FPGA SYSTEM FOR PREVENTING TCP SYN FLOOD ATTACK

Shaila R. Ghanti[1] and G.M. Naik[2]

[1,2]*Dept. of Electronics, Goa University, Goa, India,* [1]*E-mail: gmnaik@unigoa.ac.in*

Abstract: Today it is very important that servers are to be well protected. In preventing server against various network attacks such as DDOS attacks a preventive system needs to deal with various network conditions and it should have an adaptive functionality. In this paper, we present an innovative concrete method of adaptive preventing system against the TCP SYN flood DDOS attack. The preventer of TCP SYN flood attack reconfigures itself to identify the attack packets based on attack vulnerability. It prevents the SYN flood attack generated without spoofing and also from spoofed IP addresses. The manuscript also gives FPGA architecture for implementation of TCP SYN flood preventer.

Keywords: TCP SYN flood attack, DDOS, Computer security and reconfigurable preventive system, FPGA

1. INTRODUCTION

In today's scenario Internet has become an important resource of life. We are dependent on many servers on the internet for lot of information retrieval and services. As the internet has become very popular, the numbers of attacks on it have also increased tremendously and the attack pattern also varies randomly. According to 2010 Arbour network security report[1], DDOS (Distributed denial of service) attack has increased 102% times as compared to the previous year. Among various DDOS attacks, TCP SYN flooding is the most common one and known as one of the most powerful flooding methods. It still dominates DDOS attacks according to the NANOG report [2].

In view of this, it is essential that the computers/ servers/network need to be protected from the attacks. These preventive systems need to stop attacking packets from reaching the server. Since the attack patterns are varying vigorously, the preventive system should be adaptive type or reconfigurable type based on the attack type. Most of the preventive systems against SYN flood attack have fixed configurations. As the attack pattern varies with time, there is a strong need that the preventer should be reconfigurable based on the attack flow at a given time. Because of the technological growth it was possible to implement hardware based architecture in a FPGA module for high speed processing.

1.1 DDOS Attack

DDOS attacks are large-scale cooperative attacks typically launched from a large number of compromised hosts. There are several types of DDOS attacks. Some of them are SYN flood attack, ICMP flood attack, UDP flood attack etc.

TCP *three way handshake* protocol is used to set up TCP connection between the client and server. The client sends the SYN request packet to the server to set up connection and the server in turn returns the SYN/ACK to the client. The server reserves the resources like backlog queue. The client on receiving this sends the ACK back to the server as in figure 1. Once the server receives the ACK packet the connection is set up between the server and client.

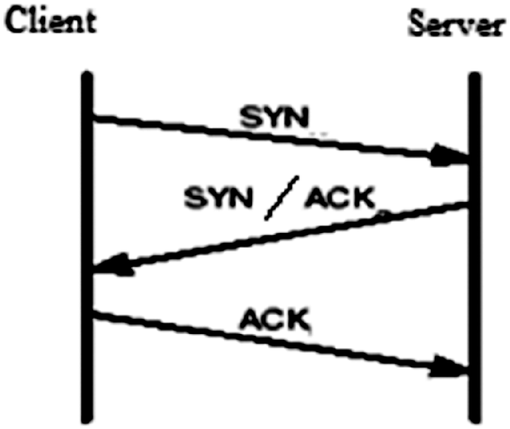

Figure 1: TCP 3 Way Handshake

During the TCP SYN flood attack the client sends many SYN packets to the server and the server in turn sends the SYN/ACK to client. But the client will not send back the ACK packet. This results into large number of half open connections at the victim side. All the half open connections are stored in backlog queue. Once the backlog queue is full the server denies genuine client requests. Hence the server cannot be accessed by a genuine client. During TCP SYN flood attack the attacker may send the spoofed or not spoofed IP address attack. The server services are not available to the users.

