A novel approach for the detection of SYN Flood Attack

SRI.Y.Madhavi Latha
Dept of Electronics and Computer engineering
KLUniversity
Vijayawada, India

Ms.G.Sindhuri
Dept of Electronics and Computer engineering
KLUniversity
Vijayawada, India

Mr.K.Sachin
Dept of Electronics and Computer engineering
KLUniversity
Vijayawada, India

Ms.K.Sravani
Dept of Electronics and Computer engineering
KLUniversity
Vijayawada, India

Abstract: Denial of service attack(DoS) is causing a serious and financial damage in recent years. They are performed easily by utilizing the weakness of the network protocol. There are many types of Dos attack namely IP spoofing SYN Flood. If should be notable that the firewall host hardly filters the SYN flood attacks, and the spoofed IP address keeps the position of the attacker from being traced.(edit the sentence).Therefore it is important for network administers to develop means to comprehend the latest trend of DoS attack. In this paper firstly we proposed the detection method of SYN flooding attack , secondly show the applicability of our method with prospective evaluation results and in the finally section mentioned the future scope of our method.

Keywords:Dos attack,SYN flood,intruder

1.INTRODUCTION:

The internet has become an inseparable part of our life which serves billions of users daily. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies .It also involves huge amounts of information sharing.In such situation any system connected to internet is subject to threat.

One such major threat is Dos attack(Denial Of Service). A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer or network resource unavailable to its intended users by exhausting the sever's resources[1] . Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person, or multiple people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Symptoms of denial-of-service attacks include: Unusually slow network performance (opening files or accessing web sites), Unavailability of a particular web site, Inability to access any web site, Dramatic increase in the number of spam emails received .Dos attack has number of forms of occurrence One such major Dos attack is

SYN flood attack. A SYN flood[2] occurs when a host sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet(Acknowledge), and waiting for a packet in response from the sender address(response to the ACK Packet). However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

Moreover, nowadays users whose computers have been used for attacks without their knowledge come under scrutiny even though they are not real attackers. For example, Botnet Traffic Filter developed by Cisco uses a blacklist to filter the connection from doubtful IP addresses or domains if they can be a member of a botnet [3]. Appearing a member of a botnet within administrative network has the possibility that even innocent traffic is filtered by such blacklists. Because of this, to detect the latest trend of attacks promptly is desirable for network administrators in order to stop any unintentional attackers appearing within their administrative network.The SYN flood attack is a major threat in real internet and is handled by tracing the backscatter information[4]

2.MECHANISM OF SYN FLOOD ATTACK:

Initially let us consider the tcp connection which is to be established between the clients.

TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. To begin a TCP connection, the client connects the server to set up a connection, which is called a three-way handshake. First, the client will send a SYN packet to the server, requesting a connection. Then the server will respond to the connection request using a SYN-ACK packet, and store the request information in the memory stack. The state of this connection then turns to be SYN-RECV. To prevent the system from depleting its memory, each operating system will limit the number of concurrent TCP connections in the SYN RECV state. After receiving the SYN-ACK packet, the client will confirm the request using an ACK packet. When the server receives the ACK packet, it checks the memory stack to see whether this packet is used to confirm an existing request. If it is, that TCP connection is moved from the SYN RECV state to the ESTABLISHED state. After this, the client and server have finished the three-way handshake and can start data transfer. Where as in SYN flood attack the illegal client or the intruder sends large amounts of information in order to keep the server busy and it do not send the ACK packet back to the server as a result of which the server holds a half-open connection and becomes unavailable to its genuine users.

3.OUR METHOD OF DETECTION FOR SYN FLOOD ATTACK:

In our method we identify the illegitimate client who is causing the attack and disconnect the client.

We implemented this procedure in a virtual environment .Initially we have a server and the number of clients can be varied depending on the requirement. We connect each client to the server using the port number. Information exchange is done between the server and clients. We also maintain the number of bytes transferred. We maintain a backend database-we create a database server and maintain the information. In this database we maintain two tables. In first table we store the connected and disconnected time. In the second table we have attributes like the number of files sent by a client, time for each client. Based on these we identify the intruder in a particular time interval the client which sends the same file number of times is detected as the intruder. When we try to connect a client which is beyond the capacity of server, the connection is rejected. i. e, denial of service occurs ,then the server checks for the intruder in the clients connected to it presently .If any intruder is identified ,it is displayed and is disconnected from the server.

