International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 7 693 – 696

Security Review and Study of DoS Attacks on LTE Mobile Network

Girish Tiwari
Ujjain Engineering College,Ujjain (MP)
Email:tiwari_girish@yahoo.com

Ashvini Kumar
Ujjain Engneering Cillege ,Ujjain(MP)
Email:ashvinik22@gmail.com

Abstract- The main objective of 3GPP long term evolution (LTE) is to provide a secure communication, high data rate and better communication for 4G users. LTE support all IP based data and voice with speed in order of hundreds of mega-bytes per second. Increase speed in accessing internet. Network to be attached by hackers using some attacks like spyware ,malware ,Denial-of-Service (DoS) and Distributed Denial-of-Service(DDoS) .This paper associated with security problem in LTE network and brief summary of DoS attack , DDoS attack and security vulnerabilities in LTE networks.

*****

Introduction-

The next generation of wireless technology 4G Long-Term Evolution (4G-LTE) is a 3GPP network evolution. LTE is currently being deployed commercially by mobile operators around the world. This advanced wireless core network technology helps mobile operators to build an over lay network over the existing cellular radio networks for supporting high speed data bit rate and other advanced value-added application services. LTE system supports dual radio access by attaching to both 3G and 4G radio networks using combined attach. It enables 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 moves out of 4G LTE coverage areas. Initial network deployments started during the year 2009, and currently many vendors around the globe are deploying this data network and associated advanced data services [4]. Telia Sonara deployed the first LTE deployment in Norway and Sweden [2]. In 2012, there were 62 million LTE mobile subscribers and is forecasted to have up to 920 million by the year 2017. 4G LTE subscribers will be expected to have one in five mobile data subscribers in 2017 which is an increase from one in 25 in the year 2012 [3]. In addition to the widespread deployment of mobile data network, innovations in the mobile devices, android, iOS based Smart-phones drive the mobile data expansion. In 2012, 0.9 Exabyte per month were transferred using wireless networks and in 2017 it is expected to grow up to 11.2 Exabyte per month [4]. These new devices support the use of high speed network to browse the Internet, games, streaming videos and access to social networking sites Facebook, Twitter and Linked In and increase the data usage[1]. Fourth generation or 4G) is intended to support broadband performance and enable voice/video multimedia applications. The enabling technologies and standards for 4G wireless communications allow for significant increases in data rates over 2G (second generation), 3G (third generation) and 3.5G wireless technologies[1]. At the present time, LTE (Long Term Evolution) and WiMAX (Worldwide Interoperability for Microwave Access) are the two technologies considered as candidates to achieve the 4G wireless performance objectives. As we that 4G technology used for very dig speed as compare to other but simultaneously system complexity become high.As mobile technology growing very high speed simultaneously numbers of attackers also increase they use attacks like spyware ,malware ,Denial-of Device(DOS) attack and Distributed Denial-of Service (DDOS) attacks etc. The effects of malious are typically divided into three main classical aspects confidentiality ,integrity and availability .confidentiality refers to communication being accessed only by authorized person .integrity implies the wholeness trustiness of received data without accidental or intentional modification. Availability denote accessibility and usability of service upon an authorized request.

Network Architecture

LTE network has two main components eUTRAN and EPC (evolved packet core)

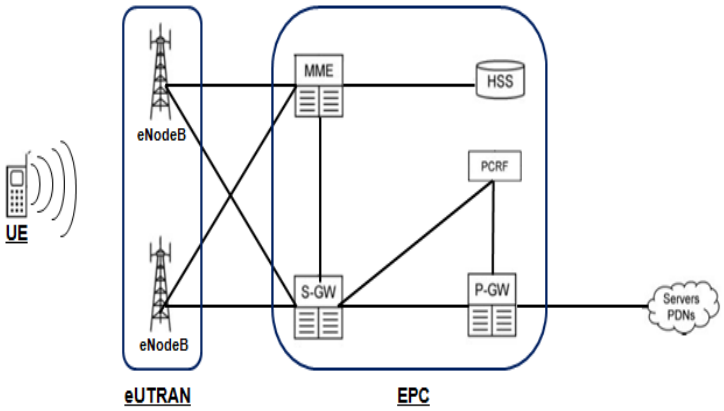

Fig. 1 LTE architecture [2]

