Real Time Filtering Malicious Packets Modeling against Distributed Denial of Service Attacks

N. Sundareswaran
Department of Computer Applications
MepcoSchlenk Engineering College
Sivakasi, Tamilnadu,India

A. D. C.Navin Dhinnesh
Department of Computer Applications
MepcoSchlenk Engineering College
Sivakasi,Tamilnadu,India

***Abstract*--Developing a comprehensive defense mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention. In this paper we explore the scope of DDoS flooding attack problem and attempt to combat it. This ensures that the victim network is not seriously congested in time of attacks so that legitimate users still are able to access the host.The malicious packets are dropped at the source such that bandwidth consumption is quiet reasonable. It becomes more complicated to recognize the original attacker because of the use of spoofed IP address under the control of attacker. A legitimate source may require stringent performance requirements raised by new applications such as digitalized voice and video.Those new applications often require guaranteed throughput and bounded transmission delay.we highlight need for a distributed solution and some of the metrics that can be used in evaluation and conclude comprehensive distributed collaborative filtering mechanism against DDoS flooding attacks.**

Keywords:DDoS; Spoofed IP; malicious packets

I. INTRODUCTION

Denial of Service (DoS) attacks which are intended attempts to stop legitimate users from accessing a specific network resource. Today, DDoS attacks are often launched by a network of remotely controlled, well organized and widely scattered Zombies or Botnet computers that are simultaneously and continuously sending a large amount of traffic or service requests to the target system. Zombies that are part of a Botnet are usually prepared through the use of worms, Trojan horses or backdoors. Figure 1 shows the architecture of DDoS attack.

Examples – In Feb 2000 Yahoo! Experienced one of the first major DDoS flooding attacks that kept the company's service off the internet for about 2 hours. In Oct 2002, the Domain Name System (DNS) service to internet users around the world shut down for an hour because of DDoS flooding attack. In Feb

2004, the SCO group website inaccessible to legitimate users [1]. This attack was launchedby using systems that had previously been infected by the mydoom virus. Several online banking sites have slowed or grounded to a halt by series of powerful DDoS flooding attacks. Currently, there are three main DDoS attacks are co

mmon [1].

- Vulnerability attack – Send some malformed packets to the victim to confuse a protocol or an application running on it.
- Network/ Transport level flooding attack – Disrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity.
- Application level flooding attack – Disrupt a legitimate user's services by exhausting the server's resources (e.g. CPU, memory, disk/database)

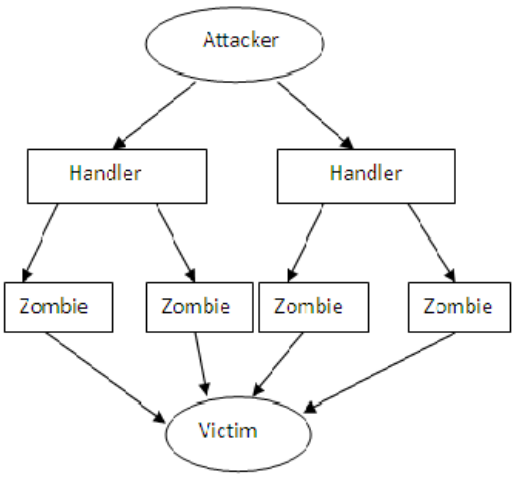

Fig.1. Architecture of DDoS attack

II.NETWORK/TRANSPORT-LEVEL DDoS FLOODING ATTACKS

These attacks have been mostly launched using TCP, UDP,ICMP, and DNS protocol packets.

A. Attack Identification

Normally the rate of traffic in one direction is proportional to that in the opposite direction during normal operation on the internet. Hence a significant difference between the rates

of traffic going to and coming from a host or subnet can indicate that the network prefix is either the source or the destination of an attack [3].

This scheme aims to detect DDoS flooding attack traffic by monitoring both inbound and outbound traffic of a source network and comparing the network traffic information with predefined normal flow models. It attempts to stop attack traffic originating from a network at the border of the source network [2]. Attack flows are identified and filtered if they mismatch the normal flow model. Continuously analyzing Management Information Base**(MIB)** can help victims to identify when a DDoS attack is occurring, During a DDoSattack, it is possible to map network packets statistical abnormalities related to different parameters.

B. Attack Filtering Methods

The ultimate goal of any DDoS filtering mechanism is to detect them as soon as possible and stop them as near as possible to their sources. The process of **tracing back** the spoofed IP addresses that was used in the attack is called IP trace back. Usually routers in the path to the victim can mark packets. So that the victim can identify the path of attack traffic and distinguish it from legitimate traffic after detection.

Type	Code	Checksum
Identifier		Sequence Number
ICMP Payload (4 Bytes)		

Fig.2 ICMP Packet Structure

C. Literature Survey:

Window based flow control mechanisms have been widely used for traffic control in packet switched networks. Figure 2 shows the packet structure. For instance, a window based flow control system used returned acknowledgements to regulate data transmissions, since acknowledgements may incur a rather large and variable delay that are not compatible with the most real time applications [2].Alternative methods such as rate based data traffic control algorithms monitor the transmission rate of statistical data flows and enforce network resource usage to prevent interference [1] – [2].

