International Conference on Advanced Computing, Communication and Networks'11

DDOS Mitigation Techniques-A Survey

DHWANI GARG

Department of Computer Science and Engineering, Delhi Technological University (formerly Delhi College of Engineering), Shahbad Daulatpur, Main Bawana Road, Delhi – 110042, India

e-mail: dhwanigupta@gmail.com

Abstract

Distributed Denial of Service (DDOS) attacks are one of the most widely spread problems faced by most of the Internet Service Providers (ISP's) today. Mitigation of these attacks has gained utmost importance in the present scenario. A number of mitigation techniques have been proposed by various researchers. They enable us to distinguish between legitimate and illegitimate traffic and accordingly either drops or detects the unwanted packets.Thus enabling us to mitigate the impact of these attacks on the servers.

This paper focussing on Distributed Denial of Service attack, surveys, classifies and also systematically analyzes the various proposed mitigation techniques during the last decades by the researchers. In the present Comparative Analysis of some of the common techniques along with a tabular study of those techniques has also been discussed .

Keywords--- Distributed Denial of Service, Time to Live(TTL), Congestion Control

1. INTRODUCTION

The use of information is gaining widespread importance with the advent of Internet and Information Technology. Today information is considered as an asset and as an asset information needs to be protected from outside attacks. Information can be protected by hiding it from unauthorized access, protecting it from unauthorized changes and making it available to only authorized users. A key research area in this field has been 'mitigation' of DDoS attacks. Mitigation is the process of minimizing the effect of an ongoing attack. One of the simplest way to mitigate these attacks is to simply drop the packets, but this method is very complex. Researchers therefore in proposing, applying and extending these mitigation techniques have countered a large number of these techniques which are applicable in different conditions. For instance, Abraham[10] in 2003 and Raktim[1] in 2010 proposed mitigation techniques based on Path identification and attestation; Nicholas[5] in 2007 proposed Client puzzles to mitigate DDOS attacks whereas Antonis Michalas[14] 2010.Ruiliang Chen[15] proposed Throttling or rate limit to mitigate these attacks. The aim of this paper, therefore, is to survey categorically on the proposed mitigation techniques for DDoS attacks so as to understand the researches conducted by various researchers which will be overviewed in section 2 of this paper. Section 3 will deal with the basic knowledge on DDoS attacks whereas section 4 will deal with the need to mitigate these attacks. The complete set of Mitigation techniques can be captured from the survey of the literature. Conclusions drawn from literature survey, classification and their analysis are being highlighted in Section 5 of this paper.

2. OVERVIEW OF RELATED RESEARCH AND PROJECT

A number of useful related techniques of mitigation have been reported in this literature.

Abraham Yaar 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 [18]. 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 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.

Antonis Michalas, Nikos Komninos, Neeli R. Prasad and Vladimir A. Oleshchuk presented Client puzzle approach to prevent DDoS attacks in ad hoc network. In this approach every node that is trying to contact another node has to solve two puzzles. The first one is a discrete logarithm problem (DLP) and the solution of this puzzle will help the connection initiator to create and solve the second puzzle which is considered to be the most difficult [14].

Biswa ranjan Swain and Bibhudatta Sahoo presented Probabilistic Approach and HCF method to mitigate these attacks. In this approach the researchers have developed a probabilistic approach to find out the number of malicious packets arriving at the server. After calculating the Probability of the packets being malicious we filter the packets from the given no. of packets. They proposed a formula to calculate the Probability which will be discussed in Table1.

Yinan Jing, Xueping Wang Xiao and Gendu Zhang presented IP Traceback based Rate Limiting approach to mitigate DDOS attacks. Max-min fairness algorithm used by previous researchers it is found that it punishes both attackers and legitimate users equally under a meek attack. The survival ratio(i.e the percentage of legitimate packets received by the victim in all legitimate packets) of IP Trace back is very high reaching over 90%, therefore, this algorithm not only regulates the traffic to ensure the victim's load but also improves the survival ratio of legitimate packets.

