DDoS Attacks Impact Analysis on Web Service Using Emulation

Daljeet Kaur[1] and Monika Sachdeva[2]
[1]*Department of Computer Science & Engineering,*
SBS State Technical Campus, Ferozepur, Cantt–152001, India
E-mail: [1]Daljeetkaur617@gmail.com, [2]Monika.sal@rediffmail.com

***Abstract*—Banking, transportation, power, health, and defense are essential services being operated and these operations now days are being replaced by affordable and easily accessible Internet-based applications. It is all because of rapid growth and success of Internet in every sector. Unfortunately with it's the rapid growth, count of attacks has also increased incredibly fast. A Denial of Service (DoS) attack is a malicious effort to keep endorsed users of a website or web service from accessing it, or limiting their ability to do so. A Distributed Denial of Service (DDoS) attack is another type of DoS attack in which many computers are used to cripple a web page, website or web-based service. The services are severely degraded and hence lot of business loses are incurred due to these attacks. To objectively evaluate DDoS attack's impact, and the effectiveness of a potential defense, we need precise, quantitative and comprehensive DDoS impact metrics that are applicable to web services. To meet this requirement, the cyber-DEfense Technology Experimental Research (DETER) testbed has been developed. In this paper, we have created dumb-bell topology and generated background traffic as Web traffic. Different types of DDoS attacks are also launched along with Web traffic by using attack tools available in DETER testbed. Finally impact of DDoS attack on Web server is measured in terms of metrics such as throughput, percentage link utilization, and normal packet survival ratio (NPSR).**

Keywords: Terms-Internet, Distributed Denial of Service Attack, throughput, Percentage Link Utilization, Attack Traffic, Legitimate Traffic

I. INTRODUCTION

The main objective of Internet was providing an open and scalable network, which could offer easy, fast and inexpensive communication mechanisms, it was indeed very successful in accomplishing this particular goal. During Internet design, the functionality aspect was of much concern rather than security, which leads to several security issues that create a room for various attacks on the Internet. Internet security can be defined in terms of confidentiality, authentication, message integrity and non-repudiation out of which Availability is one of its main aspect. Attacks such as denial of service and its variant distributed denial of service attack target the availability of services on the Internet. Threat to the Internet availability is a big issue which is hindering the growth of online organizations those rely on having their websites 100% available to visitors, users and customers. A Denial of Service attack is an attempt by a person or a group of persons to decay an online service. This can have serious consequences, especially for companies like Amazon and eBay which rely on their online availability to do business. Recently there have been some large scale attacks targeting high profile internet sites [1, 2, 3, and 4]. Consequently, there are now a lot of efforts being made to come up with mechanisms to detect and mitigate such attacks. Even though the first denial of service attacks did not take place a long time ago (tools that automate setting up of an attack network and launching of attacks, started appearing in 1998), there is an abundance of denial of service attacks that have been used. Broadly speaking the attacks can be of three forms. a) Attacks exploiting some vulnerability or bug in the software implementation of a service to bring that down. b) Attacks that use up all the available resources at the target machine. c) Attacks that consume all the bandwidth available to the victim machine. The third type of attacks is called bandwidth attacks. A distributed framework becomes especially suited for such attacks as a reasonable amount of data directed from a number of hosts can generate a lot of traffic at and near the target machine, clogging all the routes to the victim.

II. DDOS ATTACK OVERVIEW

The normal functionality of the Internet servers is disabled during DDoS Attacks by exhausting resources. An attacker can create a huge volume of attack traffic and consume the bandwidth of the bottleneck link in the victim network to exhaust its resources. Due to the lack of application of security engineering in the development of operating systems and network protocols, hackers are provided with lot of insecure machines on internet. These insecure and unpatched machines are used by DDoS attackers as their army to launch attack [5]. An attacker or hacker gradually implants attack programs on these insecure machines. Depending upon sophistication in logic of implanted programs, these compromised machines are called Masters/Handlers or Zombies and are collectively called bots and the attacked network is called botnet in hacker's community. Hackers send control instructions to masters, which in turn communicate it to zombies for launching attack. The zombie machines under control of masters/handlers (running control mechanism), transmit attack packets as shown in Fig. 1, which converge at victim or its network to use up either its communication or computational resources [6].