These solutions detect and drop attack packets at or near the destination network where the attack packets have already traversed the network and consumed considerable bandwidth. The aggregate traffic at the destination router may consist of hundreds of thousands of flows. It is hard for the router to distinguish between legitimate and malicious packets. So damage is unavoidable [3].

III. PROPOSED PACKET FILTERING METHOD

This ensures that the victim network is not seriously congested in time of attacks so that legitimate users still are able to access the host. The attackers may generate attack packets with randomized source IP address which makes it difficult to find the sources of the traffic [4]. The goal of these attacks is to consume link bandwidth, preventing legitimate users from accessing the services. Figure 3 shows the process flow structure.

A. Process Flow

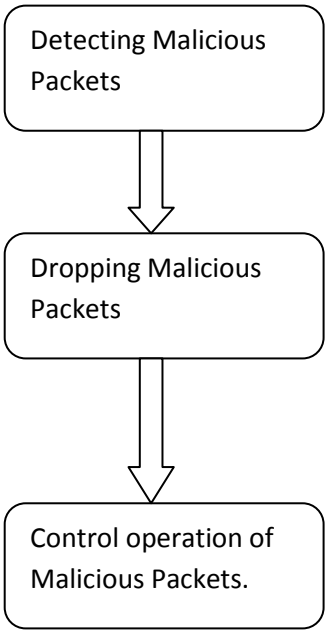

Fig.3. Process flow structure

B. Trace back technique

It is probabilistically mark packets at intermediate routers along the path and sent to the destination. The destination reconstructs the entire path from these marked packets.

C. Detection and Control

It detects DDoS attack and assumes that the normal packet rate going in one direction is proportional to the rate of other direction. When it detects disproportional then it is suspicious and are dropped when necessary. It also sends pushback messages to the upstream routers asking them to control the rate of malicious traffic [5].

High packet arrival time associated with long response time indicates a possible DDoS attack.High rate flows are the responsible for the congestion. If the average response time is between the minimum and maximum threshold, the source router is not sure whether any client is conducting an attack. It then sends an ICMP request message to the victim asking its output queue usage rate. Upon receiving a message from the source router, the victim calculates its output queue occupancy rate and sends the value back to the source router. a code will be set in the CODE field of the ICMP response message to represent whether the queue is in an increasing or a decreasing state [3]. The source router justifies whether increasing or decreasing flow by computing probability.

D.Flow rate threshold

Choosing a proper value for the identification is one of the most important issues. Smaller values T can result in monitoring more flows than necessary. Larger valueds of T

can result in failure to identify attack traffic. T varies for different network conditions [1]. It also depends on composition of the normal traffic.

E. Analysis of TCP Packet Traffic

Here source hosts reduce their sending rate when they detect congestion. Their arrival rate in a large time window is low. In this case, threshold value can be small (T_{sf})In case of UDP traffic [2], we should consider a large value for the threshold

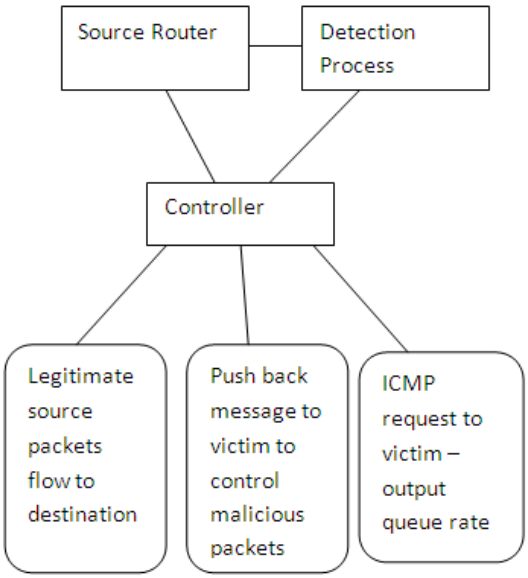

Fig 4. General modeling structure of controller

because packet rate in the window can be larger valuein the network (T_{lf}).Figure 4 shows the general modeling structure of controller

IV.DROPPING SCHEME

It measures the arrival rate of the input flows. A flow here is defined by source IP, destination IPand the protocol. By measuring packets response time, source router know whether there is congestion at the destination network. Dynamic routing protocol load balance incoming traffic into different routers in order to relieve congestion [5].

After identifying the high rate flows, we start to trace back the source IP, this source is scrutinized to separate the attack packets and legitimate packets. The secret bit field is used to detect the malicious packets [4]. This secret bit field is filled up by random key generator and this task will be managed by public key cryptography. The malicious packets are dropped at the source such that bandwidth consumption is quiet reasonable.

A. Destination Validation

All the nodes, the terminal routers as well the intermediate routers along the path participate in validation. All the routers along a given path, store information about the traffic they observe and exchange information periodically [3]. It does not implement traffic validation at each node because it suffers from very high packet overhead. Figure 5 illustrates the source router filtering.

