International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Protective Selective Jamming Attack for 4G/LTE Networks

Kasimbee Shaik
M.Tech (DSCE)

Abstract**—** *Increasing demands for high-speed broadband wireless communications with voice over long term evolution (LTE), video on demand, multimedia, and mission-critical applications for public safety motivate 4th-generation (4G) and 5G communication developments. The level IP-based LTE and LTE-Advanced innovations are the normal key drivers for 5G. Be that as it may, LTE, with its slipped by security mechanism and open nature, leaves an immense proviso for interlopers to risk the whole correspondence network. The time and data transfer capacity expending validation technique in LTE prompts benefit interruptions and influences it to unfit for open wellbeing applications. To provide food the predominant LTE security and administration necessities, we propose the protective selective jamming mechanism, which is composed of two dependent protocols: 1) Privacy-protected for DDoS attack and 2) Selection for attacking users. The PSJM supports seamless communication with a minimum signaling load on core elements and conceals users' permanent identifiers to ensure user privacy. We simulate the proposed conventions for authentication with the broadly acknowledged robotized approval of Internet security conventions and applications instrument. A relative examination of data transfer capacity and energy utilization is likewise performed and demonstrated through NS2 tool that the proposed 4GCPAM beats the current arrangements.*

Keywords—Security, Authentication, 4G/LTE, Public safety, Network access, Mobile communication.

I. INTRODUCTION

The forth generation of mobile networks, known as Long Term Evolution (LTE) or Evolved Packet System (EPS) is currently being deployed worldwide and has an impressive impact on the world given that the total number of subscriptions, 6.8 billions, is approaching world population figure, 7.1 billion [1]. The forth generation of mobile networks has been optimized for data transmission and is designed to provide broadband data at speeds of around 100 Mbps for the downlink and 50 Mbps for the uplink, very low delay, improved Quality of Service (QoS), interoperability with 2G and 3G systems and high levels of security.

Its security protocols have been improved compared to 3G Universal Mobile Telecommunications System (UMTS) in order to make it resilient to new attacks. These new attacks were possible because of the massive increase of computing power, of the availability of complex attack tools, and of the security vulnerabilities that the protocol had. The technical specifications of EPS are frequently being updated, thus showing an increased research interest and a coherent strategy to improve the security of 4th generation networks.

LTE broadband communication is gaining importance in emergency and rescue operations, where voice calls will remain an essential service, even for PS systems. These voice calls in PS systems rely on voice over LTE [2]. PS communication security is of paramount importance in public safety LTE (PS-LTE) networks, which includes confidentiality, authentication and user privacy management [3]. Furthermore, with the increasing demands for information security and privacy in daily life and businesses, the success of the PS-LTE depends on its security and service level [4].

An LTE Access Network (referred to as Evolved Packet System (EPS) by 3GPP) comprises of the Evolved UMTS Terrestrial Radio Access (E-UTRA (also called LTE)) and the Evolved Packet Core (EPC). The LTE Access Network GIR [5] identifies the possible congestion points for E-UTRA access to the EPC and in the EPC. The possible congestion points within the functional entities (FEs) and interfaces are described along the bottom of the Figure. This figure also shows the interconnection to IMS-based Core Network and the 2G/3G wireless networks which are out of scope or discussion in this paper.

Congestion does not impact LTE Access Network FEs and the associated interfaces equally, since certain resources are typically more limited than other resources. Also, priority mechanisms that are introduced to mitigate congestion at particular points in the architecture may affect other congestion points. For example, an access control mechanism applied over the E-UTRA air interface will reduce the total traffic load on an eNodeB, as well as reduce the aggregate traffic load that reaches other LTE Access Network FEs.

In the United States, LTE is being used as a framework for the nationwide public safety network known as First Net. The objective of First Net is to provide a nationwide wireless broadband interoperable public safety network that provides reliable communications among first responders. Of most prominent concern are crises caused by a adversary, for example, a fear based oppressor association, whose assault may include radio sticking against cell systems to guarantee confuse and create additional frenzy. All things considered, against jamming countermeasures should be considered.

The U.S. military has considered utilizing specially appointed LTE-construct systems to keep officers in light of the battlefield associated, and additionally for shipborne correspondence with maritime airplane. Dissimilar to military models, cell benchmarks are openly accessible, implying that enemies may use this information and target frail indicates in the convention improve the viability of their assaults. Radio sticking assaults are a genuine risk to any military or battlefield interchanges connect and should be represented.

