Performance Measurement of Web Services under UDP Attack using GENI Testbed

Rinkel Mehto
Department of Computer Science and Engineering
SBSSTC, Frozepur, Punjab, India

Dr Monika Sachdeva
Department of Computer Science and Engineering
SBSSTC, Frozepur, Punjab, India

Sunny Behal
Department of Computer Science and Engineering
SBSSTC, Frozepur, Punjab, India

Abstract-Today, Internet is the primary medium for communication which is used by number of users across the Network. As one of the major security problems in the current Internet, a denial-of-service (DoS) attack always attempts to stop the victim from serving legitimate users. A Distributed Denial of Service (DDoS) attack is a DoS attack utilizing multiple distributed attack sources. The majority of DDoS attacks target the network and transport layers. During study of all work we came to know that most of the researchers had done similar work on Simulation based techniques. In this paper, we have measured the performance of Web services under DDoS attack using Real time testbed (GENI). GENI is Global Environment for network innovations. In this work, GENI test bed has been explored and topology has been created on which HTTP legitimate traffic and UDP attack traffic have been generated. Another application i.e User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. Avg.Response Time , Avg.Round Trip Time (RTT) and Throughput in terms of good-put and bad-put is computed to measure impact of DDoS attacks on Web HTTP services.

Keywords – DDoS attacks, Throughput, GENI, Response Time, Internet, Availability, UDP, Traffic.

I. INTRODUCTION

Internet attacks have become a fact of life, with data breaches of high profile companies and organizations making headline in the news practically on a daily basis. One common type of internet threat is a denial of service (DoS) attack. With no advance warning, a DDoS attack can easily exhaust the computing and communication resources of its victim within a short period of time.Resources of a network such as network bandwidth and network switches are mostly the victims of DDoS attacks [1]. Denial of Service means an Attack that is an attempt by an attacker to exhaust the resources available to a network, application or services so that the authorised users can't gain access. The majority of attacks are commonly referred to as DDoS attack , Such attacks are DoS attacks launched from multiple different hosts simultaneously; and in the case of a botnet, could be 10s, 100s or 1000s of machines globally distributed [2]. In a DoS attack, a attacker uses a single Internet connection to either exploit a software vulnerability or flood a target with fake requests usually in an attempt to exhaust server resources (e.g., RAM and CPU). Confidentiality, authentication and non repudiation are desirable security aspects for secure communication. More people are aware that availability and access of control are also urgent requirements of secure communication because of the notorious Denial of Service (DoS) attacks that provide by the illegitimate users into a network, host, or other piece of network infrastructure to harm them, especially it is done against the frequently visited websites of a number of high-profile companies or government websites [3]

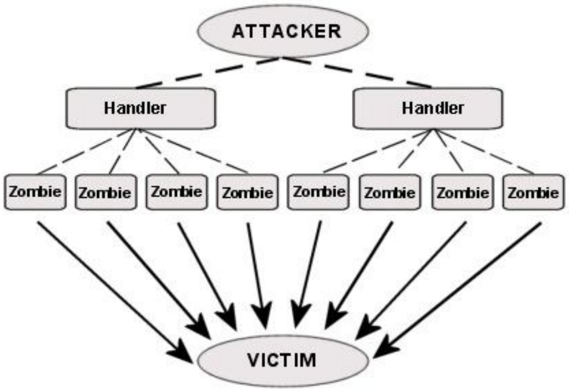

Figure 1. Architecture of DDoS Attack

In Fig.1 attacker send attack programs on insecure machines. These compromised machines are Zombies that are also known as bots and the attack network is called botnet in hackers community depending upon sophistication in logic of implanted programs. In this, hackers send control instructions to masters, which then intercommunicate it to zombies for launching attack [4]. Typical DDoS attack has two stages, the first stage is to compromise susceptible systems that are accessible in the Internet and then install attack tools in these compromised systems. This is known as turning the computers into zombies. In the second stage, the attacker sends an attack command to the zombies through a secure channel to launch a bandwidth attack against the targeted victim [3]. The current attacks on some cyber sites like Amazon, Yahoo, e-Bay etc and their resultant disruption of services have uncovered the weakness of the Internet to Distributed Denial of Service attacks. It has been observed through reports that TCP is used in more