Hence we need to protect our server from DDOS TCP SYN flood attack. The TCP SYN preventer should identify the TCP SYN attacks and it should block the attack from reaching the server. The attack may be spoofed/ not spoofed type and the attacker information may change with respect to time, as any client at a given time acts as an attacker. Hence TCP SYN preventer should be of reconfigurable type. It reconfigures itself about the genuine client SYN request and attacker SYN request based on the attack.

1.2 FPGA

A Field Programmable Gate Array is a chip containing Configurable Logic Blocks. An FPGA can be reprogrammed to perform different functions. FPGA is used for many real-time network processing engines [9], [10], [11] due to its ability to reconfigure and to offer abundant parallelism. Due to these Characteristics we propose to use FPGA in our setup.

2. RELATED WORK

There are many methods available in the literature to detect the SYN flood attacks and also mitigate the attacks. Existing methods available are SYN cache [3], SYN cookies [4], "Robust Scheme to detect SYN flooding attack"[5], SYN defender [6], SYN Kill, "Three counter Defense mechanism"[7] etc.

We propose TCP SYN preventer based on the concept of SYN Defender [6] and "Three Counter Defense Mechanism" [7]. Our proposed TCP SYN preventer overcomes the disadvantages of these two [6,7] methods.

The SYN defender working principle is when it receives the SYN packet, the packet is not forwarded to the server. Instead it generates the SYN-ACK back to the client. If the client sends the ACK back then the SYN defender will in turn set up the connection with the server as in figure 2.

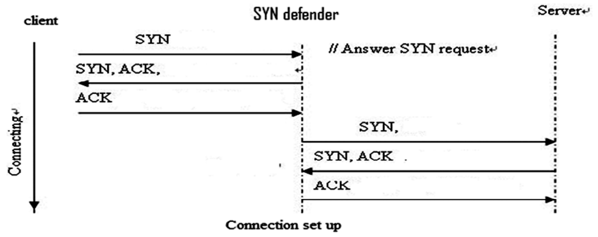

Figure 2: SYN Defender

The main disadvantage of SYN defender is every time there is a SYN request, it stores the SYN packet and waits till it receives the ACK. Hence it takes more time to process each and every request. Once the genuine client has set up the connection and if there is request for connection again, the SYN defender waits for ACK from the client. Only then the connection is set up. This means there is more delay involved every time. It is a fixed type and not a reconfigurable type.

The "Three Counter Defense Mechanism for TCP SYN Flooding attacks"[8] uses three counters to store information about the genuine clients, new clients and others. The detection scheme utilizes the inherent TCP valid SYN-FIN pair's behavior. The mitigation starts after it detects that there is an attack. The mitigation works based on counter information.

The disadvantages of this method are as below

- Here the assumption is made that a genuine client sends a connection request more than once. Hence every genuine client's first new request will be denied and only the second request is serviced.
- However the attackers may retransmit every SYN packet more than one time to destroy the function of mitigation scheme.

Considering these disadvantages there is a need for a more robust and adaptive system. Taken into account the requirement of of reconfigurability and the technological growth in embedded system we propose a innovative method.

3. PROPOSED METHOD

3.1 Basic Concept

Proposed "FPGA System for preventing TCP SYN flood attack" is connected between the internet and the server for securing the Web server as in figure 3 below.

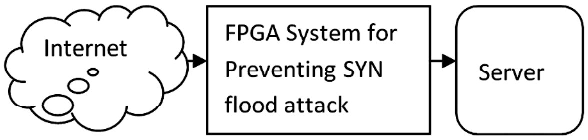

Figure 3: FPGA System for Preventing TCP SYN Flood Attack

FPGA System for preventing TCP SYN flood attack is to be implemented for our proposed algorithm and the block diagram is shown in figure 4 below.

