IJRECE VOL. 4 ISSUE 3 JULY.- SEPT. 2016 ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)
DOI: 10.13140/RG.2.2.33498.75205

Security Survey and Study of DDos Attack on LTE (4G) Network

Lakhbir Kaur[1], Chitender Kaur[2]
[1]M.Tech (Scholar), [2]Assistant Professor
Department of computer Science, CEC Landran, Mohali, Punjab

Abstract **-** Long haul Evolution, for vulnerabilities, to check the uncompromised and right Processing of encryption/decoding system, examine the impact of the adjustments in the abilities, and afterward proposed a more productive calculation. For the extent of this examination, up and coming security is vital because of its wide size of utilization; be that as it may, the reason for this training is to exhibit a present helplessness in the LTE encryption strategy. LTE-Advance (LTE-A for short) as one of the 4G Wireless portable broadband frameworks prescribed by 3GPP has been one of the patterns of ebb and flow remote mechanical and exploration centers. Be that as it may, its discharge 13 (4G) has a few security issues, e.g., when a User Equipment enters the correspondence territory of an eNB, i.e., a base station, and commonly validates each other with Mobile Management Entity/Home Subscriber Server, a few parameters conveyed in a message conveyed to UE by MME are decoded, just giving respectability checking.

Keywords: Long –Term Evolution, LTE-Advance, Wireless Mobile Broadband and Security Problems.

I. INTRODUCTION

With the swift extension of wireless communication and multi-media requests such as Internet browsing, communicating gaming, mobile [1] TV, video and audio streaming, the mobile communication equipment needs to meet different supplies of mobile data, mobile intentions and moveable multi-media processes. Keeping in mind the end goal to quarter the expanding portable information use and the new sight and sound solicitations, LTE and LTE-An innovations have been measured by the 3GPP as the developing versatile message advancements [2] for the cutting edge broadband versatile remote systems. The LTE framework is wanted to be a bundle based framework containing less system components, which recoups the framework limit and scope, and conveys high presentation as far as high information charges, low get to dormancy, flexible transmission capacity operation and consistent coordination with other present remote correspondence frameworks. The LTE-A framework determined by the 3GPP LTE Release 10 improves the current LTE frameworks to bolster greatly created information use, lower latencies and better otherworldly proficiency. What's more, both of the LTE and LTEA frameworks procurement level IP availability, full interworking with shifted remote access systems and numerous new sorts of base stations, for example, base stations and hand-off handles in a large scale cell system. Because of the outline of the new elements, it acquires a great deal of new security challenges in the configuration of the security developments of the LTE and LTE-A frameworks.