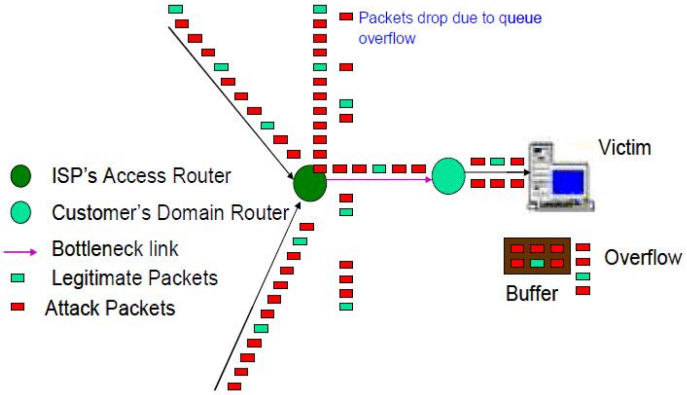

Figure 2. Packets drop under DDoS Attack

than 85 per.of the DoS attacks [5]. The UDP flooding attack is the most commonly used attack. It consists of a stream of spoofed and UDP packets directed to a listening ports of the victim. The Web servers are not only but also any systems connected to the Internet providing UDP and TCP based network services, such as FTP servers or Mail servers, are also susceptible to the UDP and TCP SYN flooding attacks [6].

In this paper We have used GENI testbed to evaluate our metrics in experiments using Linux [3]. GENI stands for Global Environment for Network Innovation. GENI provides a virtual laboratory for networking and distributed systems research and education. GENI is well suited for exploring networks at scale, thereby promoting innovations in network science, security, web services and applications. GENI is a new, nationwide suite of infrastructure supporting ”at scale” research in networking, distributed systems, security, and novel applications. It is supported by the National Science Foundation, and available without charge for research [7].

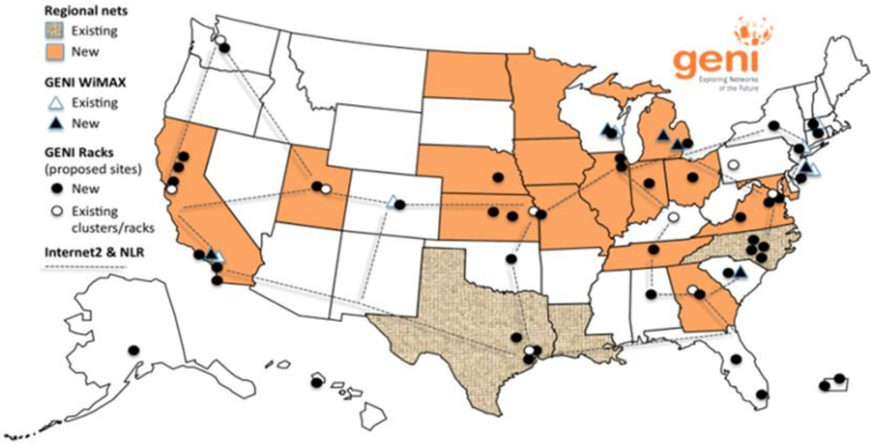

Figure 3. Architecture of GENI

Why should we use GENI for Experiment?

A. *Large-scale experiment Infrastructure:-*

GENI can potentially provide you with many resources than is typically found in any one laboratory. It gives you access to hundreds of widely distributed resources including compute resources such as virtual machines , and network resources such as links, switches and WiMax base stations.

B. *Non-IP connectivity across resources:-*

GENI allows you to set up Layer 2 connections between compute resources and run your own Layer 3 and above protocols connecting these resources.

C. *Deep programmability:-*

With GENI you can program not only the end hosts of your experimental network but also the switches in the core of your network. This allows you to experiment with novel network layer protocols or with novel IP-routing algorithms.

D. *Reproducibility:-*

You can get exclusive access to certain GENI resources including CPU resources and network resources. This gives you control over your experiments environment and hence the ability for you and others to repeat experiments under identical or very similar conditions.

E. *Instrumentation and measurement:-*

GENI has two instrumentation and measurement systems that you can use to instrument your experiments. These systems provide probes for active and passive measurements, measurement data storage and tools for visualizing and analyzing measurement data [8].

