EFFECT OF HALF-OPEN CONNECTION LIFETIME IN DEFENDING AGAINST DDOS ATTACK

[1]**S.Meenakshi**, [2]**Dr.S.K.Srivatsa**,
[1]Assistant Professor, Department of Information Technology, Sathyabama University,Chennai.,
[2]Senior Professor, St. Josephs' college of Engineering, Chennai
E-mail : [1]kaviraj_3@hotmail.com

Abstract

The explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. This has increased the need to protect the data and the resources from disclosure and to protect the entire network from network based attacks. There are many attacks intended to deprive legitimate users from accessing network resources and functions. Denial of service (DoS) attack is an attack on the availability of Internet services and resources. Flooding based distributed denial of service (DDOS) attack presents a very serious threat to the stability of the Internet. In spite of many intrusion detection mechanisms, many find it difficult to withstand against large scale attacks. We want to design a comprehensive mitigation mechanism against the DDoS attack. In this proposed system a comprehensive solution is given against the attack. In the proposed system the detection accuracy has been increased by varying the half-open connection lifetime. This work can be done by using consensus algorithms for exchanging the information between the detection systems. So the overall detection time would be reduced for global decision making.

Key words: DDOS attack, sequential test method, Consensus method.

I. INTRODUCTION

1.1About DDoS

A denial of service attack (dos) which purports to deny a victim providing normal services in the internet. A Distributed Denial of Service attack is a large-scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet.

In a DDoS attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting our computer and its network connection or the computers and network of the sites we are trying to use, an attacker may be able to prevent us from accessing email, websites, online accounts(banking , etc.,), or other services that rely on the affected computer.

The DDoS attack is launched by sending an extremely large volume of packets to a target machine through the simultaneous cooperation of a large number of hosts that are distributed throughout the Internet as shown in figure.1. The attack traffic consumes the bandwidth resources of the network or the computing resource at the target host, so that legitimate requests will be discarded. The impact of these attacks can vary from minor inconvenience to the users of a web site, to serious financial losses to companies that rely on their on-line availability to do business.

1.2.DDoS attack examples.

According to CIAC(Computer Incident Advisory Capability),the first DDoS attacks occurred in the summer of 1999. In February 2000, the first major DDoS attack was launched against Yahoo.com. This attack kept Yahoo off the Internet for about 2 hours and cost yahoo a significant loss in advertising revenue. Another DDoS attack was on October 20,2002 against the 13 root servers that provide Domain Name system (DNS) service to the Internet users. If all 13 root servers were to go down there would be disastrous problems accessing the world Wide Web. The attack lasted for an hour and caused 7 out 13 root servers to shut down. This shows the vulnerability of Internet to DDoS attack. More powerful DDoS attacks could disable the Internet services in minutes.

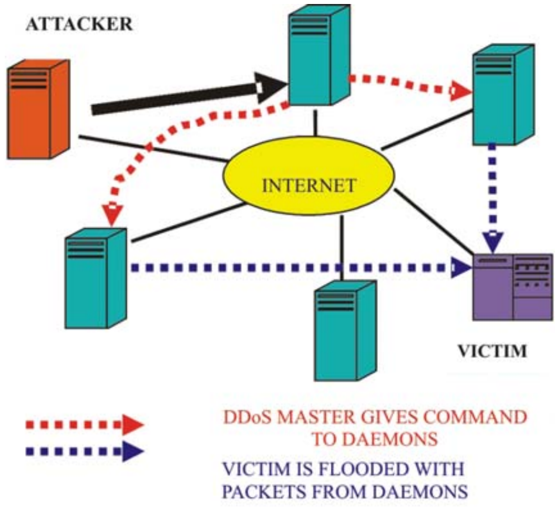

ATTACKER
INTERNET
VICTIM
DDoS MASTER GIVES COMMAND TO DAEMONS
VICTIM IS FLOODED WITH PACKETS FROM DAEMONS

Fig. 1. Distributed Denial of Service Attack

1.3.Flooding.