3. DDOS ATTACKS AND MITIGATION TECHNIQUES

A. DOS and DDOS attacks

Denial of Service attacks are considered when a computer or a network is incapable of providing the desired services. The attacks occur when the services of the network are intentionally blocked by the another user. These types of attack doesn't cause damage to the data but make the resources unavailable to the users.

A DDoS attack uses a large number of computers to cause a coordinated DoS attack against one or more resources. As shown in Figure1,a DDoS attack is composed of given components.

- **a.** The real attacker
- **b.** The handlers or master hosts capable of controlling multiple agents
- **c.** The zombie hosts who generates a stream of packets.
- **d.** Victim or target host

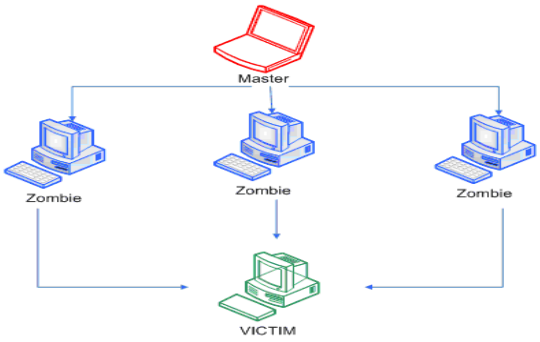

Figure: 1 DDOS attack [21]

The attacker implements several techniques to launch a DDoS attack, it may either send a large number of spurious messages to server and thereby increasing the load on server and forcing it to crash. Another technique an attacker can use is by deleting the response messages to the client from the server, making the server to think that it has not responded to the requests. The attacker can also act as a client and send same client's request to server several times thus overloading the server. A DDoS attack is an attack which prevents the legitimate users from accessing the victim computing resource or the network resource. DDoS is a large scale attack which is coordinated with the help of compromised computers called as 'zombies' which help in making a DDoS attack successful.

A DDoS attack uses many computers to launch a coordinated DOS attack against one or more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting accomplices computers which serve as attack platforms.

B. *Types of DOS Attacks*

- **a. Land Attack:** As shown in Figure 2,in this attack the IP packets having same source and destination address are used which causes the machine to enter into a loop thus launching the land attack.

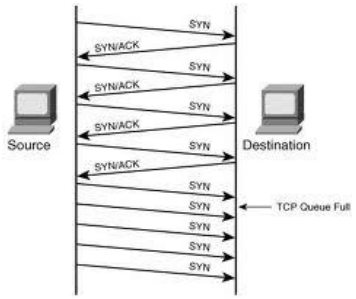

Figure 2: Land Attack [22]

b. Teardrop Attack: This attack uses IP's packet fragmentation algorithm to send corrupted packets to the victim machine thus making it hang. Figure 3,depicts a teardrop attack.

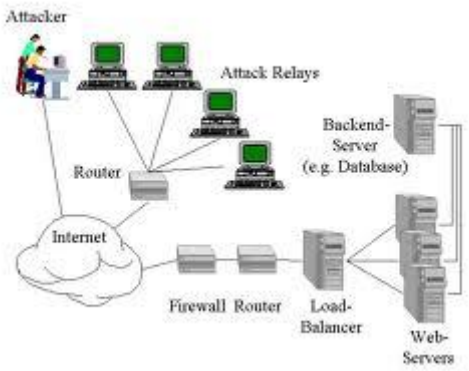

Figure 3: Teardrop Attack [30]

c. Ping of Death Attack: In this attack ICMP ping messages longer than TCP/IP specification of 65536 is used to freeze the system as depicted in Figure 4.