GENI Key Concepts

1) Project :- A project organizes research in GENI, containing people and their experiments. In GENI project is created and led by a single responsible individual user. A project may have many experimenters as its members and an experimenter may be a member of many projects. The Project user is accountable for all actions by project members in the context of the project. GENI provide a portal for a individuals researcher. In GENI has provide a unique account for the researcher that's why Only authorise faculty and senior members of an organization can be project leads (eg. students cannot lead the project).

2) Slice :- GENI Slice is the unit of isolation for experiments. In GENI, all the experiments lives in a slice. Only experimenters who are members of a slice can make changes to experiments in that slice. A container for resources used in an experiment. GENI experimenters add GENI resources to slices and run experiments that use these resources. An experiment can only use resources in its slice. The Project Lead is automatically a member of all slices created in a project. A slice is a container in which you perform multiple experiments such as make topologies for taking some nodes.

3) GENI Aggregates :- In Geni, Aggregate provides resources to GENI experimenters. For example, a GENI Rack at a university is an aggregate; GENI experimenters may request resources from this aggregate and add them to their slice. Different aggregates provide different kinds of resources. Some aggregates provide networking resources that experimenters can use to connect compute resources from multiple aggregates [9].

II. RELATED WORK

To measure the effect of DDoS defense approaches, analyzation of impact of DDoS attack is very important [10]. As per no benchmarks are available for measuring effectiveness of DDoS defense approaches [11]. Most of the researchers works on the existing strategies compare good-put and normal packet survival with and without attack and with defense [12]. Some of defense approaches have calculated the response time [13]. By measuring normal packets survival ration proves to be most important because it clearly reflects accuracy of the defense and normal packet loss [14]. In many papers, researchers have used percentage of failed transactions [15] (transactions that do not follow QoS thresholds) as a metric to measure DDoS impact [16]. They define a threshold-based model for the relevant traffic measurements, which is application specific. It indicates poor services quality when a measurement exceeds its threshold. One another metric [17] i.e Server timeout has been also used. Because legitimate traffic drop i.e. collateral damage is not indicated. Researchers have used good put, mean time between failure and average response time as performance metrics [13]. As per metrics such as goodput, bad-put, response time, number of active connections , ratio of average serve rate [18] and request rate, and normal packet survival index properly signal denial of service for two way applications such as HTTP, FTP and DNS, but not for media traffic that is sensitive to one-way delay, packet and jitter [19].

III. RECENT DDOS ATTACK INCIDENTS

While most people agree the Internet of Things is a magnificent concept, it also poses a significant security risk. The majority of Internet-connected devices is not equipped with proper security precautions. In theory, any device connected to the internet can be hacked by unathorised user and taken over by malicious individuals. Over the past few months, Lizard Squad hacked CCTV cameras and webcams all over the world to execute its DDoS attacks. Targets ranged from banks to governments, and gaming sites to ISPs. .A botnet of over 25,000 bots lies at the heart of recent DDoS attacks that are ferociously targeting business around the world. More exactly, were talking about massive Layer 7 DDoS attacks that are overwhelming Web Servers, occupying their resources and eventually crashing websites [20].

IV. PERFORMANCE METRICS

In present work, distributed denial of service attacks are different than the kinds that we saw at the dawn of the millennium when the threat emerged. They're becoming more nuanced and they could result in a lot more than a downed web servers. In order to measure the impact of DDoS attacks on different web services, we have performed a

Table -1 Recent DDoS Attacks

S.no	Attack Date	Name of Company	Impact
1.	23 Feb,2016	Serbian President Website	Server overwhelmed by large number of legitimate and false connection request
2.	23 Mar,2016	NASA	Impact on Primary website
3.	28 Mar,2016	University of Georgia	Blocked all internet access for everyone on Campus
4.	1 Apr,2016	Blighty's govt. funded Education Network	Academic network Janet clobbered with DDoS attack
5.	24 Apr,2016	KKK Website	KKK website shutdown by ghost squad's DDoS attack
6.	6 May,2016	Global Bank	Disrupted the website of Greece's Bank
7.	25 May,2016	NSI	Traffic Management problem affected

