International Journal of Computer Applications Technology and Research
Volume 3– Issue 7, 420 - 426, 2014, ISSN: 2319–8656

Router Based Mechanism for Mitigation of DDoS Attack- A Survey

Tamana
Department of CE
UCOE, Punjabi University
Patiala, India

Abhinav Bhandari
Department of CE
UCOE, Punjabi University
Patiala, India

Abstract: Today most of the activities like trade, e-commerce are dependent on the availability of Internet. The growing use of internet services in the past few years have facilitated increase in distributed denial of service attack. Due to DDos attacks, caused by malicious hosts secured data communication over the internet is very difficult to achieve and is the need of the hour. DDos attacks are one of the most widely spread problems faced by most of the internet service providers (ISP's). The work which had already been done was in the direction of detection, prevention and trace-back of DDos attack. Mitigation of these attacks has also gained an utmost importance in the present scenario. A number of techniques have been proposed by various researchers but those techniques produce high collateral Damage so more efforts are needed to be done in the area of mitigation of DDos attacks.

This paper focuses on **Distributed Denial of Service attack, surveys, classification and also proposed mitigation techniques revealed in literature by various researchers.**

Keywords: ***distributed denial of service, congestion control, flooding attack, legitimate traffic;***

1. INTRODUCTION

The current Internet is vulnerable to attacks and failures. The past events have illustrated the Internet's vulnerability to distributed denial of service (DDos) attacks. The number of Denial of Service (DoS) and Distributed Denial of Service (DDos) attacks on the Internet has risen sharply in the last several years. Distributed Denial of Service (DDos) attacks have become an increasingly frequent disturbance. Internet Service providers are routinely expected to prevent, monitor and mitigate these types of attacks which occur daily on their networks. Denial of service attack is an active type of attack that affects availability infrastructure of the internet. The DoS which is considered here creates flood which uses bandwidth of the channel to be used by clients for legitimate work from server machine.

DDos attacks are often launched by a network of remotely controlled, well organized, and widely scattered Zombies or Botnet computers that are simultaneously and continuously sending a large amount of traffic and/or service requests to the target system that occupy a significant proportion of the available bandwidth. Hence, DoS attacks are also called bandwidth attacks. The aim of a bandwidth attack is to consume critical resources in a network service. Possible target resources may include CPU capacity in a server, stack space in network protocol software, or Internet link capacity. By exhausting these critical resources, the attacker can prevent legitimate users from accessing the service. A crucial feature of bandwidth attacks is that their strength lies in the volume rather than the content of the attack traffic. This has two major implications:

(1) Attackers can send a variety of packets. The attack traffic can be made arbitrarily similar to legitimate traffic, which greatly complicates defense.
(2) The volume of traffic must be large enough to consume the target's resources. The attacker usually has to control more than one computer to generate the attack traffic. Bandwidth attacks are therefore commonly DDos attacks.
They are very hard to defend against because they do not target specific vulnerabilities of systems, but rather the very fact that the target is connected to the network. All known DDos attacks take advantage of the large number of hosts on the Internet that have poor or no security; the perpetrators break into such hosts, install slave programs, and at the right time instruct thousands of these slave programs to attack a particular destination.

