A Comprehensive Mechanism to reduce the detection time of SYN Flooding Attack

S.Meenakshi[†] **Dr.S.K.Srivatsa**[††]
[†] Research scholar, Sathyabama University, Chennai
[††] Senior Professor, St. Josephs' college of Engineering, Chennai

Summary:
We are currently in the bronze age of information security. 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. A Denial of Service (DoS) attack is an attack which prevents legitimate users from using a victim computing system or network resource. Flooding based Distributed Denial of service (DDoS) attack presents a very serious threat to the stability of the Internet. We want to design a comprehensive mitigation mechanism against the DDoS attack. In the proposed system the entire attack detection process is divided into two levels due to the distributed nature of DDoS attack.In the first level the individual detection systems are installed in all autonomous systems to perform local detection. In the second level the all the detection systems exchange their messages using consensus method to take global decision. 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. So the overall detection time would be reduced for global decision making. Defense in depth is an essential feature of the proposed work.

Key words:
Denial of service, Consensus method, early alert, Majority selection.

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[Jelena Mirkovic and Peter reiher(2004)].DDoS attack is an explicit attempt by attackers to prevent legitimate users a service from using that service. Internet servers are more vulnerable to SYN Flooding attack which is one of the resource depletion attack.

Flooding based distributed denial of service (DDOS) 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, 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. This is shown in Figure 1.

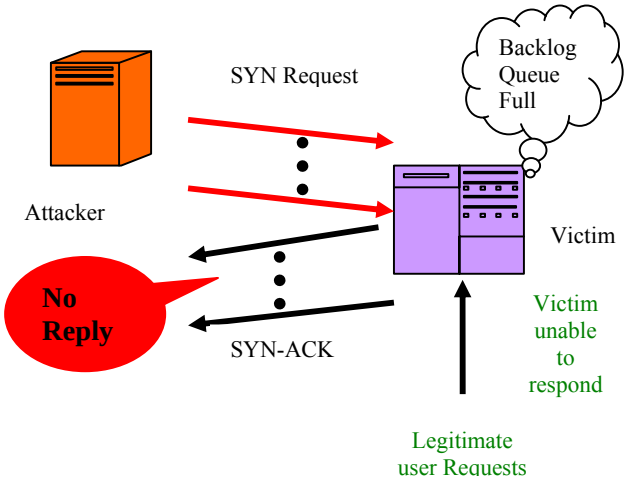


Figure 1 SYN Flood attack

The first DDoS attack occurred in 1999 [Computer Incident Advisory Capability(CIAC) Report]. In February 2000, the first major DDoS attack was launched against Yahoo.com. Another DDoS attack was on October

Manuscript received January 5, 2009
Manuscript revised January 20, 2009

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.[Jelena Mirkovic and Peter reiher(2004)]

This paper is organized as follows. The complete system architecture is given in section 2. Section 3 describes the implementation and performance. Conclusions are provided in section 4.

