An Optimistic Approach of DDOS Attack Detection and Mitigation

[1]Sakshi Kakkar, [2]Dinesh Kumar

[1]Dept. of CSE, Gaini Zail Singh Punjab Technical University Campus, Bathinda, Punjab, India
[2]Gaini Zail Singh Punjab Technical University Campus, Bathinda, Punjab, India

Abstract

DDoS attacks is a grave network security problem that comprised a serious threat to reliability of services deployed on server.Flooding attack with Spoofed and Non-spoofed packets is a very harmful type of the DDoS attack.In this paper we consider the flooding attack with IP Spoofing packets.In IP Spoofing ,the attacker forged its IP address and flood the packets continuously towards the victim Server.Various number of techniques have been proposed by various researchers in the literature.In this study,we discuss how the DDos attack launched in real time environment using GNS3 emulator tool and its detection using packet analyser tool .Two techniques have been implemented on cisco router to mitigate the attack (i)Filtering based on source IP address intergrated with ports in Access control list(ii)Filtering Based on source IP address integrated with flags in access control lists .with the thereotical analysis and simulation the results show that second approach dropped spoofed packets with respect to previous approach.In this paper the parameters considered are traffic rate, No. of rules in the list,No. of bytes transfered in particular time.

Keywords

Dos,DDos,IPSpoofing,ACL,GNS3 0.8.6

I. Introduction

As internet communication has become more dependent nowadays for the modern life, any disruption like DDoS attacks can cause various harms to the social and business networks.DoS attack is defined as the attack launched from one single point host to a specific host.DDoS attack is defined as an army of compromised computers, which launch the attack to A specific host or more than one host or network,such that victim host can no further capable of providing its services or resources .The main purpose of the attacker is to disable popular sites,banks etc for the financial gain, economic gain or revenge etc.DDoS can also be described as the attacker source use many spoofed addresses to a particular host,such that this attack can be launched from one single point source to single point destination. These kind of attacks causes data destruction, unauthorized access, internal data and program modification [11]

II. IP Spoofing Based DDoS Attacks

It is one of the most dreadful type of the DDoS attacks. It is defined as the attack in which attacker sends the forged source IP address, with the intention of hiding the identity of the sender. It makes difficult to differentiate between the legitimate packets and illegitimate packets.This type of attack causes the congestion in the network by sending continuously packets which are also known as flooding.

In this paper TCP SYN Flooding attack [11] attacks are considered

III. Literature Review

[1] A new approach Mutual Egress Filtering (MEF) is presented in this paper. MEF is a antispoofing method which is used to provide continuous deployment incentives.In this technique an access control list is applied to the egress router which is used to drop all the spoofed packets whose source address does not belong to the autonomous system.

Pack, G.[2] has discussed about the defense technique against the flooding attacks.Access control list is implemented on routers The main motive of this paper is to pass legitimate traffic on the base of its IP address and port numbers and to stop the congestion on the network using ACL.

Maheshwari, R. has Studied Comparative study of proposed Distributed probabilistic Hop count filtering with the previous approaches[3] probabilistic hop count filtering and hop count filtering to detect IP spoofing attacks .The limitation of this technique is that it is used only for the detection of attack traffic but not to mitigate it.

Bahaa Qasim [4] has suggested a scheme to mitigate the DDoS attacks named as IP tables .IP tables are a command-line tool which is used as firewall scripts in linux to deny the attack traffic. The field in IP, TCP, UDP, ICMP header packets was filtered. Wireshark which is a packet analyser tool is used to capture the packets and based on that detection of traffic, mitigation approach has applied.

Soldo, F in this paper has studied about the blocking of the malicious traffic using the source based filtering approach using access control lists [5]

Thakar, U [6] has presented the optimistic approach to improve the performance of firewall by reducing the packet matching time . The clustering index method is used in which ACL rules are arranged. This paper concludes that the performance is beter if there are more number of rules.

This paper considers one of the most difficult type of the DDoS attack named as IP spoofing [12] which is very difficult to defend .In this paper a technique is proposed which uses router specific features information to detect the IP spoofing This paper deals with the one of most famous attack based on TCP/IP protocol such that server don’t respond to other users.

