Critical Security Review and Study of DDoS Attacks on LTE Mobile Network

James Henrydoss, Terry Boult

Department of Computer Science,
University of Colorado at Colorado Springs,
Colorado Springs, CO.
jhenrydo@uccs.edu,
tboult.vast@uccs.edu

Abstract

Mobile network is currently evolving into data centric architecture. Long Term Evolution (LTE) based next generation 4G technology is being deployed by cellular operators around the globe. LTE supports all-IP based data, voice and streaming network with speeds in the order of hundreds of megabits per seconds. Increased speed in accessing Internet and other advanced services exposes mobile data network to be attacked by hackers using spyware, malware, phishing and distributed denial-of-service (DDoS) attacks, which were predominantly affecting Internet-only datacentres in the past. This paper presents a detailed review of security framework and authentication procedures built into the LTE system architecture evolution (SAE). A brief summary of DDoS attacks and security vulnerabilities in LTE network included. This paper reviews the diameter interface and associated security problems using it in LTE network. This paper proposes using explicit-congestion notification (ECN) based method to address congestion issues in diameter interface.

Keywords: LTE, NAS, Ciphering, Integrity, EAP, AKA, DDoS, ECN

1. INTRODUCTION

4G Long-Term Evolution (4G-LTE) is a 3GPP GSM/UMTS 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 [22]. 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 [23]. In addition to the widespread deployment of mobile data network, innovations in the mobile devices, android, iOS based Smartphones 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 [24]. 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.

1.1 Network Architecture

LTE network has is built using packet switched backbone and core network using end to end IP connectivity. LTE operates in lower 700 MHZ and upper bands of 1700/2100 MHZ frequencies. 4G LTE service providers in the US, AT&T, 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 (SC-FDMA) 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 different Quality of Service (QoS) [3]. The heartening

978-1-4799-3711-0/14/$31.00 ©2014 IEEE

part of the LTE network architecture is the Evolved Packet Core System (EPS) architecture as outlined in Fig.1. EPS system consists of the following two major components: (i) EPC Core Network with Evolved Packet Core Network System Architecture Evolution (EPC/SAE) and (ii) the new Radio Access Network (E-UTRAN). The Evolved UMTS RAN (E-UTRAN) is from the original 3GPP UMTS radios NodeB base station system. Evolved NodeB (eNodeB) works in LTE and as well co-exists with the GSM and UMTS network to support fallback procedures. EPC forms the main part of Core Network (CN).

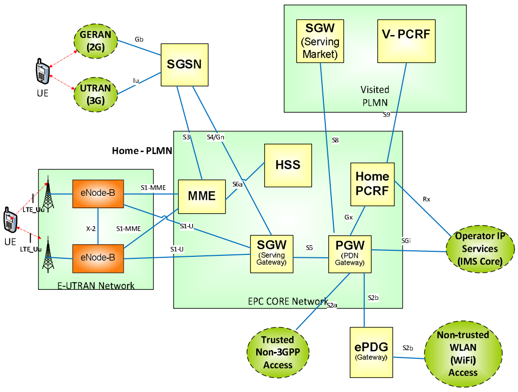

Fig.1 LTE Architecture

2. 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.

3. 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.

4. DoS/DDoS ATTACKS in LTE Mobile Network

Advent of smartphones with data access combined with advanced services like web 2.0, video streaming along with data-intensive mobile applications spur 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 [35]. 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 [16].

4.1 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 [16, 17]. 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 [20].

4.2 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 smartphone 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].

4.2.1 Mobile BotNet

Mobile malware and spy wares are on the rise. Due to rapid influx of the latest mobile gadgets supported by many different operating systems, mobile botnet is gaining traction among security researchers. Latest smartphones are considered to be frontiers in botnet and DDoS based attacks. Research studies suggest that botnets' availability in mobile phones and the possibility of launching attacks into data center by using smartphones are on the rise [12]. Mobile malware is spreading fast. Recently, many studies find that the Android malware-based botnets send text message spams. Android based Smartphones are having powerful devices on the market with dual and quad core CPUs and over 1GHz processing power. The user can use these devices to launch attack on mobile core network similar to the issue addressed in IM (Instant Messaging) network faced by the US operator [6]. A botnet inside a mobile device can be used to flood the EPC core with flood of attach and detach messages to the EPC core gateways by performing the same connection procedures in a loop. As per the latest reports, over ninety-seven percent of malwares are originating from Android Smartphones. Based on these abovementioned assumptions, smartphones with powerful processing capability and in combination with advanced LTE network poses a serious threat to mobile core network which can pump attack vectors similar to any other desktop PCs. Botnet infected mobile devices can flood the network with DDoS attacks is a real threat. Hence, counter measures to prohibit such attacks need to be researched [18].

