A NOVEL SECURITY SYSTEM FOR PREVENTING DOS ATTACKS IN 4G/LTE NETWORKS

Karri babu[1], Dr. K Venugopala Rao[2]
[1]*Research scholar, Department of CSE, Rayalaseema University, Kurnool, Andhra Pradesh, India-518002.*
[2]*Professor, Department of CSE, G Narayanamma Institute of Technology and Science, Hyderabad, Telangana, India-500008.*

Abstract: By using cryptographic strategies, LTE is composed. The verification which is common between LTE network elements with the well being components which are incorporated with its design that is getting built. A well known industries and organizations have distinguished unprotected security which is ought to be evaluated by under network distribution. The security related issues and problems in wireless networks would remain as a trending issue of argument. Then, LTE/SAE standard security can be adjusted to these difficulties upward, which turn out to be stronger and secured. The selection of jamming mechanism to protect security for the network process but it doesn't support for the internet related firewalls in previous work. In this paper, a novel system of securityhas been initiated in that system with firewall is executed between the core transport network and the internet network to prevent DoS attacks. The traffic travels through the firewall that decides whether to allow or reject the packet based upon the rules set which was implemented as entitled as Evolved Packet Core (EPC). The network's performance analysis has been improved by using the method of comparison which was proposed with existing models. The comparative analysis of method which was proposed in end to end delay and throughput is better than the existing methods utilizing the Network simulation tool (NS-2).

I. INTRODUCTION

LTE that might consider as short for long term evolution [1] is the standard wireless communicationof fourth generation. It contributes data of high speed for data terminals and mobile phones. LTE primarily will allow the high rate of data, with a minimum delay, the capacity because of the bandwidth that is scalable and the flexibility it has. The UE (user equipment), for instance laptops or smart phones will get connected to the network that is wireless over the eNodeB (base station) in the E-UTRAN (Evolved UMTS Terrestrial Radio Access Network). The E-UTRAN will connect to the (Evolved Packet Core)EPCstand on IP.EPC will be connecting to the provider of the wire line IP network [2]. EPC is also core network which makes LTE very simple, efficient and scalable.

The additional security improvements were publicized in 4G LTE over 3GPP [3]. For instance, the abstraction's advance layers are added to the name of the unique identifiers (ID) for an end-mobile device (UE). Any kind of USERNAME has been ended up within 2G being suited for SIM minute card. In addition to eventually 4G LTE within 3G, the temporary criminals are to be able to grab the identities. The other device which has ability to support the secured measures within 4G has got ended up being to distribute the safe signalling between the UE additionally MME (Mobile Management Entity) [4]. A new risk to mobile users has come from the switch to IP (Internet Protocol). All the mobile networks which 4G are all-IP, while 3G networks are the combination of IP and mobile signalling protocols (SS7).

IP is well-known and open than the unclear protocols of mobiles in the past. It has been undertaken successfully by the hackers for several years by opening up many potential threats. Withholding the service attack is the most prominent one among the other security issues. There are two creative approaches to convey DoS in LTE systems. The predominant kind of DoS strike is against a specific UE.

A malicious audience [5] of radio could be utilized the planning of asset data alongside the CRNTI to send an uplink signal of control at the time which was planned. Hence, preferring clash at the eNodeB and the issues of administration for the genuine UE. In the recent past, arriving UEs are defenceless to a second kind of DoS strike. UE is allowed to remain in dynamic mode but kill its radio handset to spare force utilization. This is realized by means of the DRX (Discontinuous gathering) period.

UE is enabled to parcels transmission on the grounds that the UE which have earnest activity to send during a long DRX period. This could make a potential security gap on the other side. As a sample, aggressors could fill C-PDU bundles between the DRX period be brought about DOS strikes against UE's which are arriving recently. Another type which is third of DoS attack [6] could be based on the buffer status reports used byan eNB for scheduling of packet balancing the load, and control over the admission. Attackers can send the reports by impersonating a real UE. If the impersonator sends reports of buffer status that report more data to send than that are actually buffered by the real UE. It will cause behavioural change of admission control algorithms. If the eNB recognizes many such fake reports of buffer status from several UEs, it might have belief that there is a heavy load in this cell. Accordingly, the eNB might not accept UEs which are newly arrived.

