DoS Attack: A Novel Approach to Mitigate

Bibin Vincent[1] Radhika S[2]
[1,2]Department of Electronics and Communication Engineering
[1,2]Vijnan Institute of Science and Technology, Ernakulam, Kerala, India

Abstract— Denial of service attack is one of the major problems faced by the internet today. According to the existing internet architecture, any host can disrupt legitimate traffic by flooding a link between any other hosts. When the traffic send through a link becomes more than the bandwidth of the link, then the router will drop the excess traffic it receives, as the forward link is filled with traffic. As a result, the legitimate traffic may be dropped and in turn the valid user will not be able to access the server and make avail its service. This paper explains the mechanism which is used to mitigate the flooding attacks in the internet. The sender before sending data to the receiver has to obtain the permission to send, from the receiver. This permission is called as capability. Once the permission is obtained, the sender attaches the capability to the data it sends. The routers will check the validity of the capability and the amount of data allowed in a particular time, which will be mentioned in the capability. The routers will process the packet and the check whether the packets are valid or not according to the information available in capability. If the packets are valid the router will forward otherwise will discard the packet. We introduce this mechanism in inter ISP, with one ISP acting as centralized control. When a router in an ISP detects an attack, it will send alert message to the centralized ISP. When the centralized ISP receives the same alert message from different ISP, it will conclude that distributed denial of service attack has occurred. The centralize ISP, then send control messages to other ISPs about the attack and the victim and also inform to reduce the data rate to that victim. Thus, this method will provide a better way to limit denial of service attack and thereby also limit distributed denial of service attack.

Key words: Capability, DoS, DDoS, ISP

I. INTRODUCTION

A denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its intended users. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable [1]. Denial-of-Service (DoS) attacks have become an increasing threat to the reliability of the Internet. The denial of service attack that we emphasis is on flooding attack. The link gets flooded when the total packets approaching the link is greater than the total link capacity or link bandwidth. The approach discussed in this paper is a continuation of an earlier work, which limits the DoS attack [7].

The paper discussed an approach in which a sender should obtain permission from the receiver prior to the transmission of data. This permission is known as capability [7]. If a receiver does not want traffic from a sender, it can simply refuse to grant capabilities to the sender, and the traffic will have lower priority. This allows the receiver to control the traffic it receives and prevent attackers from congesting links by flooding. We introduced this mechanism in inter ISP, thereby limits distributed denial of service attack (DDoS) also. There will be a centralized ISP which decides whether DDoS attack had occurred or not and informs to other ISPs to discard the attackers in their network, if any.

II. RELATED WORKS

The network ingress filtering [1], the earliest method to limit denial of service attack, was not found very effective because of the following reasons: All the ISP's must implement this. If at least 10% of them doesn't implement this, there will be no defence.

A more effective method has been developed to traceback the origin of flooding packets [3]. Here the location of the source is located and the decision is made on the source whether it is a valid source or not. The problem of this method is that only 16 bits are used to store path information. This is not very large and may be insufficient for long paths. Also destination becomes aware of it only if attack sustains for long.

An advance mechanism has been introduced in which the congested router asks the upstream routers to limit the amount of traffic during the time of severe congestion which can be due to flash crowd or denial of service attack [4]. When a router get congested it will ask the upstream routers, from where heavy traffic is arriving, to rate limit the flow of data. There is no way to distinguish between DoS attack and flash crowd in this mechanism. Also this mechanism will trigger only when the link gets congested to a threshold value. Mayday[5] and Secure Overlay Services(SOS)[6] provide much higher security against DoS attack but the implementation cost of these methods are much higher also they add a lot of latency.

III. OVERVIEW: CAPABILITY APPROACH

The capability approach, deals with the provision of providing the permission to send, by the receiver to sender. The receiver will send the permission in the form of capabilities upon the reception of request packet. The request packet is send by the sender. Once the sender received the capability, it can send the data with capability attached to it. When router receives a packet, it will check the capability and if it is valid, the router will forward the packet, otherwise deny.

A. Request Packet

To obtain the capability, the sender should first send the request packet to the receiver. Each router will insert a pre-capability in the request packet on the way to receiver [7]. The format of pre-capability is shown in figure 1.