Flooding based distributed denial of service (DDOS) attack presents a very serious threat to the stability of the

Internet. SYN Flooding: Although this type of attack benefits from TCP protocol features (TCP three-way handshake), we consider it as a flood attack, since its impact is due to flood principles. Due to the importance of this DDOS attack type, we present a detailed explanation of how it works.

TCP connection establishment (3 way handshake).

When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages as shown in Figure.2.

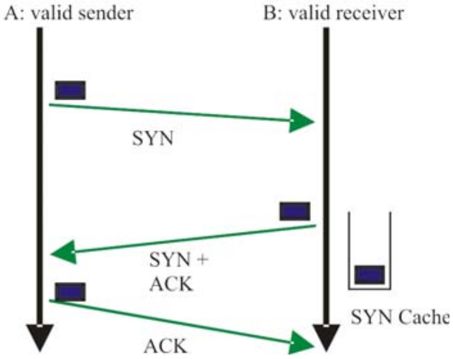


Fig. 2.TCP Three Way Handshake

i) The client system begins by sending a SYN message to the server.

ii) When the server receives the "SYN" message, it reserves some of its resources for the expected connection and sends a "SYN-ACK" message back to the client.

iii) The client then finishes establishing the connection by responding with an ACK message.

iv) After reception of the last message "ACK" from the server, the connection is successfully established and the two peers are able to start exchanging their data.

1.4.Problem Definition

The attacking system sends SYN messages with spoofed source IP address to the victim server system. These appear to be legitimate but in fact reference a client system that does not exist or that will not respond to the SYN-ACK messages as shown in Figure.3. This means that the final ACK message will never sent to the victim server system. The allocated resources of the half-open TCP connections will only be released after time-out. Since system resources are finite and limited, the system will soon be unable to accept any new incoming connections. The magnitude of the combined traffic is significant enough to exhaust system resources.

Flooding based Distributed Denial of service (DDoS) attack presents a very serious threat to the stability of the Internet. Due to the large scale nature of Internet, It is observed in the last few years that DDoS attack methods are becoming more sophisticated.

In spite of many intrusion detection mechanisms, many find it difficult to withstand against large scale attacks. We want to design a comprehensive mitigation mechanism against the DDoS attack.

This paper presents the design details of a distributed defense mechanism against DDoS attack. The DDoS attack cannot be addressed through isolated actions of defense nodes.

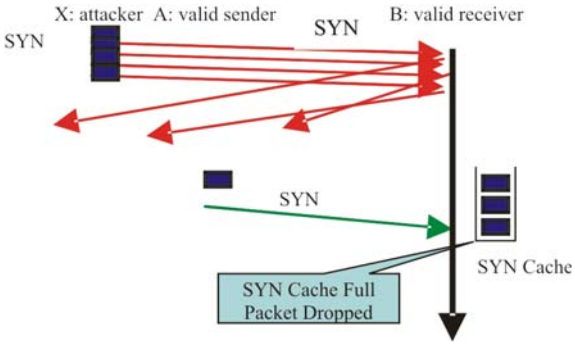


Fig. 3. TCP SYN Flooding

We used a comprehensive detection mechanism in the edge routers of each network. They act as local detection system for that network. Each local detection system communicates with other detection system using consensus method to take global decision against the DDoS attack. The true positive ratio considerably increased in this system.

The remainder of the paper is organized as follows: Section.2 explains about literature survey.Section.3 details our proposed work. Section.4 discusses about the implementation - Architecture, use of consensus method to detect DDoS detection. Section.5 discusses about the simulation results and performance using network Simulator NS 2.29.Section.6 states conclusion.

II. LITERATURE SURVEY

In traditional intrusion detection system (IDS) [data is collected in each node and analyzed by a central node. It fails to detect attack that involves more than one node.

Cheng Jin et al (2002) proposed a defense mechanism against spoofed traffic using hop count filtering. It needs a systematic procedure for setting parameters for hop count filtering.