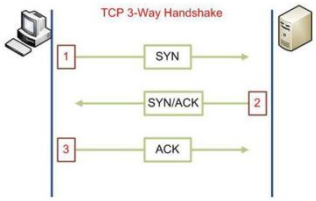

Figure 4: Ping of death attack [24]

d. Flood Attack: In this type of attack, as seen Figure 5, the attacker sends a large amount of traffic that the victim could handle which slows down the victim leading to its crash. This prevents legitimate users from accessing the victim.

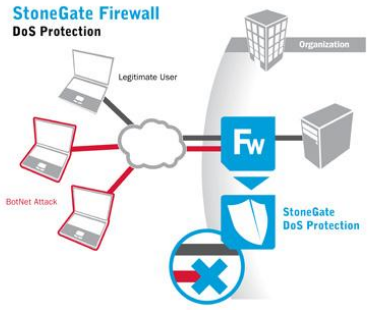

Figure 5: Flood Attack [28]

e. Synchronization attack: The attacker opens multiple half-open connections with the victim and victims keeps them open waiting for acknowledgements and floods the target with SYN messages spoofed to appear to be from unreachable internet address as shown in Figure 6.

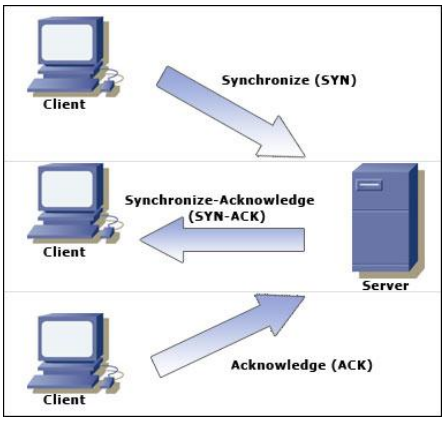

Figure 6: Synchronization attack [27]

f. Amplification attack: From Figure 7,this attack uses the broadcast IP address feature which is found on most routers to amplify and reflect the attack. When the attacker decides to send the broadcast message directly, this attack provides the attacker with the ability to use the systems within the broadcast network as zombies.

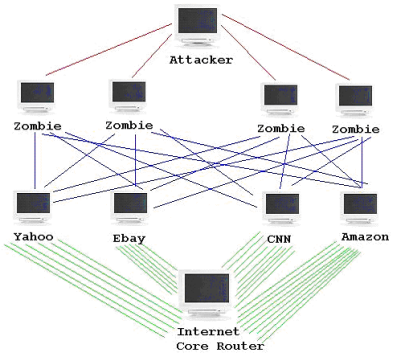

Figure 7: Amplification attack [25]

g. Smurf attack: The attacker sends a ping request to a broadcast address at a third party on the network. This ping request is spoofed to appear to come from the victims network. As shown in Figure 8, the whole network thus acts as a smurf amplifier.

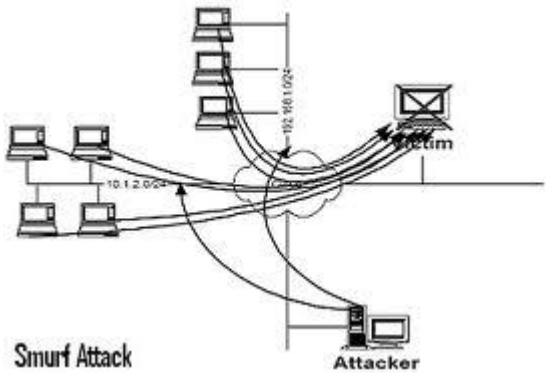

Figure 8: Smurf attack [31]

h. DDOS attack: As shown in Figure 9, in this the attacker gets hold of compromised systems called as zombies that are infected with Trojan horse and virus programs and perform attacks on target machines. It is the most widely used type of attack.