2. DDoS ARCHITECTURE

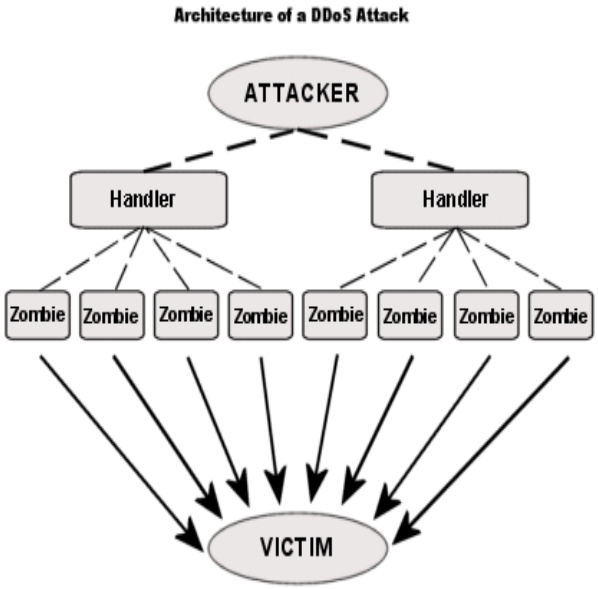

Figure 1 Architecture of DDoS

The remaining part of this paper is organized as follows: Section 2 represents the architecture of DDoS, Section 3 Classifies attacks on various parameters, Section 4 describes Related work, Section 5 elucidates mitigation technique, Section 6 Architecture of explained technique i.e pushback. Section 7 is our conclusion.

3. ATTACK CLASSIFICATION

The types of attack are categorized as following:

• **Classification by degree of autonomy**, that is divided to manual, semi- automatic, or automatic. The automatic methods could be further classified by their communication mechanism (direct, indirect), host scanning strategy (random, hitlist, signpost, permutation, local subnet), vulnerability scanning strategy (horizontal, vertical, coordinated, stealthy), and propagation mechanism (central, back-chaining, autonomous).
• **Classification by exploited weakness**, that is either semantic or brute-force.
• **Classification by source address validity**, that is either spoofed or valid. The spoofed mechanisms could be further divided into routable or non-routable based on address routability or random, subnet, enroute, fixed based on spoofing technique.
• **Classification by possibility of characterization** and if it is characterizable, then whether the traffic is filterable or non-filterable.
• **Classification by attack rate dynamics**, which is either constant, increasing, or fluctuating rate.
• **Classification by the impact on the victim**, which is either disruptive (self, human- or non-recoverable) or degrading.
• **Classification by victim type**, which is application, host, resource, network, or infrastructure.

• **Classification by persistence of agent set**, that can be constant or variable.
The categorization for either known or expected defense mechanisms in [16] is summarized below:
• **Classification by activity level**, which was divided to preventive and reactive. Preventive defense mechanisms were further partitioned to attack prevention (system and protocol security) and DoS prevention (resource accounting and multiplication). Reactive methods were split to either classification by attack detection strategy (pattern, anomaly or third-party) or classification by attack response strategy (agent identification, rate-limiting, filtering, or reconfigration).
• **Classification by cooperation degree**, that can be autonomous, cooperative, or interdependent.
• **Classification by deployment location**, that can be victim network, intermediate network, or source network.
• **Classification by attack response strategy**, which had the following subcategories: agent identification, rate limiting, filtering, and reconfigration.

4. RELATED WORK

Distributed Denial of Service attacks have been a real problem for less than three years, and not much published work exists on the subject. Related work falls into two categories: old work that can also be used in countering DDos attacks, and new work specifically aimed at this task. Originally, it was suggested that DDos attacks could be countered by applying resource allocation techniques on network bandwidth. Integrated Services and Differentiated Services are two approaches aimed at isolating flows with specific quality of service (QoS) requirements from lower-priority traffic. It is not clear if this approach would help; Web traffic, which is a significant fraction of network traffic, is likely to remain best-effort, so it will not be protected by QoS requirements. It is also not clear to what extent compromised sources could fake traffic to show it belonged to QoS-protected flows. There is also an approach that is similar to pushback that was described in an Active-Networks-based defense against flooding attacks. There are many congestion-control mechanisms, which might alleviate some of the effects of congestion due to DDos attacks if only they were globally deployed. Random Early Detect (RED) and its variants tries to identify flows that do not obey TCP-friendly end-to-end congestion control, and preferentially drop them. There is also a large body of work (*e.g.*, Fair Queuing, Class-Based Queuing) aimed at allocating specific fractions of the available bandwidth to each flow so that they all get served. The main problem with these approaches is that packets belonging to DDos attacks do not have readily-identifiable flow signatures, and can thus not be identified by these mechanisms. This is the reason why the concept of Aggregate-based Congestion Control was developed. The common problem that all the tracking techniques are trying to solve is that source addresses in attack packets cannot be trusted, because they are very easy to forge. If all edge routers in the entire Internet were implementing source address filtering,