Assaults on LTE can be assembled into two general classes: denial of service (DoS) and data extraction. Jamming assaults are regularly used to cause benefit disturbance or DoS; assaults that concentrate data or cause DoS by focusing on the higher layers fall under the class of digital assaults. Radio jamming is broadly defined as an attack in which a jammer transmits energy to disrupt reliable data communication. Jamming is performed through an RF assault vector, while digital assaults utilize arrange assault vectors. In this article we are just worried about jamming. An imperative property of jamming is that it generally focuses on the beneficiary; paying little respect to how close the jammer is to the transmitting node. Thus, jamming the LTE downlink, the signal transmitted by a base station and got by cell phones, focuses on the cell phones, while jamming the uplink focuses on the base station. RF caricaturing alludes to transmitting a phony flag intended to take on the appearance of a genuine signal [6].

II. RELATED WORK

This section gives a brief outline of the security issues and communication overhead issues in the LTE EPS-AKA as well as the corresponding solutions proposed to date and their shortcomings. Starting with the security issues related to IMSI, a static user identity guarantees confidentiality in an LTE access network. IMSI is necessary to clone any user. To establish a secure connection, it is mandatory to avoid the use of IMSI on air by replacing it with any other temporary identity, which is called the Temporary Mobile

Subscriber Identity (TMSI) [9]. In contrast, the authentication protocols in recent research works transmit the unencrypted IMSI on air during the initial attach request, which allows intruders to tamper with the IMSI [8], [10]. Another major rising threat is redirection attack, where a fake Evolved Node B (eNB) redirects the user attach request to a foreign network when a user is eligible or intends to connect to its home network. In this case, the foreign network charges the mobile user based on a rate that is higher than the rate offered by the home network.

EPS Integrity algorithms (EIA), such as EIA1, EIA2, and EIA3, are being used in LTE. EIA2 is preferred for integrity protection in the proposed system as it utilizes AES as the underlying cipher and Cipher-based Message Authentication Code (CMAC) as the upper-level Message Authentication Code (MAC) structure, which has been proven to be secure. In contrast, EIA1 and EIA3 are polynomial MACs, which have the linear property and are prone to linear forgery attack and trace extension forgery attack [11], [12]. The lack of forward secrecy and vulnerability to man-in-the-middle attack are still security problems of LTE EPS-AKA, as an unencrypted authentication procedure is carried out between the UE and core network [8], [13], [14]. In the future, LTE systems are envisioned to support critical PS communication, where seamless communication between the victims and responders in tactile and emergency scenarios is required [7], [15].

III. EXPERIMENTAL DESIGN

The existing security mechanism is based upon the self adaptive mechanism with decentralized approach against specific jamming assault in 4G/LTE systems. The specific jamming assault is a type of forswearing of administration assault, which is utilized to cause the assets inaccessible for specific reason. Self-adaptive in the title implies that every node is separately fit for attaching the specific jamming assault without anyone else. The proposed demonstrate is perfectly applicable for the 4G/LTE networks working on TDMA (time division multiple access) and effective against distributed denial of service attack. The proposed scheme is aimed to work at MAC layer. Also the proposed scheme is aimed to solve the problem of energy consumption. The new scheme in the paper is created to put the least effect on the energy consumption and helps the 4G/LTE networks to establish stronger connectivity when the security scheme is implemented.

The self versatile decentralized arrangement against specific jamming assault is viable against the denial of service (DoS) assaults just as a large portion of the assaults propelled on the 4G systems are distributed denial of service (DDoS) attacks, which is not protected using this scheme. The existing security scheme is very complex, which delays the packet exchange between the nodes according to the scheme adds a heavier overhead on the BTS over the 4G/LTE networks. The security scheme in existing model is based on a formula to find the integral code for authentication purposes. The change technique is utilized to implant and check the safe code, which is inclined to hacking on the grounds that it depends on a scientific equation.

The detection of colluders in a sophisticated collusion attack is that at least one of the compromised nodes will have the highly non stochastic behavior. Here the error of non-traded off nodes, not withstanding when it is extensive, originates from countless components, and in this way should generally have a Gaussian appropriation. Therefore, rather than taking a look at the root mean square greatness of blunders of every sensor, we take a look at the measurable dissemination of such mistakes, evaluating the probability whether they originated from a typically appropriated irregular variable. Nodes that are very improbable to have originated from a regularly dispersed arbitrary variable, potentially with a bias, are disposed of.