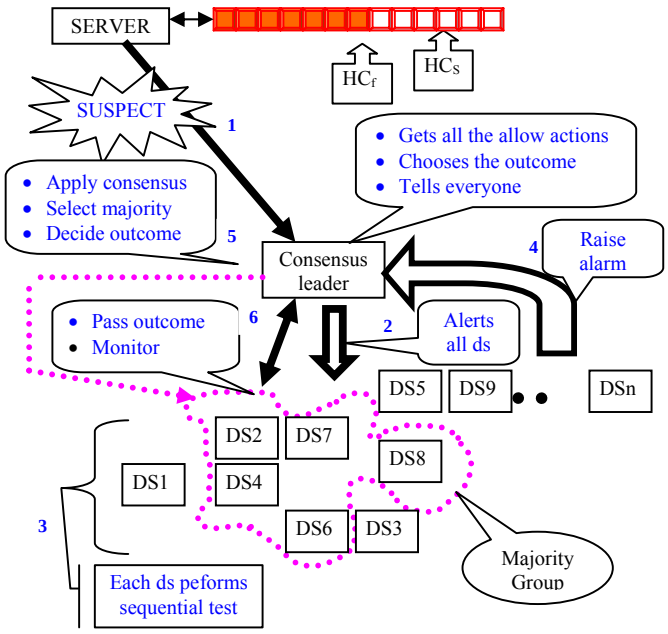
Cheng Jin et al (2002) proposed a defense mechanism against spoofed traffic using hop count filtering. It needs a systematic procedure for setting parameters for hop count filtering. In IP trace back system [Minho Sung et al (2003)] assistance from hosts present outside the network is needed. Many existing 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. 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. In the proposed work there many autonomous systems (AS) present. Each AS has one (or) two detection systems (DS). One is acting as a leader detection system(LDS) among many DS. All DS are controlled by the leader. All DS must work together in order to protect victim system from SYN flooding attack.The benefits of the proposed are as follows: **Global decision making:** Due to the distributed nature of DDoS attack, each DS finds only partial DDoS anomalies. Hence, all DS must work together to detect DDoS attack. In the proposed system consensus method is applied over all DS in order to take global decision against attack. **Earlier prevention of DDoS attack:** Prevention and early detection of DDoS attack is very important. This feature will minimize the expected delay of detecting DDoS attack after it's occurrence. **Use of consensus method:** Consensus method is used for exchange of information between detection systems and to make global decision.

2. System Architecture

The architecture of proposed system is shown in figure SYN flooding attack creates many half-open connections in the backlog queue of the victim system. Each backlog queue has one threshold value to indicate the maximum number of half-open connections before SYN protection starts. This default threshold value is taken as HCs(Half-open connection second). In the proposed system architecture one more threshold value for same is set(HCf- Half-open connection first). This extra threshold value is useful for early detection of DDoS attack. Hence , the detection time is simply decreased. The Complete system architecture is shown in figure 2. The backlog queue has a well defined size(Maximum number of half-open connections that it can accommodate). When the backlog queue value of the victim reaches HCf(the lower bound), immediately it sends a suspicion to the leader detection system. The LDS alerts all DS to start the checking process. Each detection system performs the check over the incoming packets destined towards the victim. Each detection system has two phases for detecting anomaly.

Each performs sequential test over outgoing and incoming packets ratio and monitors the packets with unknown(new or not familiar) IP address. Then each DS will raise alarm when this belief crosses the threshold and also pass these values to the LDS. Upon receiving these values from all DSs , consensus method is applied by the LDS over the DSs. **Consensus method:** The LDS has to select the majority group from all DS. It compares the values received from each DS with it's threshold value .The DS whose value is above this threshold then it wins this check. Moreover the number of DS winning this check must be greater than n/2, where 'n' is the total number of DS. Then the LDS calculates the filtering value and passes this outcome to members of majority group. Each DS calculates the relative filtering value based on deviation of its own value from global threshold value. Periodically the leader checks the no of half open connections at the victim server. If it is below HCs, then the leader instructs the DS of majority group with the same filtering value. (Here 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 HCs, then the filtering value is decided as Maximum among the majority group. The process stops when either all the majority group DS's incoming rate converges or the number of half-open connections converges below HCf.



Detection Systems= DSi for $1 \leq i \leq n$

Figure 2 System Architecture

3. Implementation and Performance

The proposed system was simulated in NS-2. We simulate the entire network with scenario given in table 3. The system consists of four AS with a total of 25 nodes. There are four daemon systems present to generate attack traffic towards one victim system. There are five DS to protect the victim and one among these is LDM. With this scenario the system is tested under various conditions.

The performance of the system is measured with various half-open connection life time 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

Table 3 Simulation scenario

The Figure 4 Shows the screen shot of the simulation. The system consists of four AS with a total of 25 nodes. There are four daemon systems present to generate attack traffic towards one victim system. There are five DS to protect the victim and one among these is LDM. With this scenario the system is tested under various conditions.