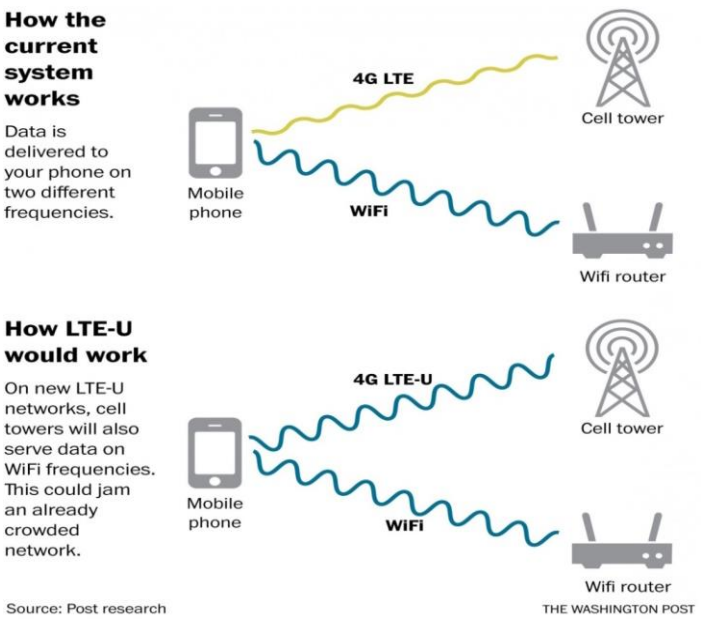


Fig.1: Long Term Evolution

II. LTE Architecture

LTE network is contained of the Evolved Packet Core and the E-UTRAN. The EPC is an all-IP and fully packet swapped backbone network in the [3] LTE systems. Voice service, which is conventionally a circuit switched network service, will be handled by the IP multimedia subsystem network. The EPC contains of a MME and a Serving Gateway, a Packet Data Network Gateway together with Home Subscriber Server. When a UE connects to the EPC, the MME signifies the EPC to perform a common authentication with the UE. E-UTRAN comprises the Evolved Worldwide Terrestrial Radio

DOI: 10.13140/RG.2.2.33498.75205

Access Network Base Stations, called eNodeBs, which transfers with UEs [4].

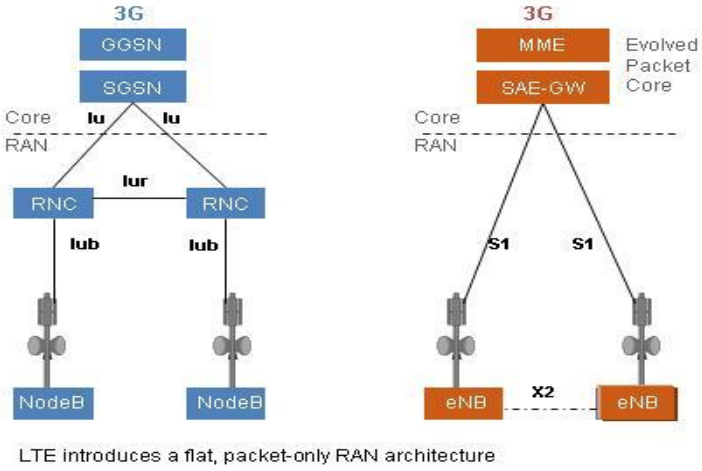


Fig.2: Long –Term Evolution Architecture

Table no: 1 Attacks in LTE Network

Attack		Adversary type	Vulnerability		Potential Fix
Group	**Description**		**Type**	**Possible trade off**	
Location link	Link loc over timer (L1)	Passive	Under specification	(perceived) security vs obtainability	Policy to guarantee GUTI freshness
Location link	Leak loaser grained loc (L2)	Semi passive	Application software architecture	Security vs functionality	Tool like darshak & snoop snitch to visualize suspicious signaling to subscribers
Location link	Leak fine graind Loc (L3)	Active[7]	Specification & implementation flow	(supposed) security vs obtainability	Network authentication for requasts ciphering for responses
Down grade to non LTE	Down grade to non LTE	Active	Specification Flow	Security vs performance	Time based recovery[8]
Down grade to non LTE	Danny all services	Active	Specification Flow	Security vs performance	Time based recovery

III. D DOS ATTACK

In DoS attacks, that unauthenticated attach requests sent from a compromised UE/eNodeB to flood the MME and in go to the HSS, foremost to a DoS attack. However their DoS attacks are against the network and not against LTE subscribers. Done imitations the authors in [9] show that Botnets can cause DoS attacks by exhausting subscriber traffic capacity over the air interface. provides an overview of new effective attacks (smart jamming) that extend the variety and efficiency of basic wireless jamming. However according to both aforementioned flooding and jamming attacks are non-persistent DOS attacks hence not measured as a threat to address in the LTE architecture. In contrast, our DoS attacks are tenacious and targeted near the UE (subscribers). LTE security architecture and a detailed list of safety vulnerabilities current in the LTE networks have been presented in [10]. Our attacks are not presented in this survey. Resource stealing and DoS attacks against VoLTE, whereas our focus is against LTE access network protocols. To the best of our information, there was no preceding work evaluating practical attacks on LTE access networks in the literature.