The eUTRAN is a set of base stations called eNodeB connected directly to mobile users via radio interface the main function of these base station is to provide connection to users to EPC with good management of radio resources.LTE operates in lower 700 MHZ and upper band of 1700/2100 MHZ frequencies. 4G LTE service providers in the US, AT&T, mobile and Verizon operate using both lower and upper bands. LTE supports both the versions of duplexing (i.e., transmit and receive) methods Time-Division Duplexing (TDD) and Frequency-Division Duplexing (FDD) combined with the downlink modulation scheme, Orthogonal Frequency Division Multiple Access (OFDMA) to achieve maximum peak downlink data rate of 100 Mbps. In Frequency-Division LTE (FD-LTE), a pair of separate frequencies will be used for transmission and reception. In Time-Division LTE (TD-LTE), a single frequency will be used with time-split to transmit and receive using the same frequency carrier. Uplink transmission uses Single-Carrier Frequency Division Multiple Access (SCFDMA) to achieve maximum throughput of 50 Mbps using 20 MHZ bandwidth [4]. A scalable bandwidth of 20 MHZ from 1.4 MHZ, 3 MHZ, 5 MHZ, 10 MHZ and 15 MHZ along with faster response time thanks to the high data rate, unlike its previous cellular counterparts, enables LTE to out swim the contemporary 4G technology choices. The LTE provides a migration path for GSM and CDMA based operators by facilitating the convergence of wireless technology. The primary goal of this new technology is to improve spectral efficiency, bandwidth and throughput by means of deploying cost effective network elements using open standards with improved data and application services for the end users. It is expected to support lower latency, high level of security to support quality of service.

SECURITY REQUIREMENTS

One of the key requirements of LTE-EPS system is to support the exact or better level of security protection than that of security provided by the 3G UMTS-AKA implementation recommended in release-7 3GPP system architecture. 3G UMTS security mechanism has been adapted to suit the LTE network. LTE specification is very closely adhering to the 3G UMTS security implementation which was proven to be effective. The following key security functions are defined based on 3GPP recommendation for 3G and 4G services. User confidentiality which protects the user identities, e.g., IMSI (International Mobile Station Id), IMEI (International Mobile Equipment Identification), authentication which supports mutual verification of network and devices, the network, user plane (U-plane) confidentiality mechanism, control plane (C-plane) confidentiality and end-to-end integrity. In addition, the following key security requirements need to be implemented. Support at a minimum same level of security as implemented in 3G UMTS network with impacting user experience.

Provide security against the latest threats from Internet through user plane when the user accesses the Internet sites or from any malicious URL pages, e.g., virus, worms, XSS (Cross-site scripting) attacks, email phishing, malware and spy wares. The security functions provided by LTE should not get affected during the handover from 3G to 4G LTE network;

Universal Subscriber Identity Module (USIM) must be continued to use [1]. 3GPP Release-99 or later releases must use USIM application on the UICC to authenticate from the EPS system. In addition, key hierarchical system has been introduced which enables changing keys for different purposes.

DoS/DDoS ATTACKS in LTE Mobile Network

Advent of smart-phones with data access combined with advanced services like web 2.0, video streaming along with data-intensive mobile applications boost the data usage in wireless networks. Unlike Internet giants like Google, Yahoo, Apple and Microsoft, mobile operators are ill-equipped and not prepared for the security attacks on a massive scale. According to the infrastructure security survey conducted by Arbor Networks, the mobile operators are not prepared to defend the network against attacks in terms of network visibility, security control [5]. Nearly sixty percent replied no visibility to the network traffic of their packet cores and nearly forty-six percent experienced customer outages. Due to all-IP nature of 4G LTE network, mobile operators are vulnerable to security attacks and distributed denial of service attacks is on the rise on mobile networks. Based on this report, DDoS is number one security threat to Internet data centers. These DDoS attacks can be classified based on the attack volumes. One single attacker will generate low-traffic volume (DoS) and multiple attackers using coordinated agents using botnet command and control centers (C&C) can generate heavy traffic volume, e.g., DDoS attacks using a cluster of compromised computers or botnets [6].

Flowchart of Proposed Security System

The flow chart of the proposed security system is shown in Figure 2. The Fig shows that as the data request from different mobile enters into the security system involving the firewall (software or hardware), it first checks for the IP address and then checks the request rate of each mobile host with respect to its IP address. The System checks if the request rate of any mobile host is less then specified

 ISSN: 2321-8169
693 – 696

threshold then the request can easily pass through and access the server across the internet otherwise if the request rate is equal to the threshold, the requesting host is given a delay and as the timeout expires it is granted internet access services. During the delay, other mobile hosts with request rate lesser then the threshold are granted web services. In this way, the system is prevented from a complete shutdown due to overload of data requests. The algorithm defined by includes 3 steps for detecting signaling DoS. For the identification of each UE (User Equipment), the data traffic of each UE is recorded in a database. If cumulative summation score of a specific UE is over than threshold k, it will detect Signaling DoS attack.