Timestamp (8 bits)	Hash(src IP, dest IP, in iface, out iface, time, secret) (56 bits)

Fig. 1: Precapability [7]

All rights reserved by www.ijsrd.com

The router secret in the pre-capability is unique for every router. The pre-capability is inserted into the packet by the intermediate routers.

B. Packets with Capabilities

Once the receiver obtained the request packet with pre-capabilities, then the job of receiver is to find the capability. This task is accomplished by hashing the received pre-capability. The format of capability is shown in figure 2.

Timestamp(8 bits)	Hash(precapability, N, T) (56 bits)

Fig. 2: Capability [7]

Initially, the receivers will grand permission to all requests it receives. The sender which received the capability will send data packets with capabilities attached to it. The routers will verify the capability, as it receives, and if found, any sender misbehaving, then the router will discard the packets from that sender. The condition to find the misbehaving sender is based on the capability. In fig 2, N is the number of bytes and T is the time in seconds. It points that the sender can send a maximum of N bytes of data in next T seconds. The routers will keep track of the data send by the senders. The capabilities will expire after its expiry time.

If any sender is trying to send more than the allowed size as mentioned in its capability, the router will simply discard the packet. The capabilities should be bandwidth efficient as well as secure. For this reason 64 bit capabilities are used [7]. When a sender obtains new capabilities from a receiver, it chooses a random flow nonce and includes it together with the list of capabilities in its packets. When a router receives a packet with a valid capability it caches the capability relevant information and flow nonce. Subsequent packets can then carry the flow nonce and omit the list of capabilities [7].

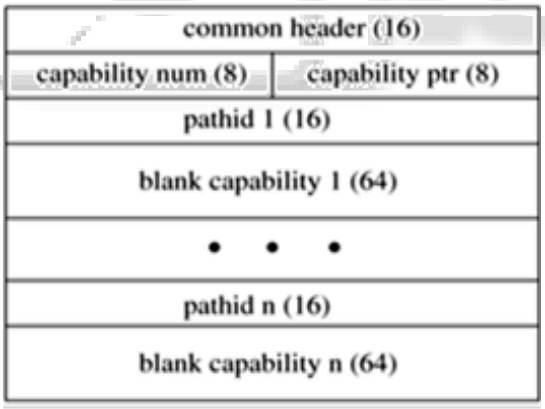


Fig. 3: Request Packet Header [6]

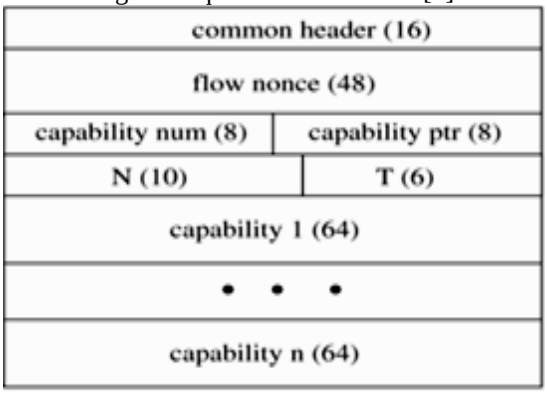


Fig. 4: Regular Packet Header [6]

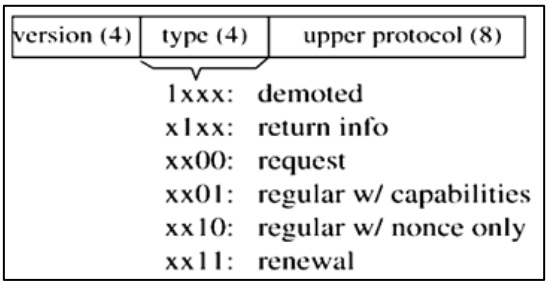


Fig. 5: Common Header [6]

C. Route Changes and Failures

If route change occurs, a packet may arrive at a router that has no associated capability state, either because none was setup or because the cache state or router secret has been lost. When such situation occurs, such packets are demoted to same priority as legacy traffic by changing a bit in the capability header. They are likely to reach the destination under the normal operation of the network that is when there is little congestion. The destination then notifies the sender by setting a bit in the capability header of the next message sent. This tells sender that it must reacquire the capability [7].