IV. OVERCOMING SMALL CELLS SECURITY AND DEPLOYMENT CHALLENGES

Improvement in-building coverage, plugging coverage gaps in country or remote areas and supplementing macro capacity – these are compelling operator needs that will propel LTE small cells from beginning to massive placement over the next few years. Deepening threats to subscriber communications and network substructure will also require

DOI: 10.13140/RG.2.2.33498.75205

workers to maintain even higher security and protection levels, as they organize small cells into less physically endangered public environments.[11] The sheer volume of small cells (expected to be 10-40 times additional than macro cells) and the usage of Internet backhaul (which is inherently insecure) presents some placement challenges for safety and defense that are unique to small cells and must be addressed by the operator.

V. PROBLEM FORMULATION

- Long Term Evolution (LTE) / Wimax are one of the emergent network technologies which are helpful in increasing the capacity and speed with different radio interfaces to improve the network performance.
- Its main aim is to improve the network performance with the help of digital signal processing and modulation concepts which simplifies the network
- Security is one of the main issues in 4G LTE systems. The intruders could eavesdrop on conversations and gain fraudulent access to the network easily
- After looking at various authentication and ciphering algorithms, Researchers finds the lot of vulnerability problem in security mechanism in LTE/ Wimax
- There can be a lot of call dropping probability or handoff problems in these type of mobile communication standards.
- There can be multiple copies of enodeB which increases the unnecessary load on the network which will degrade the performance of the wireless network.
- So these are some issues which should be resolved for the reliable communication of the network to increase the network security

