SAFEGUARDING SMART GRID AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS

S.Venkatvijay[1], H.Kumaran[2], V.Sivaganesh[3]

[1,2,3] *Department of Information Technology, Pondicherry Engineering College, Pondicherry, (India)*

ABSTRACT

Smart grid (SG), is a two way connected power system which allows easy monitoring and maintenance of power system. It is also considered as the next generation power grid. This power grid is prone to a large number of threats in the form of data alteration attack, identity spoofing attack, distributed denial of service (DDOS) attack, etc. The availability of smart grid is frequently affected by security breaches like the DDOS attack. This attack may be in the form of an interruption access or use of authenticated information which could lead to disruption of delivery. In our proposed work, our aim is to detect and isolate DDOS attack on Smart Grid by scanning incoming packets to the network and detecting the attack by using Marking Scheme, Time to Live(TTL) value and Media Access Control value(MAC) value. Marking based Detection and Filtering (MDADF) mechanism is also employed in order to mark each incoming packet using multiple routers.

Keywords: Distributed Denial of Service attacks (DDOS), Marking scheme, Media Access Control value (MAC) value, Smart grid, Time to Live (TTL) value

I. INTRODUCTION

Smart grid is one of the latest methods of connected power systems for supplying power to consumers in an efficient manner with high data security using digital technology [1]. The addition of communication and intelligence to the existing power system is indicated by the use of the word ‘smart’ in Smart Gird. The advantages of smart grid over the conventional system are as follows reduced maintenance and working cost, security control, efficient transfer of electricity, etc.

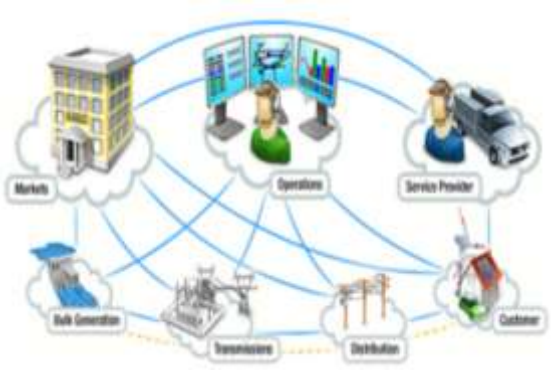


Fig.1 Smart grid model

Figure 1 depicts the various components of smart grid. It consists of seven primary components as follows: Customer, Transmission, Service Provider, Distribution, Bulk generator, Operations and Markets. Bulk generation involves extracting the power from natural resources in huge quantity. The electricity is transferred to customers by means of distribution. A two way communication channel exists between customers and the sub stations.

Although Smart Grids are highly beneficial to customers yet it possesses a few drawbacks. Security breaches have become very common over the internet which includes Distributed Denial of Service Attack which aims at bringing down the availability of services to the customers by overloading the traffic [5]. Cyber security is an important issue to be considered while working with Smart Grid. It acts as a threat to a wide variety of resources ranging from banks to news websites.

In DDOS attack, the attacker tends to control single or multiple vulnerable systems in order to create a spoofed IP address. Spoofed IP address is used to hide one's identity by changing the source IP address.

Table I
Comparison of Results of Related Work

Authors	MAC Value Analysis	TTL Value Analysis	Marking Scheme
Yao chen	×	×	✓
Ryo	×	✓	×
Cheng Jin	×	✓	×
Qiang	×	×	✓
Yaar	×	×	✓
Proposed work	✓	✓	✓

II. EXISTING WORK

The main aim of Smart Grid systems is to improve the performance of the conventional system by providing high availability, enhanced security, easy maintenance and reduced cost. Some of the threats to the system are DDOS attack, identity spoofing, eavesdropping, intrusion attack, etc[3]. Cyber Security has provided a set of guidelines so as to reduce such kind of attacks to the system and ensure availability, integrity and confidentiality to customers. In our work, we concentrate on availability being affected by an attack namely, Distributed Denial of Service attack.

When the resource or service is made unavailable to a legitimate user it is termed as Denial of Service attack [6]. In Distributed Denial of Service attack, multiple systems are used to attack a single system causing denial of service attack. In DDOS attack, it is extremely difficult to differentiate between a normal and a vulnerable resource that target and exploits a single machine, when spread over a vast network. It is difficult to handle such attacks since blocking single IP locations from where the threat originates, is a tedious task.

DDOS is considered to be one of the greatest threats since it is capable of creating a huge volume of unwanted traffic [5]. It primarily focuses on preventing access to a particular resource, for example, a website. In order to arrive at a solution for DDOS attacks, there is a necessity to study the impact of such attacks on Smart Grid systems. In order to analyse its affects, we have considered five papers and obtained the following details as shown in Table 1.1, on the basis of TTL value analysis and marking scheme.