D. Packet Headers

Capabilities are piggybacked rather than using separate packets. There are two types of packets, request packets and regular packets. Request packet Carry a list of blank capabilities and path identifiers, which are filled in by routers. Request packets are sent by the sender to the receiver. The request header is shown in figure 3. Regular packets have two formats: packets that carry both flow nonce and a list of valid capabilities and packets carry only a flow nonce. The regular packet header is shown in figure 4.

The common header information is same in both request packet and in regular packet. The format of common header is shown in figure 5. Regular packets have two formats: packets that carry both a flow nonce and a list of valid capabilities, and packets that carry only a flow nonce. A regular packet with a list of capabilities may be used to request a new set of capabilities. We refer to such packets as renewal packets. If a regular packet does not pass the capability check, it may be demoted to low priority traffic that is treated as legacy traffic. Such packets are called demoted packets. We use the lowest two bits of the type field in the capability header to indicate the type and the format of packets: request packet, regular packet with a flow nonce only, regular packet with both a flow nonce and a list of capabilities, and renewal packet. One bit in the type field is used by routers to indicate that the packet has been demoted. A request will be combined with the first packet a sender sends, such as a TCP/SYN. When a destination receives the request, it must decide whether to grant or refuse the transfer. If the destination chooses to authorize, it sends a response with TCP SYN/ACK, else sends TCP RST.

IV. INTER ISP COMMUNICATION

Internet architecture consists of several ISPs connected together. One ISP will act as centralized ISP for controlling other ISPs. One router from each ISP is connected to a router in centralized ISP as shown in figure 6.

All rights reserved by www.ijsrd.com

All ISP will work according to the capability approach explained in the previous section, if both the source and destination belongs to the same ISP. In this case the source will first send the request packet to the intended receiver. On the way to the receiver, the intermediate routers will insert pre-capabilities to the packet. The sender finds the capability upon the reception of request packet and sends the capability to the sender.

As shown in figure 6, routers R2 and R3 are connected to the router R4 in centralized ISP. Attacker A in regional ISP1 is sending traffic more than the allowed amount, which is mentioned in its capability. Router R1 will generate an alert message when it receives more than the allowed amount of data from attacker A. The router R1 will then send this alert message to router R4 in centralized ISP and also it will block any further data from attacker A. Upon the reception of alert message by router R4, it will inform all the routers in other ISPs, to which it is connected about the details of the attacker.

If the source and destination belongs to different ISP, then only the routers in the sender's ISP provides pre-capability and performs packet checking. If the router detects any attack from a sender, it will send an alert message to centralized ISP. The alert message contains source address and destination address. If the number of same alert messages received by centralized ISP exceeds some predefined threshold value, then it will come to a conclusion that, a distributed denial of service attack has occurred. In this case, the centralized ISP informs all the routers, to which it is connected in different ISP, to reduce the data rate to that particular destination or to modify the condition to limit the attack. Modifying the condition can be done by reducing the value of N or T in the capability.

