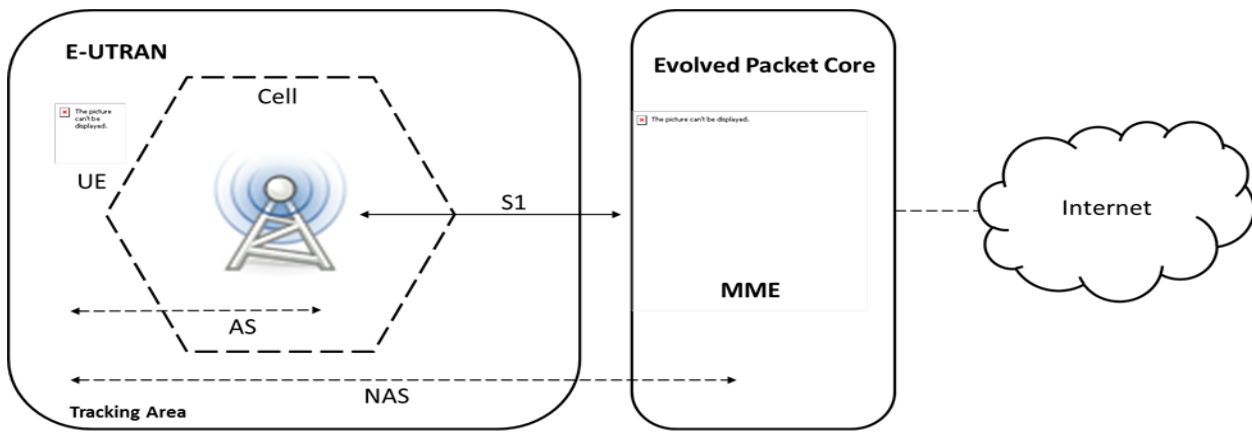
Different security Issue arises in wireless 4G network due to threats and attacks [2]. These attacks on physical layer and MAC layer attacks in 4G. These issues affect the integrity of the system. Attacker targets the physical layer or the MAC layer.

1. Physical layer issue

A private key is used between the two users when both the users do not have the private key then physical layer is used there, to convey the information between them and its need to discuss the different security issue in physical layer [9].

Wimax and LTE have two keys at the physical layer. These are interference and scrambling attacks. Interference is considered due to the noise and multicarrier noise such as white Gaussian. In multicarrier interference, attacks recognized the carrier used by the system and inject a narrowband signal, into this carrier.

Scrambling is also an interference targeted by an attack. An attacker targets on management [4].

2. Mac layer issue

There are the different issues arise on the Mac layer. These are location tracing, when unauthorized user traced the location, and get the information. Denial of service is the second, between them when the bandwidth is stealing; then, bandwidth stealing is another security issue arises. Other issues related to its architecture also arise. [5] These are the, mainly reason, the security issues on Mac layers. Wi-max and LTE are the major standard here. We mainly discuss the security issues on the physical and Mac layer.

There are different security issues arises on the physical and Mac layer of the LTE standard. Discuss both, physical and Mac layer of the system. LTE security verifies by authentication, integrity and encryption. In the first verify UE's identity by challenging the UT use the key and report a result after checking it [10]. Femtocells generally have low power and lower rate of data transmission. So that it can be used by the user. Long term evolution standard is used to meet with its demands. But different challenges arise due to the use of this. Those challenges affect the integrity of the system. One of them is interface of the air between the mobile device and the femtocell. Attackers attack on this air interface. Other attack is on the femtocell itself. And, third one is attacked on the core network. These are the attacks, affected the integrity of the system [8].

III. LITERATURE SURVEY

(1) In[2],explains about the fourth-generation technology. its security issues, architecture of fourth generation. Also, the threats on the fourth generation. Analyzing threats on fourth generation.

(2) In [4], outline all the security challenges in fourth generation. It can be achieved by investigating the security mechanism. In this paper uses the X.805 standard. So, gives a brief idea about, all the security issues.

(3) In [5] studies of different security advances and challenges that is associated with fourth generation technologies. It studies the security standard of fourth generation technology and architecture and design for long term evolution.

(4) In [6] brief study of the advances in security issues. This paper describes the fourth-generation architecture, security issues related to the fourth generation and all the threats and risk on fourth generation technology.

(5) In [7] represents the different security issues of fourth generation. This paper also explains the physical layer issues and technical issues on fourth generation. And, also represents the security models of fourth layer and threats on fourth generation.