4.2.2 Signalling Amplification Attacks

LTE employs an all-IP based flat network architecture based on the evolved packet core and RAN. It helps to process the signalling and packet core efficiently by having separate interface for control and data plane. This new LTE architecture entices the hackers to use signalling based attacks in which the attackers can use flood of signalling messages to drain the network resources and affect the network performance. LTE wireless networks employ advanced radio resource control procedures to support admission control for the resources scheduling. The LTE network attach procedures involve large collection request and responses messages between the devices, RAN and mobility management network elements. If not properly managed, this signalling traffic can result in large-scale exploitation in generating DDoS attacks. Cellular network can be attacked using this vulnerability. Instant Messaging (IM) messages generated from poorly designed applications running on Android handsets [6]. In addition, DDoS attacks were carried out on network data center to bring down the data network of enterprise customers [28].

4.3 Network Access Issue

In LTE network, UEs use EPS-AKA authentication mechanism to access the services in EPC core. The main purpose of the EPS-AKA authentication is to authenticate both the UE and the network to agree on keys, K_{ASME}. This procedure triggered by the network, when the user tries to attach to LTE network. When UE connects to MME via eNodeB, MME is the key node which executes the initial authentication engine and verifies the mutual authentication between nodes. It also validates the final checksums (XRES and RES) calculated by the MME and UE. Current implementation contains many features to the enhance network access security e.g. Serving Network ID (SNid) has been added to EPS AKA algorithm to protect the network from redirection and replay types of attacks. A replay attack is a form of network attack in which a valid data transmission is maliciously repeated or delayed. There are security functions Access Stratum (AS) and Non-Access Stratum (NAS) has been implemented. Access Stratum (AS) provides security protection between the UE and the eNodeB and Non Access Stratum (NAS) implements security protection between the UE and the MME (UE ->MME). Privacy protection of customer identifiers e.g. IMSI is one of the major concerns during initial UE attach procedures in LTE network using EPS-AKA procedure. During GUTI attach the current MME cannot retrieve IMSI hence UEs have to disclose the original IMSI to MME over the air. MMEs request the identity of the user by sending identity request and the UE responds with an identity response which includes the actual IMSI. Over and above, during the initial attach request procedure; the MME queries the HSS even before authenticating the user. Unauthenticated access requests force the network to send queries to MME from a compromised UE/eNodeB and in turn to HSS even before the UE authentication. It triggers hackers to launch malicious denial-of-service attack into HSS services from a fraudulent user using radio jamming [17].

4.4 IMS Security Issues

LTE is primarily a high-speed data network to support ultra-fast Internet browsing capabilities. Voice over LTE (VoLTE) is extending LTE based data network to support voice services using IMS based multimedia overlay network. IMS based multimedia service network is deployed over 4G LTE network to support voice and multimedia like streaming video and other data services. An IMS subscriber needs the mutual authentication to be performed with the LTE network before getting access to multimedia services. First, the UE performs EPS-AKA authentication procedure with EPC core network and secondly, it executes IMS AKA authentication with IMS call processing servers. In order to access the multimedia services, LTE users have to be authenticated in both LTE network layer and IMS service layer [13]. UE has to perform dual AKA authentications, one for LTE network access using EPC core and the second for accessing IMS core for voice services using two different APNs. In order to use the IMS based multimedia services, it is mandatory for the UE to perform both EPS-AKA and IMS-AKA authentication. Dual authentication, adds additional overhead in the power consumption of UEs. Also, it introduces complexity of UE architecture design. To perform IMS authentication, the UE needs new IMS Subscriber Identity Module called ISIM located within the same SIM UICC card which also stores IMS authentication keys for EPC authentication keys. IMS Serving Call Session Control Function, S-CSCF processes UE requests to perform authentication using the IMS-HSS, which has a stored copy of IMS-authentication keys.