As it can be observed from Table 1, MAC value analysis hasn't been ventured in any of the work. In our proposed work, we aim to prevent the DDOS attack by considering all the three parameters namely, MAC value analysis, TTL value analysis and marking scheme.

III. PROPOSED WORK

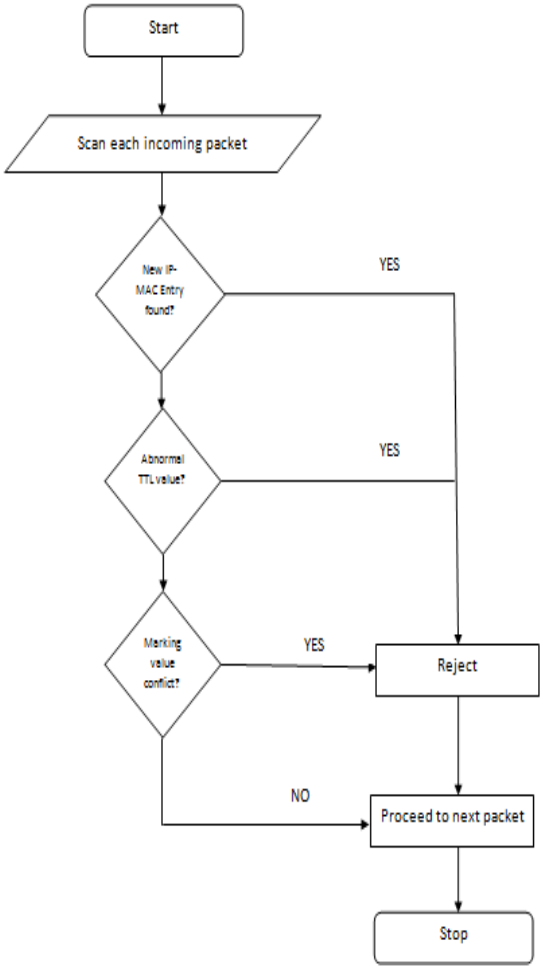


Fig.2 Flow chart of proposed work

In our work, three methods are used to prevent and mitigate DDOS attack. The three techniques are Marking Scheme, TTL Value analysis and MAC value analysis [7]. If the packets travelling in the network are found to be positive in any of the three techniques, then the packet will not be allowed to enter into the grid and will be rejected. MAC value analysis can be done only if the spoofed packet is created within the network. The packets

that originate within the network have no change in their TTL values[9]. Hence, this analysis can be done only on packets that originate external to the current network.

Marking Scheme is carried out by the coordination of multiple routers which try to eliminate the DDOS attack. The flowchart clearly depicts the working of our system.

3.1 Marking Scheme

The traditional method to eliminate Distributed Denial of Service attack is by dropping all the packets that originates from the source address of the attacker. Because of the advent of spoofed IP address, detecting the source address of the attacker has become a tedious task. Even though the source address is changed yet the path the spoofed packets travel is determined by routers and the network topology [8].

Marking scheme is capable of differentiating packets from an attacker and legitimate user by making use of markings that is associated with each packet. The user can check the marking value and thus discard a spoofed packet. Hence the victim is capable of safeguarding himself from DDOS attack.

In our proposed system for marking scheme, we have established duplex link connection between 'N' routers and 'M' clients. DropTail queue treats every packet in the same manner and it is setup on the routers. Once the queue limit has exceeded, no new packets will be accepted until the buffer space is having sufficient space to accept new incoming packets. By making use of Variable Bit Rate (VBR) flow, UDP and FTP traffic is generated.

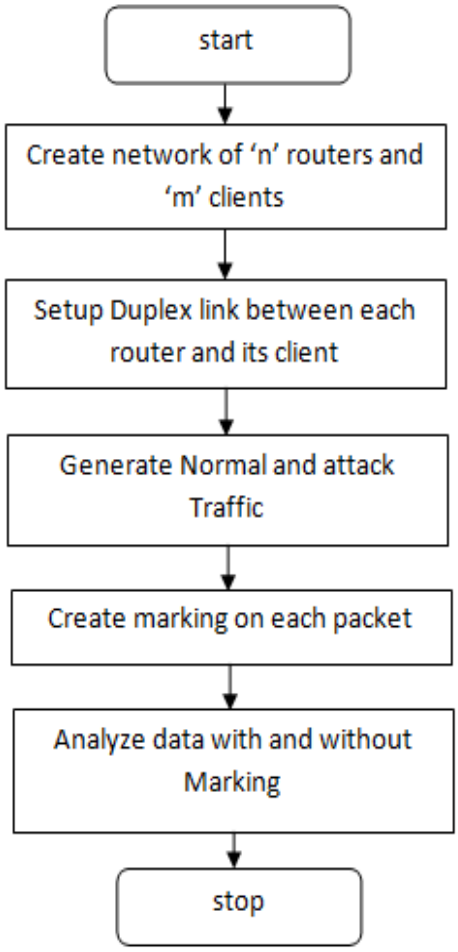


Fig.3 Marking Scheme Flowchart adapted from [1]

3.2 TTL Value Analysis

Generally every IP in the network goes through approximately thirty routers before reaching the receiving end. Those packets which possess strange TTL values are considered as malicious packets and they are eliminated and prevented from routing to the destination.

