Comparative Study Of Preventive Algorithms Of Ddos Attack

Divyashree Chavan, Colleen Francis, Elbin Mary Thomas, Prathama Moraye

Abstract- Threats of distributed denial of service (DDoS) attacks have been increasing day-by-day due to rapid development of computer networks and associated infrastructure, and millions of software applications. In this type of attack, multiple systems attack a single target simultaneously, to consume the resources within very less time and thereby shut down the system. DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. The growing frequency, increasing sophistication, and growing seriousness of DDoS attacks have made defending against them quite a challenge. Because there's no complete defence against such an attack but a practical defense includes prevention strategies. This paper presents a comprehensive overview of DDoS attacks, types of DDos attacks, attacks on various OSI levels. Also the algorithms for DDos prevention like cracking algorithm and hop count filtration are described and their comparative analysis is made.

Index Terms— Cracking, Ddos, Flooding, Hop count, Reflectors, Spoofing, TTL, .

1 Introduction

The Internet has played an important role in society in many ways such as in economics ,government ,business and our daily personal life. Among various Internet based attacks, Denial of Service (DoS) attack is the most critical and provides continuous threat in cyber security. They are characterized as attempts to flood a network, disrupt connections between two computers,prevent an individual from accessing a service or disrupt service to a specific system. DoS attacks either forces a victim computer to reset, or consume its resources . Due to which,the targeted computer can no longer provide its intended services to its legitimate users. Early DoS attacks used to generate packets from a single source which was then aimed at a single destination.

The evolution of the DoS attack describes a single source attacks against multiple targets, multiple source attacks against single targets, and multiple source attacks against multiple targets. Around 2001, a new type of DoS attack became rampant, called a Distributed Denial of Service attack, or DDoS. In this case ,multiple systems are used to attack a single target. The flood of incoming traffic to the target will force to shut down the system. Due to which, the legitimate requests to the affected system are denied. As DDoS attack is launched from multiple sources, it very difficult to detect and block than a DoS attack. It , leads to revenue losses and increase the costs of mitigating the attacks to restore the services. Most recently since September 2012, online banking sites of 9 major U.S. banks (i.e., Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, PNC, Capital One, Fifth Third Bank, BB&T, and HSBC) have been continuously the targets of series of powerful DDoS flooding attacks launched by a foreign hacktivist group called "Izz ad-Din al-Qassam Cyber Fighters" .[1]

2 Types of Ddos attacks

DDoS attacks can be generated in two different ways:direct attack and reflector attack.

2.1 Direct attack

In a direct attack, a large number of attack packets are sent to the victim machine directly. In this attack, the attacker spoofs the source IP address so that the response is misdirected and goes elsewhere.[9]

2.2 Reflector attack

In case of an reflector attack, many innocent intermediate nodes known as reflectors(Botnets or Zombies) are used to generate an attack. An attacker sends packets that require responses to the reflectors with the packets' inscribed source address set to the victim's address. The attack packets can be constructed using TCP, UDP, ICMP or IGMP protocols.[9]

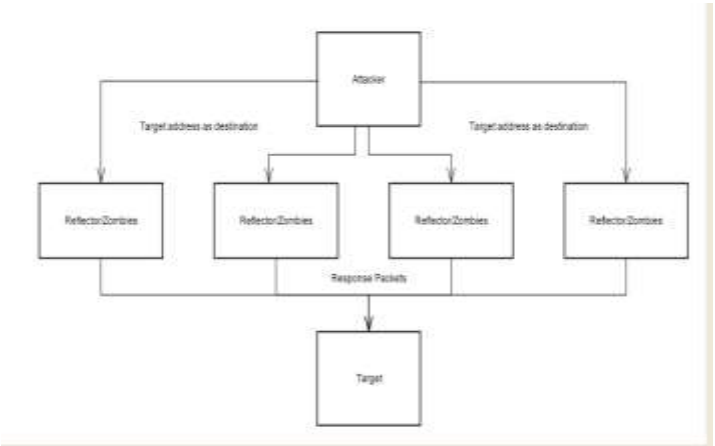

Fig 1.Reflector attack

3 Ddos attacks at various levels

3.1 Ddos attack on application layer.

An application layer distributed denial of service attack is usually initiated by hiring machines, bots, or taking control

of remote systems. These components are used to ping multiple fake requests to server making the services of an application or server unavailable to its intended users. Such an attack targets everything that can eat huge chunks of the bandwidth, processing speed, and memory to slow down or disrupt services.