IMS services use 4G LTE as the core network access method and hence security vulnerabilities on 4G LTE network will in turn affect the IMS core as well. Prior to VoLTE deployment mobile operators did not deploy end-to-end IP based voice services using VOIP network. Security vulnerabilities were reported in VoIP network. This VOIP based implementation opens up traditionally closed door network to potential security attacks which might span from password stealing, ID-spoofing to distributed denial-of-service-attacks, telephony DoS (TDoS) types of attacks. The IMS AKA algorithm is vulnerable to several types of denial-of-service attacks and man-in-the-middle types of attacks. Spambots based attacks on SIP signalling when used with VoIP implementation has already been observed [5, 13, and 11].

5 Diameter Interface Issues

Diameter is an authorization, authentication and accounting (AAA) protocol for exchanging subscriber profile information for authentication, on-line, off-line charging, quality of service (QoS) using client-server communication. In LTE network, 3GPP mandated diameter [34] and SIP as signalling interface to replace legacy, difficult to penetrate SS7 signalling system protocol which was used for many years in 3G, 2G, landline cellular, and switching network [1]. Diameter interface used for signalling between many core network nodes and services which includes (Home Subscriber Server) HSS, Mobile Management Entity (MME), Policy Control Resource Functions (PCRF), Mobility Gateways SGW/PGW and IMS core. IP Multimedia Subsystem (IMS), Cx, Dh, Dx, Rf, Ro, and Sh interfaces are supported by diameter protocol. 4G LTE roll out using evolved packet core network introduces fresh architectural concepts with new all-IP based signalling interface made possible because of diameter signalling protocol. At the same, it introduces challenges in congestion management and traffic handling mechanisms. In 3G networks, the radio network controller (RNC) is the main signalling bottleneck with combined signalling and bearer traffic. In comparison to SS7, diameter interface significantly increases the amount of signalling, termed as a signalling storm into 4G mobile core. Cisco forecasted seventy-five percent traffic growths between the years 2012-17 from 60 million to 992 million. At the same time, mobile carriers seek to fully monetize the network resources and they cannot afford to waste resources. Chatty mobile apps constantly poll their servers for updates. This background activity causes devices to constantly connect to the carrier network. Each connection attempt produces numerous signalling messages and consumes precious bandwidth [24, 48]. For example, many core networks signalling between MME and HSS originate from necessary and unnecessary signalling in the radio network. Diameter injected signalling flood is an emerging threat to mobile core networks which will impact 4G LTE rollouts affecting both the mobile operators and equipment vendors. Since, diameter is an IP based protocol, which uses either TCP (Transport Control Protocol) or SCTP as transport layers and so the TCP/SCTP's congestion issues applies to diameter as well. As well, it is exposed to the same type of attacks directed at fixed IP networks. In 2012, Japanese mobile operator, NTT DoCoMo suffered a major outage due to diameter routing agent signalling flood that disrupted network services. According to further analysis, the operator referred to a free mobile voice an application that runs on Android OS as the main cause of the problem that led to the outage.

This service interruption was caused by a malfunctioning android application on smartphones. It is very important for the operators to understand the cause, source and forms of signalling floods and prevent the mobile core network from network outages [41]. Diameter uses TCP (Transport Control Protocol) or SCTP transport mechanism implemented over IP. This transport mechanism exposes this interface in LTE network to TCP congestion issues during surge of incoming diameter queries. This becomes bottleneck during high volume traffic generated using DDoS/DoS attacks. When a diameter server becomes overloaded or congested, it requires the ability to gracefully shed its load by informing the client senders to scale down the traffic volume or else, it will expend all its resources in parsing, and responding to the messages which will lead to collapse of the server node. The following lists the overload reasons: In adequate capacity in CPU, memory and I/O resources to process the messages; intermediary network node failures; network initiated traffic flood; subscriber initiated traffic and DoS/DDoS attacks from the network. One of the key problems of overload and congestion is the complete failure of the node and network sent messages which will affect the network quality of service and performance. Diameter supports explicit and implicit mechanism of informing the client but is not adequate. There are many limitations in using diameter in comparison to its predecessor legacy SS7; First of all, diameter is not an end-to-end protocol and so there is an issue when a diameter interface is overloaded to gracefully bring down its load. Diameter mechanism for supporting this graceful shutdown is not adequate and it expects the engagement of lower transport layers. Diameter is end-to-end IP based protocol. Unlike its predecessor, SS7- protocol used in mobile network, it does not support congestion control and management. This is one of the key issues addressed in this work. It is prevalent in mobile network to deploy more than one radio access technologies (RAT) 2G/3G and 4G., Typically sending traffic to diameter interface at HLR/HSS/GWY/PCRF using 2G, 3G and 4G LTE is very common which feeds an aggregated heavy volume of subscriber query traffic during flood of registration messages. Failover of pending transactions to the new node during failure conditions for unsuccessful transactions are not addressed in this protocol. In addition, diameter based protocols operate hop-by-hop and not aware of end-to-end overload conditions.

