Detecting and Preventing the Intrusion in LTE Network by using Flow Based Technique

[1.] Srinivasan. L,
Assistent Professor,
Deportment of Computer Science & Engineering,
Sree Sakthi Engineering College,

[2.] Jothikumar. V,
Student ,
Deportment of Computer Science & Engineering,
Sree Sakthi Engineering College,

[3.] Kowsalya. R,
Student ,
Deportment of Computer Science & Engineering,
Sree Sakthi Engineering College,

[4.] Riyappan. R
Student ,
Deportment of Computer Science & Engineering,
Sree Sakthi Engineering College

***Abstract*— In the LTE (Long Term Evaluation) network user are increased day-by-day. As a result there is heavy traffic and also security has been decreased. Intruder performs the malicious activities in the network. Intruder increase the network traffic and sends the intruder packet in the network. The traffic detection function will found the packet using the random packet inspection scheme. The packet will be identified and removed from the network by scanning the header of the packet in the Flow-based technique. Using IP BLOKING algorithm, the IP address of the intruder packet is blocked for some time period. This increases network security, latency, efficiency and decreases network traffic. The inspection cost is low.**

Keywords*— *Intruder, Malicious, Random Packet Inspection, Flow Based Inspection, Latency, Efficiency

INTRODUCTION

Now a day the LTE users are increased in the world. The LTE networks need an internet connection was launched in 7 countries. The VOLTE has no network connections to make a call. The mobile data traffic is globally increased. The mobile data traffic will grow at a CAGR (Compound Annual Growth Rate) of 47 percent from 2016 to 2021, reaching 42.0 EB per month by 2021.Due to this data traffic the highly challenge for providing a high speed network, and highly risked in the network security, network attacks and the malicious activities perform in the network by intruder. Mainly two types of attacks present in the network. That are active attacks and passive attacks. In the passive attacks only the intruder will listen the communication done in the network. No changes made in the network packets. It's to lose the privacy of the network user.

But in the active attacks listen the communication packets and also make some changes in the network packets. This to affect both privacy and security. The security ensuring in the LTE network is highly challenged one. The network need more effective algorithm for security. The intruder will send a malicious packet in the network. The intruder packet is not easily identified in the high speed network.

In high speed networks need more effective IDS (Intrusion Detection System). The TDF (Traffic Detection Function) is used to detect the malicious packets in the LTE network.

RELATED WORK

The LTE users will grow on the current days. In the LTE users need the fast and secured communication. Both network speed and security will affected by the intruder. Ensuring the security of LTE network becomes difficult, because the large volume of data passing through the network. So the effective intrusion detection system (IDS) is need to provide the security for the network.[5] in the network attacks are mainly split in two types, one is passive attacks and another is active attacks. In the passive attack, the attacker only lesion the network read the all communication and won't change anything on the message. In the active attacks, the intruder will perform the any malicious activities on the message.

[1] The ids is to scan the packet header and payload. That should be achieved by the deep packet inspection mechanism to scan the packets. There is more time need to inspect the packet all packets pass through the network. To avoid that scan the packet randomly. That random packet picking is done by the random packet picking algorithm. In the deep packet inspection, inspect the packets header and payload.

Methodology

1. *Random Packet Inspection Scheme* :

In High speed network, packet transfer rate is high. If each and every packets inspected for identifying the intruder packets, it causes network traffic, affects the inspection rate and may occur time delay. The inspection of packet is very difficult in the high speed LTE network. To avoid this problem, we randomly pick packets from the network and inspect for malicious packets. The process of random packet picking, Fig.1 t_0 represent the 1st time period of packet picking from the network, and t_1, t_2 are the next packet picking times for the inspection. The time between the t_0 and t_1 packet picking is the time for the $t0^{th}$ packet inspection time. Based on the t0th packet inspection time is the next packet picking time interval.

The time between the i^{th} and $(i\text{-}1)^{th}$ packet is the i^{th} packet inspection time. Let $t_p = t_i - t_{(i-1)}$ be the time interval between the i^{th} and $(i-1)^{th}$ packet inspections. This to calculate the inspection cost detection latency and detection rate.