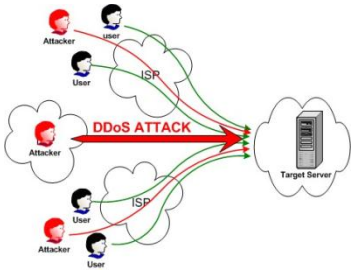

Figure 9: DDOS attack [26]

C. DDOS Countermeasures

DDoS Countermeasures consists of four elements: Prevention, Detection, Mitigation and Traceback.

a. Prevention: This is the most basic step to defend against these attacks. The most important factor is to remain aware and vigilant about the occurrence of these attacks. Although periodic system updates and system patches are important but the users should be aware of the undiscovered weaknesses and understand how these attacks occur .

b. Detection: The most important component while designing the DDOS countermeasures is to determine and establish the methodology of an ongoing attack. In most of the systems applications or software is implemented in order to detect and observe the traffic pattern. The applications detect or observe the anomalies and perform appropriate action and observe which action is to be taken in order to minimize the effect of an attack. Most attacks are detected by server.

c. Mitigation: Mitigation is the process to minimize the effect of an ongoing attack. The simplest and easiest method to perform this is to drop the packets belonging to the attacker. But the basic problem with this strategy is to distinguish between legitimate or illegitimate client. Attackers are making their attacks sophisticated to the extent that it is impossible to determine if a packet belongs to legitimate client or an attacker.

d. Traceback: This method determines the source of the attack and is commonly referred as IP traceback. In most of the DDoS attacks the attacker spoofs the identity of the attack packets by selecting a different source IP address. Before forwarding the packets the server will check the IP address of the packet. Packet Marking is one such method where routers will place a unique mark in the header of each packet which will be used to differentiate between the client and the attacker.

D. Mitigation of DDOS attacks

a. Load Balancing: This technique is accompanied by increasing the bandwidth on critical connections to prevent them from going down in case of an attack. Replicating servers can also be used to for protection in case of a DDoS attack. In this technique the objective is to balance the load on the server in order to protect it from crashing.

b. Throttling: This technique uses Max-Min fair server centric router throttles. In this servers are adjusted with the logic to adjust the incoming traffic to levels that will be safe for the server to process. This will prevent the servers from getting flooded with the malicious packets.

c. Drop Requests: This is the simplest technique where requests are simply dropped when the load increases. The requester may also be required to solve a hard puzzle which will require a large amount of memory space causing them to stop sending DDoS attack traffic.

4. COMPARATIVE ANALYSIS

Collection of mitigation techniques along with their formula is depicted in Table 1 and the definition of the terms used, is discussed below the table. The comparison of two techniques (some of the techniques) is discussed below.

a. Probabilistic HCF vs Simple HCF

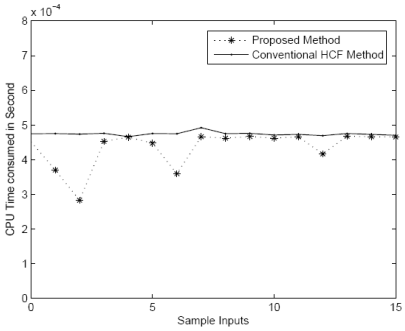

Figure 10:Comparison of time taken b/w probabilistic HCF and simple HCF [18]

i) In Simple HCF we check each and every packet and let them enter to the server on the confirmation of their non-maliciousness.

ii) But in Probabilistic HCF we calculate the probability of number of packets being malicious and according to that we mitigate the attack.

iii) From figure10, it is proposed that Probabilistic HCF saves time as a resource as compared to simple HCF. It takes less time than the HCF method because of the complexity of the execution of HCF method because it takes two steps in execution (alert and action states).

iv) In HCF the computation and memory overhead is there but in probabilistic approach the overhead is less as we does not check all the packets.

v) In Probabilistic approach very less amount of packets get undetected as probability is used as a measure to detect malicious packets whereas HCF method used the threshold for considering the packets to be malicious

b. Attack Diagnosis Vs Parallel Attack Diagnosis

i) Attack Diagnosis effectively thwarft attacks involving a moderate number of zombies but it is not appropriate for large scale attacks.

ii) Parallel attack diagnosis can throttle traffic coming from a large number of zombies simultaneously.

iii) Attack Diagnosis trace back and throttles the traffic of one zombie at a time.

iv) Parallel Attack Diagnosis can handle multiple attack paths simultaneously.

v)Attack Diagnosis (AD) does not use the XOR field , but Parallel Attack Diagnosis (PAD) uses it for distinguishing different attack paths.