The key issue in using diameter mechanism is lack of availability of overload protection with end to end security mechanisms. When a diameter node, especially the server or agent heavily loaded with simultaneous open transactions, it should be able to throttle down by requesting clients to slowdown the traffic. This will help servers to recover the CPU processing time and other resources expended in processing. The existing mechanisms supported by diameter interface, both explicit and implicit, are not sufficient to handle this traffic congestion due to overload issue [34]. In addition, current implementations do not support graceful shutdown and expects the use of congestion control mechanism supported by the underlying transport layers, TCP or SCTP. Diameter error responses sent as per base diameter specification is inconsistent as the receiving node can mix up this either as a protocol or as application level error. To support security and traffic management similar to the legacy SS7 network, LTE mobile operators need to implement diameter core network elements such as the Diameter Signalling Controller (DSC), the Diameter Routing Agent (DRA), and the Diameter Edge Agent. Traffic surges can cause congestion in diameter interfaces. DoS/DDoS attacks can trigger such activity. Few mobile operators in the US (e.g., AT&T and T-Mobile) recorded DDoS attacks and network outage due to message surges affected subscribers for few hours. A multi-hour distributed denial-of-service attack aimed at major US operator's DNS (Domain Name System) servers has disrupted data traffic for the company's enterprise customers [28]. According to 3GPP standards TR23.843 [14], overload on diameter interface can impact the following services: denial-of-services, loss of mobile broadband connectivity, loss of location information for emergency services and lawful intercept; loss of policy-control implementation and billing errors lead to loss of revenue. During congestion, there is no way available for the server to communicate congestion overload level to the clients. Diameter protocol needs modification with appropriate error responses reporting mechanism. The cause code used in error responses, "DIAMETER_TOO_BUSY" in server to client responses does not relay the congestion collapse due to overloaded conditions. In addition, the transport layer may not be aware of congestion issues happening at the application layers. As per 3GPP spec, by employing Diameter Routing Agent the traffic load congestion issue can be mitigated but this does not eradicate the issue. Also, the diameter routing agents (e.g., DRA) nodes play an important role for load balancing and overload prevention control over the diameter interfaces. As discussed above, the 3GPP case study also pointing to the modification of diameter related congestion issues. As per 3GPP recommendation, diameter interface can be enhanced and equipped to support the following congestion related defects (i) Cause code of 3004, "DIAMETER_TOO_BUSY for server client in responses (ii) Transport layer may be not aware of the application layer responses and so implementing congestion control at transport layer is not possible. (iii) Diameter server will be spending CPU time and resources in processing the surge of queries and responding with reject messages. A process is required to inform the diameter clients the congestion status occurring at the server end and so the client can throttle the rate.

5.1 ECN Based Congestion Mitigation

As recommended in 3GPP case study, which uses transport layer to implement congestion management procedures, this research work proposes the use of ECN (Explicit Congestion Notification) based congestion notification method to be implemented at the transport level between diameter client and servers. It leaves out the diameter routing agent untouched. Explicit Congestion Notification (ECN) is an extension to TCP/IP protocol [21]. ECN supports end-to-end notification of network congestion and abatement status without dropping any packets. It is an optional feature in most of the routers and needs to be turned on for implementing this proposal. ECN uses the two least significant bits of the "DiffServ field" in the IPv4 or IPv6 header to encode four different code points: 00 – Non-ECN-Capable Transport, Non-ECT, 10 – ECN Capable Transport, ECT(0), 1 – ECN Capable Transport, ECT(1),11 – Congestion Encountered, CE. Explicit Congestion Notification is an extension proposed to RED (Random Early Detection) which marks the packet instead of dropping the packets when the average queue size is between MINth and MAXth [7]. ECN algorithm marks the diameter IP packets before the congestion occurrences. This method is useful for error sensitive protocols like TCP and its variants. It operates based on congestion avoidance algorithm which prevents the surge of messages as the router by means of learning from ECN markings at the senders end. Upon receipt of a congestion marked packet, the TCP receiver informs the sender in the subsequent ACK message about imminent congestion, which will in turn trigger the congestion avoidance algorithm at the sender. ECN requires support from both the ECN enabled routers and as well the end hosts. Figure below explains the ECN capable router with diameter client and servers.