this task would be greatly simplified. Of course, most machines where the packets are originating have been compromised by an attacker, and their owners do not even know that they are being

used for an attack. Also, even if the hundreds or thousands of machines that an attack is coming from were known, it is not clear what could be done about them. Finally, it has been suggested that intrusion detection systems or firewalls be used to detect an attack in progress, and notify upstream elements accordingly. We view Aggregate-based Congestion Control and Pushback as complimentary to many of these approaches. For example, a good map of the network with reliable historical traffic profiles from traces can be used to determine sudden changes in traffic profiles that could signal an attack, or help determine how to allocate rate limits in pushback messages.
A number of useful related techniques of mitigation have been reported in this literature. Abraham presented a new packet marking approach i.e. Pi (short for Path identifier) in which path fingerprint is embedded in each packet which enables a victim to identify packets traversing same paths[10]. In this scheme each packet traversing the same path carries the same identifier. Path identifier fits in each single packet so the victim can immediately filter traffic after receiving just one attack packet [10]. Xiuli Wang proposed Pushback to mitigate DDos attacks. It is based on improved Aggregate based congestion control (IACC) algorithm and is applied to routers to defend against bandwidth consumption attacks [1]. In this scheme we first match the attack signature of the packet, if it is matched packet is sent to the rate limiter which will decide whether to drop the packet or not. From the rate limiter the packet is sent to the Pushback daemon which will drop these packets with the help of upstream routers. Ruiliang Chen and Jung- Min Park combined the packet marking and pushback concepts to present a new scheme called as Attack Diagnosis. In this scheme an Intrusion Detection System is installed at the victim that detects the attack. The victim instructs the upstream routers to start marking packets with trace back information based on which victim reconstructs the attack paths and finally upstream routers filter the attack packets. Abraham[17] in 2003 and Raktim[2] in 2010 proposed mitigation techniques based on Path identification and attestation; Nicholas[10] in 2007 proposed Client puzzles to mitigate DDos attacks whereas Antonis Michalas[4] 2010. Ruiliang Chen[15] proposed Throttling or rate limit to mitigate these attacks.

5. MITIGATION TECHNIQUE

PUSHBACK - A technique in which routers learn a congestion signature to tell good traffic from bad traffic based on the volume of traffic to the target from different links. The router then filters the bad traffic according to this signature. A pushback scheme is given to let the router ask its adjacent routers to filter the bad traffic at an earlier stage. By pushing the defense frontier towards the attack sources, more legitimate traffic is protected.

6. PUSHBACK ARCHITECTURE

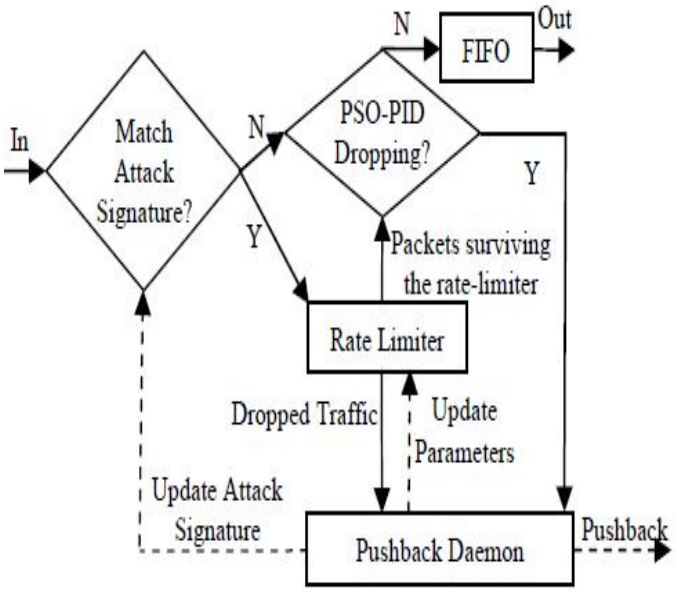

Figure 2 Pushback based on ACC

The input traffic consists of all incoming links of a router. Pushback can be expressed as the following steps:

Step 1 Whether a packet matches attack signature (congestion signature)?
Step 2 *If so*, the packet is sent to the rate limiter, which decides whether a packet is dropped or forwarded according to congestion level. The surviving packets are sent to the PSO-PID drop, go to Step4.
Step 3 *If not*, the packet is sent to the PSO-PID drop directly.
Step 4 The PSO-PID drop decides whether to drop the packet or add the packet to the FIFO output queue.
Step 5 All dropped packets from both the rate limiter and the PSO-PID drop are sent to the Pushback daemon. The daemon requires the upstream routers to drop these packets, periodically updates the parameters of the rate limiter and the attack signature, and also informs the upstream daemons to update theirs.