II. LITERATURE SURVEY

Elramly, Salwa, in "SMSHM: Secure Mesh Mode Protocol to Enhance Security of 4G Networks" displayed that to make sure the protection of the client as well as the utilized system, the backing of security is mandatory for all the

correspondence. The report highlights several vulnerabilities of security and it offers other convention to reinforce the security in mode of lattice. This convention would depend on bio-crypto frameworks that provide solutions to secure an initial network entry, and attain protection between two different hubs in the system. The convention that incorporatesan Advanced Encryption Standard & Biometric Digital Key forthe system messages as well as the key distribution [7].

Marco Tiloca in "SAD-SJ: A Self-Adaptive Decentralized Solution against Selective Jamming attack in the wireless sensor networks, in Emerging Technologies & Factory Automation (ETFA)" has been initiated in number of application situations that include the industrial applications as well as factory automation. In such particular situations, Time Division Multiple Access (TDMA) has been used most of it for the correspondence of information between the sensor hubs. But later, the systems of TDMA-based sensors have been inclined especially to particular jamming strike which is a specific kind of administration dissent to network the ability to depend genuinely impede. In that article, it was presented SAD-SJ, which is a self-versatile and decentralized arrangement of MAC layer against impedance particularly in system TDMA-based sensors. SAD-SJ doesn't need afocal element but sensor hubs has been depending on local information and allow them to join and leave the system without affecting other action hubs. It also illustrates that SAD-SJ has compelled extra cost as far as figuring, interchanges and vitality utilization [8].

Sanzziri, Ameva, in "SESAME: Smartphone Enabled Secure Access to Multiple Entities" has been introduced an architecture based cell phones to have secure client access to web benefits which require input through password. The architecture that was described exploits biometric sensors which are accessible in present day's cell phones at the time of verifying a cell phone client to provide guarantee that his character cannot be covered by another person. The client can obtain to administrations of web utilize a password of mind blogging that put away as a part of its cell phone, but without entering the complex password physically. In this process, the architecture will overcome a huge portion of password limitations of security that takes into an account the techniques of validation for the day. Specially, to gear up the present difficulty that is connected with the complex passwords utilization. The architecture has not just suggested works consistently with the web benefits present day as it doesn't oblige change to the authentication mechanisms which existing are being utilized by the servers, but it can likewise reached out to use the specific biometric information of a accreditations of man rather than passwords to receive to web administrations and the digital physical frameworks later on [9].

Han, Chan-Kyu, and Hyoung-Kee Choi in "Security Analysis of handover the key management in 4G LTE/ SAE networks" portrays one of the difficulties which is remarkable of fourth generation innovation is one way to fill the security lack by which a traded off or single gadget could risk a whole versatile system due to the open process of these systems. To connect this test, the key administration exchange in the 3GPP LTE/ SAE has been planned to reject a key as a consequence of trade off and segregate the corrupted network devices. This analysis discriminates and the vulnerability points of key management transfer are known as desynchronization assaults. These assaults weaken secure communications between the users and mobile networks [10].

Alezabi, Kamal Ali, in "An authentication which is efficient and key agreement protocol for 4G (LTE) networks" have been initiated authentication in LTE networks. It is a crucial procedure on the grounds that most of the assaults from happening between this stage. The attackers which attempt to be authenticated, and then it dispatches system resources and prevent authentic clients of system administrations. The requisites Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) have got utilized as a part of LTE AKA convention is known as Evolved Packet System Alias (EPSAKA) convention to protect LTE system, whereas it experiences regardless distinct vulnerabilities. For instance, the identity of the client's disclosure, overhead calculation, Man In The Middle (MITM) attack and delay authentication. In the article, feasible EPS-AKA convention (AKA-EEI) has been suggested to overcome the current issues. The initiated convention is depending on the key exchange exponential simple password (SPEKE) protocol [11].

III. PROPOSED FRAMEWORK

A novel security system has been proposed to prevent DoS attacks in this paper. A system in which a firewall has been implemented in between the core transport network and the internet network is known as EPC (Evolved Packet Core). A packet inspection in deep has got installed for the sake of packets' identification to transfer. The utilization of these two methods, the firewall with the deep packet inspection welfare in a way that one component's failure doesn't leave the network unprotected. The traffic which was generated by host has been directed towards EPC from the way it has passed by firewall in the combination with the deep packet inspection. The traffic travel across the firewall and deep packet inspection, and it allows or rejects the packet based on the set of rules that are implemented by the administrator of firewall. According to the proposed set of rule, a specific threshold e.g. a numerical value of 40 has been assigned as the threshold limit. It means the several requests which are made by one host got connected to the network and would request for the services that shouldn't exceed from 60 times per minute.