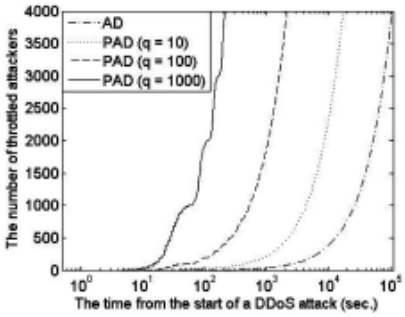

Figure 11:No. of throttled attacks over time [15]

c. Source Router Preferential dropping vs Pushback Technique

i) Source Router Preferential Dropping (SPRD) controls attack faster than Pushback as seen in Fig. 11.

ii) In SPRD good packets are dropped only during the initial few seconds of the attack.

iii) Pushback involves collateral damage to good traffic during the whole attack period due to its local Aggregate congestion control (ACC's) inability to differentiate good packets from bad packets.

iv) SRPD drops more attack packets than Pushback. SRPD dropping outperforms Pushback as it minimises adverse effects on legitimate traffic and increasing attack packet drop rates.

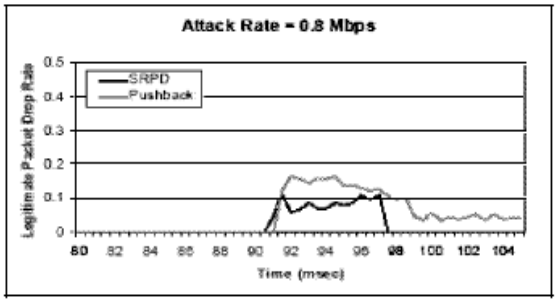

Figure 12: Legitimate packet drop rate compared to pushback [14]

d. Path Fingerprint Vs Pushback Technique

i) Pushback works on aggregates i.e packets from one or more flows carrying common traits.

ii) Path Fingerprint is a per-packet deterministic mechanism[10].

iii) In Pushback there is a problem of identifying common traits as DDoS packets share little similarity whereas in Path Fingerprint each router identifies the common markings helping in better identity of particular traits.

iv) Path Fingerprint moves Pushback filters close to the attack

e. HCI-MPR vs HCF

i) Computational time of HCI-MPR is less as compared to HCF as seen in Fig.13.

ii) In HCI-MPR there is improved processing power of server and minimum loss of resources as compared to HCF.

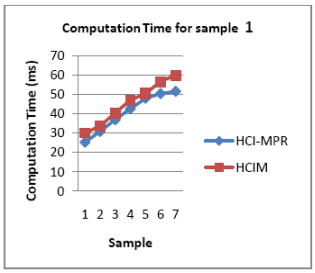

Figure 13:Graph showing computation time [14]

5. CONCLUSION

This survey presents existing mitigation techniques for DDoS attacks. In particular I have analyzed the attacks based on the severity of attack, position of attack and Time to Live field of attack. The survey does not concentrate over any specific concerns of the technique as one technique is not sufficient to gain quintessence of DDoS attack. Hence, the survey results indicate that carefully chosen technique can be very beneficial in DDoS attacks and can provide useful information to Internet Service Providers for decision making and future improvements.