6.1 Congestion control as a DDos defense and mitigation key:

If we could unequivocally detect packets belonging to an attack and drop just those, the problem would be solved. However, routers cannot tell with total certainty whether a packet actually belongs to a ‘good’ or a ‘bad’ flow; our goal will be to develop heuristics that try to identify most of the bad packets, while trying not to interfere with the good ones. Again, Mahajan et al. introduce the concept of Aggregate-based Congestion Control (ACC); in this context, an aggregate is defined as a subset of the traffic with an identifiable property. For example, “packets to

destination D", "TCP SYN packets", or even "IP packets with a bad checksum" are all potential descriptions of aggregates. The task is to identify aggregates responsible for congestion, and preferentially drop them at the routers.

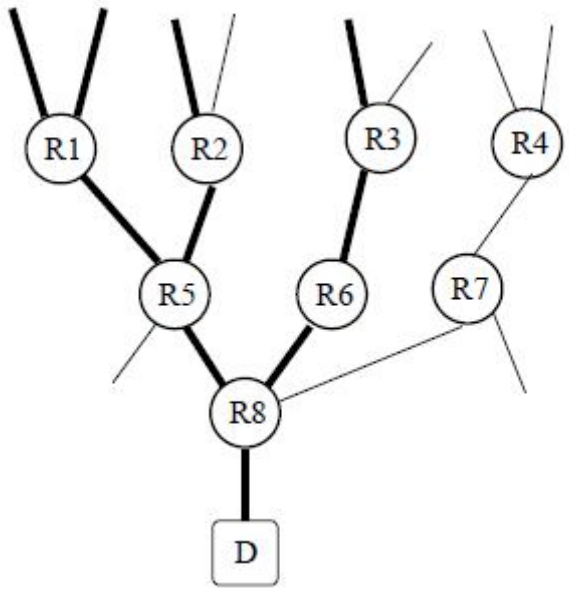

Figure 3 A DDos attack in progress

To illustrate Pushback, consider the network in Figure 3. The server D is under attack; the routers Rn are the last few routers by which traffic reaches D. The thick lines show links through which attack traffic is flowing; the thin lines show links with no bad traffic. Only the last link is actually congested, as the inner part of the network is adequately provisioned. In the absence of any special measures, hardly any non-attack traffic would be reaching the destination. Some non-attack traffic is flowing through the links between R2-R5, R3-R6 R5-R8, R6-R8, and from R8 to D, but most of it is dropped due to congestion in R8 D. Throughout this paper we shall be referring to 'good', 'bad', and 'poor' traffic and packets. Bad packets are those sent by the attackers. Bad traffic is characterized by an attack signature, which we strive to identify; what can be really identified is the congestion signature, which is the set of properties of the aggregate identified as causing problems. Poor traffic consists of packets that match the congestion signature, but are not really part of an attack; they are just unlucky enough to have the same destination, or some other properties that cause them to be identified as belonging to the attack. Good traffic does not match the congestion signature, but shares links with the bad traffic and may thus suffer.

In figure 3, some of the traffic entering R4 is good (the part exiting R7 that is not going to R8), and some is poor, as it is going to D. There may be some good traffic entering R5 from the links above, and exiting from the lower left link, but depending on how congested the links R1-R5 and R2-R5 are, it may suffer. The other links have a mixture of bad and poor traffic. Now, no matter how smart filters R8 could employ, it cannot do anything to allow more good traffic originating from the left side of the graph to reach D. All it can do is preferentially drop traffic arriving from R5 and R6, hoping that more good traffic would flow in via R7. With Pushback, R8 sends messages to R5 and R6 telling *them* to rate-limit traffic for D. Even though the links downstream from R5 and R6 are not congested, when packets arrive at R8 they are going to be dropped anyway, so they may as well be dropped at R5 and R6. These two routers, in turn, propagate the request up to R1, R2, and R3, telling *them* to rate-limit the bad traffic, allowing some of the 'poor' traffic, and more of the good traffic, to flow through.