Users have granted the services of the server by forwarding the data requests over the network according to the specified threshold. By the time the request rate of one mobile host outreaches the set threshold level, a delay would be given before satisfying the request of the user and the user has to wait for the set time out. Meanwhile, the request from another mobile host which has a different IP address would be served. In this approach, an absolute shut down of the total network would get minimized by different hosts serving after the

interval. This situation could be achieved by implementing the security system with a firewall which got merged with deep packet inspection that keeps the record of each IP address of mobile hosts, the request rate and the threshold value and it allows the hosts with requests lesser then the threshold to manage the internet services as illustrated. The DoS attacks are blocked to certain extent by deploying the proposed security system. The system permit to supply services of the server to different mobile that hosts based on the request rate and the threshold value which is specific. An attacker who sends floods of messages to the server could consume the resources for a specific time period that depends on the threshold set. So, prevention of blocking the data connection of the mobile subscribers get connected to the server by not letting any sole mobile host or an attacker that takes up all the available bandwidth and flood the server with requests and finally thwarting the impact of DoS attacks.

3.1 Algorithm

Initialize network
For i = 1: N
Receive data traffic
Begin
    Received by firewall
    Inspect RR of each data
If (RR > ThreshRR)
    Check for Delay
    Set TO for node
If (TO == expired)
    Connect to Server
Else
    Add CID in route path
    Update network with CID as MN
End If
End If
End for

In above algorithm, mentioned different notations presented below:
N= total number of nodes
FW – firewall
RR – request rate
ThreshRR – Threshold RR
IP- ip address of nodes
TO – timeout
CID - Client ID
MN - Malicious Nodes

It is very crucial to separate the effect of DDoS attack from the network to increase the working efficiency of network. The packet level of algorithm restraining has been utilized for the removal of DDoS attack for the enhancement of efficient working of network. The algorithm that has proposed would keep the track of flooded packets in the transmission.
The restraining algorithm packet level supports to control the incoming packets' flow into the base station by which the base station wouldn't be flooding with the requests. But, it helps to control the congestion at this stage. So for the purpose of check validity of an incoming packet will be performed packet filtering on the TTL basis values of each and every incoming packet.

IV. RESULT AND DISCUSSION

The proposed model has been named as the Firewall based packet level identifier (FBPLI) algorithm. The proposed model was suffered various types of experiments to evaluate real-time performance of the proposed model in varioussituations and conditions. The proposed model was evaluated on the basis of various network performance parameters.

PARAMETER	VALUE
Application Traffic	CBR
Transmission rate	1000 bytes/0.5ms
Radio range	250m
Packet size	1000 bytes
Maximum speed	30m/s
Simulation time	50sec
Number of nodes	20
Area	800x700
Routing protocol	AODV
Routing method	FBPLI,PSJA

Table1: Simulation table

In this paper, we assume that 20 sensor nodes are randomly distributed over an 800x700m^2 field by considering the Radio range as 250m.In the Table1, shows that the system parametersused in our simulations. Here we use Application Traffic as CBR (Constant Bit Rate) it can be support for control the traffic in network, Routing Protocol as AODV and it is used for routing level in network, Routing Methods are FBPLI, PSJA in our simulation, this routing methods are efficiently used for performing the network outcomes. Next the Transmission rate is 1000 bytes/0.5msby considering the Packet size as 1000 bytes and with a Maximum speed 30m/s and the total Simulation time is 50 sec.

Evaluation results:

In this section, we utilize the Firewall based packet level identifier method. According to the delay, packet delivery ratio and the prevention of DDoS attack, we present experimental results of the algorithm which are introduced below.