Fig.2 the flow of the random packet inspection takes place. First the packet is pick from the network is done in a certain interval time, that the packet's inspection tag is in yes condition or not. If that tag contain the yes ("Inspection=Y") the inspection is initiated. Then execute the packet inspection

procedure. First change the inspection tag into No (Inspection=N), then generate the next inspection interval time $t_{p,i}$, and calculate the inspection time required for the corresponding packet inspection time. And start the timer with inspection time. When the timer is expired the next packet will get form the network and ready for the next packet inspection. After the execution, the Flow-based scanning is to scan the packet header deeply. If the packet not contains. any malicious or different activity in our packet header that packet will pass through the network usually. Else the packet contain any malicious activities in the packet header that packet will drop by the mechanism.

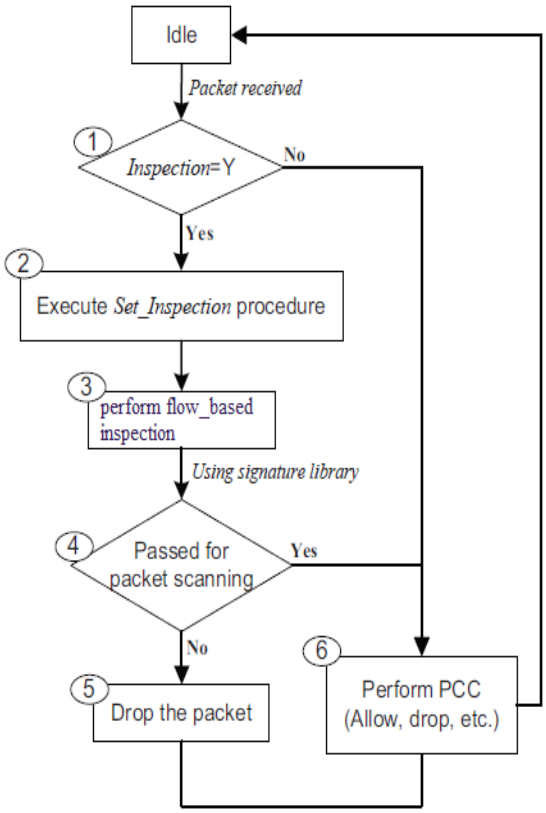

Fig. 2 : Flow of Random packet inspection

This the random packet inspection method to achieve the effective inspection, low detection latency, and the detection rate. The inspection time will low because of picking the packet from the network by using the random packet picking technique.

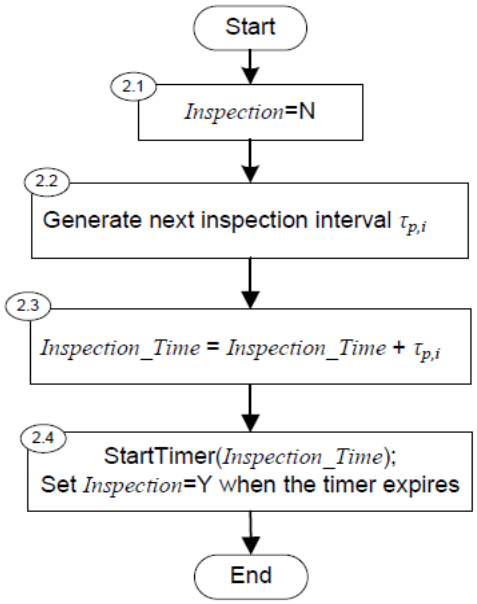

Fig.3: set_inspection procedure

2. *Flow Based Inspection*

The Flow Based inspection is widely used for the Network Intrusion Detection System (NIDS). This is likely to the network monitoring, traffic analysis and security applications. [2] This method is characterized by the flow of the data in a network. In this Flow Based inspection the payload of the packet won't provide for the inspection, and it provide the information about the network flow and the packet information. It is also called as the Network Behavior Analysis method.

In the Flow Based Inspection method to inspect the packet based on the information's like a, number of packets, amount of bytes transferred in a flow, and start and end time of a flow. The Exporter have these information's are in a form of records, called "Flow Records" for the NIDS. These analysis system is used to detect the intrusion in the network. Fig.4 The Flow_Based intrusion detection system contains the two main components that are, exporter and the collector. The flow exporter extract the packet header from the each packet comes for the intrusion. The exporter is create the flow records from observing the traffic flow of the network and send records to the network collector. The collector store records comes from the exporter of the network, for the further analysis of the network. So this Flow_Based Inspection method to decreases the inspection latency.