8.	13 Jun,2016	South Africal State Broadcasting Corporation	Broad casting gets blocked due to DDoS attack
9.	16 Jun,2016	Muslim Brotherhood's Website	Official language website forced to go offline after DDoS attack
10.	16 Jun,2016	A10 Network	Network ceases data lost

number of experiments in distributed real base environment [21]. To setup a satisfactory experiment for measuring DDoS impact on web services, we should consider topology, legitimate traffic and attack traffic. The following subsections describe in more details about the test methodology and chosen performance metrics. We have generated a random network consist of HTTP, UDP and clients, servers. In our distributed system, multiple legitimate clients connected with server and two attack source is used as DDoS fooding attack [22]. We have measured impact of DDoS attack using following metrics:-

A. Throughput (Vα):- Throughput is the rate of sending or receiving of data by a network in terms of how many bits they pass per second.

$$V\alpha = (bl + ba)/\nabla$$

(bl) represents no. of legitimate bytes, (ba) represents no. of attack bytes and ∇ represents time window for analysis respectively. Throughput is divided into good-put and badput respectively. Goodput is the application-level throughput (i.e. the number of useful information bits delivered by the network to a certain destination per unit of time). The amount of data considered excludes protocol overhead bits as well as retransmitted data packets.

B. Response Time (β):- Response time is a measure of the amount of time required for a packet to travel across a network path from a sender to a receiver [3].

$$\beta = tc + td + ts$$

for example, The time taken for a packet to travel from client to server (tc)+ server delay (td)+ time required for packet to reach to client from server (ts).

Performance metrics are shown in Table 2:-

Table -2 Performance Metrics

Metric	**Description**
Throughput(Vα)	(bl) represents no. of legitimate bytes, (ba) represents no. of attack bytes and ∇ represents time window for analysis respectively
Response Time(β)	time taken for a packet to travel from client to server (tc)+ server delay (td)+ time required for packet to reach to client from server (ts)
Round Trip Time(μ)	x is time to travel from source to destination and y is time to travel from destination back to source

C. Round Trip Time (μ):- Round Trip Time is the length of time, it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received. Its also called round trip delay time.

$$\mu= x + y$$

x is time to travel from source to destination and y is time to travel from destination back to source.

V. EXPERIMENTAL SETUP

In order to analyze the effect of DDoS attacks on web service [13], we have performed a number of experiments in real-time environment on the GENI (Global Environment for Network Innovation) test-bed. In Geni, We have used GENI Desktop tool for performing experiment. Geni Desktop support multiple ways to visualize a slice, and Make it easy to apply an operation to a subset of resources within a slice. Geni Desktop is extensible web-based GUI providing a windowing system for interacting with GENI tools and supports single sign-on to all GENI tools [6]. It is quick access to, and visualization of, commonly used measurement data. It is a windowing system interface which can be used with/without instrumentation. To setup a satisfactory experiment for analyzing DDoS effect, we should consider topology, legitimate traffic and attack traffic [3], [23].

A. Experimental Topology:-

In our Experimental topology, first step is to create a network topology using a GENI Desktop as shown in Fig.4 in which the Node-0 is a server and Node-1 to Node-10 is clients. These clients nodes are used to send legitimate traffic to server (node-0). The attacker nodes are Node-11 to Node 20 that sends attack traffic to server (node-0).In which add a global node that is an extra node (VM). Global node is automatically added to your slice when you use the GENI Desktop tool. The main purpose of the Global node is to be the collection point for all instrumentation and measurement of data collected by the slivers .In our case we have used Web, HTTP and UDP applications to run on topology. Here we have used httperf for generating legitimate traffic. After this, in order to generate attack traffic, attack clients are attached with our topology. Then experiment is again performed at low rate and high rate . Now whole of the traffic is monitored and on-line analysis is done. The output pcap file is used for measuring all performance metrics.