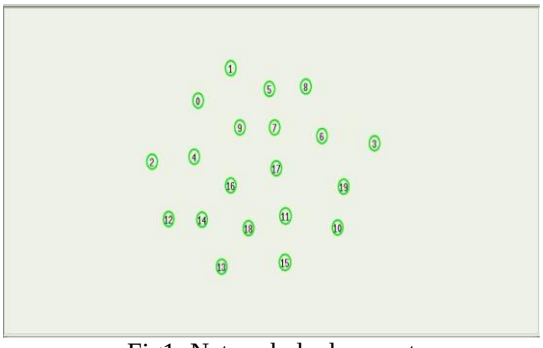


Fig1: Network deployment

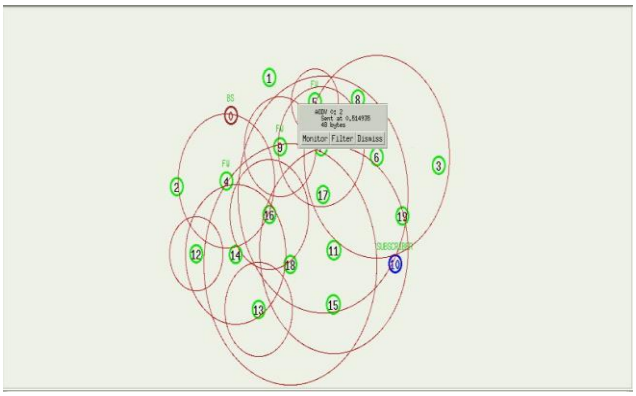


Fig2: Broadcasting process in Network

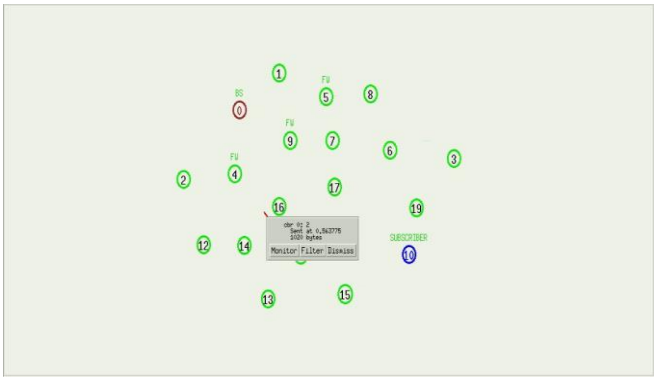


Fig3:Data transmission between subscriber and BS

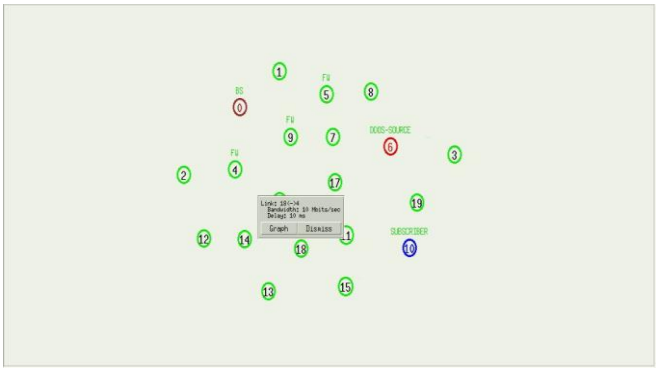


Fig4: Data transmission between Hop node and FU node

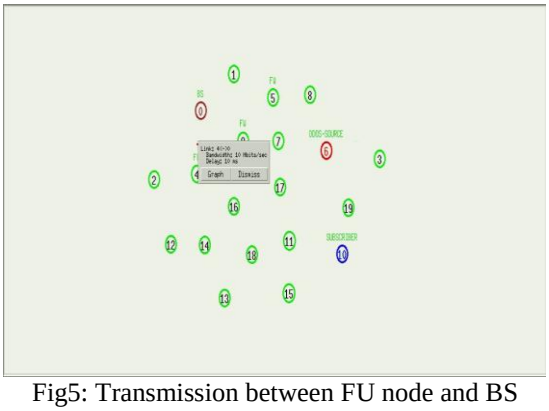
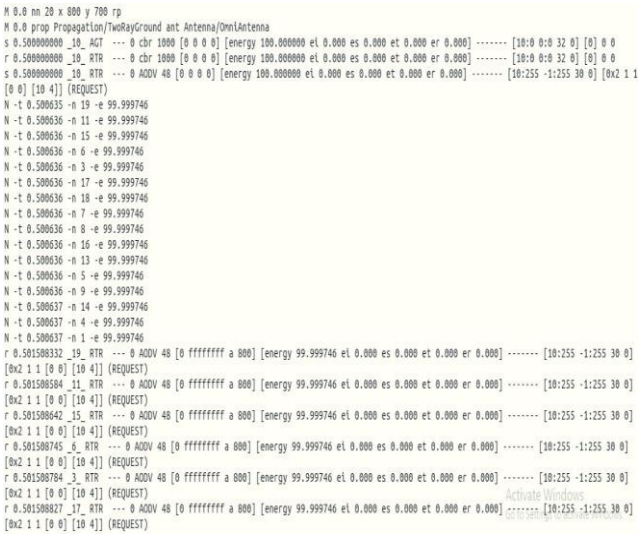