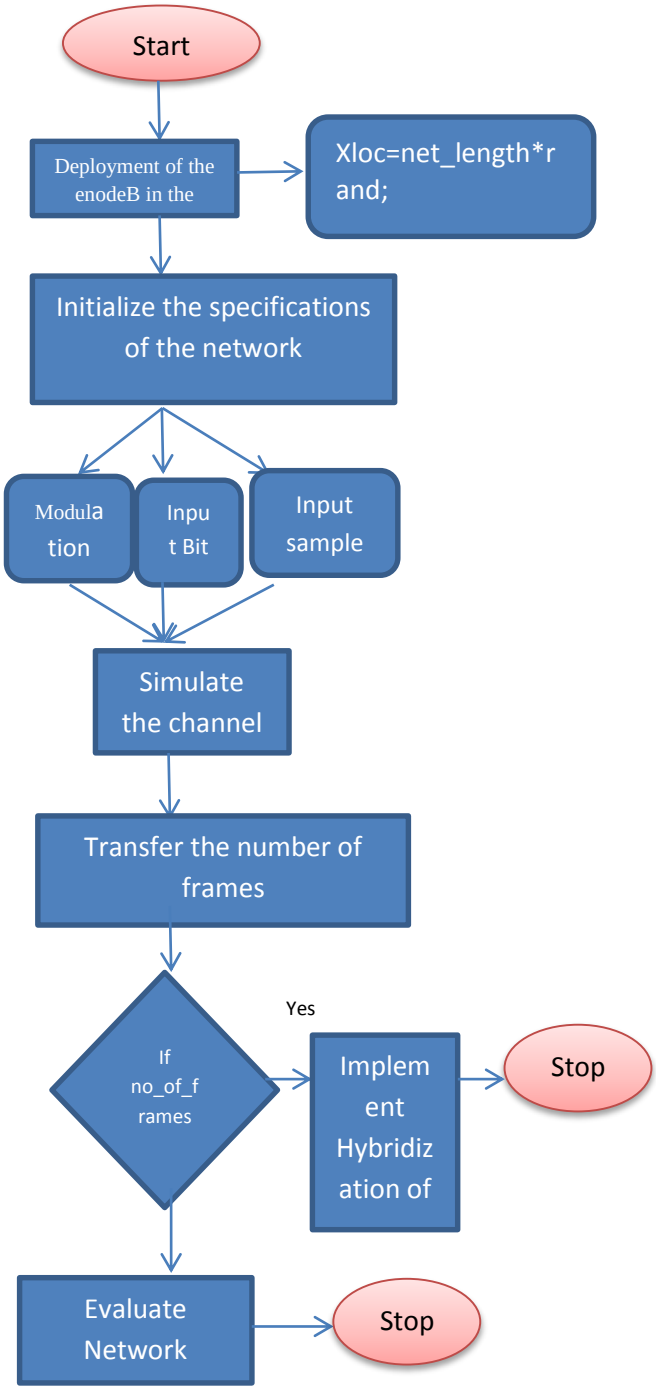
VI. OBJECTIVES

- To study the fundamentals of wireless information tendencies and their prone and corns for the security threats.
- To implement the attack using LTE technology trends to analyze the performance in the presence of threat in the network.
- To implement Hybridization of RSA and DES key encryption algorithms for network security.
- To evaluate the performance in terms of number of frames loss, Throughput and Latency to improve the Quality of service in LTE wireless standard technology.

VII. PROPOSED WORK

To begin with we need to enter the quantity of enodeB in the system. At that point we introduce the details of the system like system length, width, enodeB ids. Then we include the bit rate, Modulation request to regulate the parcels in the system

Simulate the channel models through which the packets will transfer .Then we will transfer the number of frames and if the number of frame losses increases then we will implement the hybridization of security algorithms names as RSA and DES. Then we will transmit the frames in the secure manner and will evaluate the parameters which will describe the evaluation of performance of the network.



DOI: 10.13140/RG.2.2.33498.75205

Fig.4 Proposed Work

VIII. CONCLUSION

The 4G LTE system is a generally unexplored zone for security assessment. In this work, we reveal that LTE may not be a sound voice answer for 4G LTE from the security stance. This paper distinguishes few key security vulnerabilities in LTE portable system framework engineering usage. It audits the conceivable security assaults as far as flagging surge from breaking down applications recorded against versatile system utilizing DDoS assaults.

IX. REFERENCES

[1]. Liu, Chin-Yu, et al. "The untrusted handover security of the S-PMIPv6 on LTE-A." Computer Communications Workshops (INFOCOM WKSHPS), 2015 IEEE Conference on. IEEE, 2015.

[2]. Liyanage, Madhusanka, et al. "Leveraging LTE Security with SDN and NFV."networks 2: 4.

[3]. Qiang, Li, et al. "Security Analysis of TAU Procedure in LTE Network." P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2014 Ninth International Conference on. IEEE, 2014.

[4]. Rasheed, Iftikhar, et al. "Analyzing the security techniques used in LTE Advanced and their evaluation." Digital Information Management (ICDIM), 2013 Eighth International Conference on. IEEE, 2013.

[5]. Siwach, Gautam, and Amir Esmailpour. "LTE Security potential vulnerability and algorithm enhancements." Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on. IEEE, 2014.

[6]. Taylor, Carol-Lyn, David Nolan, and Stan Wainberg. "Priority capabilities in LTE supporting national security and emergency preparedness next generation network priority services." Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE, 2013.

[7]. Tu, Guan-Hua, et al. "How voice call technology poses security threats in 4G LTE networks." Communications and Network Security (CNS), 2015 IEEE Conference on. IEEE, 2015.

[8]. Zhu, Li, et al. "Research on 3GPP LTE Security Architecture." 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing. 2012.

[9]. Brouet, Jérôme, and She Feng. "Lte and future evolutions for the benefits of security wireless networks." Wireless Mobile and Computing (CCWMC 2011), IET International Communication Conference on. IET, 2011.

[10]. Cao, Jin, et al. "A survey on security aspects for LTE and LTE-A networks."Communications Surveys & Tutorials, IEEE 16.1 (2014): 283-302.

[11]. Choi, Hyoung-Kee, Chan-Kyu Han, and Dae-Sung Choi. "Improvement of security protocol for Machine Type Communications in LTE-advanced."Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International. IEEE, 2015.