Three Counter Defense Mechanism for TCP SYN Flooding Attacks

S.Gavaskar
Research Scholar,
Madurai Kamaraj
University, Madurai.

R.Surendiran
Lecturer
Madurai Kamaraj
University, Madurai.

Dr.E.Ramaraj
Technology Adviser
Madurai Kamaraj
University,Madurai.

ABSTRACT
Nowadays network growing rampant manner and uses as transfer medium like data, money transaction, information etc. Even though internet plays a vital role still there is some vulnerability. Ex: virus, spam, hacking, DOS, DDos, etc. We are focusing Distributed Denial of Service; there is plenty of Denial of Service mechanism existed in that we took SYN Flood attacks.

With this view my proposed work is, an efficient method to detecting and mitigation against TCP SYN flooding attacks using *Three Counters Algorithm*, which detects spoofed IP packets up to 80%.

KeyWords: DDos, TCP SYN, SYN flood.

1. INTRODUCTION:

Internet servers which are giving essential services become the target to many attacks. There are many attacks intended to deprive legitimate users from accessing network resources and functions. Distributed Denial of Service (DoS) attack is an attack on the availability of Internet services and resources. Bandwidth depletion and Resource depletion attacks are two main classes of DDoS attack DDoS attack is an explicit attempt by attackers to prevent legitimate users a service from using that service.

1.1. DDos Attack

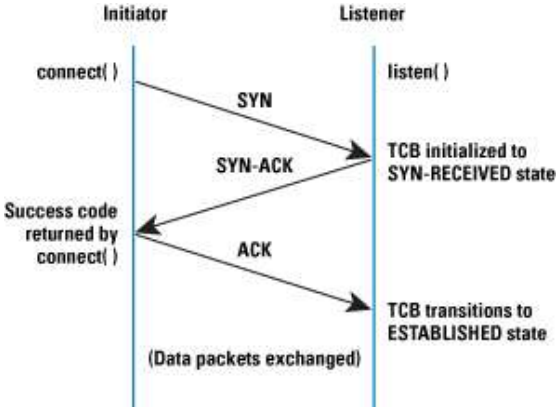
Denial of service [2] is accomplished technologically. The primary goal of an attack is to deny the victim(s) access to a particular resource. It is an explicit attempt by attackers to prevent legitimate users of a computer-related service from using that service. But, as any information and network security issue, combating denial of service is primarily an exercise in risk management. To mitigate the risk, we need to make business decisions as well as technical decisions. Managing the risks posed by denial of service requires a multi-pronged approach:

- Design the business for survivability. Have business continuity provisions in place.
- Design the network for survivability. Take steps that help to ensure that critical services continue in spite of attacks or failures.
- Be a good netizen (net citizen). The potential to be attacked depends on the security of other sites and vice versa. The threat to network is directly proportional to the extent that other Internet users, including home users, adhere to good practices. Conversely, the threat that your network represents to others is directly proportional to the extent that your organization adheres to good practices. Denial of service may be indistinguishable from a heavy (but otherwise legitimate) load on your network. For example the victim might be flooded with legitimate connections to his web site as a result of a major news event.
- Users might have difficultly connecting to the web site simply because so many people are trying to connect at one time and not because it is the target of a denial-of-service attack. It is important to establish criteria by which it can be declared that the site is "under attack" and invoke emergency procedures. Mitigation strategies for attacks and heavy legitimate traffic may be similar.

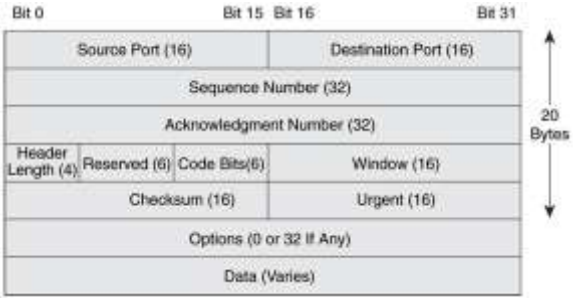
1.2. TCP IP connection:

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. Besides the Web, other common applications of TCP include e-mail and file transfer. Among other management tasks, TCP controls segment size, flow control, and data exchange rate.

The basis of the SYN flooding attack lies in the design of the 3-way handshake that begins a TCP connection. In this handshake, the third packet verifies the initiator's ability to receive packets at the IP address it used as the source in its initial request, or its return reach ability.