The survey provides a historical view and uncovers gaps in existing research. The presented literature is based on a uniform representation of existing techniques and is aided by storing the information in a structured way for ease of processing

Table 1: Comparison of Mitigation Techniques

S. No	Name of Technique	Year	Formula Used	Description
1.	HCI-MPR	IEEE-2011	$P(m, l) = e^{-\lambda p}(p^m \lambda^m)/m!.e^{-\lambda(1-p)}(1-p)^l \lambda^l / l!$	This is based on mathematical equations to find the malicious packets and proposes an inspection algorithm to mitigate DDOS attack.
2.	Client Puzzle	IEEE-2010	$\Pi(n) = \frac{1}{2}.[\frac{n}{3}].n+\frac{1}{8}.(-1)^{1+n}.\frac{3}{4}.[\frac{n}{3}]$	In this method cryptographic puzzles are generated that a client must answer correctly before it is given services, which pushback the load to the source of an attack in case of overload.
3.	Egress Filtering	IEEE-2010	d $e_f^{(t+1)} = (q_f^{\sim(t+1)} - S_{max}(r_f^{\sim(t+1)}) + / q_f^{\sim(t+1)}$	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.
4.	Ingress Filtering	IEEE-2010	$di_f^{(t+1)} = (1-\frac{ce_f^{(t)}}{ci_f^{(t)}(1+\beta_i^{(t)}}$)+	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.

5.	Preferential Dropping	IEEE-2010	$d_i^{(n+1)} = (1- \frac{l_i^{(n)}}{m_i^{(n)}} \frac{}{(1+\beta_i^{(n)}} +$	This method simply drops the request when the load increases either by server or router with the requester making the request system to solve a hard puzzle.
6.	Probabilistic HCF	IEEE-2009	P{N1=n,N_2=m} = $e^{-\lambda p}\frac{(\lambda p)^n}{n!} e^{-\lambda(1-p)}\frac{(\lambda(1-p)^m}{m!}$	In this method the average arrival rate of packets and error probability of packets is used to calculate the number of malicious packets then filtering is done using the HCI-Algorithm.
7.	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.
8.	Distributed Throttling	IEEE-2007	$r_s := (L_s + U_s) / f(k)$	This method sets the routers that access the server with a logic to adjust the incoming traffic to levels that are safe and prevent flood attacks.
9.	IP Trace Back- Rate Limiting	IEEE-2006	$N_L F_L < B < (N_A+N_L)$ x F_L	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.
10.	Path Fingerprint	I IEEE-2003	P[M(R_i→R1)=M(R_j→R2))∧ (M(R1→R3)=M(R2→R3))]=$\frac{1}{2^{2n}}$	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.
11.	Simple HCF	Int. Jrnl Database Theory and Apln.	------	Hop Count value i.e. difference between initial TTL and final TTL of the spoofed IP packets is not consistent with legitimate IP packet is used to build HCF table which helps in mitigating DDOS attacks.

λ – poisson's distribution of packets arrival rate at the server

p – probability of malicious packets arriving at the server

1-p – probability of non-malicious packets arriving at the server

n – joint probability of malicious packets among total traffic

m - joint probability of non-malicious packets among total traffic

M – total no. of packets arrived with poisson's distribution λ

$de_f^{(t+1)}$ - dropping probability for egress filtering

$q_f^{(t+1)}$ - no. of packets from ISP

$r_f^{(t+1)}$ – no. of packets to the ISP

S_{max} – maximum packet symmetry during normal case

$di_f^{(t+1)}$ - dropping probability for ingress filtering

S_{min} - minimum packet symmetry during normal case

r_s - throttle rate

L_s - Lower water mark

U_s - upper water mark

f(k) – estimate of no. of throttle points

$l_i^{(n)}$ - no. of packets in hash table 2

$l_i^{(n)}$ - no. of packets in hash table 2

M (Ri) – n-bit marking that router Ri inserts

$d_i^{(n+1)}$ - dropping probability for n+1 time

$m_i^{(n)}$ - no. of packets in hash table 1

N_L - pieces of legitimate flows

F_L - rate of flow of packets

N_A - pieces of attack flows

B – bandwidth

N_2- no. of non malicious packets

N_1- no. of malicious packets

6. REFERENCES

[1] Palvinder Singh Mann, Dinesh Kumar "A Reactive Defense Mechanism based on an Analytical Approach to Mitigate DDoS Attacks and Improve Network Performance" International Journal of Computer Applications, January 2011.