IV. Methodology

In this paper the procedure follow a number of steps:

1. The co-simulation environment setup was created by using the emulation tool GNS3 and VMware workstation.
2. In joint simulation testbed by using Vmware workstation prepared DDoS flooding attack
3. Detection of the flooding attacks by capturing all the packets with the use of wireshark which is alredy installed in GNS3
4. A new approach is considered for the mitigation of the DDoS flooding attacks.

In this section of the paper, the emulation tool being used and its working principle have been described.

A. Topology Creation

1. Emulation Tool Used

The work is performed using the emulation tool GNS3

0.8.6(graphical network simulator). Gns3 is multiperform,open source graphical network environment graphic network emulator which allows the emulation of network topologies using the Cisco IOS router platforrm

2. Emulation Setup

A network consists of 1 server,1 admin,3 legitimate users and 1 attacker ,three 3700 series routers, 1 hub,1 switch and connect them with ethernet cable. Configuration of Cisco routing with ospf (open shortest path first routing).Assigning an IP address to server,hosts and routers.

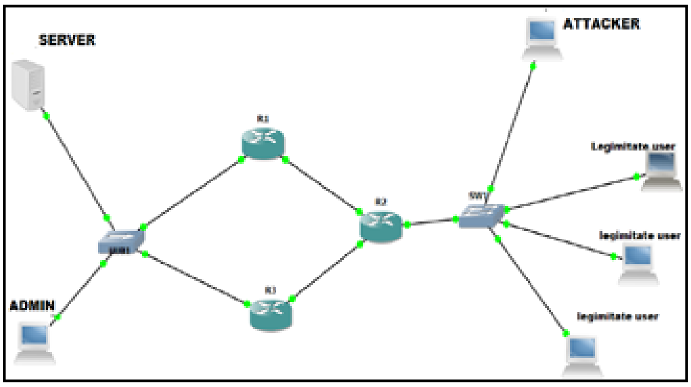

Fig. 1:

3. DDoS IP Spoofing Based Flooding Attacks

The packets for flooding attack was generated by running the command on bactrack terminal,the operating system which is installed on VMware workstation.

The command is

#Hping3 –S Victim Address –a Attacker address –p 22 –flood

Description

-S flag indicate SYN flag on its TCP mode

-p 22 sends the packets to port 22 on victim machine.

--flood describes as fast as possible the flag sends the packet

Victim Address here is server address

With this command approach we can easily launch the attack on the victim server.we can also launch UDP flooding attacks and ICMP flooding attack by using this command but we must have to change the port number.

4. Detection of the Attack

The next step of this work is to detect the attacks which were launched on the victim server. For this we use wireshark to capture all the flooding packets. Wireshark is a packet sniffer tool which is used between the user and the network.some files are gathered for a certain period of time after capturing the packets..Based on all above information we detect the spoofed IP address flooding and then apply a mitigation technique to block DDoS flooding attacks.

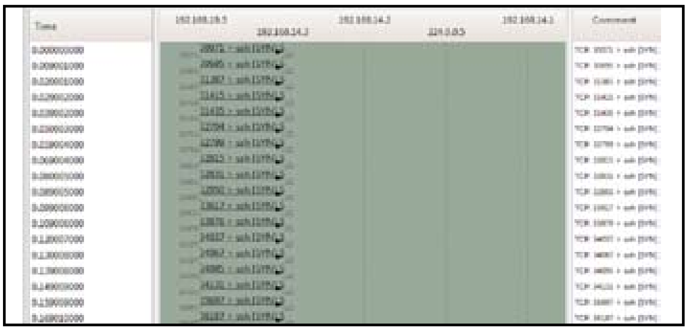

Fig. 2:

In our work wireshark shows that the attacker machine is not responding to the server's SYN,ACK flags set,but the attacker send continuously SYN flag to congest the entire network. When thousands of requests comes from one attacker ,the server will not able to respond to any other legimitate user requests of services or resources.Mitigation using access list.

5. Mitigation Technique

In this paper ,we propose a technique ACL on the cisco routers for the filtering of IP spoofed packets.AcL[11] block all the illegitimate spoofed flooding attack packets based on its predefined rules.

Access control lists is defined a list of rules or statements..ACL list is prepared by the network administrator.network decides the access rights for different users and network resources.ACL rules are being processed from top to bottom in a sequential order

In this paper we perform the two techniques of mitigation of IP spoofed packets

In the previous Research Access control lists are used to filter or based on certain fields defined in the statement. These statements define the pattern of the IP packet fields like source IP address,destination IP address, source port number,destination port number and protocol that would be found in an IP packet. When an IP packet arrives through the interface list of ACL on the router will be scanned from top to bottom rule in the ACL. If the rule matches with the patteren of incoming packet ,then router permit to allow its service otherwise it denies. At first the previous work filtering based on its source IP Address and its port number is applied on the oubound interface of the cisco router in GNS3. Here we use the TCP protocol.