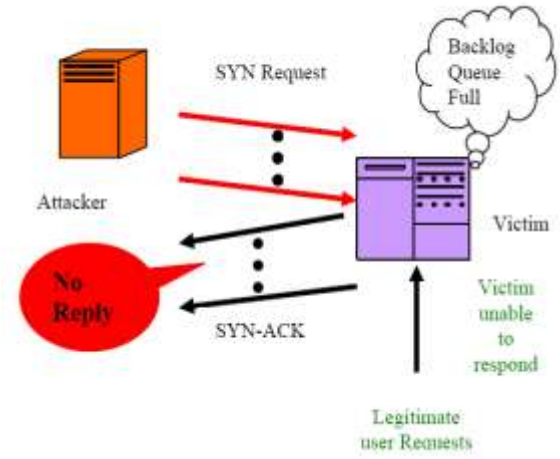


This diagram shows the TCP/IP header formation and what the bits available to usage and checking are.



1.2. SYN flood Attack

Internet servers are more vulnerable to SYN Flooding attack which is one of the resource depletion attacks. Flooding based distributed denial of service (DDOS) [4] attack presents a very serious threat to the stability of the Internet. Flooding attacks intend to overflow and consume resources available to the victim (memory, Bandwidth) by sending a continuous flood of traffic. SYN flooding is the most common and well-known DoS attack. In SYN flooding [5], the attacking system sends SYN request with spoofed source IP address to the victim host. These SYN requests appear to be legitimate. The spoofed address refers to a client system that does not exist. Hence final ACK message will never sent to the victim server system. This results into more number of half-open connections at the victim side. A backlog queue is used to store these half-open connections. These half-open connections bind the resources of the server. Hence no new connections (legitimate) can be made, resulting in Denial of Service. The victim server is unable to respond to the requests coming from legitimate users



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. A defense mechanism against spoofed traffic using hop count filtering. It needs a systematic procedure for setting parameters for hop count filtering. In IP trace back system 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, 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. Due to the readily available tools, "Flooding" attack becomes most common DDoS attack. We want to have a good solution for flooding attack. SYN flooding DDoS attacks are most common and well known attacks. Due to the explosive growth of the Internet, flooding based DDoS attack methods are becoming more sophisticated. A single security component cannot properly defend a network. Hence many security components working together can defend a victim (or) network. Defense in depth is an essential feature of the proposed work.

2. TYPES OF ATTACKS:

There are several types of attacks are there in DDos, some of these

- **SYN Attack**: A SYN flood attack occurs when a network becomes so overwhelmed by SYN packets initiating uncompletable connection request that it can no longer

process legitimate connection requests, resulting in a denial of service (DoS).

- **ICMP Flood**: An ICMP flood occurs when ICMP pings overload a system with so many echo requests that the system expends all its resources responding until it can no longer process valid network traffic. When enabling the ICMP flood protection feature, administrators can set a threshold that once exceeded invokes the ICMP flood attack protection feature. (The default threshold value is 1000 packets per second.)
- **UDP Flood**: Similar to the ICMP flood, UDP flooding occurs when UDP packets are sent with the purpose of slowing down the system to the point that it can no longer handle valid connections. After enabling the UDP flood protection feature, administrators can set a threshold that once exceeded invokes the UDP flood attack protection feature. (The default threshold value is 1000 packets per second.)
- **Port Scan Attack**: A port scan attack occurs when one source IP address sends IP packets to 10 different ports at the same destination IP address within a defined interval (5,000 microseconds is the default). The purpose of this scheme is to scan the available services in the hopes that one port will respond, thus identifying a service to target.

In this paper we will look depth about the SYN flood attack. The paper provides the efficient detection mechanism for SYN flood attack and how to mitigate SYN attacks.

3. PROPOSED METHODS:

3.1. Detection Scheme

We determine *valid SYN packets* as the pure SYN and SYN/ACK packets, and *valid FIN packets* as the FIN and RST packets that close the TCP connections which either complete the three-way handshake or have a *valid SYN packet* in the same traffic direction before this packet. Then there are more *valid SYN packets* than *valid FIN packets* under SYN flooding.

When we receive a SYN or SYN/ACK packet, the counter of *valid SYN packets* is increased. We use this concept as our research. A filter is a simple space-efficient data structure for representing a set in order to support counting process. When we receive a FIN or RST packet, the item of its *4-tuple (source &destination IP and ports Address) is* also extracted and queried from the filter. If this item is in the filter, the counter of *valid FIN packets* is increased, and this item is deleted from the counting filter. If not, this packet is not a *valid FIN packet*, and nothing is needed. Our Three counters algorithm scheme utilizes the change of the discrepancy between *valid SYN and FIN packets*.

3.1.1 Efficient Router

An efficient router can detect the SYN flood attacks. Every network should have one router in terms we have to design our network. Ever entry of packet should be monitor then check the IP address if it's legitimate then only it can allow to networks. If there is any IP spoofing technique happen in the IP header that packet will restricted. Using router we can detect the SYN flood attacks because SYN flood attacks happen after the packets came into the system by the unauthorized user. If we use router in every networks the earlier stage itself spoofed packets detected, it's very easy to solve the problem compare with after happen the attack.