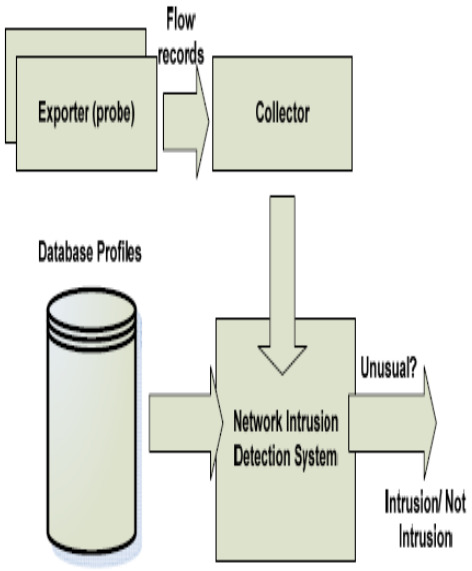

Fig.4: Flow_Based Components

3. Ip Blocking Algorithm

In this session describe about IP BLOCKING ALGORTHM. The Ip Blocking Algorithm is used to block the intruder Ip address for some time period. Dropping packet form the Flow_Bsed scanning the Ip of the dropped packed is fetched from the packet. Using the Ip of the packet block that particular Ip address. These to that corresponding Ip address is not able to communicate via that network in some time period. If the tome period is expire the blocked ip will released by the algorithm. Because the intruder perform the activities in the normal users ip also. So after block release the user will access the network ueually. These to block the intruder's participation in our high speed network and decreases the traffic of produced by the intruder.

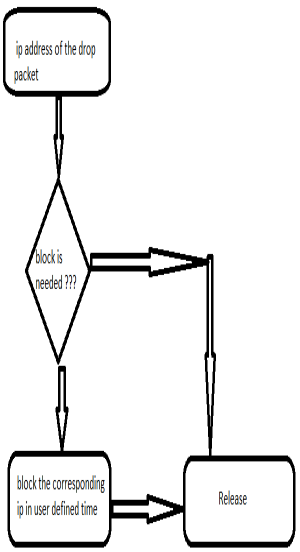

Fig.4 Ip blocking algorithm

The time period of the particular Ip in the blocked state, that time interval is user defined. In the fig.4 the ip blocking algorithm is explained well. If the time period gets high, the attacks will come down, because the intruder will no able to send the packets in the corresponding network. so this to reduce the network traffic and increase the security. This method to avoid the DOS attack in the mobile network.

CONCLUSION

In the mobile network the security threads are increased and also the volume of data traffic is grows in the LTE network. That the high speed network causes a many security problems. Mainly the intruder will affect the network, and send the intruder packets in the network. That the intruder packets to affect the network speed and also the reliability of the network. So that the intruder packet will find from the network and remove from it. For that, the Random Packet random Picking Algorithm is used to pick the packet form the network randomly and the Flow Based Method to inspect the packet.

This to avoid the intruder packet flows in the network, and also reduce the traffic of the network. The Ip Blocking algorithm is used to block the corresponding Ip address comes from the dropping packet that the Ip address in the blocked state in some time period. That's to increase the network efficiency, detection rate, detection latency, and inspection rate of the packet. This to achieve the low cost inspection.

I. REFERENCES

[1] Intrusion detection in LTE network by using random packet inspection scheme. Year: Sep2017. Authors: Sok-Ian Sou,

[2] An overview of flow-based and packet-based intrusion Detection performance in high speed networks. Authors: Hashem Alaidaros1, Massudi Mahmuddin1, Ali Al Mazari2

[3] Securing web server against ddos attacks. Authors: Navaneethakrishnan , Rajasekar

[4] Monitoring the Misbehaving Nodes in Manet Using Audit-Based Misbehavior Detection (Amd) Method. Authors: Alagumuthukrishnan1, Dr.K.Geetha2, J.Blessy Achsah3 and A.Ancy Mary4.

[5] Network security and types of attacks. Authors: Mohan, pawar, anuratha