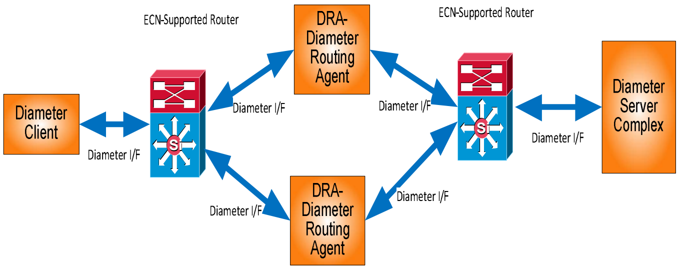

Fig.2 Proposed ECN based diameter routing architecture

During congestion, traffic will carry both the DDoS attack packets and benign user data packets. By means of congestion notification method, service availability of the hosted servers will improve and at the same time this method will not drop the DDoS attack packets. At the same token, it will serve the user without any interruption to the service offered. By efficiently managing the queue buffer size, high throughput threshold can be maintained. It supports high-burst tolerance due to DDoS spikes while sustaining desired rate. The only problem is identifying the malicious traffic along with benign sources. Both malicious and benign traffic will be injected into the receiver and downtime due to congestion will be minimized. All the routers between senders and receivers should have the ECN capability. If there are “n” routers in between, the first marked packet arrives at the initial sender after injecting 2(n+1) packets. If “n” value increased, the latency in responding to the congestion trigger will increase.

5.2 Simulation Study

We conducted simulations to evaluate the ECN based queue management for using it as a transport layer mechanism for use with TCP variants. We used ns-2 simulator to study this ECN based implementation. We have used the code publicly available as part of ns-2 development kit and simulation scripts [7, 39]. This simulation study was conducted on i386 based desktop using UBUNTU OS 12.04.

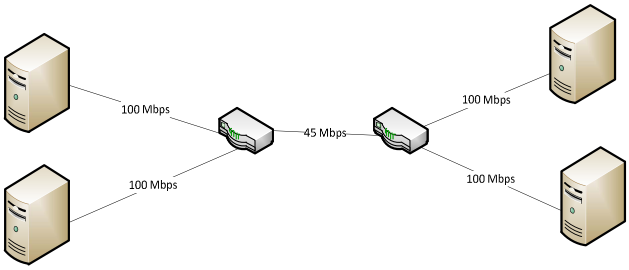

Fig.3 NS-2 Network Topology

NS-2 simulation scripts used RED gateways modified to set the ECN-CE (congestion experienced) bit in the IP packet header. Simulation shows the use of ECN-CE (Congestion Experienced bit) bits, ECN-CWR (Congestion Window Reduction) bit and ECN-Echo bits in the TCP header. Multiple CE bits inside IP header demonstrate the congestion occurrence. Study results show that the ECN bits enablement and alleviating packet drops with IP headers carrying ECN bits to intimate the congestion status to senders. Simulations demonstrated the advantage of ECN mechanism in avoiding packet drops by sending notification to the end nodes, which reduces the unwanted to delay to enhance the throughput. In addition, by means of ECN mechanism, end nodes are informed quickly, and directly the congestion status without waiting for timeout and duplicate acknowledgement packets.

6 RELATED WORK

LTE security architecture and a detailed list of security vulnerabilities existing in the LTE networks have been presented [4, 13]. Ref [16, 17] summarizes DDoS attack and vulnerabilities in LTE mobile network. Data-Center TCP (DCTCP) research work makes use of ECN congestion control algorithm to manage the queue. ECN is being used in both the new transport protocols like data center-TCP, DCTCP and datagram control protocol DCCP. DC-TCP sources extract multi-bit feedback during congestion from the single-bit stream of ECN marks by estimating the fraction of marked packets. DCTCP proved to support the following features: manage bursts, maintain high throughput, and keeps queuing delays very low [29, 38]. In DECnet bit congestion avoidance algorithm, the gateway sends congestion notification bit in packet headers based on the average queue length [36]. In SDN based overlay lay networking (OVN), to avoid getting lost in protocol translation, the Explicit Congestion Notification (ECN) markings are lost unless they get extended across the OVN. OVN aware ECN translation protocol proposed which will retain ECN information in layer-2 3 tunnelling [37].