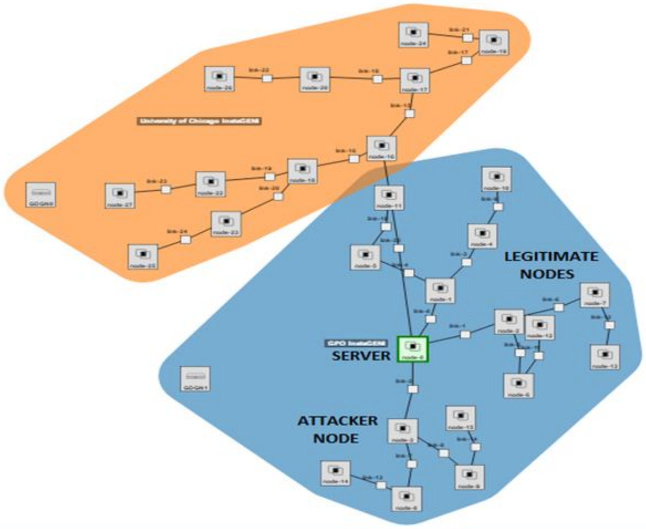

Figure 4. Experimental Topology

B. Legitimate Traffic:-

The typical traffic in current Internet is HTTP and UDP. We have used Node-1 to Node-5 legitimate client nodes which send requests to the server Node-0 for 190 seconds.

Table -3 Tool used for Experiment

Tool Name	Description
GENI Desktop	For Performing Experiment
HTTPerf	For Generating Legitimate Traffic
Bonesi	For Generating Attack Traffic
TCPdump	For Capturing the Packets
Wireshark	For Analyzing the Packets

C. Attack Traffic:-

In this, We have used UDP flooding attack to generate DDoS attack. In our Experiment, Node-11 to Node-20 are attack nodes but we have used only two attacker nodes for launch attack . This experiment is again performed at low rate and high rate traffic. The starts and stop time is same both of attacks traffic to the server for 60 sec to 140 sec. Then we have analyzed performance of DDoS attacks on UDP attack. Table III shows attack parameters used in our real-time experiment.

VI. RESULTS AND DISCUSSION

The effect of DDoS attacks on the performance of UDP attack is analyzed below:-

A. Throughput

Throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node. Throughput is usually measured in bits per second. We have measured throughput in terms of good-put and bad-put as shown in Fig.5 and Fig.6. In our Results, throughput is divided into good-put and bad-put respectively.