Fig5: Transmission between FU node and BS



```
M 0.0 nn 20 x 800 y 700 rp
M 0.0 prop Propagation/TwoRayGround ant Antenna/OmniAntenna
s 0.500000000 _10_ AGT  --- 0 cbr 1000 [0 0 0 0] [energy 100.000000 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:0 0:0 32 0] [0] 0 0
r 0.500000000 _10_ RTR  --- 0 cbr 1000 [0 0 0 0] [energy 100.000000 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:0 0:0 32 0] [0] 0 0
s 0.500000000 _10_ RTR  --- 0 AODV 48 [0 0 0 0] [energy 100.000000 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0] [0x2 1 1
[0 0] [10 4]] (REQUEST)
N -t 0.500635 -n 19 -e 99.999746
N -t 0.500636 -n 11 -e 99.999746
N -t 0.500636 -n 15 -e 99.999746
N -t 0.500636 -n 6 -e 99.999746
N -t 0.500636 -n 3 -e 99.999746
N -t 0.500636 -n 17 -e 99.999746
N -t 0.500636 -n 18 -e 99.999746
N -t 0.500636 -n 7 -e 99.999746
N -t 0.500636 -n 8 -e 99.999746
N -t 0.500636 -n 16 -e 99.999746
N -t 0.500636 -n 13 -e 99.999746
N -t 0.500636 -n 5 -e 99.999746
N -t 0.500636 -n 9 -e 99.999746
N -t 0.500637 -n 14 -e 99.999746
N -t 0.500637 -n 4 -e 99.999746
N -t 0.500637 -n 1 -e 99.999746
r 0.501508332 _19_ RTR  --- 0 AODV 48 [0 ffffffff a 800] [energy 99.999746 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0]
[0x2 1 1 [0 0] [10 4]] (REQUEST)
r 0.501508584 _11_ RTR  --- 0 AODV 48 [0 ffffffff a 800] [energy 99.999746 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0]
[0x2 1 1 [0 0] [10 4]] (REQUEST)
r 0.501508642 _15_ RTR  --- 0 AODV 48 [0 ffffffff a 800] [energy 99.999746 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0]
[0x2 1 1 [0 0] [10 4]] (REQUEST)
r 0.501508745 _6_ RTR  --- 0 AODV 48 [0 ffffffff a 800] [energy 99.999746 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0]
[0x2 1 1 [0 0] [10 4]] (REQUEST)
r 0.501508784 _3_ RTR  --- 0 AODV 48 [0 ffffffff a 800] [energy 99.999746 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0]
[0x2 1 1 [0 0] [10 4]] (REQUEST)
r 0.501508827 _17_ RTR  --- 0 AODV 48 [0 ffffffff a 800] [energy 99.999746 el 0.000 es 0.000 et 0.000 er 0.000] ------- [10:255 -1:255 30 0]
[0x2 1 1 [0 0] [10 4]] (REQUEST)
```

Fig6: Trace file of routing

In above screenshots, Fig 1 shows all nodes placed in network and deployment of nodes is in network properly. Here all nodes displayed based on topology values and all properties of NAM window it should be mentioned. Fig 2 shows the broadcasting occur throughout the network. Here broadcasting occurs for communication purpose. All nodes should be involved in this process. Fig 3 shows that data communication process in network. In this process, subscriber node and base station are involving in simulation. Fig 4 mentioned above screenshot of nam, it considering link between hop node and FU node. Here bandwidth and delay shows average level of routing in network. Fig5 shows that, data delivery form FU node to base station. In this, data delivering protocol and time interval then how much data should be delivered these all are shows. Fig 6 shows trace file of network. It represents overall end to end process in simulation.