Such packets are generated by the attacker by making use of special kinds of tools. The TTL value is set by the computer based on protocol used to send the packets and the operating system. The TTL values can be used to compute the number of routers between source and destination.

3.3 MAC Value Analysis

Those IP addresses associated to the same MAC is considered to be originating from the same interface, so if any malicious activity is discovered, the packets can be discarded by maintaining a table that consists of source addresses along with IP address and MAC address.

In case of single attacker, detecting the source address is an easy task with the help of fake MAC address. MAC value analysis is restricted to within the network only as it wouldn't be able to detect any kind of variation from packets originating outside the network.

IV. EXPERIMENTATION

Network Simulator NS2 is used to simulate the network where multiple routers are employed to produce a marking for each packet.

4.1 TTL in Marking Scheme

IP spoofed packets tend to travel in a path which completely differs from the original path that is allocated for a particular IP address. Therefore, the DDOS attack can be identified by making use of performance metrics that is capable of detecting deviation over the change in original path.

Fig.4 indicates that the average computation time of the proposed system is much better than the existing system. Computation time is the time taken for the process to run. Thus in the proposed system time is saved as it is found to be better than the existing system

4.2 TTL in MAC Security

For MAC value analysis, random flooding of packets is generated using NS2 simulator. The network is monitored and IP and MAC addresses are identified with time stamp. Malicious packets are identified when the help of their MAC addresses and are discarded.

From fig. 5, we infer that the average computation time of the proposed system is much better than the existing system. At the earlier stage too it was found to be faster and even at this stage it's found to take lesser time compared to the existing system.

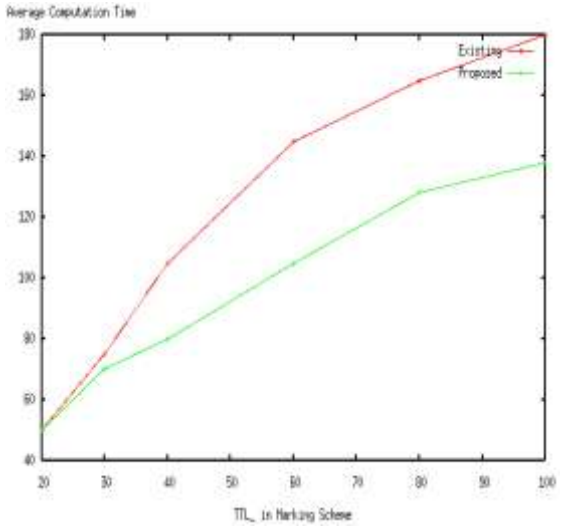


Fig. 4 Comparison of TTL in marking scheme between existing and proposed work

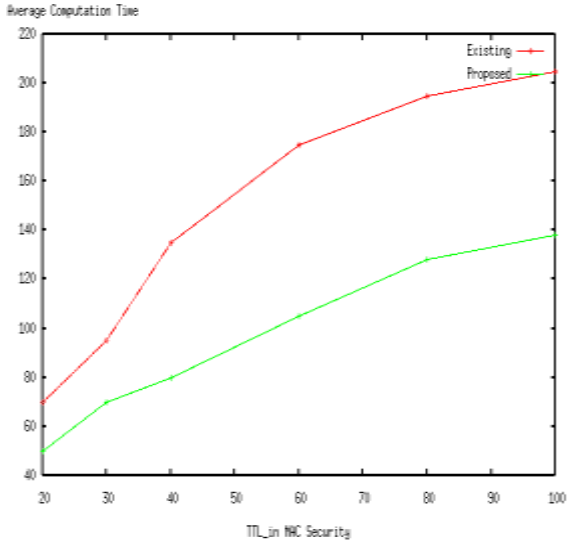


Fig. 5 Comparison of TTL in MAC Security between existing and proposed work

V. RESULTS

The following results have been observed from the packet delivery ratio and Time versus Throughput analysis in order to avoid DDOS attacks.