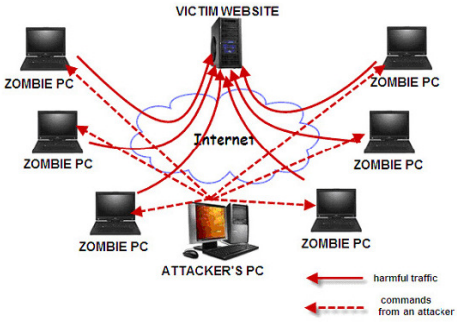

Fig. 1 DDoS Attack Architecture

Mirkovic *et al.* [6] and Peng *et al.* [7] have categorized DDOS attacks into two broad categories: flooding attacks and vulnerability attacks. Flooding DDoS attacks consume resources such as network bandwidth by overwhelming bottleneck link with a high volume of packets. Vulnerability attacks use the expected behavior of protocols such as TCP and HTTP as an advantage to the attacker. The computational resources of the server are tied up by seemingly legitimate requests of the attackers results in preventing the server from processing transactions or requests from authorized users.

Flooding DDoS is basically a resource overloading problem. The resource can be bandwidth, memory, CPU cycles, file descriptors and buffers etc. The attackers bombard the scarce resource(s) by utter flood of packets. In Figure 2, a flood of packets is shown, which congests the link between ISP's edge router and border router of victim domain [8].

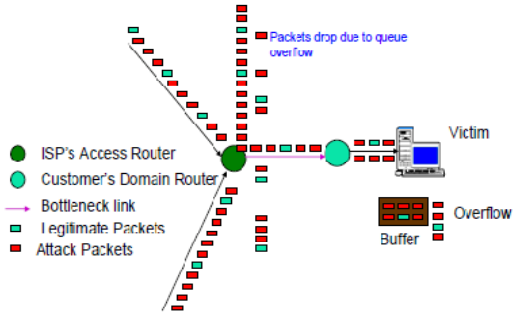

Fig. 2 Packets Drop During DDoS Attack

Attack packets keep arriving at user machine as per the distribution fixed by attacker, whereas legitimate clients cut short their packet sending rates as per flow control and congestion signals. A state comes when whole of bottleneck bandwidth is seized by attack packets. Thus, service is denied to legitimate users due to narrow bottleneck bandwidth. However, resources of connecting network are not a problem in case of commercial servers as these are hosted by the ISPs, quite close to their backbone network with high bandwidth access links. But server resources such as processing capacity, buffer limit etc., are put under stress by flood of seemingly legitimate requests generated by DDoS attack zombies [8]. Each request consume some CPU cycles. Once the total request rate is more than the service rate of server, as shown in Figure 2, the requests start getting buffered in the server, and after some time incoming requests are dropped due to buffer over run. The congestion and flow control signals [9], [10] force legitimate clients to decrease their rate of sending requests, whereas attack packets keep coming. Finally, a stage comes when only attack traffic is reaching at the server.

III. Related Work

The impact metrics of DDoS attack are closely related with measuring effectiveness of DDoS defense approaches. At present there are no benchmarks [11], [12] in terms of effective metrics for evaluating the impact and defense strategies of DDoS attack. Most of the existing strategies compare good-put under attack, without attack, and with defense [13]. Some of recent measurements [14] have also emphasized on response time. Evaluating the normal packets survival ratio proves to be the most important metrics as it clearly reflects accuracy of the defense and normal packet loss index [15], [16]. For measuring the impact of DDoS, Jelena *et al.* [17], [18] have used metric of percentage of failed transactions (transactions that do not follow QoS thresholds). They have defined an application specific threshold-based model for the relevant traffic measurements. When a measurement exceeds its threshold, it indicates poor services quality. But the absolute duration of threshold cannot be set since transaction duration depends on the volume of data being transferred and network load. Server timeout has been used as a metric in [19]. However collateral damage in terms of legitimate traffic drop is not indicated. Sardana *et al.* [20] have used good put, mean time between failure and average response time as performance metrics whereas Gupta *et al.* [21] have used two statistical metrics namely, Volume and Flow to detect DDoS attacks. As per [17] metrics such as good-put, bad-put, response time, number of active connections, ratio of average serve rate and request rate, and normal packet survival index [16] properly signal denial of service for two way applications such as HTTP, FTP and DNS, but not for traffic like media applications that is sensitive to one-way delay, packet and jitter.

