ENHANCING THE RECENT SECURITY OF LTE AGAINST ATTACKS

[1] S.Hendry Leo Kanickam, [2] R.Vijaya balaji,
[1]Assistant Professor, [2]Student,
[1] Department of Information Technology,
[1] St.Joseph's College, Trichy, Tamilnadu, India

Abstract : The long-term evolution (LTE) network provides highly developed services for billions of users with its higher bandwidths, excellent spectrum efficiency, and lesser latency than legacy cellular networks. The most important objective of 3GPP long term evolution (LTE) is to provide a safe communication, high data rate and excellent communication for 4G users. LTE support all IP based information and voice with velocity in order of hundreds of mega-bytes per second. It increases the speed and access through the internet. The LTE is remaining as the key of wireless technology. Network is used in fourth generation because it provides high data rates to the huge number of users at a time. It gives the high speed of data to when compared with other generation so widely used in broad scope. But it still suffers from new security threats as it's IP-based on heterogeneous architecture. There is a need to perform a quickly and accurate network security measurement in the LTE network. To achieve LTE network security measurement, security-related data (in short security data) collection and data analysis for attack detection are necessary as prerequisites. In this paper we present an enhancing recent security of LTE networks and against attacks of LTE networks. We present taxonomy of recent security according to the LTE network structure. Then we present different type of attacks in LTE networks.

IndexTerms- LTE network, security of LTE network, types of attacks.

I. INTRODUCTION

The Internet of Things will bring about billions of devices connected to through the internet. In the cellular network, machine type communications using LTE is under consideration by a lot of operators. LTE was designed to provide broadband high-speed data service with very low latency. Machine type communication is another type of services, have a different set of requirements, namely low-rate, low-overhead, low-power consumption, and low-cost. To address these necessities and also to minimize impact from machine traffic to human traffic, 3GPP has been working on many LTE features such as power saving, overload control, signaling reduction, complexity reduction, and coverage enhancement. The cellular networks have shown a marvelous growth in the earlier period decades from its First Generation (1G) to 4th Generation which is still growing hence termed as Long Term Evolution (LTE). Recent cellular networks support a large number of services that go away from traditional voice and short messaging traffic to include lofty bandwidth data communications. These networks are based on 3GPP standards for wireless communications, such as the Universal Mobile Telecommunication System (UMTS) for current 4G access networks. Release 14 of the 3GPP standards resulted in the deployment of Long Term Evolution (LTE). 3GPP has started discuss and study of 5G technologies.

LTE provides capability to user equipments (UEs) by means of a centralized assignment of radio resources. A newly enhanced physical (PHY) layer is implemented based on orthogonal frequency division multiple access (OFDMA) and considerably improves the performance of the earlier wideband code division multiple access (WCDMA). LTE system supported to dual radio access by attaching to both 3G and 4G radio networks using joint attach. It make possible data only access to high speed LTE data network, and circuit-switched fallback CSFB to existing 2G, 3G and high-speed packet switched data network when the user can move out of 4G LTE coverage part.

This paper associated with recent security problem in LTE network and brief summary of attack in LTE networks. The recent security is involve considerable modify at the PHY layer of LTE networks which could be very challenging to execute on a commercial network and would necessitate collaboration within the industry. Than next section are attacks of LTE networks and some attacks solution. This session briefly explain all the attacks in networks.

II. LITERATURE REVIEW

This paper has brief information on 4G LTE Mobile Network and Security Requirements. The network will identify some security vulnerabilities in the LTE mobile network. This reviews some potential security attacks, such as malware, spare gear, denial service (DoS) and distributed refusal service (DDoS). Explain how the security system works. We may have occupied about how the removal of the upcoming packets is reduced by attacks. SDN (software defined network) and RTBH (remote induced black hole) can be prevented using a routing approach [1].

In this demonstration of opinion paper, we look at the persistent simpler but effective pressing attacks that extend the basic jam range when minimum power is required. The goal is to have this traditionally overlooked threat and awareness of security research work in this area. We, in parallel, are implementing smart jam as well as some proposed security solution [2].

We examined various security threats in the LTE system on this paper, whose analysis and comparison to deal with these attacks [3].

We discussed the attacks on LTE / LTE-A network under the network architecture. We focused on reviewing the work on data collection and analysis for the purpose of identifying major attacks on LTE / LTE-A network. In order to highlight the open publications and future research trends, we have presented our assessment criteria and evaluated the current literature. Finally, we proposed a communications data collection and data analysis model relating to security measurement on LTE / LTE-A network [4].