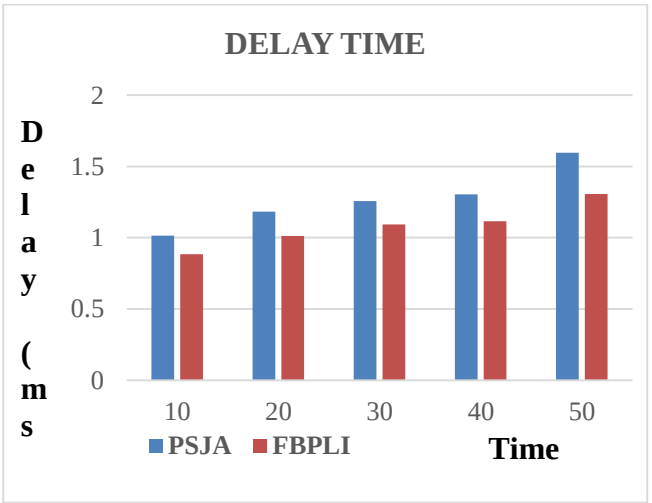


Fig7: End to End Delay

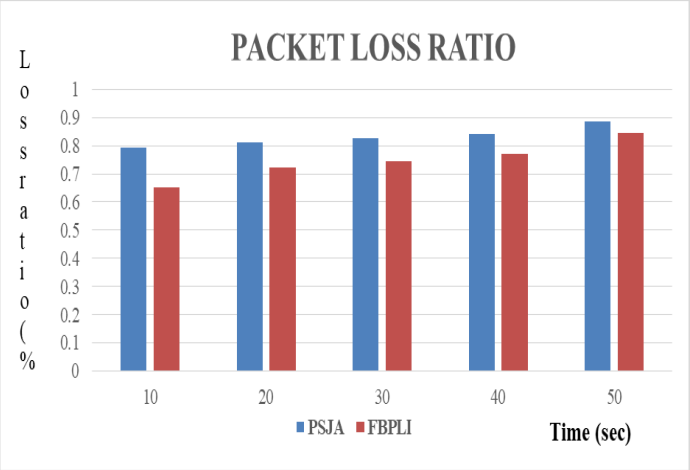


Fig8: Packet dropping ratio

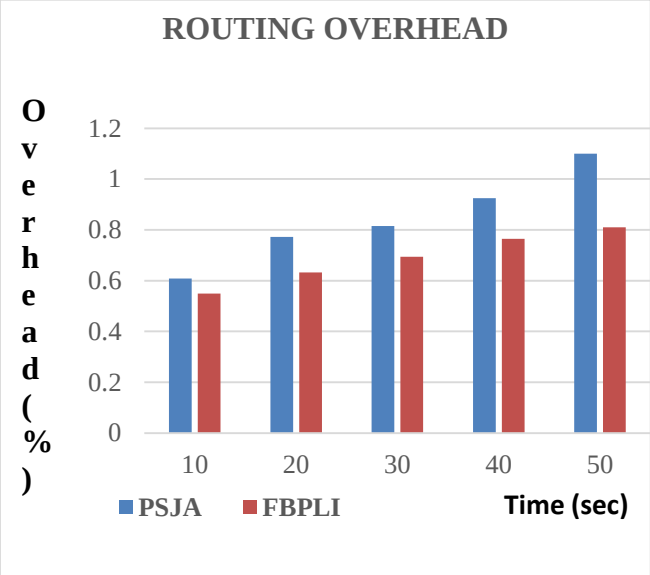


Fig9: Routing overhead

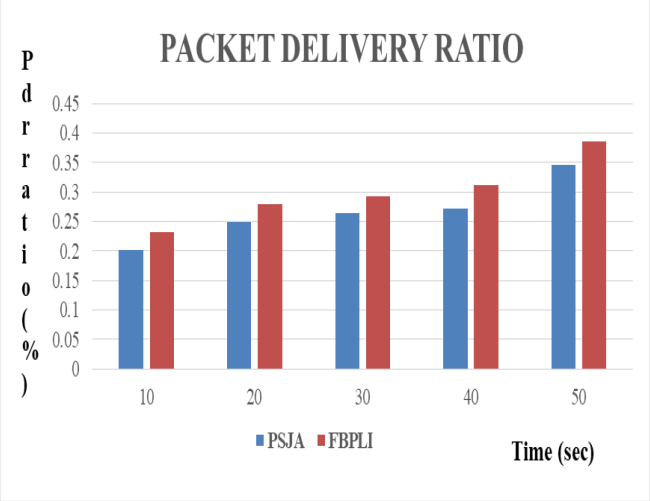


Fig10: Packet delivery ratio

In Fig 7, graph shows and represents end2end delay and it shows a simulation time versus delay. The performance of Firewall based packet level identifier algorithm improves delay time it means decrease the delay between communication nodes compare to preventive selective Jamming algorithm. Fig 8 shows and represents packet loss ratio and it shows a simulation time versus loss ratio. The performance of Firewall based packet level identifier algorithm improves loss ratio it means reduce the loss ratio compare to preventive selective Jamming algorithm. Fig 9 shows and represents routing overhead and it shows a simulation time versus overhead. The performance of Firewall based packet level identifier algorithm improves the routing overhead it means decrease the overhead compare to preventive selective Jamming algorithm. Fig 10 shows and represents packet delivery ratio and it shows a simulation time versus delivery ratio. The performance of Firewall based packet level identifier algorithm improves the delivery ratio it means save the packet transmission compare to preventive selective Jamming algorithm.

V. CONCLUSION

The selective attack of jamming has been prevented with the EPC (Evolved Packet Core) scheme. This scheme is efficient in energy consumption and network lifetime. EPC scheme was developed as the novel security system solution against the selective jamming. The deep packet installation has been installed to identify the packets that are to be transferred. The utilization of two methods, the firewall with the deep packet inspection benefits in the way that failure is one of the component that will not leave the unprotected network. The generated traffic by the host has got directed to EPC from where it has passed through the firewall in the combination with deep packet inspection. According to the initiated set of rule, a specific threshold that is a numerical value of 40 has been assigned as a threshold limit. It means the number of requests which are made by one host which is connected to the network and requesting for the services that shall not exceed from 60 times per minute. The predominant element is to remove the effect of DDoS attack from the network to increase the efficiency