Angelos Stavrou et al(2002) proposed a novel architecture called Secure overlay Services(SOS), which proactively prevents DoS attacks.In this method only authenticated traffic can enter the overlay network.This was proposed for emergency services. It is not suitable for general –purpose public servers.

In IP trace back system [Minho Sung et al (2003)] assistance from hosts present outside the network is needed. Many existing work are time consuming and need help from hosts present outside the network. So, Dynamic Anti DDOS systems which consume less time and need no help from outside the network is necessary.

In perimeter defense system using multicasting [Shigang Chen et al (2005)], even when there is only one flooding source, the rate-limit filters are temporarily placed on all edge routers, though most are removed after a short period of time since they do not cause any packet to be dropped. This method is not much efficient and time consuming.

Cooperative defense against DDoS attack [Guangsen Zhang et al(2006)] , gives a global infrastructure using Gossip algorithm. It gives a distributed proactive DDoS detection and defense mechanism. The information sharing overhead is a problem to be considered in this method. Only optimal gossip period is necessary to overcome this problem.

A Distributed Denial of Service (DDoS) attack is a large-scale, coordinated attack on the availability of services at a victim system or network resource. As the traffic is not aggregated enough in the intermediate network, current single deployment detection systems can not detect DDoS attacks with high accuracy. Traditional Intrusion Detection Systems (IDS) result in high false alarms when used to detect DDoS attacks. Due to the readily available tools, “Flooding” attack becomes most common DDoS attack. They intend to overflow and consume resources available to the victim. When the number of attackers is very large, the flows from each attacker can be very small to detect. So, detection based on instantaneous deviation will be useless. Because, the deviation will be very small in small flow. [Multtops, D-ward][Mirgovic 2002,John ,John Haggerty Et.al.,2005,Gil and poleto 2001]. Most of the DDoS detection system models are based on traffic flow rates. As many new applications are coming up and End user's behavior also varies, it is difficult to get a general efficient model based on traffic flow alone.

III. PROPOSED WORK

In this proposed system consensus method is implemented in a layered architecture to protect server from DDoS attack. It holds a key to the practical use of the security. The system automatically identifies the DDoS attack and then blocking the malicious traffic before it causes harm.

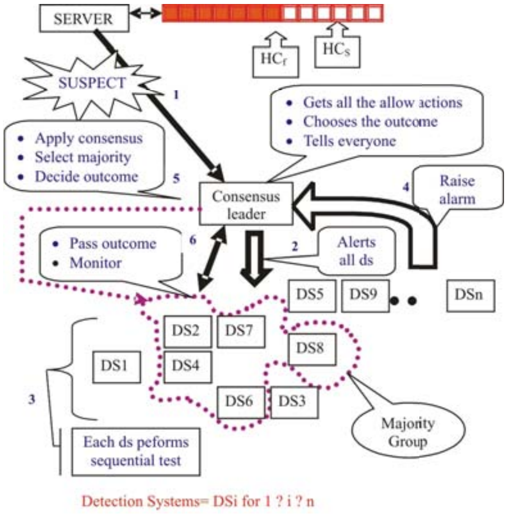
This two level architecture requires sophisticated method to exchange information between detection systems and to make global decision in the second level. So consensus method of information exchange and decision making is used in the proposed method. Moreover in this method large number of detection systems are involved. If all detection systems are involved in global decision making, then there will be longer delay in response to DDoS attack. So, a majority group(It consists of fewer detection systems than actual number of detection systems) is selected from the set of all detection systems. The detection systems which are members of this majority group only will participate in global decision making. The system is tested with various half-open connection lifetime. The detection accuracy of the system is measured under theses different scenarios.

IV. IMPLEMENTATION

The system architecture is shown in figure.4. The proposed method consists of two levels. A group of processes cooperating to provide a highly available service need to agree on which processes are currently functioning as members of the group.

Processes : Detection systems
Service : suspect and prevent DDoS

Currently functioning members : Only few detection systems are selected among Many to do the service .