Examples of application layer attack are:

3.1.1. HTTP Flood

In HTTP flood DDoS attack the attacker exploits seemingly-legitimate HTTP GET or POST requests to attack a web server or application. HTTP floods do not use malformed packets, spoofing or reflection techniques, and require less bandwidth than other attacks to bring down the targeted site or server. The attack is most effective when it forces the server or application to allocate the maximum resources possible in response to each single request.

3.1.2. Slowloris

Slowloris is a highly-targeted attack, enabling one web server to take down another server, without affecting other services or ports on the target network. Slowloris does this by holding as many connections to the target web server open for as long as possible. It accomplishes this by creating connections to the target server, but sending only a partial request. Slowloris constantly sends more HTTP headers, but never completes a request. The targeted server keeps each of these false connections open. This eventually overflows the maximum concurrent connection pool, and leads to denial of additional connections from legitimate clients.

3.2 Ddos attack on network and transport layer

The main target of this type of attacks is to overwhelm the network infrastructure consisting of servers, routers and switches by sending a large volume of attack traffic. These attacks can be generated by exploiting protocol weaknesses. Network/Transport layer attacks can be further characterized according to degree of automation, exploited vulnerabilities, types of attack networks used, attacks rates generated, victim types and impacts of the attack.

Examples of network/transport layer protocol are:

3.2.1.SYN Flood

A SYN flood DDoS attack exploits a known weakness in the TCP connection sequence (the "three-way handshake"), wherein a SYN request to initiate a TCP connection with a host must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood scenario, the requester sends multiple SYN requests, but either does not respond to the host's SYN-ACK response, or sends the SYN requests from a spoofed IP address. Either way, the host system continues to wait for acknowledgement for each of the requests, binding resources until no new connections can be made, and ultimately resulting in denial of service.

3.2.2. UDP Flood

This DDoS attack leverages the User Datagram Protocol (UDP), a sessionless networking protocol. This type of attack floods random ports on a remote host with numerous UDP packets, causing the host to repeatedly check for the application listening at that port, and (when no application is found) reply with an ICMP Destination Unreachable packet. This process saps host resources, and can ultimately lead to inaccessibility.

3.2.3. ICMP (Ping) Flood

Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. This type of attack can consume both outgoing and incoming bandwidth, since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown.

4 ALGORITHMS FOR DDOS PREVENTION

4.1. Modified Cracking Algorithm

The research paper [3] have found an algorithm cracking algorithm to prevent ddos attack by limiting the no of access to user. This helps to determine whether user is ddos attacker or legitimate user. When an attackers using genuine address, the proxy server uses the Deficit Round Robin algorithm to collect the address of the client request.If an attacker sends packets much faster than its fair share, the scheduling policy will drop its excess traffic. More Over, for each genuine IP address, the system will perform accounting on the number of packets that reach the firewall but are dropped by the scheduler; its IP address will be blacklisted.[3]

In research paper [2] the more efficient methodology is proposed to prevent ddos attack by limiting the no of access to user or client. The database is maintained between client and server which maintains the list of registered clients. So based on the database maintained the access is provided to registered users. In case of unregistered users the no of requests are checked and if threshold is not reached then access is granted. Also it depends on one more factor called "peak hours". During peak hours the request from the unregistered user is blocked temporarily.

Algorithm
Step 1 Maintain the database for the list of users,X
Step 2 Analyse the User
Get the username of the incoming user.
User=name of the incoming user
Match it with the user list in the database
For i=0 to X.count
If User=X(i).Name then
X. Login_count++
Status="Registered"
Else
X. Login_Count++
Status="Unregistered"
End if
Next
Step 3 Response to the Request
If Status="Registered" then
Process the Request and send the Response
End if
If Status="Unregistered" then
Add name to the alert list, A
A.Name=User