IV. Experiment Setup

We used SEER (Security Experimentation Environment) GUI BETA6 environment [22] [23] to evaluate our metrics in experiments on the DETER testbed using. The test bed is located at the USC Information Sciences Institute and UC Berkeley, and allows security researchers to evaluate attacks and defenses in a controlled environment.

A. *Experimental Topology*

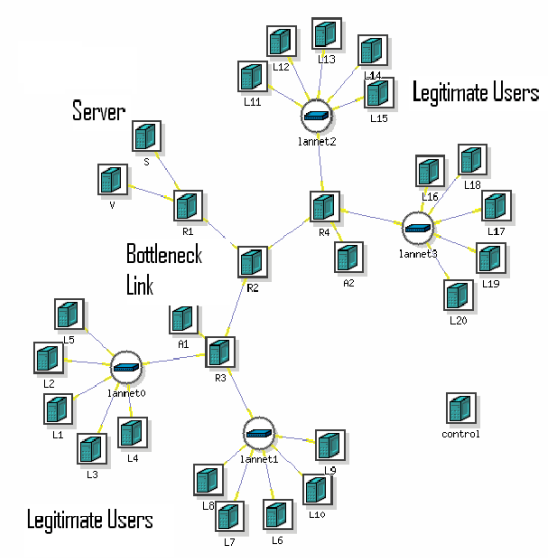

Fig. 3 Experimental Topology

Figure 3 shows the experimental topology and Figure 4[24] shows our experimental topology definition for Web applications in which R1, R2, R3 and R4 are routers, node S is server and L1-L20 are clients. They send legitimate requests to server S via router R1 and R2.

```
set ns [new Simulator]
source tb_compat.tcl
#Create the topology nodes
foreach node { V S R1 R2 R3 R4 L1 L2 L3 L4 L5
L6 L7 L8 L9 L10 L11 L12 L13 L14 L15 L16 L17
L18 L19 L20 A1 A2 control }
{
#Create new node
set $node [$ns node]
#Define the OS image
tb-set-node-os [set $node] FC4-STD
#Have SEER install itself and startup when the
node is ready
tb-set-node-startcmd [set $node] "sudo python
/share/seer/v160/experiment-setup.py Basic"
}
#Create the topology links
set linkRV [$ns duplex-link $V $R1 100Mb 3ms
DropTail]
set linkRS [$ns duplex-link $S $R1 100Mb 3ms
DropTail]
set linkRA1 [$ns duplex-link $A1 $R3 100Mb 3ms
DropTail]
set linkRA2 [$ns duplex-link $A2 $R4 100Mb 3ms
DropTail]
set linkRR3 [$ns duplex-link $R2 $R3 100Mb 3ms
DropTail]
set linkRR4 [$ns duplex-link $R2 $R4 100Mb 3ms
DropTail]
set linkRR2 [$ns duplex-link $R2 $R1 1.5Mb 0ms
DropTail]
set lannet0 [$ns make-lan "$L1 $L2 $L3 $L4 $L5
$R3" 100Mb 0ms]
set lannet1 [$ns make-lan "$L6 $L7 $L8 $L9 $L10
$R3" 100Mb 0ms]
set lannet2 [$ns make-lan "$L11 $L12 $L13 $L14
$L15 $R4" 100Mb 0ms]
set lannet3 [$ns make-lan "$L16 $L17 $L18 $L19
$L20 $R4" 100Mb 0ms]
$ns rtproto Static
$ns run
```