Detection Systems= DSi for 1 ? i ? n

Fig. 8. System Architecture

CONSENSUS ALGORITHM

STEP1: The server (victim) keeps track of no of half open connections. There are two threshold values are kept.

Threshold value first -HC_f

Threshold value second -HC_s

STEP2: There is a leader detection system. It

- gets all the allow actions
- Chooses the outcome(filtering value)
- Tells everyone

STEP3: When the number of half open connections reaches HC_f , then it passes the suspection to the consensus leader. The leader alerts all detection systems.

STEP 4: In each detection system the sequential test is performed and based on that test, they raise alarm as follows.

Each detection system passes the following information to the leader.

- actual incoming rate
- actual exit rate
- actual acceptance rate
- Deviations

Percentage of unmatched request vs reply Destined to the victim - DV_{um} . Percentage of excess amount of packets

Coming through the detection system than the actual acceptance rate -DV_{ex}

STEP 5: The leader detection system receives the above information from many detection systems that suspect and raise alarm.

STEP 6: The leader now applies the consensus among these values and decides the outcome which is the filtering value to be applied in selected detection systems at the end.

The leader has the predefined threshold value TV_{dev} for the deviation DVum.

STEP 7: Now among the many detection systems involved, the majority group is selected by the following method.

For the detection systems DS1, DS2, DS3,…DSn , who raised alarm, the following check is done.

STEP 8: The DV_{um} of detection systems DS1, DS2, DS3, DSn are checked with this threshold value TV_{dev}. The particular detection system DSi is included in the majority group if and only if the following condition satisfies.

DV_{um} of detection system DSi > TV_{dev}

Let the no of DS wins this check be 'm

STEP 9: Now to check the majority the leader has to decide the outcome only if (n-m) is greater than or equal to n/2.

STEP 10: Deciding the outcome (filtering value)

The Outcome (filtering value) =Max DV_{um} among the majority group/2

STEP 11: This outcome is passed only to the members of majority group. The relative value is then calculated by the individual DS and filtering is done.

STEP 12: Periodically the leader checks the no of half open connections at the victim server. If it below HC_s, then the leader instructs the DS of majority group with the same filtering value. (Here the it checks whether the actual packet rate converges to acceptance rate or not).If the no of half open connections is greater than or equal to HC_s, then the filtering value is decided as Max DV_{um} among the majority group

STEP 13: The process stops when all of the DS in majority group DS incoming converges or the no of half open connections at victim converges below HC_f.

The above method is applied over the system for various values half-open connection lifetime.

V. SIMULATION RESULTS AND PERFORMANCE

The system has been implemented in NS-2 simulator. The following table 4. shows the parameters used for the simulation.

Table .4. Simulation values

Number of nodes	25
Number of Autonomous systems	4
Victim System	One
Daemons systems	Four
Number of LDS (Leader Detection Systems)	One
Number of DS (Detection Systems)	Five

For the simulation a network with four AS(Autonomous systems) have been used. For the attack traffic four systems were used. The attack traffic consists of simultaneous flow of packets. In each AS one or two detection systems are used. There is one Leader detection system (LDS) Which applies consensus method among all other local detection systems exist. There is one victim system . The system has been tested under various conditions to measure the performance. The system has been tested by varying the half open connection lifetime of victim server's queue(Half-open connection queue).

The table 5. Shows the different values used for the simulation.

Table 5. Various life time used for Simulation

Half Open Connection Life Time (Seconds)				
4	6	7	9	12

A. Detection Accuracy

Prevention and early detection of DDoS attack is very important. The objective is to minimize the expected delay of detecting DDoS attack after its occurrence. For this reason, good lower bound is to be fit on the expected time between false alarms before the DDoS attack. In the proposed system a local threshold is used to go to "suspected" state which triggers early detection of DDoS attack. The figure 6 shows the detection accuracy of the system .