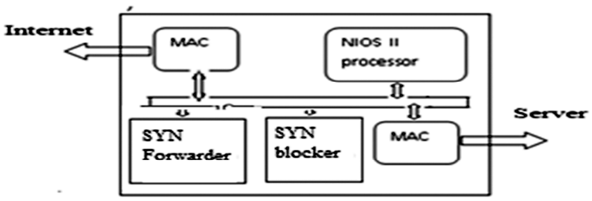

Figure 4: FPGA System Architecture for Preventing TCP SYN Flood Attack

Proposed SYN preventer has two main blocks as below

SYN forwarder: Forwards SYN packets to the server without any delay if the SYN request is from the genuine client.

SYN blocker: If the SYN packet is from attacker then it drops the SYN attack packets or forwards only if there is an ACK

SYN preventer maintains information about the genuine and attack client information. The genuine client SYN requests are forwarded and the attack SYN requests are blocked or processed to find whether its a genuine request.

Though the TCP SYN preventer identifies the genuine SYN packets and attack packets, its not sufficient , because in SYN flood attack the attacker will not send the same attack packets instead it sends new stream of SYN packet (often spoofed) connection requests frequently. Thus TCP SYN preventer always reconfigures itself or learns by itself dynamically about the genuine client information and attack information based on the traffic flow at a given time.

SYN preventer maintains two types of counters, **good registry** and **bad registry**. All genuine clients information is stored in good registry and attack clients information is stored in bad registry. The genuine clients are ones which have already established the connection with the server atleast once.

Good registry/bad registry maintains 4-tuples (source IP, source port, destination IP, destination port) of SYN packet and a counter as shown in the table 1 below.

Table 1
Information Stored in Good/bad Registry

Source IP address	Source port address	Dest.IP address	Dest port address	counter

The counter in table 1 is used to store information about half open connections set or not. If it is 0 it means at a given time, no half open connection is set. If it is 1 that means a client has already set up half open connection as explained in table 2 below.

Table 2
Counter Details

Counter	*Meaning*
0	No half open connections is set
Non zero	Half open connection is set

3.2 SYN Preventer Algorithm

SYN forwarder: Whenever the SYN packet is received by the SYN preventer it extracts the four tuples from packet. If there is hit(it is found in) from good registry, the SYN packet is forwarded to the server without any delay. The details SYN forwarder is shown in flowchart as in figure 5.

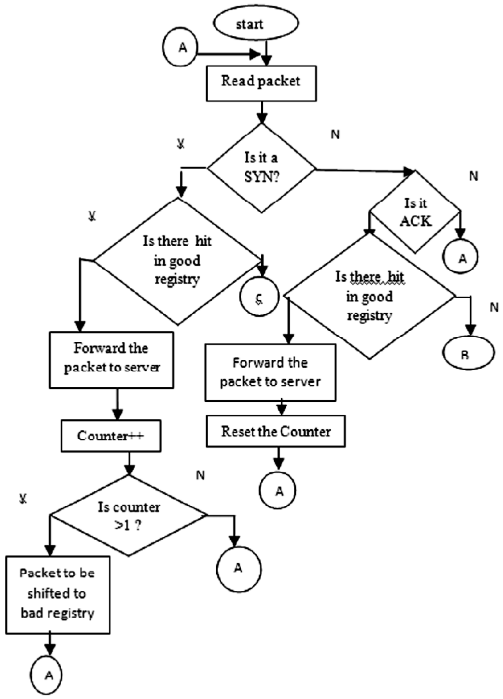
start
A
Read packet
Is it a SYN?
Y
N
Is there hit in good registry
Y
S
Is it ACK
N
A
Is there hit in good registry
N
B
Forward the packet to server
Counter++
Forward the packet to server
Reset the Counter
A
Is counter >1 ?
Y
N
Packet to be shifted to bad registry
A
A

Figure 5: Flow Chart of SYN Forwarder

After forwarding, the corresponding counter contents are checked.

- If the counter is zero, it means no SYN request has been sent and hence the counter is incremented to 1, indicating the SYN request is already sent to the server.
- If the counter contents are 1, the corresponding counter contents are incremented. If Counter contents have reached 2 that means more than 1 SYN request is generated and may be a possible attack or spoofed SYN attack. Then the packet information from good registry is transferred to the bad registry.