A.Alert_count++
If A.Alert_count < Threshold_Value
If Server_peak_period=True
Add User to Temp_Blocked List
Temp_Block=User
End if
Else
Block the user permanently
P_Block=User
End if
If Server_peak_period ! = True
Unlock the user in Alert list, A
A.Name.Status=Unlock
Process the Request and the Response
End if
End if

Flowchart:

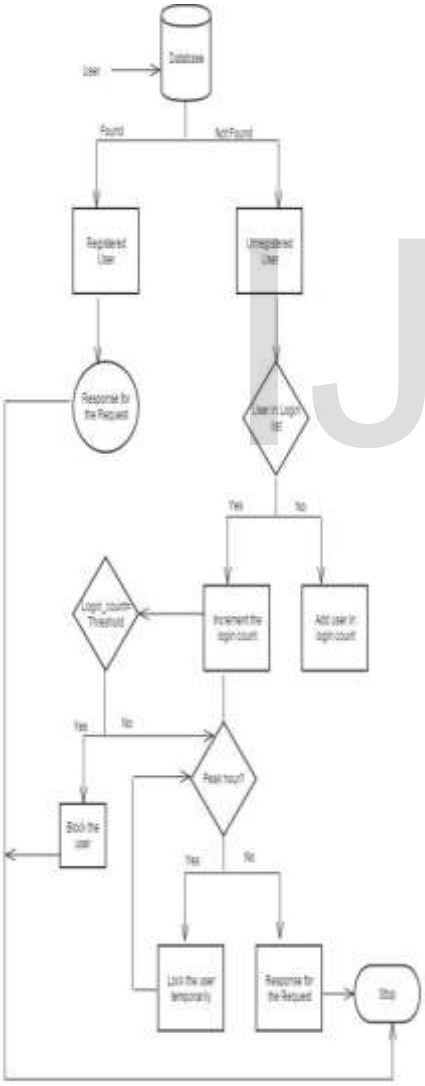

Fig 2.Flowchart for modified cracking algorithm.

4.2 Hop Count Filtration (HCF)

The IP Header contents a 8-bit field called TTL (Time To Live) whose value is decremented by 1 before forwarding packet to next hop. The no of intermediate hops can be calculated using initial TTL value and final TTL value on reaching final destination.
No of hops=initial TTL - final TTL .
The final TTL value is available with the destination.
But the problem in computation of no of hop counts is that not all operating systems uses same initial TTL values.
According to paper [12], most modern Operating Systems use only a few selected initial TTL values, 30, 32, 60, 64, 128, and 255. This set of initial TTL values covers most of the popular Operating Systems, such as Microsoft Windows, Linux, variants of BSD, and many commercial Unix systems. It is observed in paper [12] that most of these initial TTL values are far apart, except between 30 and 32, 60 and 64, and between 32 and 60. Since Internet traces have shown that few Internet hosts are apart by more than 30 hops , which is also confirmed by our own observation, one can determine the initial TTL value of a packet by selecting the smallest initial value in the set that is larger than its final TTL. Hence by comparing the hop counts it is checked whether the packet is legitimate or not.
Algorithm:
Step 1 Get Tf=final TTL and S=Source address from IP packet.
Step 2 Get Hc=Stored correct hop count
Step 2 Ti=30
Step 3 Hops=Ti – Tf.
Step 4 If (Hops==Hc)
Packet is legitimate ,end
Step 5 Change value of Ti and go to step 3//check for different values of Ti(30,32,60,64,128,255)
Step 6 Packet is illegitimate.
Flowchart

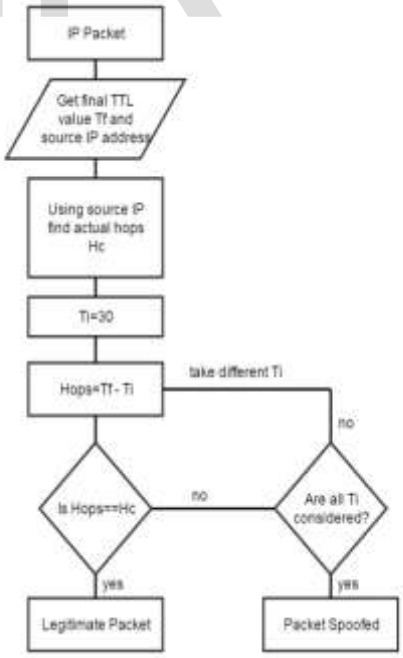

Fig 3.Flowchart for hop count filtering algorithm.