Access Control List

```
10 permit tcp 192.168.13.0 0.0.0.255any eq 80
20 permit tcp 192.168.13.0 0.0.0.255 any eq 110
30 permit tcp 192.168.13.0 0.0.0.255 any eq 22
40 permit tcp 192.168.13.0 0.0.0.255 any eq 23
 50 permit tcp 192.168.13.0 0.0.0.255 any eq 53
60 permit tcp 192.168.13.0 0.0.0.255 any eq 21
10 permit tcp 192.168.15.0 0.0.0.255 any eq 80
20 permit tcp 192.168.15.0 0.0.0.255 any eq 110
30 permit tcp 192.168.15.0 0.0.0.255 any eq 22
40 permit tcp 192.168.15.0 0.0.0.255 any eq 23
50 permit tcp 192.168.15.0 0.0.0.255 any eq 53
60 permit tcp 192.168.15.0 0.0.0.255 any eq 21
10 permit tcp 192.168.16.0 0.0.0.255 any eq 80
20 permit tcp 192.168.16.0 0.0.0.255 any eq 110
30 permit tcp 192.168.16.0 0.0.0.255 any eq 22
40 permit tcp 192.168.16.0 0.0.0.255 any eq 23
50 permit tcp 192.168.16.0 0.0.0.255 any eq 53
60 permit tcp 192.168.16.0 0.0.0.255 any eq 21
10 permit tcp 192.168.17.0 0.0.0.255 any eq 80
20 permit tcp 192.168.17.0 0.0.0.255 any eq 110
30 permit tcp 192.168.17.0 0.0.0.255 any eq 22
40 permit tcp 192.168.17.0 0.0.0.255 any eq 23
50 permit tcp 192.168.17.0 0.0.0.255 any eq 53
60 permit tcp 192.168.17.0 0.0.0.255 any eq 21
```

In this list filtering is based on its ip address and its port number. this technique uses 24 rules in access list to block the traffic based on source IP address and port number.

In our proposed work we use the technique filtering of the spoofed IP address and flags. filtering based on the flag can only done with named,extended ACLS.When the packet comes through the interface list of ACL it will be scanned in sequential order ,if it matches the rule given by the network adminstrator based on its flag and souce IP address then router permit that packet to pass through it other wise it denies the packet by declaring it as a spoofed packet.

Based on our work various rules are applied on the outbound interface of the cicco router in GNS3

ACCESS CONTROL LIST

```
10 permit tcp 192.168.13.0 0.0.0.255 any syn
20 permit tcp 192.168.13.0 0.0.0.255 any ack
30 permit tcp 192.168.13.0 0.0.0.255 any rst
10 permit tcp 192.168.15.0 0.0.0.255 any syn
20 permit tcp 192.168.15.0 0.0.0.255 any ack
30 permit tcp 192.168.15.0 0.0.0.255 any rst
10 permit tcp 192.168.16.0 0.0.0.255 any syn
20 permit tcp 192.168.16.0 0.0.0.255 any ack
30 permit tcp 192.168.16.0 0.0.0.255 any rst
10 permit tcp 192.168.17.0 0.0.0.255 any syn
20 permit tcp 192.168.17.0 0.0.0.255 any ack
30 permit tcp 192.168.17.0 0.0.0.255 any rst
```

In this method filtering based on TCP flags and source IP address is performed in GNS3 and blocked all the spoofed IP address attack.This technique uses 12 rules in Access control List to block the traffic.

V. Experimental Results

To evaluate th performance of the proposed technique ,we use the simulation environment GNS3 integrated with vmware workstation and show the results in graphs .