As a result, the server's resources are not misused and are made available for its intended users.

TABLE 1:

CLIENT ID	CONNECTED	DISCONNECTED
Client 1	18:05	18:45
Client 2	19:10	19:30
Client 3	4:05	4:30
Client 4	10:15	-

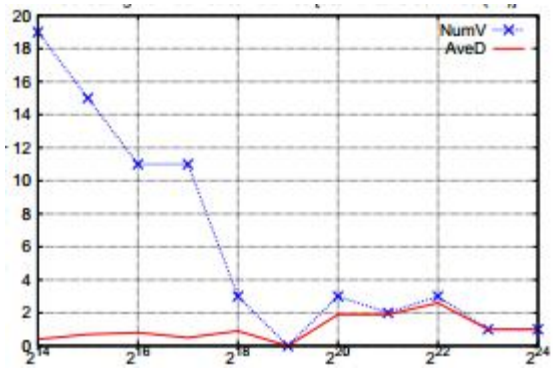
TABLE 2:

CLIENT ID	NO OF FILES SENT	FILE NAME	NO OF TIMES SENT	SENT_TIME
Client 1	4	S.txt	5	18:08
		A.txt	3	18:15
		Sin.java	4	18:32
		abc.java	9	18:40
Client 2	2	Sam.java	1	19:15
		We.java	1	19:20
Client 3	3	Jo.txt	1	4:10
		Har.java	1	4:16
		Jan.txt	1	4:22

50 nodes

Intruder	Detection Rates (success/trials)
Client 1	100%(10/10)
Client 2	100%(10/10)
Client 3	100%(10/10)
Client 4	90%(9/10)
Client 5	90%(9/10)

GRAPH:



X-axis: Number of times file sent

Y-axis:Number of Clients

4.ADVANTAGES:

-The intruder detected is disconnected automatically.

-The server need not wait to complete the three way handshake and need not restore the half-open connections.

-No ACK/SEQ changing work is to be done.

5.RESULT:

Our method successfully detects the intruder causing the SYN flood attack among all the clients. We discuss our results below.

6.CONCLUSION:

In a network where information sharing or file transfer plays a major role ,our method identifies the illegitimate client from the number of clients and disconnects it from the server.Thus it saves the time and resources of the server which is very economical in the real-time.

7.FUTURESCOPE:

We can implement this in real time and we can also store the ip address or the client-id of the intruder so that next time when that particular client sends a request to the server, it seeks the permission of the

admin so that the information sharing can be done in a more secured manner.

REFERENCES:

[1] CERT Coordinate Center, "Denial of Service Attacks,"http://www.cert.org/tech tips/denial of service.html.

[2] CERT. 1996. CERT Advisory CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks. Go online tohttp://www.cert.org/advisories/CA-1996-21.html.

[3] "Combating Botnets Using the Cisco ASA Botnet TrafficFilter," White Paper, Cisco, Jun. 2009.

[4] Evaluation of a Distributed Detecting Method for SYN Flood Attacks Using a RealInternet Trace Masaki Narita, Takashi Katoh, Bhed Bahadur Bista, Toyoo TakataIwate Prefectural University Graduate School of Software and Information Science

[5] R. R. Kompella, S. Singh, and G. Varghese, "On scalableattack detection in the network," IEEE/ACM Transactions onNetworking, vol. 15, no. 1, pp. 14–25, Feb. 2007.

[6] H. Wang, D. Zhang, and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 4, pp. 193–208, October-December 2004.

[7] G. Zhang and M. Parashar, "Cooperative detection and protection against network attacks using decentralized informationsharing," The Journal of Networks, Software Tools, and Applications, Kluwer Academic Publishers, vol. 13, no. 1, pp.67–86, 2010.

[8] J. Lemon, "Resisting SYN Flooding DOS Attacks with SYNCache," in Proc. Conf. USENIX BSD, February 2001.

[9] M. Narita, T. Katoh, B. B. Bista, and T. Takata, "A distributeddetecting method for SYN Flood attacks and its implementation using mobile agents," in MATES, 2009, pp. 91–102.

[10] H. Wang, D. Zhang, and K. G. Shin, "Change-point monitoring for the detection of DoS attacks," IEEE Transactions onDependable and Secure Computing, vol. 1, no. 4, pp. 193–208, October-December 2004.