We recommend three important safety research directions, an effective and efficient network based attack detection layer. As a first step, the current mobility skills of networks should be leveraged, reconfigured and adapted for security development [5].

In this article, researchers provide full threat to LTE and threats and require further investigations by security architect designers [6].

In this paper, we will provide past and continuous LTE features to MTC services. Performance Assessment shows that the LED has the ability to support a large number of MTC devices in metal layers that have limited impact for human traffic. Power Consumption Analysis The battery life of more than 10 years also explains that even deep coverage is possible [7].

III. OVERVIEW OF LTE NETWORKS

LTE (Long-Term Evolution) means a standard for a softly and efficient transition toward more advanced leading boundary technologies for increasing the ability and speed of wireless data networks. The Long-Term Evolution (LTE) has evolved to become one of the useful technologies that accomplish the 4G wireless performance scope. LTE followers are anticipated to be about 3.16 billion by the end of 2018.

Architecture of LTE:

The LTE network configuration also collects a radio access network and a central part of the network. The radio access network, called E-UTRAN, originates from the original 3GPP UMTS Terrestrial Radio Assemblage Network (UTRAN). UMTS is a short form of Universal Mobile Telecommunication System. The E-UTRAN is composed of multiple evolved Node Bs (e-Node Bs), which have the functionality of the Node Bs and assume the majority of the functions of Radio Network Controller in UTRAN. The User Equipment (UE) and the e-Node B are connected through the air interface.

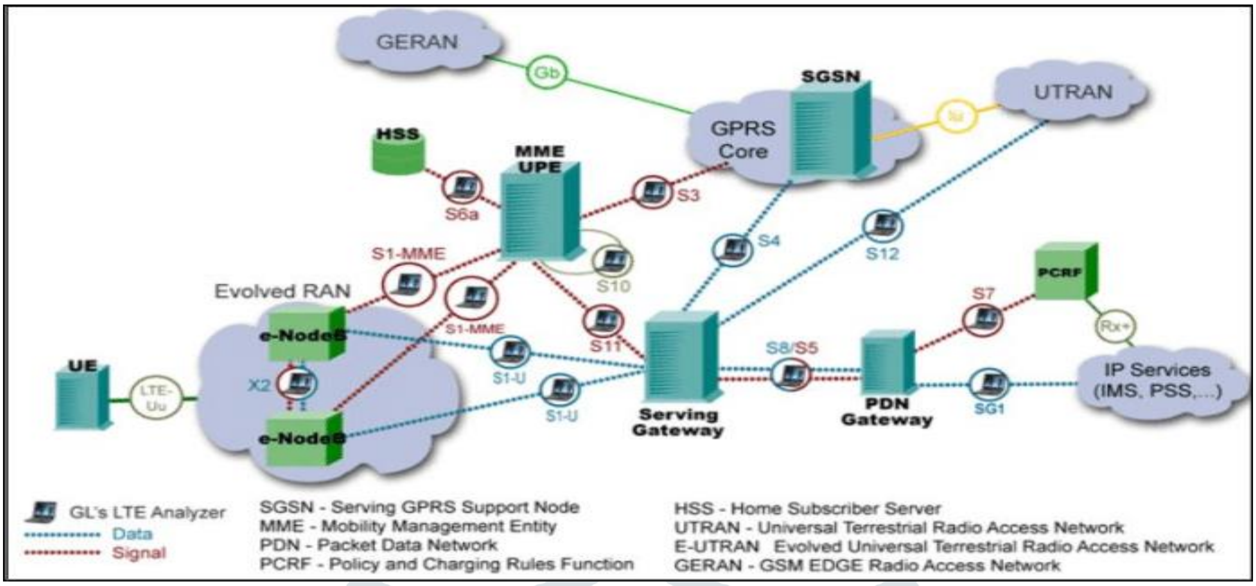
GERAN
Gb
SGSN
UTRAN
GPRS Core
Iu
HSS
MME UPE
S6a
S3
S4
S12
S1-MME
S10
Evolved RAN
PCRF
S7
e-NodeB
S1-MME
S11
Rx+
UE
LTE-Uu
X2
S1-U
S8/S5
IP Services (IMS, PSS,...)
S1-U
Serving Gateway
PDN Gateway
SG1
e-NodeB
GL's LTE Analyzer
Data
Signal
SGSN - Serving GPRS Support Node
MME - Mobility Management Entity
PDN - Packet Data Network
PCRF - Policy and Charging Rules Function
HSS - Home Subscriber Server
UTRAN - Universal Terrestrial Radio Access Network
E-UTRAN Evolved Universal Terrestrial Radio Access Network
GERAN - GSM EDGE Radio Access Network