5 COMPARATIVE ANALYSIS

The modified cracking algorithm uses database to store the client's information this increases the space complexity

where as in case of hop count filtering packets are filtered using just the TTL value and source IP address.

In modified cracking algorithm the concept of peak hour helps to control attack during excessive flooding where as if no of packets arrive at the same time in case of hop count filtering it will create an overhead. Each packet's hop count will be computed and compared which will increase the response and th e waiting time.

Modified cracking algorithm is robust as it can be used for any operating system where as hop count filtering is well suited for recent operating systems which uses normal initial TTL values.

The main drawback of modified cracking algorithm is that if the legitimate user access the server more than the threshold set then legitimate user is also blocked.

The drawback of HCF is that if any legitimate user uses the initial TTL values other than normal ones(30,32,60,64,128,255) then user may be incorrectly identified as spoofed. The paper [12] shows that such abnormal initial TTL values are used by old Operating Systems hence can overlooked.

6 CONCLUSION

In Ddos attack,multiple system attack the same target and leads to revenue losses and increase the costs of mitigating the attacks to restore the services. DDoS attacks can be generated in two different ways:direct attack and indirect attack.Attack occurs on various level such as Ddos attack on application layer and Ddos attack on network and transport layer. Http flood and Slowloris belongs to Ddos attack on application layer.SYN Flood,UDP Flood and ICMP Flood belongs to Ddos attack on network and transport layer. Algorithms used to prevent Ddos are Modified Cracking Algorithm and Hop Count Filtration. The modified cracking algorithm uses database and maintains the list of authenticated users and prevents the ddos attack by limiting the access to users or clients. In hop count filtration the TTL value is used to calculate the no of hops. By comparing the values of hops the spoofing can be avoided. The comparative analysis is made of the algorithms for prevention of ddos attack.

REFERENCES

[1] S.T.Zargar, J.Joshi and D.Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DdoS) Flooding Attacks ," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, vo l.15, no . 4, fourth quartar 2013

[2] K.Kuppusamy and S.Malathi, " Prevention of Attacks under DDoS Using Target Customer Behavior ," IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 5, No 2,September 2012

[3] V.Priyadharshini and Dr.K. Kuppusamy,"Prevention of DDOS Attacks using New Cracking Algorithm ," International Journal of Engineering Research and Applications (IJERA) ,ISSN: 22489622 ,Vol. 2, Issue 3, MayJun 2012, pp.22632267

[4] Jamaluddin. M, Touqir Anwar. M, K. Saira and M.Y. Wani,"DDoS SYN Flooding; Mitigation and Prevention ," International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December2014 ,ISSN 22295518

[5] S.Kole, D.K. Gupta, P. Goel, "Simulation of DDoS Attack & Real Time Prevention Algorithm ,"International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July2013 ,ISSN 22295518

[6] R.Singh, S.Lavania, Dr.P. Chaturvedi and N.Dhanda," Intrusion Prevention System Using Unique Application Indentification ,"International Journal of Scientific & Engineering Research, Volume 5, Issue 8,August2014 ,ISSN 22295518

[7] U. Sadhu, A.K.K.Vijaya, K.Seth, Md.T. Riasat, M.Hasan and O.Abuzaghleh ,"A Study on Various Defense Mechanisms Against DDoS Attacks ," International Journal of Scientific & Engineering Research, Volume 6, Issue 5, May-2015 ,ISSN 22295518

[8] K.Pelechrinis, M.Iliofotou and S.V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers ," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO.2,second quarter 2011

[9] N.Hoque, D.K. Bhattacharyya, and J.K.Kalita,"Botnet in DDoS Attacks: Trends and Challenges ,"IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, fourth quartar 2015

[10] S. Liu ,"Surviving Distributed DenialofService Attacks"

[11] L. Arockiam and B. Vani," Security algorithms to prevent Denial of Service (DoS) attacks in WLAN"

[12] H. Wang, C. Jin, and K.G.Shin, "Defense Against Spoofed IP Traffic Using HopCount Filtering ,"IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 1, FEBRUARY 2007