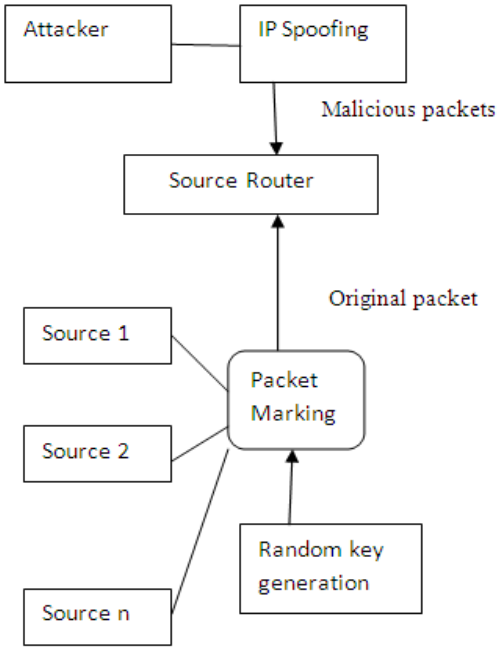

Fig.5.Source Router filtering

B. Source router

It requires the router to check for the authenticity of the packet and then forwards the packets to its downstream neighbor along the path [1]. The authenticity can be verified by calculating a hash value over the packet and matching it with that generated by the outstream router.

V EXPERIMENTAL RESULTS:

We have implemented and experimented in the Qualnet software simulation. In our experiments, we used the simple topology. The links between routers were configured with 10Mbps bandwidth, 20ms delay and 75000 byte capacity FIFO queue. Each pair of routers shares secret keys, the validation time interval was set to 1 second and the upper bound on the time to forward traffic information wasset to

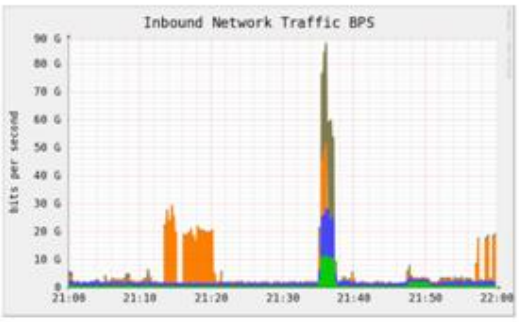

Fig. 6. Real time packet traffic

300ms. At the end of each second, the routers exchanged traffic information corresponding to the last validation interval. Each run in an experiment consisted of an execution of 80 seconds. During the first 30 seconds we generated no traffic to allow the routing fabric to initialize.

Then we generated 45 seconds of traffic. Figure 6 shows the Real time packet traffic. We then experimented with the

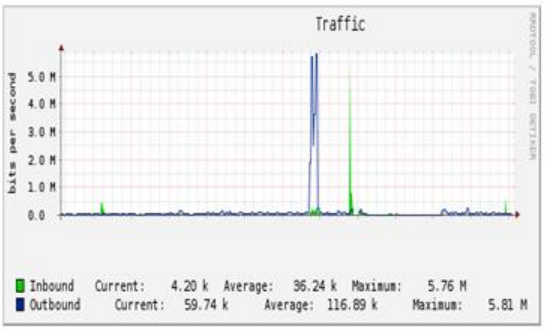

Fig 7.Performance of modeling.

ability of detecting attacks. For the first attack, the source router was instructed to drop all malicious packets for 20 seconds. As shown in the figure 7during the attack our design detected the malicious packets successfully. In the second phase the source router was instructed to drop malicious packets in the selected flows when the queue was at least 90 percent full. Our design was able to detect and drop malicious packets.

VI. CONCLUSION

In this paper, we proposed the filtering malicious packets against DDoS attacks at the source level. This ensures that the legitimate users packets are able to reach the destination. The main DDoS attack is Network/ Transport level flooding attack. This will disrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity.

Our design aims to detect DDoS flooding attack traffic by monitoring both inbound and outbound traffic of a source. The process of Trace back the spoofed IP address identified the path of attack traffic, after detection the source is scrutinized to separate attack packets and legitimate packets. Those malicious packets are dropped at the source and only original packets are allowed to send. This ensures the guaranteed throughput and bounded transmission delay. In future this design can be extended to address vulnerability DDoS attack and application level DDoS flooding attack.

REFERENCES

[1] T.Peng, C. Leckie and K.Ramamohanarao, survey of network based defence mechanisms countering the DDoS attack problems, ACM comp.surv.39,1,Article 3, Apr.2007

[2] J. Mirkovie and P.Reiher, A taxonomy of DDoS defense mechanisms, ACM SIGCOMM Computer Communication review vol.34,no.2,pp.39-53 April 2004

[3] S.Rajan, R.Swaminathan, M.Uysal and E.Knightly, DDoSResilent scheduling to conter application layer attacks under imperfect detection, IEEE INFOCOM'06

[4] R.K.C.Chang, Defending against flooding based distributed denial of service attacks. A tutorial, computer IEEE Commn.Magazine, vol 40 p 42-51, 2002

[5] S. Lin, y.Xiao, k.G.haboosi,H.Deng, and J.Zhang, Botnet: Classification, attacks, detection, tracing and preventive measures, EURASIP. J Wireless communication and networking, vol 2009