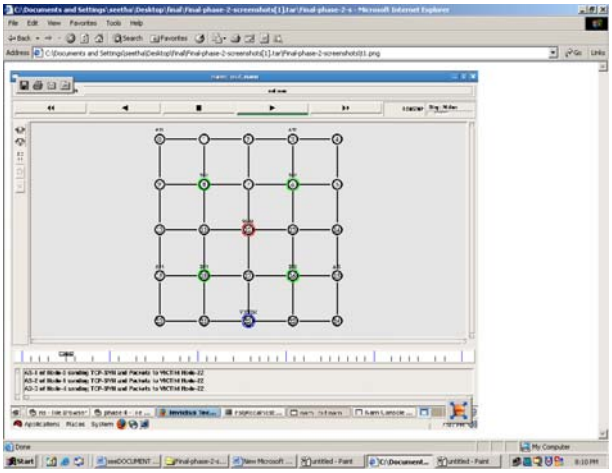


Figure 4 Screen shot of the simulation

Early alert and reducing detection time: The performance of the system is measured with various half-open connection life time values. 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. So the overall detection time would be reduced for global decision making. The system responds quickly with extra lower bound on the half-open connection life time (i.e., with HCf – lower bound for half-open connection life time) . The main aim of the system is to protect the victim from the attack (i.e., before the attack packets congest and exhaust the victim). Figure 6 shows that the detection time of the system with lower bound is smaller than the detection time of the system without lower bound. The data values are given in table 7. The fixing up of lower bound for number of half open connections is very much useful to reduce the overall detection time.

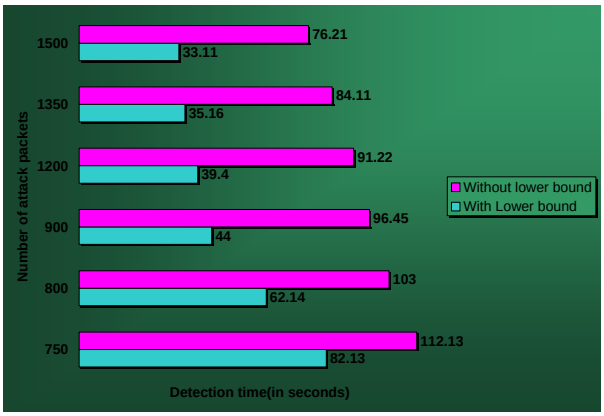


Figure 6 Effect of Early detection

BS	HC_s	HC_f	Half open connection life time
120	96	78	6 seconds

Number of attack packets	detection time (with lower bound) in seconds	detection time (without lower bound) in seconds
750	82.13	112.13
800	62.14	103
900	44	96.45
1200	39.4	91.22
1350	35.16	84.11
1500	33.11	76.21

Table 7 Detection time with and without lower bound

4. Conclusion

The flooding based DDoS attacks are very serious threat to the internet. Particularly the Internet servers which are giving essential services must be protected from these types of attacks. The proposed system is implemented for global decision making against the flooding attack. The average detection time is decreased by having lower bound on the half-open connection life time. The system's overall performance could be improved by bigger back log queue size. Above all, in order to improve detection accuracy the system applies consensus method over all the detection systems.

References

[1] Cheng Jin, Haining Wang and Kang G.Shin(2002), "Hop-Count Filtering: An Effective Defense Against Spoofed Traffic", http://www.eecs.umich.edu/techreports/cse/2003/CSE-TR-473-03.pdf.

[2] 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. http://doi.acm.org/10.1145/997150.997156

[3] 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 , http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/8412/26518/01181417.pdf?arnumber=1181417

[4] 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

[5] 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, http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT38/JRPIT38.1.69.pdf

[6] Rocky K.C.Chang,(2002),"Defending against Flooding-Based Distributed Denial-of-service Attacks:A Tutorial",IEEECommunications Magazine,October, http://dslab.csie.ncu.edu.tw/93html/paper/pdf/Defending%20against%20flooding-based%20distributed%20denial-of-service%20attacks_a%20tutorial.pdf

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