A Study on High Rate Shrew DDoS Attack

Kanika Minhas
Research Scholar
Chandigarh Engeenering College

Amanpreet Kaur
Assistant Professor
Mtech IT
Chandigarh Engeenering College

Dheerendera Singh, PhD
Professor and Head (CSE)
SUSCET, Tangori Mohali

ABSTRACT
Denial of Service attacks are frequently presenting an increasing threat to the global inter-networking infrastructure in networking area .The algorithm for TCP congestion control algorithm is highly efficient for the various networking areas and operations as well its internal assumption of end-system cooperation results are well prone to attack by high-rate flows. A Shrew attack uses the concept of a low-rate burst which is carefully designed to use the TCP's retransmission timeout mechanism in an unfair way and can affect the bandwidth of a TCP flow in a smooth manner without coming into appearance as an intruder. An Shrew attack has further classifications such as a low rate shrew attack or an high rate shrew attack. A high rated shrew attack uses the concept of timely sending high rate packet stream in low frequency. Such attack can affect the performance of a network to a large extent.

Keywords
DDOS-Distributed Denial Of Service Attack, TCP-Transfer Control Protocol, DNS-Domain Name Services, RTO-Retransmission Time Out.

1. INTRODUCTION
DDoS attacks will first of all try to stop the user from receiving required message at correct time. This type of attack may be improved to give a new form of two sorts of knowledge resource one is on the large volume of information sent over the network for the business process, therefore clean up the server for a few particular quantity of your time another one on the sensitive knowledge like military application i.e. mainly for purpose where more security is required. So this paper focuses a lot of on sensitive knowledge transmission instead of the attack that makes the business server closedown for a few amount of time and leads to large amount of loss. In DDoS attacks, maliciously attackers inject bulk of different packets into the network or forward a similar packet to several of the nodes as attainable.

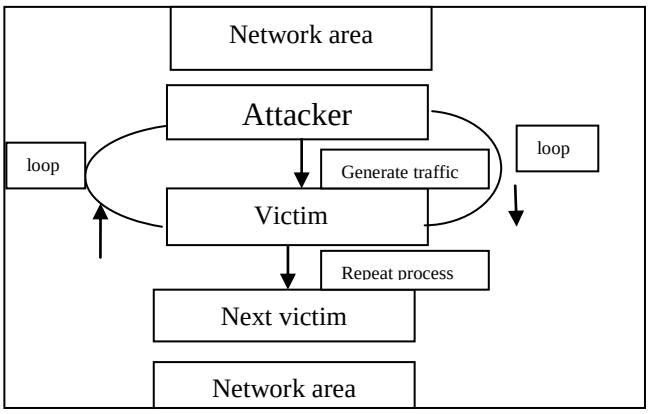

Figure 1: Simple DDOS attack

These attacks are mainly classified into two varieties one is packet flood attack and another is DDoS attack. These types of attacks can consume the information and buffer and prevent all the required packets from reaching the target and therefore affect the network performance and services. Here, aim is to divide and send the important information and retrieve that knowledge by network writing method. Network writing method is used to retrieve, divide and send original knowledge across the network. There are two key techniques random writing and linear writing. The random writing makes network writing practical and also the linear writing is economical for network writing. Attacks may also occur against the root name servers. The infrastructure of the root name server is highly distributed, using the inherent features of DNS like catching, retries, and multiple servers for the same network area with follow-up if one or more fail). The potential throughput is improved by increasing security, decrease in energy transmission, and decrease in delay. Network writing is employed to retrieve the info sent over completely different nodes. During the study for this paper the information has been split and sent over completely different router, then DDOS attacks area unit is known by matching with the edge router information already set. Once attack has been identified, the router performs packet marking and data flow marking over the routing table associated. It shows an alternate path to forward the remaining knowledge to the next neighbor router. As a future work we are able to concentrate in retrieving lost knowledge by exploring the knowledge mining techniques.

One common method of DOS attack involves affecting the target mechanism with external communications requests such that it gives no response to legitimate traffic, or response is very slow. Such attacks will lead to a server overload.