(6) In [11] gives an overview of the current threat on long term evolution network. And explains the architecture of long term evolution and the solutions to overcome these problems. And, overlooking the low range threats and set areas of focus on that should be considered in security.

(7). In [13] investigates all the attacks on long term evolution. This paper explains all the needs in long term evolution for its security. And explains, architecture of long term evolution, attacks on long term evolution and comparison with other.

Authors	Paper title	Major finding	Research methodology used	Research Prospect
[2]	A survey of security threats on 4G networks	Explain network security architecture and threats on 4G.	IP-based	Survey of security threats
[4]	Providing security in 4G system: Unveiling the challenges	Describe the different security challenges in 4G system using X.05 standard	Authentication and key agreement protocol	Using X.05 standard
[5]	Security advances and challenges in 4G wireless networks	Define the security standard of different generation and its standard, LTE and Wimax	Improve long term evolution standard predecessors	Security standard
[6]	Comprehensive survey of possible security issues on 4G networks	Explain the mail threats on 4G and its design.	Four-layer security model	8 security dimensions of 4G network
[7]	4G wireless network architecture an overview and security issues on 4G	Studies the problems on wireless network security on 4G	Integrated security model	Protect different entities
[11]	Security attacks against the availability of LTE mobility networks: overview and research directions	Discuss the threat against the LTE networks	Network based attack detection layer.	To achieve full mobility availability
[13]	Effects of signaling attacks on LTE network	Describe the effects of the signaling attack on LTE network.	Lowering the inactive bearer	Increasing the signaling volume

IV. CONCLUSION

4G network has open nature and used on the wide level. Due to the open nature different security issues arise. Particularly arise due to the attacks on 4G. There discussed, different type of attacks on LTE. Recognizing the different attacks, particular steps can be taken in this way. And, we can increase of the integrity of the system.

V. REFERENCES:

[1]. Priya Gatum, Sanveet kaur, Ramdeep kaur, swmeet kaur "Review paper on 4G wireless technology" (IJASAT, March 2014.) vol.2, issue (March 2014)

[2,]. Yongsuk Park, Member, IEEE, and Tajoon Park, Member "A survey of security threats on 4G".2007, IEEE conference,

[3]. Yulong Zou Senior Member IEEE, JiAZHU, Xiabin Wang, Senior member IEEE, And, L Ajos Hanzo, IEEE "A survey on wireless security: Technical challenges, Recent Advances, and future trends" vol.104. no.9, sept 2016

[4]. Mahdi Aiash, Glenford Mapp and Aboubaker Lasebase and Raphael Phan "Providing security in 4G Systems: Unveiling the challenges" IEEE, (AICT),2010,6th advance internal conference

[5]. N. Seddigh, B Nandy, R Makkar, J.F. Beaumont "Security Advances and Challenges in 4G Wireless Networks, 2010 Eighth Annual International Conference on Privacy, Security and Trust.

[6]. Sumant ku Mohapatra, Biswa Ranjan Swain and Pravanjan Das "Comprehensive survey of possible security issues on 4G networks" International Journal of Network Security and its applications (IJNSA) vol.7, No.2, March 2015

[7]. Javed Ahmad Saheen "4G wireless networks Architecture an overview and Security Issues on 4G" International journal of future communication and Networking, Vol.10, No. 1 (2017), pp.15-24

[8]. Igor Bilogrevic, Murtuza Jadliwala and Jean- Pierre Hubaux "Security Issues in Next Generation Mobile Networks: LTE and Femtocells"2010,2nd international femtocell workshop.

[9]. Yi-Sheng Shiu and Shih Yu Chang, Hsiano-C, "Physical layer Security in Wireless Networks: A Tutorial", IEEE, wireless communication, april, 2011

[10]. Jin Cao, Maode Ma, senior Member, IEEE Hui Li, Member, IEEE, Yueyu Zhang, and Zhenxing Luo "A Survey on Security Aspects for LTE and LTE-A Networks, IEEE communications surveys and tutorials, vol.16, No.,1, FIRST QUARTER 2014

[11]. Roger Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Network: Overview and Research Directionds" international journal of network security, vol.5, no.2, pp.145-153, sept2007,

[12]. Afrand Agah and Sajalk. Das "Preventing DoS attacks in Wireless Sensor Networks: A Repeated Game Theory Approach" International Journal of Network Security, Vol.5, No.2, PP.145-153, Sept.

[13]. Ramzi Bassil, Imad H. Eihajj, Ali Chenhab, Ayman Kayssi, "Effects of Signaling Attacks on LTE Networks, 2013, 27th international conference on Advanced Information Networking and Application Workshops.