of networkworking. An algorithm which proposed will keep the track of packets that have flooded in the transmission. The proposed method will support better authentication and lessen the traffic analysis of high level that has been provided to the network. The results of simulation show and represent the authentication which is efficient. It has provided security for routing level in the network.

VI. REFERENCES

[1]. Harzallah A., G. Jordà, C. Dubois, G. Sannino, A. Carillo, L.Li, T. Arsouze, L. Cavichia, J. Beuvier, N. Akhtar (2015) Long term evolution of heat budget in the Mediterranean Sea from MedCORDEX forced and coupled simulations. Submitted to Climate Dynamics.

[2]. Fu S, Wu J, Wen H, Cai Y, Wu B (2018) Software defined wire line-wireless cross-networks: framework, challenges, and prospects. IEEE Commun Mag 56(8):145–151.

[3]. D. Fang, Y. Qian, and R. Q. Hu, "Security requirements and standards for 4g and 5g wireless systems," GetMobile: Mobile Computing and Communications, vol. 21, no. 1, pp. 15–20, March 2018.
[4]. Schneider P, Mannweiler C, Kerboeuf S (2018) Providing strong 5G mobile network slice isolation for highly sensitive third-party services. In: IEEE Wireless Communications and Networking Conference, pp 1–6.
[5]. R. Bin Tareaf, P. Berger, P. Hennig, C. Meinel, "Malicious Behaviour Identification in Online Social Networks", *book IFIP International Conference on Distributed Applications and Interoperable Systems*, pp. 18-25, 2018.
[6]. Osanaiye, O.; Alfa, A.S.; Hancke, G.P. A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks. Sensors 2018, 18, 1691.
[7]. Elramly, Salwa, et al. "SMSHM: Secure mesh mode protocol to enhance security of 4G networks." IT Convergence and Security (ICITCS), 2013 International Conference on. IEEE, 2013.
[8]. Tiloca, Marco, et al. "SAD-SJ: A self-adaptive decentralized solution against Selective Jamming attack in Wireless Sensor Networks." Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on. IEEE, 2013.
[9]. Sanzziri, Ameva, et al. "SESAME: Smartphone enabled secure access to multiple entities." Computing, Networking and Communications (ICNC), 2013 International Conference on. IEEE, 2013.
[10]. Han, Chan-Kyu, and Hyoung-Kee Choi. "Security analysis of handover key management in 4G LTE/SAE networks." Mobile Computing, IEEE Transactions on 13.2 (2014): 457-468.
[11]. Alezabi, Kamal Ali, et al. "An efficient authentication and key agreement protocol for 4G (LTE) networks." Region 10 Symposium, 2014 IEEE. IEEE, 2014.