A. Traffic Rate

It is defined as number of packets transfer per second from source to destination.this graph shows the comparison between normal traffic and attack traffic

1. Detection of Normal Packets and Flooding Attack Packets

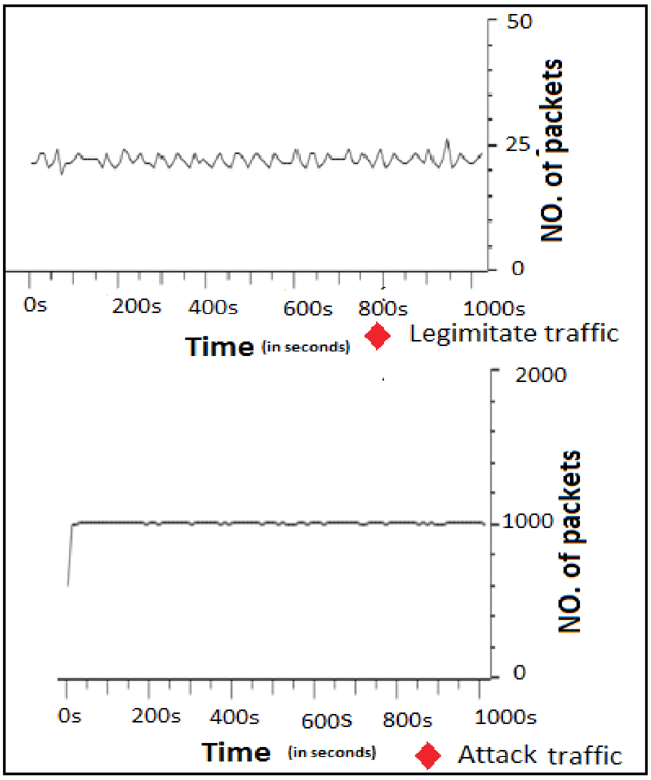

Fig. 3: Graph Between Normal Traffic and Flooding Traffic

2. Comparison of mitigation of previous approach filtering based on IP address with port numbers of the flooding malicious traffic using ACL in routers and proposed work filtering based on IP address with Flags of the flooding malicious traffic using ACL in routers.This graph shows that spoofed IP packets per second dropped is higher using proposed technique than the previous technique.

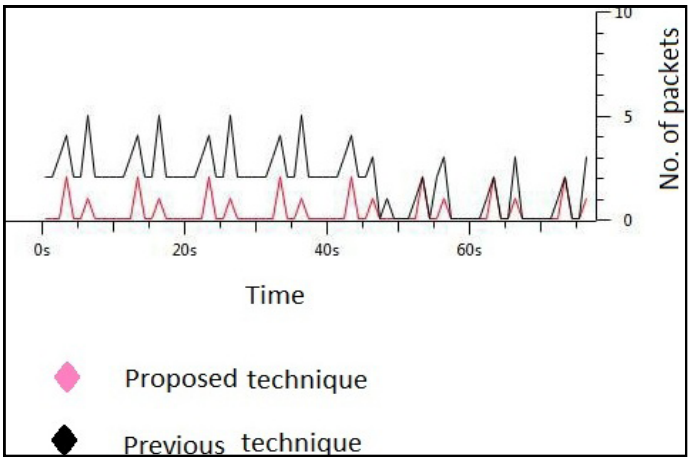

Fig. 4: Graph Between Proposed and Previous Technique

3. Data Sent: Data sent is defined as number of bytes transfer per second.This graph shows the difference of bit rate between the lnormal traffic and attack traffic.