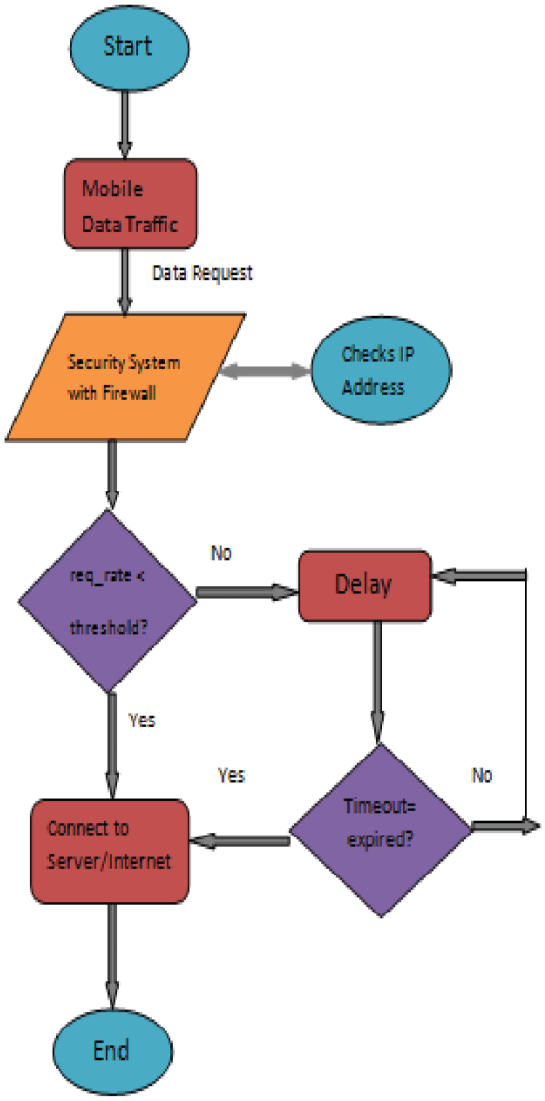

FIG 2:Security system flowchart

Denial-of-Service Attacks (DoS)

In denial-of-service (DoS) attacks, the attacker sends floods of messages to a single node from its own source to make the receiver exhausting its CPU resources and in turn prohibits other legitimate users using that server ports and services. In addition to these DoS types of attacks, hackers can launch sophisticated attacks on LTE network which can vary from malware spreading, phishing and data exfiltration using an Advanced Persistent Threats (APT) attack [6,7]. A radio jamming attack which will threaten a single-cell site could be attributed to this type of attack. Radio jamming is to disrupt the wireless communication forcefully by decreasing the signal to noise ratio by means of blasting high-power signal into the same radio band for the purpose of disrupting any radio communications in a single-cell site. The only way to stop this attack is to locate the signal transmitter and disable the transmission [2]. Since a 4G LTE network is an open architecture and IP based. The average speed of LTE is up to 150Mbps as compared to 3G which ranged from 1.5-7 Mbps. Because of the wider bandwidth, the chance of DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks are greater in 4G LTE. Now a day, one of the most common IP based attack is DoS flooding attack which can bring down the entire system Particularly the DNS Service. In DoS attacks, an attacker sends flood of messages to a server thereby consuming all its resources e.g. CPU cycles, memory, file allocation, network bandwidth etc which results in blocking the data connection of the mobile subscribers connected to that server or using its services that reduces the victim's throughput to almost zero[4].

DoS attacks are studied to exist in every subscriber's network and many mitigation mechanisms are proposed by different researchers to prevent and overcome the impact of DoS attacks. A DoS attack is usually carried out by a person or a group of persons simply to prevent a website or a service from functioning efficiently; it can be temporarily or indefinitely

Depend upon the type and target of the attacker.