3.2. Three Counters Algorithm:

In SYN floods, attacker would send a quick barrage of SYN packets from IP addresses (often spoofed) that will not generate replies to the SYN/ACKs. To remain effective, attacker needs to send new barrages of bogus connection requests frequently. Most of the SYN flooding packets would not be retransmitted. On the other hand, If a legitimate client's SYN packet is lost, it would retransmit the SYN packet several times before giving up. Our mitigation scheme utilizes the characteristic of SYN floods and client's persistence. We use three counting filters [1] to record related information:

• C-1: to record the first SYN packets of each connection;
• C-2: to record the SYN packets, whose connections have completed the three-way handshake?
• C-3: to record the other SYN packets.

The mitigation scheme starts working once detecting SYN floods. If a SYN packet is received, its *4-tuple* is extracted as an item and queried from the three Cs. The results are:

1) The item is not in any of the three Cs. This TCP connection is new, and then we drop this SYN packet and insert the item to C-1;
2) The item is in C-1. This is the second SYN packet. We pass it and move the item from C-1 to C-3;
3) The item is in C-2. We pass the packet;
4) The item is in C-3. We pass the packet with a certain probability *p*. We insert the item to C-3 and obtain the number, *n*, of this item in C-3. Let $p = 1/n$, then *p* is smaller as the increasing of *n*. If a ACK packet is received, its *4-tuple* is also extracted as an item and queried from the three Cs. The result is used as follows:

1) The item is not in any of the three Cs or in C-We drop this packet;
2) The item is in C-2. We pass this packet;
3) The item is in C-3. This TCP connection is completed. Then we pass this packet and move the item from C-3 to C-2. If the attacker uses different *4-tuple* of SYN packets, these SYN packets would be classified as the first SYN packets of each connection,

and would be dropped. If some SYN packets with the same *4-tuple* are used in the attack, a small portion of SYN flooding packets would reach the victim (such as the second SYN packets). If these SYN packets are retransmitted again and again, they are dropped with higher and higher probability. Therefore, our mitigation scheme can drop most of SYN flooding packets and protect the victim.

4. SIMULATION RESULTS:

We carry out trace driven simulations to evaluate the performance of detection scheme. Fig.1 shows the result of our detection scheme (*Sss-U*) and the scheme in [5] (*Sss-U*) under a complex SYN flooding attack. The value of *yn* greater than 1 reports the attack. It is shown that *Sss-U* can detect the attack in a single observation period while *Sss-U* can not.

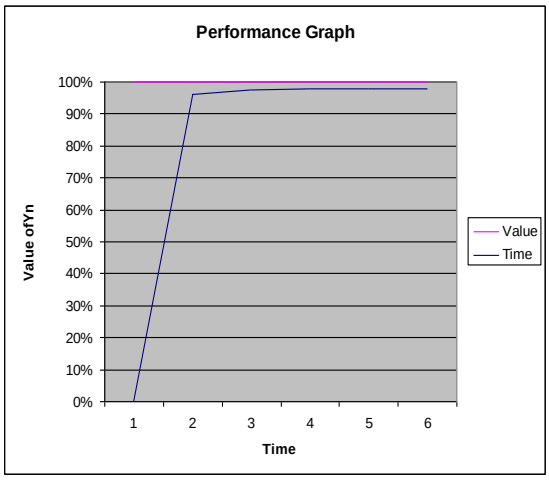


Fig: 1

5. CONCLUSION:

We proposed *Three Counters Algorithm* for SYN flooding defense attack. Our scheme includes *detection* and *mitigation*. The detection scheme utilizes the inherent TCP *valid SYN–FIN* pairs behavior, hence is capable of detecting various SYN flooding attacks with high accuracy and short response time.

The mitigation scheme works in high reliable manner for victim to detect the SYN packets of SYN flooding attack. Our scheme is stateless and requires low computation overhead, making itself immune to SYN flooding attacks. However, the attackers may retransmit every SYN packet more then one time to destroy the function of mitigation scheme. It is necessary to make it more robust and adaptive. In the mean time, we are working on evaluate the proposed scheme in real network system and study its impact on legitimate users.

6. REFERENCES

[1] 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.September .

[2] 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, Digital Object Identifier: 10.1109/TPDS.2005.74.

[3] 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, ol.38,No.1.

[4] Rocky C.Chang,(2002),"Defending against Flooding-Based Distributed Denial-of-service Attacks: A Tutorial",IEEECommunications Magazine,October.

[5] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in IEEE INFOCOM, 2002.

[6] M. V. Ramakrishna, E. Fu, and E. Bahcekapili, "Efficient hardware hashing functions for high performance computers," IEEE Transactionson computers, vol.46,no.12,pp.1378-1381,1997.