Table1: Comparative analysis of existing techniques

Name of the technique	Year	Description	Advantages	disadvantages
Egress filtering	IEEE-2010	The IP header of packet leaving are checked for filtering criteria, if criteria is met packet is routed otherwise it is not sent to destination host.	Egress filtering prevents information leaks due to misconfigration, as well as some network mapping attempts.	Decreases performance.
Ingress Filtering	IEEE-2010	In this method filters identify the packets entering the domain and drops the traffic with IP address that does not match the domain prefix connected to a ingress router.	It checks the source IP field of IP packets it receives, and drops packets if the packets don't have an IP address in the IP address block that the interface is connected to.	Keeping track of the many legitimate addresses that can go through a large ISP is next to impossible. It is better to have security as close to the source as possible.
Pushback	IEEE-2008	In this method when the congestion level reaches a certain threshold, sending router starts dropping the packets and illegitimate traffic can be calculated by counting the number of packets dropped for a particular IP address as attackers change their IP address constantly.	Pushback works on aggregates i.e packets from one or more flows carrying common traits. Most effective when attack is non isotrophic. Promising way to combat DDos attack and flash crowds.	The deployment of filters in upstream routers really depends on the downstream router's ability to estimate what fraction of the aggregate comes from each upstream router.
IP Trace Back- Rate Limiting	IEEE-2006	In this Internet traffic is trace back to the true source rather spoofed IP address which helps in identifying attackers traffic and possibly the attacker.	Reduced marking overhead due to ingress filtering. No need path construction algorithm.	Difficult to set threshold values for accurate results.
Path Fingerprint	IEEE-2003	Path Fingerprint represents the route an IP packet takes and is embedded in each IP packet, IP packet with incorrect path fingerprint are considered spoofed.	Path Fingerprint moves Pushback filters close to the attack.	Path Fingerprint is a per-packet deterministic mechanism.

Attack Diagnosis	IEEE-2003	In this scheme an Intrusion Detection System is installed at the victim which detects the attack. The victim instructs the upstream routers to start marking packets with trace back information based on which victim reconstructs the attack paths and finally upstream routers filter the attack packets.	Attack Diagnosis effectively thwarft attacks involving a moderate number of zombies.	It is not appropriate for large scale attacks. Attack Diagnosis trace back and throttles the traffic of one zombie at a time.