In this way the SYN preventer keeps on learning about the genuine client and attack client based on the current traffic flow. i.e it reconfigures itself based on the current traffic, accordingly the packets are forwarded or blocked.

When an ACK packet is received by the syn preventer, it extracts the four tuples from packet. If there is hit from good registry, the ACK packet is forwarded to the server. Then it decrements the corresponding counter indicating no half open connections is set up.

Here the SYN request is directly sent to the server from the client. The connection is set up between client and server. The SYN preventer is not involved in setting up the connection as in SYN Defender.

SYN Blocker

When SYN packet is not found in the good registry then it is searched in bad registry. If there is a hit in bad registry, the counter contents are checked. if it is 1 then the packet is dropped and counter is decremented. Syn blocker working is explained as in figure 6.

If the counter content is 0, then the counter contents are incremented and the preventer will not forward the SYN packet instead it will reply to the client with SYN/ACK. If it receives the ACK the corresponding counters are decremented and then the SYN preventer in turn will set up the connection. Then the Packet information is transferred from bad registry to the good registry.

When an ACK packet is not found in the good registry, then it is searched in the bad registry. if there is a hit in bad registry the counter contents are reset .

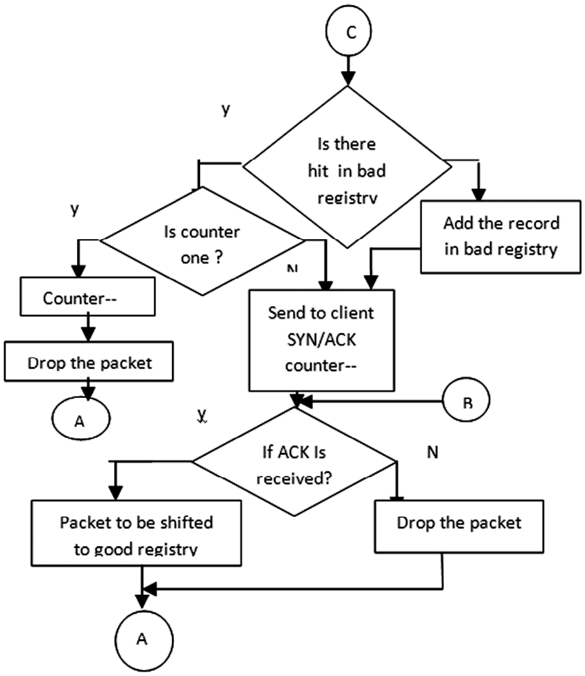
C
y
Is there hit in bad registry
Add the record in bad registry
y
Is counter one ?
N
Counter--
Send to client SYN/ACK counter--
Drop the packet
A
B
y
If ACK Is received?
N
Packet to be shifted to good registry
Drop the packet
A

Figure 6: Flowchart of SYN Blocker

3.3 Advantages of Proposed Model

Our Counter based algorithm over comes the disadvantages of The TCP SYN defender. In TCP SYN defender every TCP SYN request is not forwarded to the server instead the SYN defender waits for ACK. Then the TCP SYN defender sets up connection on behalf of client. In our proposed TCP SYN flood preventer for genuine clients it just forwards the TSP SYN request. Hence the client can directly set up the connection instead of the preventer. Hence the connection requests are passed immediately without delay.

In "Three Counter Defense Mechanism for TCP SYN Flooding attacks" the mitigation starts after attack is detected that means the attack is already sent to the server. Our TCP SYN flood preventer will prevent TCP SYN flood attack reaching the server. Another advantage is no assumptions are made that a genuine client sends more than one connection request . Hence our TCP SYN preventer for every genuine clients first new request will be serviced . Also by transmitting every SYN packet more than one time, it cannot destroy the function of mitigation.