OPEN ISSUES and DDoS Attacks

LTE network deployment supports all-IP based flat architecture. Unlike the previous versions of cellular technologies 2G, and 3G, were deployed with time-division multiplexing (TDM), Asynchronous Transfer Mode (ATM), SS7 based transport for backhaul. TDM/SS7/ATM based backhaul and core network trunks are closed to external network attacks. Hence, it opens up the RAN, core network nodes and other network elements for hacking because of exposure to Gi-Internet traffic for the PDN gateways. All-IP based architecture poses many security threats, e.g., expose the network to denial of service attacks (DoS), man-in-the middle attacks (MiTM) and replay types of attacks when the mobile user is accessing the Internet. The following section covers the security issues posed by this newly deployed 4G network in detail.

Distributed Denial-of-Service Attacks (DDoS)

In distributed-denial-of-service (DDoS) attacks, an attacker can use one or more compromised machines as a launching pad for generating flood of messages into the target machine. Typically, an attacker can use a large number of controller bots managed through command and control center (C&C) distributed in different locations to launch a large volume of such attacks. These attacks can also be generated by many different entities which can vary from a hacked mobile UE into the compromised servers which can also be used to launch further attacks. Recent research suggests attackers compromise mobile devices by utilizing the security vulnerabilities of the mobile operating system (OS) and applications downloaded from the app stores. DDoS attacks against the LTE core network can affect the entire mobility network's data services. A major US cellular operator's Instant Messaging network had an outage due to an app update. The android application installed on the smart-phone had kept on checking the central server frequently with flooding of messages into messaging and EPC core. This heavy traffic of messages into the radio and core network resulted in large numbers of radio resource control (RRC) messages that lead to network outages [6].

CONCLUSION AND FUTURE WORK

This paper gives the brief information of 4G LTE mobile network and security requirement in this network.The network identifies few security vulnerabilities in LTE mobile network.It gives review of some possible security attacks like malware, spaware,Denial-of Service (DoS) and Distributed Denial-of Service(DDoS).we also discribe flowchart ,how the security system works.In future we may work on how the removal of un-necessary packet drops by attacks.The prevention may be done by using SDN (Software Define Network) and RTBH (Remote Triggered Black Hole) routing approach.

REFERENCES

[1] James henrydoss, terry boult "critical security review and study of DDoS attacks on LTE mobole network"IEEE confrences APWiMob,Bali 28-30 Augustus 2014.
[2] Rachid KOUCH "Security of LTE/SAE network over E-UTRAIN "IEEE confrences 968-4673-7689-1,2016R.
[3] Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions", IEEE.
[4] J. Markoff, "Firm Is Accused of Sending Spam, and Fight Jams Internet," New York Times 2013.
[5] K. Ramakrishnan, and S. Floyd, "A Proposal to add Explicit Congestion Notification (ECN) to IP", RFC 2481, January 1999
[6] M. Stahlberg, "Radio Jamming attacks against two popular mobile networks, Helsinki University of Technology. Seminar on Network Security, Mobile Security, 2000
[7] A. Uchler and M. Schapranow, "Congestion Control", Seminar on Communication Networks.
[8] LTE World http://lteworld.org
[9] GSMA www.GSMA.com
[10] C. Cox, An introduction to LTE LTE-advanced SAE and 4G mobile communications, 1st ed., A John Wiley & Sons Ltd., 2012.
[11] 3rd Generation Partnership Project, 3GPP TS 33.401 V12.14.0 (2015-03), 3GPP System Architecture Evolution (SAE) / Security architecture (Release 12).
[12] D. Forsberg, G. Horn, W.D. Moeller, and V. Niemi, LTE Security, 2sd ed., A John Wiley & Sons Ltd., 2013.
[13] G.M. Koien, "Mutual entity authentication for LTE,"7 International Wireless Communications and Mobile Computing Conference IWCMC July 2011.
[14] James Henrydoss, Terry Boult , "Critical security review and study of DDoS attacks on LTE mobile network". in the Proceedings of IEEE Asia Pacific Conference on Wireless and Mobile. pp 194-200 (2014).
[15] Wouter Van Dullink, Rawi Rawdhan, " (Distributed) Denial of Service attacks via 4G/LTE network.", System and Network Engineering (2014).
[16] Jill Jermyn1, Gabriel Salles-Loustau, and Saman Zonouz, "An analysis of DoS attack strategies against the LTE RAN." Published in Journal of Cyber Security and Mobility, Vol. 3, No. 2 (2014).
[17] Wai Kay Leong, Aditya Kulkarni, Yin Xu, Ben Leong, "Unveiling the hidden dangers of public IP addresses in 4G/LTE cellular data networks." in the Proceedings of the 15th workshop on mobile computing systems and applications (2014).