Fig 4 Experimental Topology Definition

The bandwidth of all links is set to be 100 Mbps, and the bandwidth of bottleneck link (R1-R2) is 1.5 Mbps. Node A1 in topology acts as attacking node and it sends attack traffic to server S via router R1 and R2. The link between R1 and R2 is called bottleneck link. The purpose of attack node is to consume/congest the bandwidth of bottleneck link so that legitimate traffic could not get accessed by the server S.

We have generated a random network consist of Web clients, servers and attack source. In our emulated network, multiple legitimate clients connected with server and one attack source is used as DDoS flooding attacker. This emulates the real situation of DDoS flooding attack.

B. *Legitimate Traffic*

In our experiment, Web traffic is used where we have used 20 legitimate client nodes which send requests to the server S for 1-30 seconds and then 61-90 seconds with following thinking time. The configuration of said traffic parameters used to send legitimate traffic is demonstrated in Table I:

TABLE 1 EMULATION PARAMETERS USED IN EXPERIMENT

Parameter	Values
Client	L1-L20
Server	S
Attack Host	A1
Thinking Time	Minmax(0.01,0.1)
File Size	Minmax(512,1024)
Emulation Time	90sec
Bottleneck Bandwidth	1.5Mb
Access Bandwidth	100Mb
Legitimate Request Time	1-30 sec and 61-90 sec
Attack Time	31-60 sec
Attack Type	DDoS Packet Flooding
Server Delay	3ms
Access Link Delay	3ms
Backbone Link Delay	0ms

C. *Attack Traffic*

We have generated DDoS attack by using packet flooding attack. Node A1 launches attack towards S and thus consumes bandwidth of bottleneck in link R1-R2. UDP protocol is used for launching attacks. Further attack types flat, ramp-up, pulse and ramp-pulse are used in our experiment. Attack traffic from A1 starts at 31st second and stops at 60th second. Then we have analyzed impact of DDoS attacks on Web service. Table II shows attack parameters used in our emulation experiment. We have generated following flooding attack types:

Flat Attack: The high rate is achieved and maintained till the attack is stopped.

Ramp-up Attack: The high rate is achieved gradually within the rise time specified and is maintained until the attack is stopped.

Ramp-down Attack: The high rate is achieved gradually and after high time it falls to the low rate with in low time.

Pulse Attack: The attack oscillates between high rate and low rate. It remains at high rate for high time specified and then falls to low rate specified for the low tie specified and so on.

Ramp-pulse Attack: It is a mixture of Ramp-up, Rampdown and Pulse attack.

TABLE 2 ATTACK PARAMETERS USED IN EXPERIMENT

Attack Type	Flooding	Flooding	Flooding	Flooding
Attack Source	A1	A1	A1	A1
Attack Target	S	S	S	S
Protocol	UDP	UDP	UDP	UDP
Length Min	50	50	100	50
Length Max	100	50	150	50
Flood Type	Flat	Ramp-up	Pulse	Ramp-Pulse
High Rate	500	300	200	200
High Time	100	5000	5000	5000
Low Rate	300	100	50	50
Low Time	0	7000	4000	7000
Rise Shape	0	1.0	0	1.0
Rise Time	0	10000	0	10000
Fall Shape	0	0	0	1.0
Fall Time	0	0	0	10000
Sport Min	57	57	57	57
Sport Max	57	57	57	57
Dport Min	1000	1000	1000	1000
Dport Max	2000	2000	2000	2000
TCP Flags	SYN	SYN	SYN	SYN

V. RESULTS AND DISCUSSIONS

The effect of DDoS attacks on the performance of FTP service is analyzed below:

A. *Througput*

A backbone link is attacked to force the edge router at the ISP of victim end to drop most legitimate packets during a DDoS attack. In Figure 5 and Figure 6 we have concentrated on the throughput in terms of good-put and bad-put to get the measure of actual loss. So throughput is divided into good-put and bad-put respectively. Good-put is defined as no. of bits per second of legitimate traffic that are received at the server whereas bad-put gives no. of bits per second of attack traffic that are received at the server.