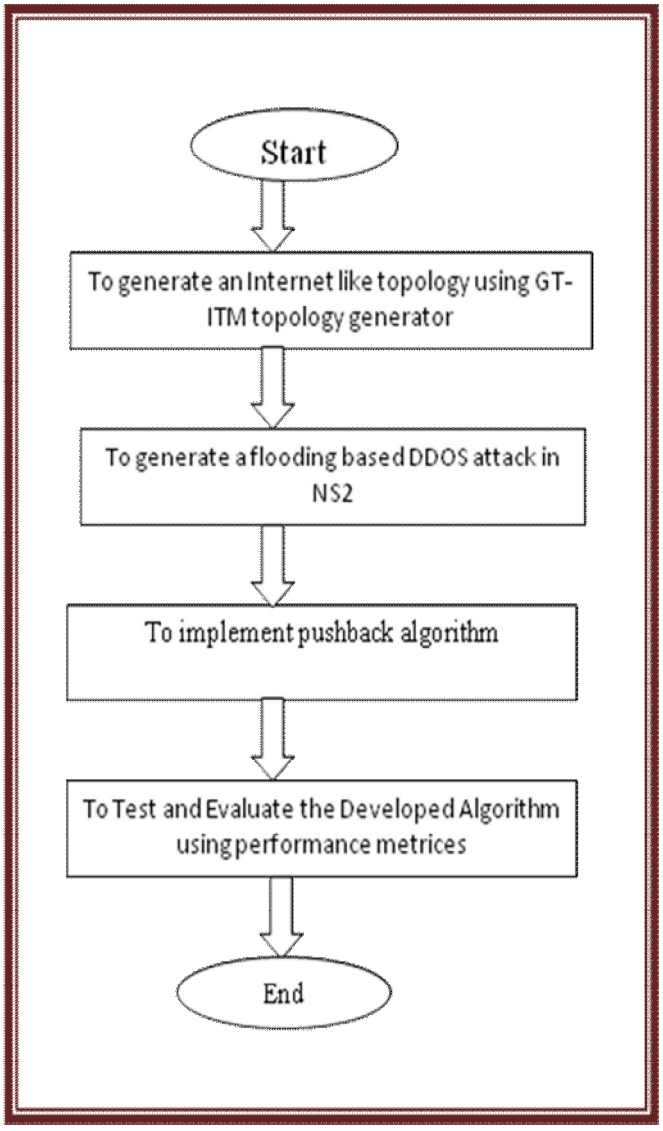

Figure 4 Generic Methodology

The topology generator can generate topology using any standard graph generator (GT-ITM, Tiers etc). Currently it supports GT-ITM topology generator only and converts the topology graph into ns format.

7. CONCLUSION

In this paper, we presented a review on Distributed Denial of Service attack and defense techniques with an emphasis on pushback technique based on router based mechanism. With such enriched attacks, the defense is even more challenging especially in the case of application layer DDoS attacks where the attack packets are a form of legitimate-like traffic mimicking in the events of flash crowds. The major challenge is to distinguish between actual DDoS attack from flash crowd.

Major challenge in the area of mitigation is that testing and evaluation of mitigation technique have not been done in a comprehensive manner. So various experimental Scenario's are needed to be considered for the same.

8. REFERENCES

[1] Xiuli wang "Mitigation of DDos Attacks through Pushback and Resource Regulation" International Conference on Multimedia and Information Technology 2008.

[2] Raktim Bhattacharjee, S. Sanand, and S.V. Raghavan. "Path Attestation Scheme to avert DDos Flood Attacks" International Federation for Information Processing,2010.

[3] Antonis Michalas, Nikos Komninos, Neeli R. Prasad, Vladimir A. Oleshchuk"New Client Puzzle Approach for DoS Resistance in Ad hoc Networks" IEEE 2010.

[4] Nicholas A. Fraser, Douglas J. Kelly, Richard A. Raines, Rusty O. Baldwin and Barry E. Mullins "Using Client Puzzles to Mitigate Distributed Denial of Service Attacks in the Tor Anonymous Routing Environment" ICC, 2007.

[5] Ruiliang Chen, Jung-Min Park "Attack Diagnosis: Throttling Distributed Denial of Service Attacks Close to the Attack Sources" IEEE 2005.

[6] Abraham Yaar, Adrian Perrig, Dawn Song "Pi: A Path Identification Mechanism to Defend against DDos Attacks" IEEE 2003.

[7] http://home.gwu.edu/~ecamposn/software.html Nscript NS-2 scripting tool

[8] http://www.isi.edu/nsnam/vint/ Virtual Internetwork Testbed collaboration

[9] http://www.isi.edu/nsnam/ns/ NS-2 website

[10] Yinan Jing, Xueping Wang, Xiaochun Xiao, Gendu Zhang"Defending Against Meek DDos Attacks By IP Trace-back based Rate Limiting"IEEE 2006.

[11] John Ioannidis, Steven M. Bellovin," Implementing Pushback: Router-Based Defense Against DDos Attacks" AT&T Labs Research

[12] DHWANI GARG," A Comprehensive Survey of Distributed Defense Techniques against DDos Attacks" International Journal of Computer Science and Network Security VOL.9 No.12, December 2009

[13] Chen, S. and Song, Q(2005).Perimeter-Based Defense against High Bandwidth DDos Attacks. IEEE Transactions on Parallel and Distributed Systems 16(6): 526-537