Advantages over SYN cookies [4]: SYN cookies work by sending a strong ISN in SYN-ACK packet to the client in response to SYN. So that ACK from client has sequence number which is enough to validate the connection. The main disadvantage of

SYN cookie is large CPU utilization to process the ISN. In our method the server processor is not utilized for preventing the SYN attack, as FPGA's are involved in preventing the SYN flood attack.

4. EXPERIMENTAL DETAILSS

To evaluate our detection method, we carried out trace driven simulations. The data sets [8] of 1999 DARPA benchmark are used in our study. We have used week 2 data sets of whch thursday data set has been used, it contains the TCP SYN attack packets. This file can be opened using tcpdump tool. Our simulations show that using this method it is possible to prevent tcp syn attack.

5. CONCLUSION AND FUTURE SCIPE

In the proposed methodology a new intelligent SYN preventer algorithm for SYN flooding defence attack has been described in detail. The preventer is based on the counter method,which includes SYN forwarder and SYN blocker. SYN forwarder basically forwards the SYN packets to the server without any delay based on genuine packet information. SYN forwarder is stateless, SYN blocker blocks the attack SYN flood packets and also the spoofed IP SYN attack packets. The SYN preventer reconfigures itself to identify the packet as genuine SYN packet or spoofed SYN packet or TCP SYN attack packet. Moreover it works independently at the victim side and no cooperation is needed from the other routers unlike in other routersunlike in many other systems. This reconfigurable concept can be implemented in any network defensive system from attacks, as attacks are varying. The basic concept of reconfigurability can be used in preventing worm attacks, Intrusion detection system (IDS), firewall , against spam attack, router etc.

The proposed method releases the challenge on the storage space and the speed to reconfigure itself.

Based on this the future work includes

- To implement the proposed TCP SYN preventer on the hardware like reconfigurable embedded system (FPGAs), this gives advantages of hardware along with option of flexibility. The hardware based systems allows the introduction of higher degree of parallelism. FPGAs support speed up to multi gigabit rate.
- To use memory efficient storage algorithms and faster content matching algorithms.

REFERENCES

[1] Worldwide Infrastrructure Security Report 2010, http:// lacnic.net /documentos/lacni cxv/WISR-2010-FINAL-LACNIC2.pdf

[2] C. Labovitz, D. McPherson, S. Iekel-Johnson, and M. Hollyman, "Internet Traffic Trends - A View from 67 ISPs", NANOG, 2008. [Online]. Available: http://www.nanog.org/meetings/nanog43/ presentations/Labovitz internetstats N43.pdf

[3] J. Lemon. "Resisting Syn Flood Dos Attacks with a Syn Cache". *In Proceeding of the BSDCON 2002*. USENIX Association, February 2002

[4] D.J. Bernstein, "SYN Cookie". Http://cy.yp.mI syncookies.html

[5] Changhua Sun; Jindou Fan; Bin Liu, "A Robust Scheme to Detect SYN Flooding Attacks", *International Conference on Communications and Networking in China*, 2007

[6] "Syndefender". Available: http://www.check point.com/products/firewall-1/

[7] S. Gavaskar, R. Surendiran and Dr E. Ramaraj, "Three Counter Defense Mechanism for TCP SYN Flooding Attacks", *International Journal of Computer Applications* (0975-8887) **6(6)**, September 2010.

[8] [MIT Lincoln Laboratory. 2000 DARRA Intrusion Detection Scenario Specific Data Sets [EB/OL]. Http://www.ll.mit.edu/ist/

[9] H. Song and J.W. Lockwood, "Efficient Packet Classification for Network Intrusion Detection Using FPGA", *in Proc. FPGA*, 2005.

[10] A. Nikitakis and I. Papaefstathiou, "A Memory-efficient FPGA-based Classification Engine", *in Proc. FCCM*, 2008, pp. 53-62.

[11] G.S. Jedhe, A. Ramamoorthy, and K. Varghese, "A Scalable High Throughput Firewall in FPGA", *in Proc. FCCM*, 2008, pp. 43-52 238-245.