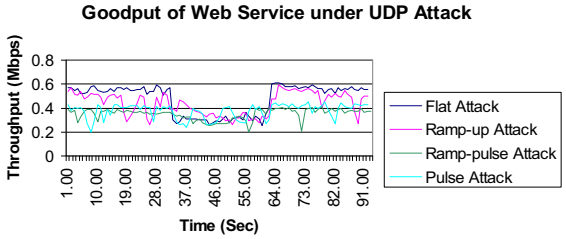

Fig. 5 Good-put of Web Traffic through Bottleneck Link During UDP Attack.

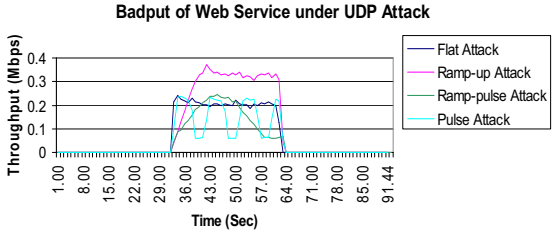

Fig 6 Bad-put of Web Traffic Through Bottleneck Link during UDP Attack

B. *Backbone Link Utilization*

Backbone Link utilization is defined as percentage of bandwidth that is carrying legitimate traffic. As shown in Figure7 Backbone Link Utilization is nearly 100% without attack. During attack, it drops more than 50%.

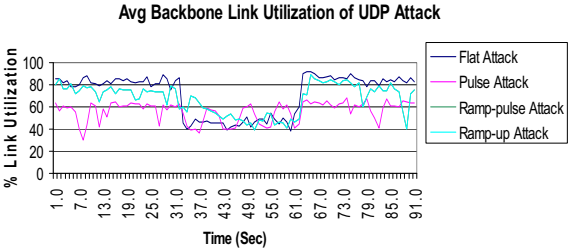

Fig. 7 Average Bottleneck Bandwidth Utilization in Web Service

C. *Normal Packet Survival Ratio (NPSR)*

NPSR is defined as ratio of good-put and bad-put. This is percentage of legitimate packets that can survive during attack. NPSR should be high. We can measure impact of attack as a percentage of legitimate packets delivered during the attack. If this percentage is high, service continues with little interruption. NPSR starts decreasing with increased rate of attack traffic and as bandwidth of the link is limited, so legitimate packets starts dropping. As shown in Figure 8100% legitimate

packets are delivered without attack but during attacks, only 50% legitimate packets are delivered.

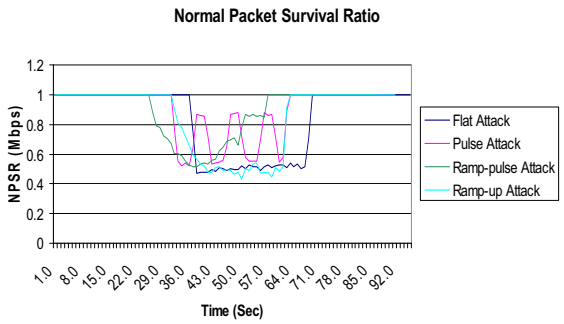

Fig. 8 Average Ratio of Legitimate Web Packets Survival during UDP Attack

ACKNOWLEDGMENT

We would like to express our gratitude to all those who gave us the possibility to complete this experimental work. We are extremely thankful to all the colleagues and faculty members for their constructive criticism and guidelines.