Fig – 1 **LTE NETWORKS**

LTE central part network is called EPC network. It provides connections to several heterogeneous access networks, containing 3GPP access networks (E-UTRAN, GERAN and UTRAN), and non-3GPP access networks (WiMAX, CDMA2000, etc.).The EPC consists of MME, Home Subscriber Server (HSS), SGW, Packet Data Network Gateway (PDN-GW) and Policy and Charging Rules Function (PCRF). The EPC reach the division of the control surface and the user surface. The MME achieves control surface functions and the SGW achieves user surface functions.

IV. RECENT SECURITY IN LTE NETWORK

Wireless cellular networks were initially designed to provide ubiquitous access for communication. Even though the second generation of mobility networks was planned with some security aspects in mind, GSM just feature cryptographic algorithms to assurance privacy and authentication. In order to secure mobile devices that use LTE wireless technologies, there should be security for the connections between the UEs and MMEs and between elements in the wire line networks and mobile stations. For fulfilling these requirements, the LTE security is considerably improved by adding (1) highly developed key hierarchy, (2) extended authentication and key agreement, and (3) additional interworking security for the NEs. The requirements are classier into key building blocks and LTE end-to-end security.

Security and hierarchy Key:

LTE has five key approach used for connections of the EPS and E-UTRAN. The keys are declared as follows: (1) KANS encryption and integrity keys are used to preserve non-access stratum (NAS) traffic between the UE and MME, (2) a KUP encryption is used to encrypt traffic between the UE and e Node B, and (3) KPRC encryption and integrity keys are used to safe the Radio Resource Control (RRC) between the UE and e Node B [8].

Key management:

LTE key management includes three functionalities are key establishment, distribution, and generation. It is necessary that LTE wireless technology has key management mechanisms that deter stealing keys, as mobile devices with IP-based infrastructure can often access dissimilar wireless networks. An Authentication and Key Agreement (AKA) process is utilized for establishing and verifying keys in LTE systems.

Authentication, encryption, and integrity protection network:

LTE depends on using ordinary updating of the authentication process by replacing sequence numbers in the messages of encryption mechanisms. The IPSec protocol and tunnels are also used for asserting the confidentiality of users' data while transmitting traffic between LTE nodes.

V. DIFFERENT TYPE ATTACKS AGAINST LTE NETWORK

Attacks have an effect on the integrity of the system. There are mostly two types of attacks, one is active attack and another one is passive attack. When the attackers only aim is to get the information and then it is passive attack. But its mean is not only taking the information, but effect the integrity of the system is active attack. Passive attack is such that traffic difficulties 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 alteration etc. Sensor network is used in wireless communication on a broad level. Larger amount of nodes relates to the sensor networks, which dissimilar problem arise. Various attacks in LTE networks are there:

1. Location Tracking Attacks
2. Disclosure of the International Mobile Subscriber Identity (IMSI) Attacks
3. Denial of Services (DOS)/DDOS Attacks
4. Radio Frequency, Spoofing and Sniffing Attacks
5. De-Synchronization Attacks
6. Rogue base station Attacks
7. Jamming Attacks

Then some of the attacks can be attack networks also like application, transport, network, MAC and physical.

1. Application-Layer Attacks
2. Physical-Layer Attacks
3. MAC-Layer Attacks
4. Network-Layer Attacks
5. Transport-Layer Attacks

Location Tracking Attacks: The blueprint of cellular phone communication technologies allows the mobile operators to know the physical locations of the users to perform continuous cellular services.

Disclosure of the (IMSI) Attacks: IMSI is enduring identifiers of a subscriber. It should be transferred as occasionally as probable for the sake of secrecy of user identity. LTE specifications reduce the IMSI transmission frequency over the air interface. In the radio transmission, a Globally Unique Temporary Identifier (GUTI) is used to identify followers.

Denial of Services (DOS)/DDOS Attacks: DoS and Distributed Denial of Service (DDoS) attacks are together acute attacks on LTE network. A general method of DoS attacks is that attackers send floods of messages to a target server and exhaust its CPU resources, making the target unable to offer services for legal users.