Denial-of-service attack is considered as violations of the Internet Architecture Board's Internet proper use policy, and also violate the rules of the internet services provider. These also commonly lead to constitute violations of the laws of individual nations. Altogether, DOS attack denies the server from providing the information and services required by the legitimate user in a network. Basically attacks are of two types one is an active attack and the other one is a passive attack. Active attack is one which attacks the network area when the network is under process i.e. traffic is being generated and packets are flowing. The passive attack is one in which the user in a network will not come to know that DOS attack has been generated.

2. RELATED STUDY
A. Impact of Denial of Service attack on multihop

"Impact of Denial of Service Attacks on Ad Hoc Networks" studied a novel DoS attack experimented by Jellyfish [1]. The relay nodes are or may be in a disorder, a delay, or there may be a periodic drop in packets that they are expected to forward in a way that leads to end-to-end congestion control protocols.

Such attacks results in increase in the capacity of ad hoc networks as they will stop them from continuing to a particular destination of all multihop flows and provide all resources to one-hop flows that cannot be detected by Jellyfish or Black Holes. It considers the fairness measures and the mean number of hops for a received packet, as an performance measures for a system under attack

B. Router request flooding attack technique

"A Secure on Demand Routing protocol" brought out Secure adhoc destination vector routing protocol that makes use of Hash chains and merkle hash tree[2]. It checked the distance to target and sequence numbers. It uses concept of path weight to find sensible place.
It implements a method referred to as Route-request flooding attack. During this each node features a rate limit to route request even it's asked to relay. But it posses drawbacks like rate limiting may delay a victim's ability to associate attack, and consequently scale back the output of victims.

C. Mitigating technique for nodes in mobile Adhoc Network

"Mitigating technique DDoS attacks exploitation protection nodes in Mobile Adhoc Networks" makes use of two types of nodes in two completely different levels like local protection node and remote protection node[3].
It makes use of messages like anm & amp. It aim to communicate between two completely different levels of nodes, If correct acknowledgement is received then transfer of messages takes place. It has few drawbacks like False positive rate, Different setting of LPN change amount, Assignment of LPN in multi-level network.

D. Evasion Technique

This technique proposed two different but complementary approaches [4]. In the first approach, simply retreat from the attacker, which may be done by either spectral evasion (channel surfing) or spatial evasion (spatial retreats)[4]. The spatial evasion aims to compete more actively with the intruder by adjusting resources, such as power and communication coding in order to achieve communication in the presence of the jammer.

E. classification of IP tarcebacking scheme

"A framework for classifying denial of service attacks," [5] shows a hybrid trace back approach in which packet marking and packet logging are combined and used together in a very novel manner to achieve the simplest of each worlds. It achieved small range of attack packets to conduct the trace back method and small quantity of resources to be allotted at intermediate routers for packet logging .

F. Tracbacking technique using data packet marking and logging

"A more sensible approach for single-packet information processing trace back exploitation packet work and marking," studied the importance of log-based information process trace back in tracing out one packet below the setting where not each AS (Autonomous Systems) supports log-based information processing trace back[6]. It has a drawback as previously existing trace back techniques start from the router to the victim and check its links till they determine that one is employed to hold the attacker's traffic.

After studying the different techniques mentioned above it is clear that each technique has its own different advantage and few drawbacks. In "Impact of Denial of Service Attacks on Ad Hoc Networks" the capacity of the ad Hoc networks can be increased which sometimes also leads to congestion in one hop flow. The router request flooding attack technique may sometimes delay the victims ability to associate attack by limiting the rate and results into lowering the output of the victims. The mitigating techniques for nodes in mobile Adhoc network is technique in which nodes communicate with each other using wireless medium and communicate with each other using network model. On the other hand the Evasion technique works on the two approaches spectral evasion and spatial evasion. These both provide a way of reducing the effect of the attack but do not give the exact directions about the main attacker node. The technique using data packet marking and packet logging was also formed but it had no record about the flow that has been marked previously.