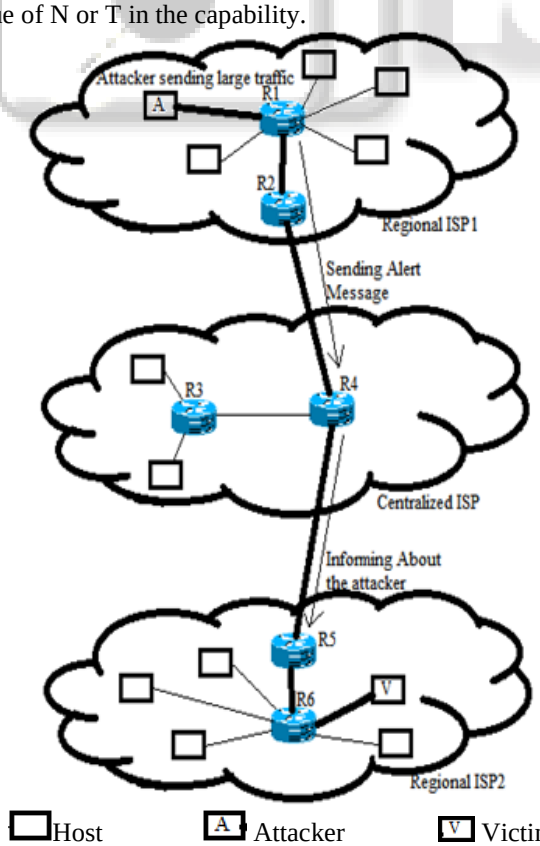


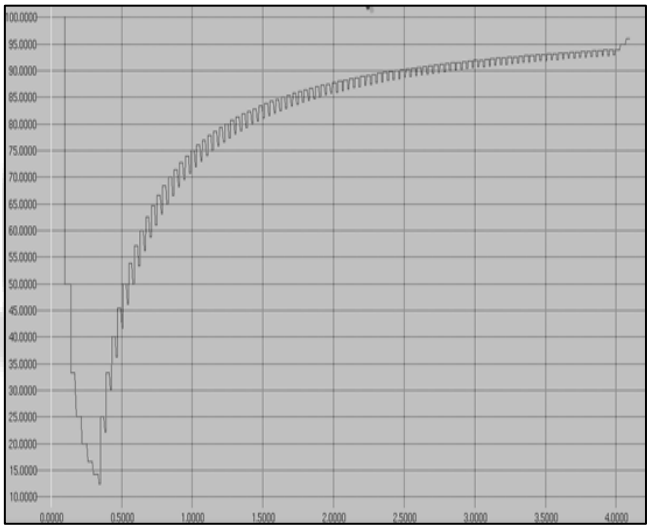
Fig. 6: Inter ISP Communication with Centralized ISP

When this action is triggered, total packets to the destination is reduced. The source address in alert message will inform all other routers in different ISPs about the attacker and also helps to discard the packets coming from that particular source.

V. Simulation Analysis

We used ns-2 to simulate the paper, to see how well this new method will limit the denial of service attack. The topology was setup according to fig 6. The set up consists of two routers and 10 hosts in each ISP. The link between hosts and router are set to 2Mb/s. The link delay is set to 5ms. The router to router link is set to 6Mb/s and the link delay is set to 2ms. The router to router link between inter ISP is set to 10 Mb/s and the link delay is set to 1 ms.

Once the source received the capabilities from the receiver, the former will start to send data with the received capability attached to it. These data are processed at the intermediate routers to check whether all the conditions according to the capabilities are met or not. If any source is misbehaving and is sending more data, then the router will block the data from that source.



Time Fig. 7: Throughput of Valid Source

Figure 7 shows the throughput of valid source. The throughput is measured during the denial of service attack is launched. The method explained in this paper will limit the denial of service attack, and helps the valid packets not being dropped due to congestion. From the graph, it is analyzed that the throughput is approximately 96%. That means 96 percentage of packets sent by the valid source reach the destination even at time of DoS attack.

VI. Conclusion

Various mechanisms have been developed to prevent denial of service attack. Starting from ingress filtering, each method has different methods to limit the DoS attack, and also has the disadvantages. But this approach based on capability dominates all other mechanisms as it first need to get permission from the receiver in order to send any data to that particular receiver. As the routers are able to check the capability, whether it is valid or not, it can discard the packets with invalid capability. In short, this approach limits DoS despite a large number of attackers.

All rights reserved by *www.ijsrd.com*

REFERENCES

[1] Amandeep Kaur, Daljeet Kaur, Gagandeep, "DDOS Attack Detection onWireless Sensor Network: A Review", International Journal of Innovative Research in Science, Engineering and Technology, vol. 6, Issue. 8, August 2017.
[2] P. Ferguson and D. Senie, "Network ingress filtering: Defeating denial of service attacks that employ IP source address spoofing," Internet RFC 2827, 2000.
[3] A. Yaar, A. Perrig, and D. Song,"Pi: a path identification mechanism to defend against DDoS attacks," in Proc. IEEE Symp. Security and Privacy, 2003, pp. 93–107.
[4] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S.Shenker, "Controlling high bandwidth aggregates in the network," ACM CCR, vol. 32, no. 3, Jul. 2002.
[5] A. Keromytis, V. Misra, and D. Rubenstein,"SOS: Secure overlay services," in ACM SIGCOMM, 2002.
[6] D. Andersen,"Mayday: Distributed filtering for Internet services," in 3rd Usenix USITS, 2003.
[7] Xiaowei Yang, David Wetherall and Thomas Anderson, "TVA: A DoS-Limiting Network Architecture", IEEE/ACM Transactions On Networking, vol. 16, no. 6, December 2008

All rights reserved by *www.ijsrd.com*