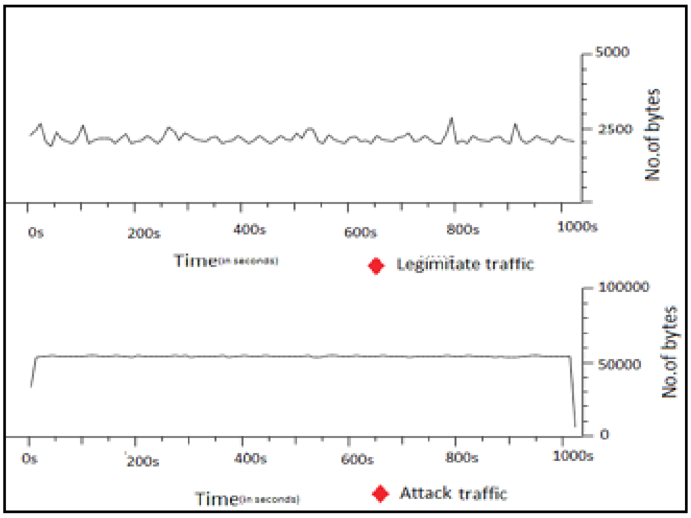

Fig. 5: Graph of Normal and Flooding Traffic

2. No. of bytes dropped after using proposed ACL technique of malicious flooding is at higher than previous technique

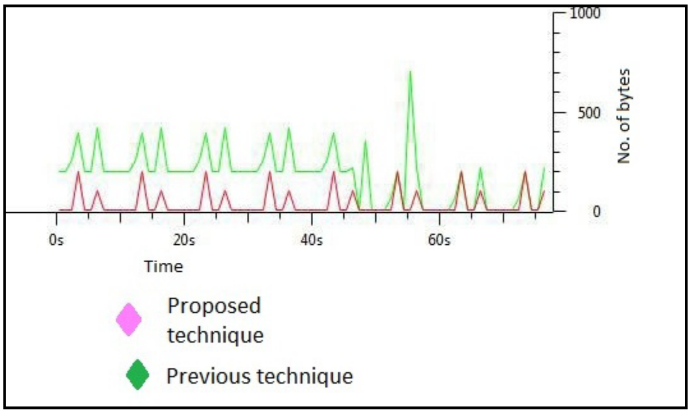

Fig. 6:

VI. Conclusion

This paper introduces scheme to generate the Access control list on cisco routers based on source address and flags used for blocking of the illegimitate packets.The real time environment is used to detect the attacks. Pros of this technique are easy to configure on router,no implementation cost(as both routers and routers are already their in network).no. of rules are less than Previous techniques , time required to scanned the rules is less and filter packet time is also less.The proposed technique give better result of filtering the packets than previous techniques. Moreover this technique works indepedently at the victim side.

In Future the study may be carried out in following directions:

1. The propose technique can be applied as stateful filtering of the spoofed IP address packets.
2. The technique will be used to reduce the set of rules in ACL

Refrences

[1] Bingyang Liu,"Toward Incentivizing Anti-Spoofing Deployment”, Information forensics and secirity, IEEE, Vol. 3, Issue-9, pp. 435-450, 2014.

[2] Pack, G.,"On Filtering of DDoS Attacks Based on Source Address Prefixes”, Securecomm and Workshops , IEEE, 2006 , pp. 1-12.

[3] Maheshwari, R.,“Defending network system against IP spoofing based distributed DoS attacks using DPHCF-RTT packet filtering technique “Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 206-209, Feb 2014.

[4] Bahaa Qasim,"MITIGATING DoS/DDoS ATTACKS USING IPTABLES”, International Journal of Engineering & Technology IJET-IJENS, Vol. 12, No. 03, June 2012

[5] Soldo, F.,"Optimal Source-Based Filtering of Malicious Traffic”, Networking, IEEE/ACM Transactions on Vol. 20, Issue 2, April 2012, pp. 381 – 395.

[6] Thakar, U.,“An Approach to Improve Performance of a Packet-Filtering Firewall”, Wireless and Optical Communications Networks (WOCN), Ninth International Conference, pp.1-5, 2012.

[7] [Online] Available: http://www.gns3.net/news/gns3-0-8-6-released/

[8] Monowar H. Bhuyan, H. J. Kashyap, D. K.Bhattacharyya, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions". The Computer Journal first published online March 28, 2013.

[9] Saman Taghavi Zargar, Joshi, David Tipper,"A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION (2013)

[10] Ahmad Sanmorino, Setiadi Yazid,"DDoS Attack detection method and mitigation using pattern of the flow", 2013 International Conference of Information and Communication Technology (ICoICT).

[11] Sakshi Kakkar, Dinesh kumar,"A survey on Distributed Denial of services”, International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014.

[12] Kavisankar, L,"A mitigation model for TCP SYN flooding with IP spoofing”, Recent Trends in Information Technology (ICRTIT), 2011 International Conference.

Sakshi Kakkar received her B.Tech. degree in CSE(Computer science) Stream from MALOUT Institute of Management & Information Technology(MIMIT) Punjab in 2012. He is currently Pursuing M.Tech Degree in CSE from Gaini Zail Singh Punjab Technical University Campus, Bathinda. Her area of research include DDoS attacks and the various techniques that are applied to detect and mitigate attacks. Besides this she has also applied the combination of his Academic and Practical Knowledge in developing different Industry oriented Software Project.

Er. Dinesh Kumar is currently working as Assistant Professor in Deptt.of Computer Science and Engineering. His Areas of research Include Computer Networking. He has Attented various International and National Conferences.