5.1 Packet Delivery Ratio verses Node Density

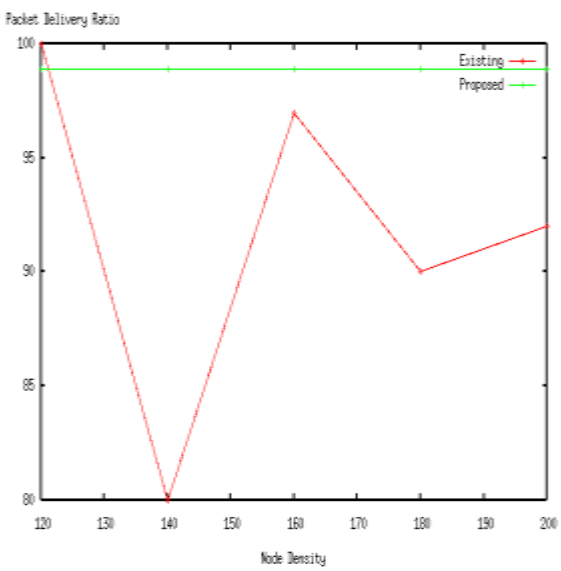
From fig. 6, we infer that the packet delivery ratio of the proposed system is much better than of the existing system as the stability in proposed system is more.

Packet delivery ratio = (Packets sent /Packets recd) *100 (1)

The system is more effective as DDOS attacks are prevented and there is no packet loss thus making the system more stable n thus the packet delivery ratio is better than that of existing system.

5.2 Time versus Throughput

From fig. 7, Throughput is the rate of successful packet delivery. Time vs throughput graph tells about the time taken for the packets to be transmitted. Since the computation time in the proposed system is less and the system being more stable as there is no loss of packets it is found to better than the existing system



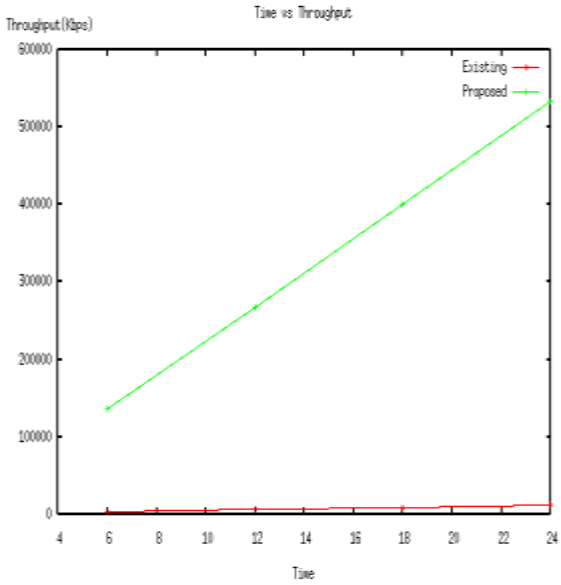


Fig. 6 Packet delivery ratio versus Node density **Fig. 7 Time versus Throughput**

VI. CONCLUSION

In the first method, TTL values can be changed hence malicious packets can go undetected. Therefore, the second scheme namely, Marking scheme, is used which marks the packet arriving through a particular path. This scheme is useful only when all the routers in a network work in a coordinated manner. In the third method, the fake packets cannot go unidentified since the MAC address for 2 different users cannot be same. Thus the proposed work helps in the prevention of DDOS attack.

REFERENCES

[1] Ye Yan, Yi Qian, Hamid Sharif, and David Tipper. A survey on cyber security for smart grid communications. Communications Surveys & Tutorials, IEEE, 14(4):998-1010, 2012.

[2] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. Smart grid the new and improved power grid: a survey. Communications Surveys & Tutorials, IEEE, 14(4):944-980, 2012.

[3] Wenye Wang and Zhuo Lu. Cyber security in the smart grid: Survey and challenges. volume 57, pages 1344{1371. Elsevier, 2013.

[4] Jingcheng Gao, Yang Xiao, Jing Liu, Wei Liang, and CL Chen. A survey of communication/networking in smart grids. Future Generation Computer Systems, 28(2):391-404, 2012.

[5] Guidelines for smart grid cyber security NISTIR 7628 Cyber Security Working Group. The smart grid interoperability panel, 2010.

[6] Monika Sachdeva, Gurvinder Singh, Krishan Kumar, and Kuldip Singh. Measuring impact of DDOS attacks on web services. 2010.

[7] Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El-Saddik, and Amiya Nayak. Detecting and preventing IP spoofed Distributed DOS attacks. IJ Network Security, 7(1):69-80, 2008.

Proceedings Papers:

[8] Ryo Yamada and Shegeki Goto. Using abnormal TTL values to detect malicious IP packets. Proceedings of the Asia-Pacific Advanced Network, 34:27-34, 2013.