Protective selective Jamming mechanism:

PSJM scheme has been designed to detect the selective jamming which is a kind of denial of service attack. It detects the threat attack and protects it from further harming the client. PSJM scheme design has been given below:

- The IDS (Cp) calculates the available bandwidth on the node.
- The Cp scans for the active connections with the node being analyzed.
- The Cp checks for the input data volumes D={dc1, dc2, dc3 … dcX} coming from the different nodes.
- The Cp decides the threshold 'Thr' value by computing upon the D matrix.
- The individual data volumes are then scanned against the threshold value 'Thr' to find the traffic abnormalities.
- The traffic streams with abnormal traffic volumes are noticed and analyzed individually.
- The traffic volume is calculated against the assigned individual connection bandwidth (AsetBW)
- If the traffic volume is found more than AsetBW ->Overhead traffic is filtered
- Otherwise -> traffic is permitted

IV. RESULT ANALYSIS

The proposed model has been named as the protective selective Jamming Mechanism (PSJM) regime. The proposed model was suffered various types of experiments to evaluate real-time performance of the proposed model in various situations and conditions. The proposed model was evaluated on the basis of various network performance parameters.

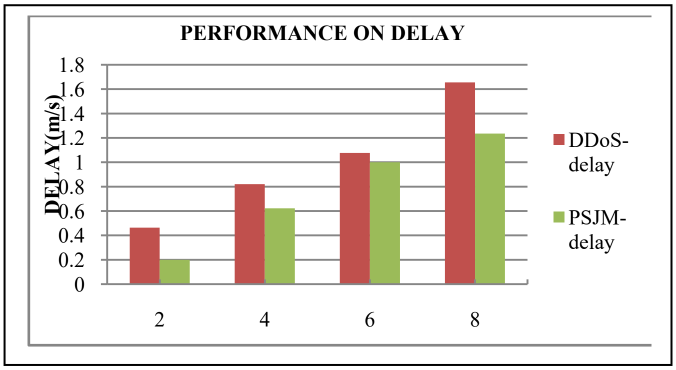

Figure1: Network delay

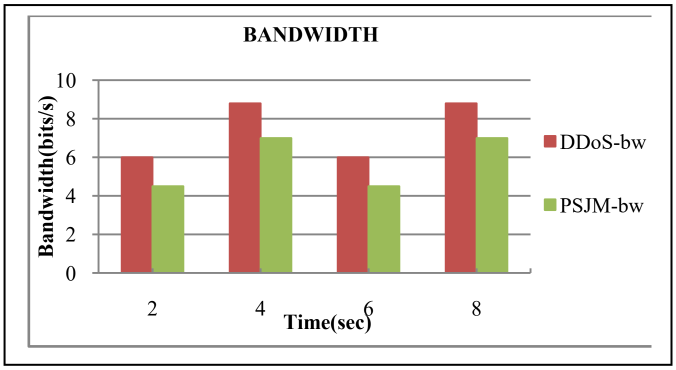

Figure2: Bandwidth

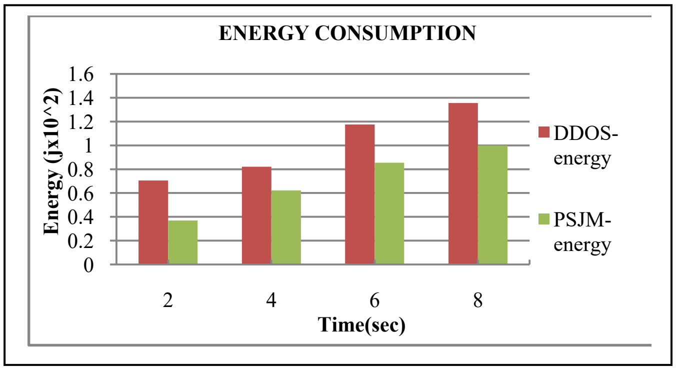

Figure3: Network lifetime

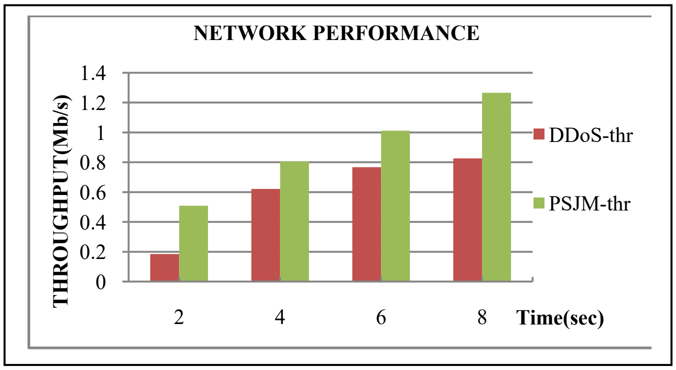

Figure4: Throughput

Meanwhile, Figure 1 shows that the delay is a little higher when the node acts as DDoS node. When a normal node wants to speak with an abnormal state node, it will cradle a few parcels first and after that begin the course disclosure process. Our protocol does not affect the less number packets delivered per minimum time interval. Figure 2 shows that the bandwidth is higher when the attack process occurs. The routing process should be depending on how much DDoS node traveling distance. Figure 3 shows that, individual node energy levels based on network routing process and routing levels more efficient it will be effect to process of attack levels. Figure 4 show that, before data delivering check the all nodes RREQ and RREP, the network throughput remains as high as the while the network scale grows.

V. CONCLUSION

With the PSJM scheme the selective jamming attack is prevented and also this scheme is efficient in energy consumption. PSJM scheme has been developed as the self versatile decentralized arrangement against selective jamming. Intrusion detection system (IDS) and intrusion prevention system (IPS) for the wireless sensor networks is also paid attention on. PSJM scheme has been designed in the multi-layered model with inter-nodal relationship competence specifically designed to work on MAC layer. PSJM scheme has been designed in the host-IDS fashion, where every node or every host is handling the intrusion detection and prevention on itself, which can be also categorized in the