2.1 Low Rate DoS

Unlike the Distributed Denial of Service, low-rate TCP targeted attacks doesn't build use of the many packets to flood the network. It affects the operating mechanism of TCP Timers therefore transfer the output of a system near to zero. These low-rate attacks generate packets in terribly large amount into the network. Therefore the packets send by the attacker will simply stay hidden with the legitimate packets and escape the Anti-Dos traffic watching systems. It's importantly necessary to know the TCP operating procedure before studying this attack. Throughout congestion in TCP, the congestion window is step by step reduced till the network is obvious. Therefore because of congestion the senders rate is reduced that reduces the output. The TCP waits for the Retransmission day trip (RTO) to expire when that the info is distributed once more. Once the congestion is additional, the RTO timer is doubled when that the packets are retransmitted. Therefore throughout an occasional rate attack, once packets are lost, TCP enters RTO. once assaulter is ready to calculate this RTO time and sends assaultive packets to form packet collision and loss, the assaulter will push the TCP into waiting state. Hence, there's no want for flooding the network with packets, however solely send packets once the timer is close to expire and push it once more into the RTO waiting time.

In such type of attack the intruder or the attacker is not known or hidden source. The server will slow down and a point it will be unable to provide the services to the user this wil be the effect of low rate shrew attack.

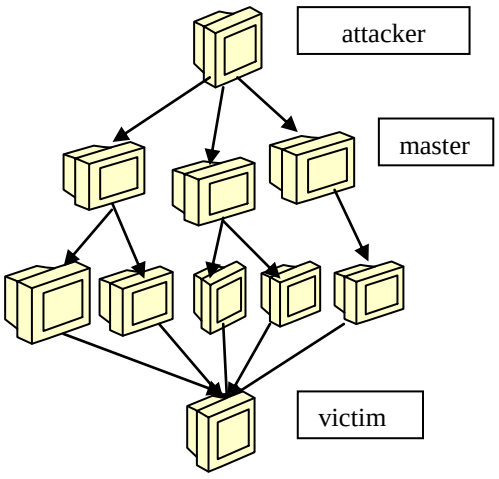

Figure 2. simple DOS attack.

In the congestion control mechanism of TCP, congestion window instantly reduces its size till the network is free from congestion. Therefore congestion in network makes sender's rate low and also lowers the throughput. When network due to traffic is congested, there may be chance to drop packets in the network. When the packets are dropped, the data is resent after the RTO expires. As the congestion exceeds in the network area, the value for RTO timer is doubled after that the packets are retransmitted. Therefore during a low rate attack, an attacker calculates the RTO time and sends low rate attacking packets traffic that creates packet collision at router and this may result of packet loss. Thus the attacker leads the TCP into the waiting state. There is no need for flooding the network with packets, but only send low rate packets traffic when the RTO timer is about to expire and push it again into waiting. This type of attack can escape the traffic monitors due to its low traffic rate and is a serious challenge for the security experts.

2.2 Classification Of DDoS Prevention Mechanism

Various methods of attack prevention many times try to:

- Stop all well known DDoS attacks from being launched in the first place or edge routers.
- It keeps the track of all the machines over Internet up to date with patches and fix security holes.

The techniques are classified as follows:

1. General techniques:

I. Disabling unused services
II. Install latest security patches
III. Disabling IP broadcast
IV. Firewallss
V. IP hopping

2. Filtering technique:

I. Ingress and egress
II. Router based filtering
III. History based IP Filtering
IV. Capability based method

Attack prevention methods are not enough to stop DDoS attacks because they are always prone to simple and mixed attack types for which signatures and patches do not exist in the database. Prevention technique can be classified into following categories:

(i) General Techniques:
These are some common measures for prevention i.e. protection of system, duplication of resources and many other that must be followed by the individual servers and ISPs in order to stop them from becoming the part of DDoS attack process.

(ii) Filtering Techniques:
These techniques include the ingress filtering, the egress filtering, the router based packet filtering, etc.