Jamming Attacks: Jamming targets receivers and interrupts communications by lessening the Signal-to-Noise Ratio (SNR) of the received signal to cause DoS attacks.

De-Synchronization Attacks: De-Synchronization attacks on the intra-MME handover management. An attacker can interrupts the forward key division using a rogue base station until the update of root key.

Application-Layer Attacks: The application layer attacks are classify as HTTP (Hypertext Transfer Protocol) attacks, FTP (File Transfer Protocol) attacks, SMTP (Simple Mail Transfer Protocol) attacks [5].

Physical-Layer Attacks: The telecast nature of cellular broadcast and flat-IP based architecture of LTE has made the physical layer more susceptible to eavesdropping and jamming attacks match up to to GSM or UMTS.

MAC-Layer Attacks: Every node in the network is allocated its own unique MAC address. When any one malicious user changes its own MAC address with some wrong affectivity, then it is known as MAC spoofing.

Network-Layer Attacks: The network layer attacks are essentially classify into three categories namely IP spoofing, IP hijacking and Smurf attack. IP spoofing is mainly a way of hide identity of the attacker for carrying out illegitimate activities.

Transport-Layer Attacks: The attacks in this layer are mainly classified into either as TCP attacks or UDP attacks.

VI. CONCLUSION

We present in this paper enhancing the recent security of LTE networks against attacks of networks. This threat is the intrinsic to the real wireless technology employed in this type of network, and its most fundamental implementation, there is no means to avoid an attacker from spreading a lofty power interfering signal on a profitable frequently band. We propose a sequence of possible security research directions that could preserve LTE cellular networks, compel and request is to protect the networks. Then three major securities in current research side, as well as an effective and efficient network-based attack detection layer. To quickly find out the very efficient wireless technology to prevent the all LTE networks.

REFERENCE:

1) . Girish Tiwari Ujjain Engineering College,Ujjain (MP) Email:tiwari_girish@yahoo.com, Ashvini Kumar Ujjain Engneering Cillege ,Ujjain(MP) Email:ashvinik22@gmail.com.
2) . RogerPiquerasJover1*, Joshua Lackey1 andArvindRaghavan2.
3) . 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.
4) . LIMEI HE1, ZHENG YAN 1, (Senior Member, IEEE), AND MOHAMMED ATIQUZZAMAN2, (Senior Member, IEEE) 1State Key Laboratory of Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an 710126, China 2School of Computer Science, The University of Oklahoma, Norman, OK 73019, USA Corresponding author: Zheng Yan (zheng.yan@aalto.fi).
5) . Roger Piqueras Jover AT&T Security Research Center New York, NY 10007 roger.jover@att.com.
6) . A. Ahlawat1*, S. Kumar21*Electronics and Communication, University Institute of Engineering and Technology, MDU, Rohtak, India 2Electronics 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.
7) . Rapeepat Ratasuk, Nitin Mangalvedhe, and Amitava Ghosh Nokia Networks, Arlington Heights, IL, USA Email: {rapeepat.ratasuk, nitin.mangalvedhe, amitava.ghosh}@nokia.com.
8) . Nour Moustafa and Jiankun Hu School of Engineering and Information Technology, ADFA, Canberra, ACT, Australia.
9) . Altaf Shaik∗, Ravishankar Borgaonkar†, N. Asokan‡, Valtteri Niemi§ and Jean-Pierre Seifert∗ ∗Technische Universit¨at Berlin and Telekom Innovation Laboratories Email: (altaf329, jpseifert) @sec.t-labs.tu-berlin.de †Aalto University Email: ravishankar.borgaonkar@aalto.fi ‡Aalto University and University of Helsinki Email: asokan@acm.org §University of Helsinki Email: valtteri.niemi@helsinki.fi.

10). Authors: Wouter van Dullink Rawi Ramdhan.

Mr.S.Hendry Leo Kanickam working as a Assistant Professor in Department of Information Technology , St.Joseph's College(autonomous) Trichy, India. He received his M.Phil Degree in Bharathidasan University in 2008 and also He is pursuing Ph.D (Computer Science) in Bharathidasan University.

Mr.R.Vijaya balaji is studying II M.Sc Computer Science in the Department of Information Technology ,St. Joseph's College (autonomous) Trichy, India