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

[3] Ping Du, Akihiro Nakao "Mantlet Triology: DDOS Defense Deployable with Innovative Anti-Spoofing, Attack Detection and Mitigation" IEEE 2010.

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

[5] Ping Du, Akihiro Nakao "DDoS Defense Deployment with Network Egress and Ingress Filtering" IEEE 2010.

[6] Biswa Ranjan Swain, Bibhudatta Sahoo "Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method" IEEE International Advance Computing Conference, March 2009.

[7] V.Praveena, N.Kiruthika "New Mitigating Technique to Overcome DDOS Attack" World Academy of Science, Engineering and Technology 2008.

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

[9] Gal Badishi, Amir Herzberg, Idit Keidar, Oleg Romanov, Avital Yachin "An Empirical Study of Denial of Service Mitigation Techniques" IEEE 2008.

[10] 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.

[11] Ruiliang Chen, Jung-Min Park, Randolph Marchany "A Divide –and-Conquer Strategy or Thwarting Distributed Denial-of-Service Attacks" IEEE 2007.

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

[13] Rajesh Sharma, Krishan Kumar, Kuldip Singh, R.C. Joshi "Shared Based Rate Limiting; An ISP level Solution to deal DDOS Attacks" IEEE 2006.

[14] Yinghong Fan, Hossam Hassanein and Patrick Martin "Proactive Control of Distributed Denial of Service Attacks with Source Router Preferential Dropping" IEEE,2005.

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

[16] W.J. Blackert, D.M. Gregg, A.K. Castner, E.M. Kyle, R.L. Hom, R.M. Jokerst "Analyzing Interaction Between Distributed Denial Of Service Attacks and Mitigation Technologies" IEEE 2003.

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

[18] Fasheng Yi, Shui Yu, Wanlei Zhou, Jing Hai and Alessio Bonti,"Source based Filtering Scheme Against DDOS Attacks" International Journal Database of Theory and Application.

[19] Antonio Challita, Mona El Hassan, Sabine Maalouf, Adel Zouheiry "A Survey of DDOS Defense Mechanisms"

[20]http://www.google.co.in/imgres?imgurl=http://www.wittenborg-online.com/file.php/1/pictures/network/ddos_attack.gif&imgrefurl.

[21]http://www.google.co.in/imgres?imgurl=http://swordfish.files.wordpress.com.

[22]http://4.bp.blogspot.com/_TJ01Mn2k4FE/TQJchrhhFCI/AAAAAAAAAJ4/QSyC33ywHfY/s1600/DoS2.jpg.

[23] http://www.trainsignaltraining.com/wp-content/uploads/2009/05/4.jpg.

[24] http://www.securitydocs.com/images/papers/dosfaq-1.png.

[25]http://www.blogymate.com/BlogPost/BlogyMate.com-BlogTH2612011111741.jpg.

[26]http://www.stonesoft.com/export/pics/stonesoft.com/pics/identity_5_0/ILLUS_dos-protection-fw.jpg.

[27] http://www.learn-networking.com/wp-content/oldimages/syn-flood.jpg.

[28] http://tula.bofh.ru/articles/539/2005-dos3.gif.

[29]http://t0.gstatic.com/images?q=tbn:ANd9GcT-e5P-LHlvR5qCNOTYbFoT_Gm26xqUWbS6bnWc4Vqesnsm7nNC

[30]http://t0.gstatic.com/images?q=tbn:ANd9GcR0_m3Cj9ecMlWm-U-idgekYUyu7BS1XthU26FWqvMcWmamODmL