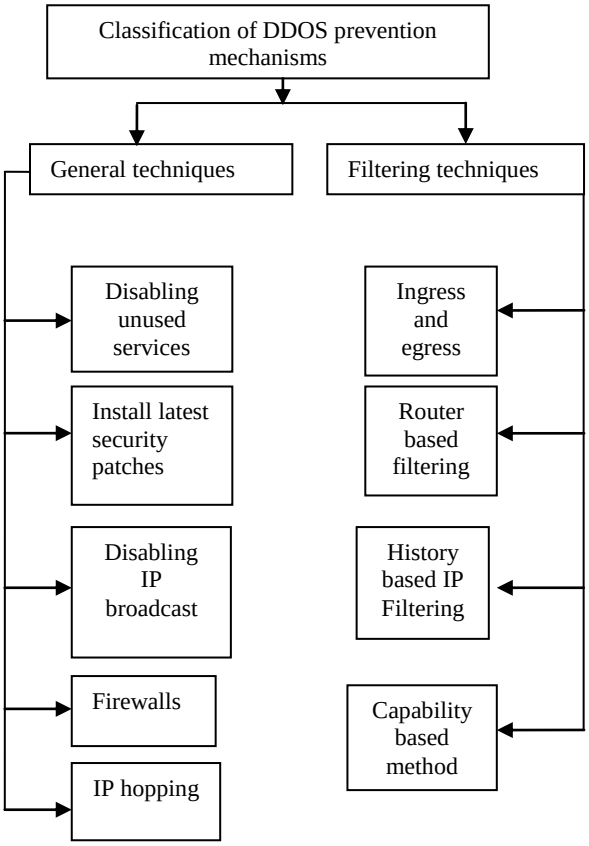

Figure 3. Classifying prevention mechanisms DDOS

A. General Techniques

I) Disabling unused services: if there are less applications and open ports in hosts then there will be less probability to exploit chances of attack by attackers. In case if the network services are not needed or are not used, then the services should be disabled to prevent or stop attacks.

II) Install latest security patches: DDoS attacks exploit chances in the target system. So the known security holes must be removed by installing all the relevant latest security patches that prevents attack in the target system.

III) Disabling IP broadcast: If the host computers and all the neighboring networks disables the IP broadcast only then the defense against attacks that make use of the intermediate broadcast nodes e.g. various flood attacks and Smurf attacks will be successful.

IV) Firewalls: It prevents users from launching simple flood attacks from machines behind the firewall. Firewalls have few simple rules as to allow or remove protocols, ports or IP addresses. But some severe attack e.g. in case if there is an attack on port number 80 (web service) then firewalls cannot prevent such attack because they cannot differentiate good traffic and DOS attack traffic.

V) Global defense infrastructure: It prevents the network from many DDoS attacks by introducing filtering rules in the most important routers of the Internet. As Internet is checked and accessed by various autonomous individual systems according to their own local security policies or rules. such type of global defense architecture is possible only theoretically.

VI) IP hopping: The change in location or IP address of the active server can prevent the DOS attack proactively within a group of homogeneous servers or with a previously defined set of IP address range. The IP address of the victim computer is invalidated by changing it with a new one. After the IP addresses change is completed all internet routers will be informed and edge routers will drop the attacking packets.

B. Filtering Techniques

I) Ingress and Egress filtering:

Ingress Filtering is a mechanism that drops the traffic with IP addresses those which do not match a domain connected to the ingress router. On other hand, Egress filtering is one which ensures that only assigned or allocated IP address space leaves the network.

II) Router based packet filtering:

Route based filtering uses the route information to filter the spoofed IP packets. Its functioning principle is that for each link in the Internet, there is a limited set of source addresses which could lead to traffic generation.

III) History based IP filtering: More often the set of source IP addresses seen during normal operation tends to remain unchanged or stable. On the other hand, in DoS attacks, most of the source IP addresses are unknown .

IV) Capability based method: This method gives destination a way to control the traffic coming towards itself. In this technique, source first sends request packets to its destination. Router marks previously marked capabilities that are added to request packet while passing through the network. The destination may or may not grant permission to the source to send the packets. If permission is granted then destination returns the capabilities, if permission is not granted then it does not supply the capabilities in the returned packet.