7 CONCLUSION and FUTURE WORK

This paper identifies few key security vulnerabilities in LTE mobile network system architecture implementation. It reviews the possible security attacks in terms of signalling flood from malfunctioning apps recorded against mobile network using DDoS attacks. A proposed solution using ECN based approach to avoid congestion in diameter interfaces has been presented. NS-2 based simulation used to evaluate the proposed method confirms the removal of unnecessary packet drops which will improve the service quality of diameter transport interface. ETSI proposed Network Functional Virtualization (NFV) based data center systems evolution using cloud infrastructure to define telecom functions with virtualization will enable the tools to monitor the security implementation to defend against DDoS attacks is under study.

REFERENCES

[1] 3GPP TS 33.401 3GPP System Architecture Evolution (SAE): Security Architecture Protocol Specification Release
[2] 3GPP TS 33.102 3G Security Architecture

[3] 3GPP TS 23.102 Services and System aspects of network architecture Release 8.7.0 http://www.3gpp.org/ftp/specs/html-info/23002.htm

[4] 3GPP TR 23.843 Study on Core Network Overload Solutions", TR 23.843 0.6.0, October 2012

[5] M. Abid, S. Song, H. Moustafa, and H. Afifi, " Efficient Identity-based Authentication for IMS Based Service Access", Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMMM '09), 2009.

[6] M. Dano, "The Android IM App that brought T-Mobile's Network to its knees," Fierce Wireless, October 2010

[7] S. Floyd, "The ECN Validation Test in the NS Simulator", URL http://www-mash.cs.berkeley.edu/ns/test tcl/test/test-all-ecn

[8] D. Forsberg, G. Horn, W. Moeller, and V. Niemi, "LTE Security", John Wiley & Sons, Ltd, 2010.

[9] LTE Security Architecture http://www.3glteinfo.com/lte-security-architecture-20110325

[10] D. Jackson, "Understanding and Combating DDoS Attacks: A Threat Analysis produced by CTU Researcher" http://www.secureworks.com/assets/pdf-store/articles/Understanding_and_Combating_DDoS_Attacks.pdf

[11] D. Jones, Mobile Editor, "2014: A VoLTE Security Nightmare?" http://www.lightreading.com/mobile/mobile-security/2014-a-volte-security-nightmare/d/d-id/706869

[12] R. Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions", http://www.research.att.com/techdocs/TD_101153.pdf

[13] M. Ma, "Security Investigation in 4G LTE Networks", IEEE GLOBECOM 2012. http://www.ieee-globecom.org/2012/private/T10F.pdf

[14] E. McMurry & B. Campbell, "Diameter Overload Control Requirements", IETF Draft-overload requirements, July 19, 2013.

[15] C. Mulliner and J.P. Seifert, "Rise of the ibots: Owning a Telco Network", in proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware), 2010.

[16] R. Piqueras Jover & P. Giura, "How vulnerabilities in wireless networks can enable Advanced Persistent Threats", in International Journal on Information Technology (IREIT) 2013.

[17] R. Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions", IEEE.

[18] J. Markoff, "Firm Is Accused of Sending Spam, and Fight Jams Internet," New York Times 2013.

[19] K. Ramakrishnan, and S. Floyd, "A Proposal to add Explicit Congestion Notification (ECN) to IP", RFC 2481, January 1999

[20] M. Stahlberg, "Radio Jamming attacks against two popular mobile networks, Helsinki University of Technology. Seminar on Network Security, Mobile Security, 2000

[21] A. Uchler and M. Schapranow, "Congestion Control", Seminar on Communication Networks. http://placebo.hpi.unipotsdam.de/webhome/matthieu.schapranow/cn/050111_-_Kuechler,_Schapranow,_-_Congestion_Control.pdf

[22] LTE World http://lteworld.org

[23] GSMA www.GSMA.com

[24] A.T. Kearney, Cisco 2013 Mobile UNI Study

[25] AT&T Distributed Denial of Service (DDoS) Defense http://www.business.att.com/content/productbrochures/ddos_prodbrief.pdf

[26] IETF RFC 3168 http://www.ietf.org/rfc/rfc3168.txt

[27] Understanding Denial of Service Attacks http://www.us-cert.gov/ncas/tips/ST04-015