self-adaptive mechanism. PSJM scheme is based upon the multi-hop authentication scheme, where the intermediate hops remains invisible between the two nodes, while the authentication process is going on between two non-neighbor nodes. The proposed intrusion prevention system offers the authentication process to filter out the attacker nodes from the network in the initial phase. PSJM system was designed to detect and mitigate the selective jamming and distributed denial of service (DDoS) on sensor networks to launch the error-free service. Through intensive simulation experiments using NS-2, we proved that every functionality works well, and jamming attack can be mitigated effectively.

REFERENCES

[1] ITU, “The world in 2013, ICT Facts and Figures”.

[2] T. Doumi *et al.*, ``LTE for public safety networks," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 106_112, Feb. 2013.

[3] L. Carlà, R. Fantacci, F. Gei, D. Marabissi, and L. Micciullo, ``LTE enhancements for public safety and security communications to support group multimedia communications," *IEEE Netw.*, vol. 30, no. 1, pp. 80_85, Jan. 2016.

[4] Nokia Networks. *LTE Networks for Public Safety Services*. Accessed: Jul. 1, 2017.

[5] Long Term Evolution (LTE) Access Network Government Industry Requirements (GIR) for National Security / Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services, Issue 2.0, January 2013.

[6] M. Labib, V. Marojevic, and J. Reed, “Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofi ng,” *IEEE Conf. Standards for Commun. and Net. Proc.*, Oct. 2015, pp. 160–65.

[7] L. Carlà, R. Fantacci, F. Gei, D. Marabissi, and L. Micciullo, ``LTE enhancements for

public safety and security communications to support group multimedia communications,'' *IEEE Netw.*, vol. 30, no. 1, pp. 80_85, Jan. 2016.

[8] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, ``A survey on security aspects for LTE and LTE-A networks,'' *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 283_302, 1st Quart., 2013.

[9] M. Abdeljebbar and R. El Kouch, ``Fast authentication during handover in 4G LTE/SAE networks,'' *IERI Procedia*, vol. 10, no. 1, pp. 11_18, 2014.

[10] M. Bartock, J. Cichonski, and J. Franklin. (Apr. 2015). ``LTE security_How good is it?'' NIST, Gaithersburg, MD, USA, Tech. Rep. 3.

[11] T. Wu and G. Gong, ``The weakness of integrity protection for LTE,'' in *Proc. 6th Conf. Secur. Privacy Wireless Mobile Netw.*, Apr. 2013, pp. 70_88.

[12] A. Zugenmaier and H. Aono, ``Security technology for SAE/LTE,'' *NTT DOCOMO Tech. J.*, vol. 11, no. 3, pp. 27_30, 2009.

[13] M. A. Andrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, ``LTE authentication protocol (EPS-AKA) weaknesses solution,'' in *Proc. IEEE Int. Conf. Intell. Comput. Inf. Syst.*, Dec. 2015, pp. 434_441.

[14] C.-K. Han and H.-K. Choi, ``Security analysis of handover key management in 4G LTE/SAE networks,'' *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 457_468, Feb. 2014.

[15] R. Favraud, A. Apostolaras, N. Nikaein, and T. Korakis, ``Toward moving public safety networks,'' *IEEE Commun. Mag.*, vol. 54, no. 3, pp. 14_20,Mar. 2016.