REFERENCES

[1] CNN. Cyber-attacks batter Web heavyweights, February2000.
[2] CNN.Immense. Network assault takes down Yahoo, February
[3] Netscape. Leading web sites under attack, February 2000 "Journal of Computer Science
[4] CERT coordination center. Denial of Service attacks
[5] J. Mirkovic. D-WARD: Source-End Defense AgainstDistributed Denial-of-service Attacks, Ph.D. Thesis,University of California, Los Angeles, 2003.
[6] J. Mirkovic and P. Reiher. "A Taxonomy of DDoSAttack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communications Review,Volume 34, Issue 2, pp. 39-53, April, 2004.
[7] T. Peng, C. Leckie, and K. Ramamohanarao. "Survey of Network-Based Defense Mechanisms ountering the DoS and DDoS Problems", ACM Computing Surveys, Vol. 39, No. 1, Article 3, April 2007.
[8] K. Kumar, R.C. Joshi, and K. Singh. "An Integrated Approach for Defending against distributed Denial-of-Service (DDoS) Attacks", IRISS-2006, IIT Madras.
[9] M. Kisimoto. Studies on Congestion ControlMechanisms in the Internet–AIMD-based WindowFlow Control Mechanism and Active Queue Management Mechanism, Master Thesis, Osaka University, 2003.
[10] S. Floyd and K. Fall. "Router Mechanisms to Support End-to-End Congestion Control," Lawrence Berkeley Laboratories Technical Report, 1997.
[11] J. Mirkovic and P. Reiher, A University of Delaware Subcontract to CLA.
[12] J. Mirkovic, E Arikan, S. Wei, R. Thomas, S. Fahmy, and P. Reiher. "Benchmarks for DDOS Defense Evaluation", In Proceedings of Military Communications Conference (MILCOM), pp. 1-10, 2006.
[13] Y. You. "A defense framework for flooding based DDoS Attacks", M.S. Thesis, Queen's University, Canada.
[14] J. Mirkovic,P. Reiher,S. Fahmy,R. Thomas, A. Hussain, S. Schwab. "Measuring denial Of service", 2nd ACM workshop on Quality of protection QoP, pp. 53–58, 2006.
[15] A. Hussian, S. Schwab, R. Thomas, S. Fahmy, and J. Mirkovic. "DDoS Experiment Methodology", DETER Community Workshop, June 15-16, 2006.
[16] K. Kumar. Protection from Distributed Denial of Service (DDoS) Attacks in ISP Domain, Ph.D. Thesis, Indian Institute of Technology, Roorkee, India, 2007.
[17] J. Mirkovic, A. Hussain, B. Wilson, S. Fahmy, P. Reiher, R Thomas, W. M. Yao, S Schwab. "Towards user-centric metrics for denial-of-service measurement" in proceedings of the 2007 workshop on Experimental computer science, San Diego, California.
[18] J. Mirkovic, S. Fahmy, P. Reiher, R. Thomas, A. Hussain, S. Schwab,and C. Ko. "Measuring Impact of DoS Attacks"In Proceedings of the DETER Community Workshop on Cyberscurity,Experimentation, June 2006.
[19] C. Ko, A. Hussain, S. Schwab, R. Thomas, and B. Wilson. "Towards systematic IDS evaluation", in Proceedings of DETER Community Workshop, pp. 20-23, June 2006.
[20] A. Sardana and R.C. Joshi, "An Integrated Honeypot Framework for Proactive Detection, Characterization and Redirection of DDoS Attacks at ISP level," International Journal Of Information Assurance and Security (JIAS), 3 (1), pp. 1-15, March 2008.
[21] B.B. Gupta, R. C. Joshi, and M. Misra, "An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach," Journal of Information Assurance and Security 3(2), 102-110, June 2008.
[22] M.Sachdeva, G.Singh, K.Kumar, K.Singh,"Journal of Information Assurance and Security 5 (2010)", pp. 392-400. International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).
[23] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab, "Experiences With DETER: A Testbed for Security Research.
[24] D. kaur, M. Sachdeva and K. Kumar," Impact Analysis of DDoS Attacks on FTP Services" International Conference on Recent Trends in Information, Telecommunication and Computing, ISBN 978-94-91587-21-3,pp. 220-228, March 21, 2014.