[28] AT&T Hit by DDoS attack and suffers DNS outage http://www.pcworld.com/article/260940/atandt_hit_by_ddos_attack_suffers_dns_outage.html

[29] DCTCP Protocol http://simula.stanford.edu/~alizade/Site/DCTCP.html

[30] The DDoS Security Threat to Mobile Networks, Retrieved from Internet sources, INFOTech Spotlight http://it.tmcnet.com/magazine/features/articles/173137-ddos-security-threat-mobile-networks.htm

[31] Advanced Persistent Threats – A Brief Description https://www.damballa.com/advanced-persistent-threats-a-brief-description/

[32] IETF RFC 4187, EAP Method for 3GPP AKA, http://tools.ietf.org/html/rfc4187

[33] 97% of Mobile Malware Is On Android. This Is The Easy Way You Stay Safe, Forbes Magazine, 2013. http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/

[34] IETF RFC 6733

[35] Internet Security Report, Arbor Networks http://www.arbornetworks.com/resources/infrastructure-security-report

[36] Ramakrishnan, K. K., and Jain, R., "A Binary Feedback Scheme for Congestion Avoidance in Computer Networks", ACM Transactions on Computer Systems, Vol.8 No.2, pp. 158-181, 1990.

[37] D. Crisan., R. Birke., K. Barabash., and R. Cohen., "Datacenter Applications in Virtualized Networks: A Cross-layer Performance Study".

[38] Datagram Congestion Control Protocol http://datatracker.ietf.org/doc/rfc4340/

[39] "ECN Web Page", http://www-nrg.ee.lbl.gov/floyd/ecn.html

[40] Seven Networks http://www.seven.com/mobile-signaling-storm.php

[41] M. Donegan, Android Signaling Storm Rises in Japan http://www.lightreading.com/mobile/device-operating-systems/android-signaling-storm-rises-in-japan/a/d-id/693138

APPENDIX –A- Simulation Results

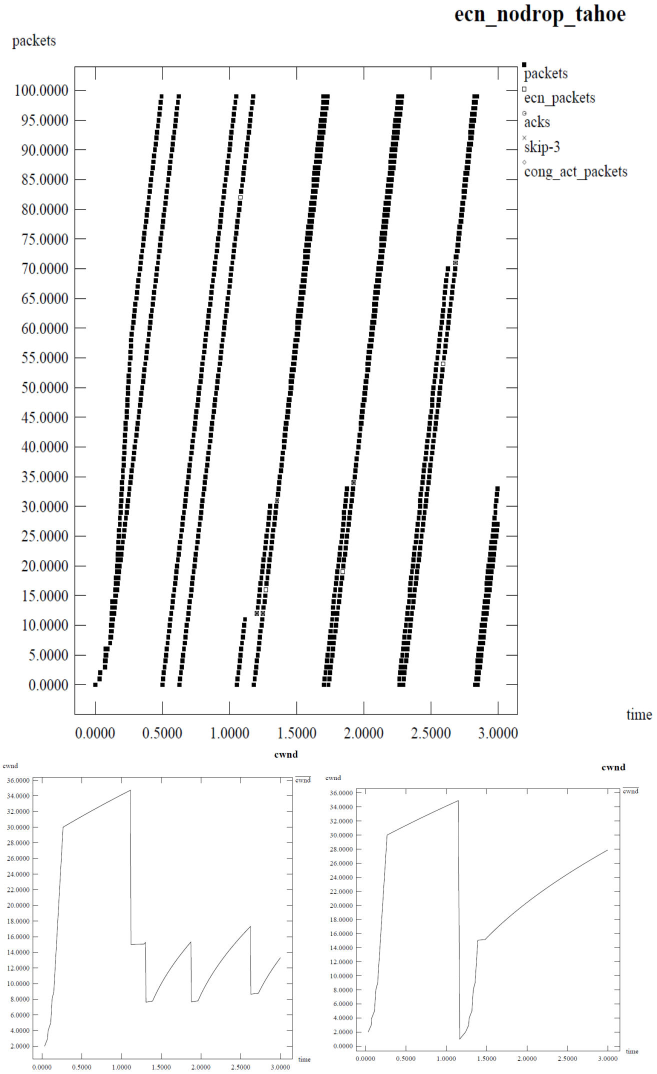

Fig.4 NS-2 simulation results with no drop of packets using ECN enablement. Packet drops observed when ECN feature disabled in the router/gateway simulation nodes.