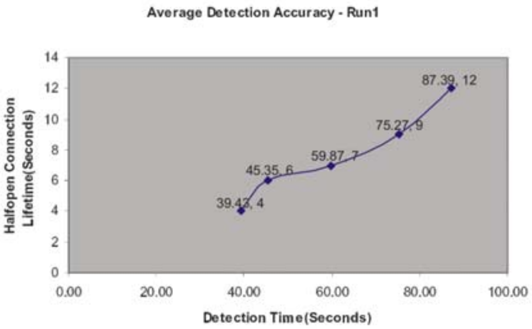


Fig. 6. Average Detection Accuracy

Based on the half-open connection lifetime, the detection time has been measured. As we used have used five different values, each time the detection time and the early alert were detected. The server is better protected with small values of life time for half-open connection. For the lifetime of 4 seconds , the system's detection time is 39.43 seconds. For the lifetime of 7 seconds , the system's detection time is 59.87 seconds. For the lifetime of 12 seconds , the system's detection time is 87.39 seconds. Thus the system is more sensitive and better protected against DDoS SYN attack , with lower values of halfopen connection lifetime.

VI. CONCLUSION

The primary contribution of the work is to design a global detection infrastructure by sharing attack information between the local detection systems. The detection systems is installed in more than one AS (Autonomous System) and also at intermediate place. Consensus method is used for message exchange between detection systems and to take global decision making. The performance of the system is examined under different scenarios by varying the half-open connection lifetime. The system is more sensitive in detecting the attack when the lifetime of half-open connection is low. Similarly early detection is achieved by having two threshold vales for the lifetime.

REFERENCES

[1]. Angelos Starvou, Debra L Cook, William G.Morein, Angelos D.Keromytis, Vishal Misra amd Dan Rubenstein, 2005, "WebSOS: An Overlay based System for Protecting Web servers from Denial of service attacks", Elseveir Science.

[2]. Cheng Jin,Haining Wang, Kang G.Shin, 2002,"Hop-Count Filtering: An Effective Defense Against Spoofed Traffic".

[3]. Gil. T.M., M. Poleto, 2001, MULTOPS: a data-structure for bandwidth attack detection, in: Proceedings of 10th Usenix Security Symposium, Washington, DC,, pp. 23-38.

[4]. Guangsen zhang , Manish Parashar, (2006), Department of Electrical and Computer Engineering,RUTGERS,The State University of New Jersey, Cooperative defence against DDoS attacks,Journal of research and Practice in Information Technology, Vol.38,No.1.

[5]. Jelena Mirkovic,Peter reiher, (2004)," A taxonomy of DDoS attack and DDoS defense mechanisms", ACM SIGCOMM Computer Communication Review, ACM SIGCOMM Computer Communication Review ,Volume 34 , Issue 2 (April 2004), Pages: 39 - 53 .

[6]. John Haggerty,member,IEEE, Qi Shi, Member,IEEE, and Madjid Merabti,Member, IEEE, October (2005), Early Detection and Prevention of Denial-Of-service Attacks: A Novel Mechanism With Propogated Traced-Back Attack Blocking, IEEE Journal On selected Areasin Communication, Vol 23, No.10.

[7]. Minho Sung and Jun Xu (2003), "IP Traceback-based Intelligent Packet filtering:ANovel Technique for Defending against Internet DDoS attacks", IEEE Transactions on parallel and Distributed Systems , vol.14.No.9.Septamber .

[8]. Mirkovic.J, G. Prier, and P. Reiher,(2002), "Attacking DDoS at the Source," presented at ICNP 2002.

[9]. Shigang Chen, Member,IEEE, and Qingguo Song, ,(2005), Perimeter–Based Defense against Bandwith DDoS Attacks, IEEE Transactions on Parallel and Distributed systems, Vol.16,No.6.

[10]. "consensus decision- making", http://en.wikipedia.org/wiki/Consensus_decision-making

S. Meenakshi, Assistant Professor, Department of Information Technology, Sathyabama University, has 15 years of teaching experience and has published nearly 15 papers in various journals and conferences. Her areas of interest are Computer Networks, Network Security .