3. CONCLUSION

The denial of service attack has various techniques for prevention and detection of the attack. Different types of prevention techniques are discussed here but there is no specific solution for the preventing the attack completely. The low rate shrew attack is the most prone and difficult one to detect as it works in a hidden manner without coming under the eye of the attack preventers. The high rate shrew attack is a type of shrew attaches which work on the principle of high rate packets stream transmitted over an network. There is no such technique yet discovered that can completely remove the attack or prevent the attack.

Therefore, mitigation techniques with some improvement and modification can be formulated based on the concept of counters which can have the record of flow in table form which further can at least reduce the effect of dos attack to some extent and also help to discover the attacker node.

4. REFERENCES

[1] Imad Aad etal, “Transactions on Networking”, “Impact of denial of service attacks on Adhoc networks”,.

[2] Y-C. Hu et al, “A Secure on Demend Routing protocol”, Mobile Communication 2002,pp:12-33.

[3] Minda Xiang et al, “Mitigating DDoS attacks using protection nodes in Mobile Adhoc Networks”,IEEE 2011.

[4] Wenyuan Xu “Jamming Sensor Networks: Attack and Defens Strategies. IEEE Network May/June 2006

[5] A. Hussain, J. Heidemann, and C. Papadopoulos, “A framework for classifying denial of service attacks,” in Proc. ACM SIGCOMM ’03, Karlsruhe, Germany, Aug. 2003, pp. 99–110.

[6] C. Gong and K. Sarac, “A more practical approach for single-packet IP traceback using packet logging and marking,” IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.

[7] Wei-Shen Lai et al, “Using Adaptive bandwidth a location approach to defend DDoS attacks”,ACM 2008.

[8] A. Hussain, J. Heidemann, and C. Papadopoulos, “A framework for classifying denial of service attacks,” in Proc. ACM SIGCOMM ’03, Karlsruhe, Germany, Aug. 2003, pp. 99–110.

[9] B.Al-Duwari andM. Govindarasu, “Novel hybrid schemes employing packet marking and logging for IP traceback,” IEEE Trans. Parallel Distributed Syst., vol. 17, no. 5, pp. 403–418, May 2006.

[10] C. Gong and K. Sarac, “A more practical approach for single-packet IP traceback using packet logging and marking,” IEEE Trans. Parallel Distributed Syst., vol. 19, no. 10, pp. 1310–1324, Oct. 2008.

[11] H. Burch and B. Cheswick, “Tracing anonymous packets to their approximate source,” in Proc. USENIX LISA 2000, New Orleans, LA, Dec. 2000, pp. 319–327.

[12] S. Acedanski, S. Deb, M. Medard, and R. Koetter, “How Good Is Random Linear Coding Based Distributed Networked Storage,” Proc. Workshop Network Coding, Theory and Applications, Apr. 2005.

[13] P.A. Chou, Y. Wu, and K. Jain, “Practical Network Coding,” Proc. Allerton Conf. Comm., Control, and Computing, Oct. 2003.

[14] C. Gkantsidis and P.R. Rodriguez, “Network Coding for Large Scale Content Distribution,” Proc. IEEE INFOCOM, pp. 2235-2245, 2005.

[15] S.Vincent and J.I.Raja, “A Survey of IP Traceback to overcome Denial of service attacks” in Proc. Recent Advances in Networking,VLSI and Signal Processing.

[16] M.Hour Yang and M.Chein Yang, “RIHT- A Novel Hybrid IP Traceback scheme” in Proc. IEEE Trans on Information Forensics and Security, April 2012, vol. 7,no. 2, pg. 789- 797

[17] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, “Practical network support for IP traceback,” in Proc. ACM SIGCOMM2000, Stockholm, Sweden, Aug. 2000, pp. 295– 306.

[18] A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, “Single-packet IP traceback,” IEEE/ACM Trans. Networking, vol. 10, no. 6, pp. 721–734, Dec. 2002.