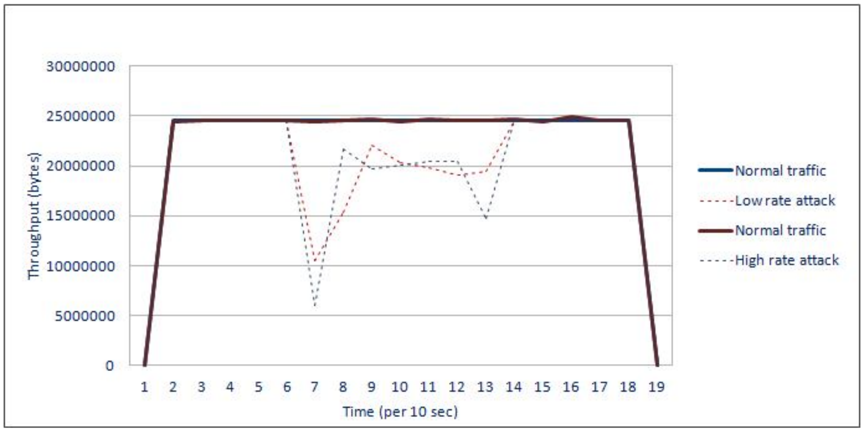

Figure 5. Goodput under DDoS Attack

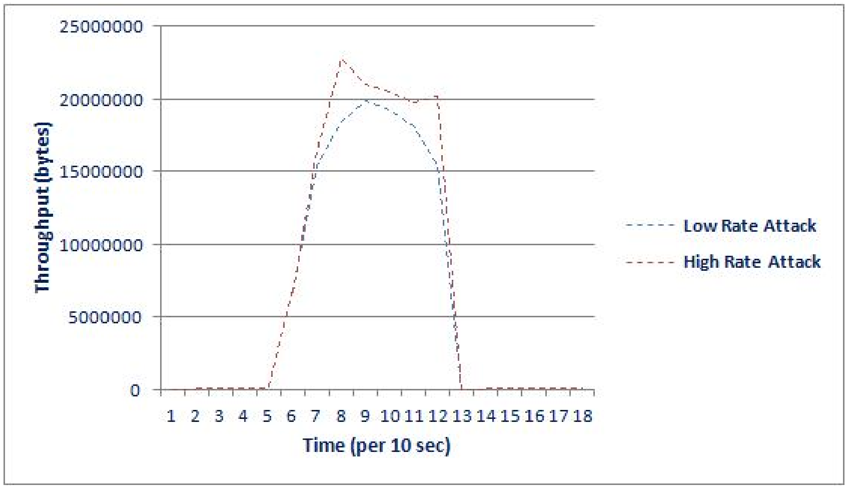

Figure 6.Badput under DDoS Attack

B. Response Time

Response time is the total amount of time it takes to respond to a request for service. Ignoring transmission time for a moment, the response time is the sum of the service time and wait time. Response time is the amount of time a pixel in a display takes to change.In Fig.7 shown the increasing response time during the attack period and without attack.

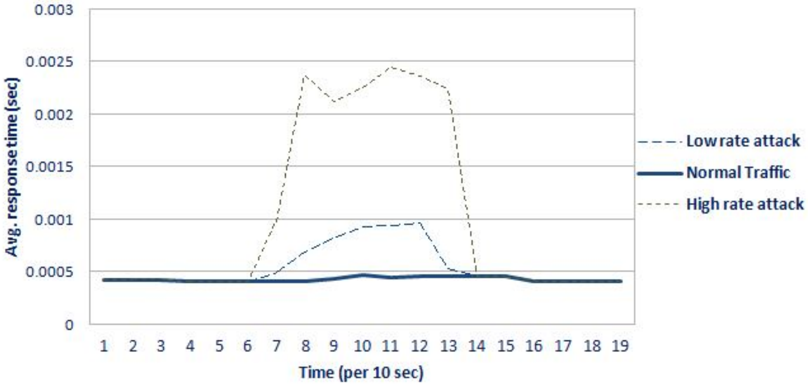

Figure 7.Avg. Response Time under DDoS Attack

C. Round Trip Time

Round Trip Time is the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again. This time delay therefore consists of the propagation times between the two points of a signal. Our experiment response time are shown in Fig.8 during the time of with attack and without attack.

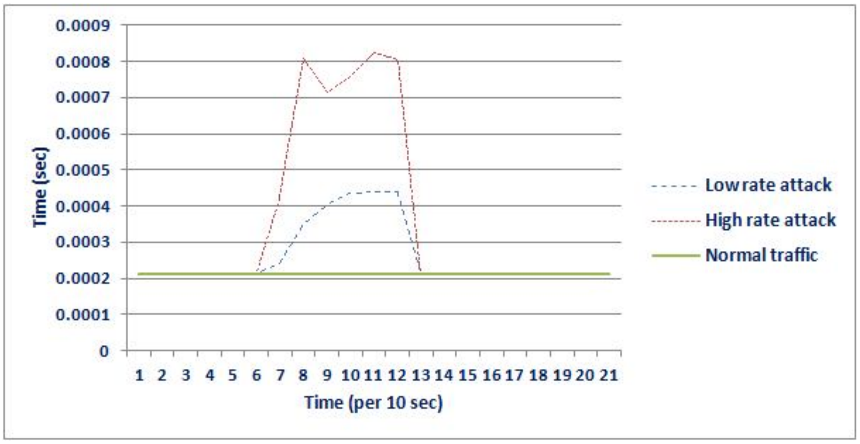

Figure 8. Avg. Round Trip Time under DDoS Attack

VII.CONCLUSION

The Internet consists of hundreds of computers distributed all around the world. Millions of people use the Internet service daily, taking full advantage of the available services at both personal and professional levels. The Distributed Denial of Service attacks are internet attacks that exhaust the resources of the target system in internet. Effective mechanisms are needed to elicit the information of attack to develop the potential defense mechanism. There are various metrics available for measuring impact of DDoS Attacks but every metric is not suitable for all applications. So,we have concentrated on transport layer for specific performance metrics to measure impact of DDoS attacks. We pointed out the possibility of DDoS attacks on Transport layer by launching the UDP attack. Moreover the quantitative measurements clearly indicated the impact of attack on diffierent web services. In our work, We have measured Throughput, Response Time ,Round Trip Time metrics.In future, We will try to adding some more realistic features to the topology, traffic parameters and Attack parameters (such as Large topology, high rate attack , large number of legitimate nodes , large number of attack nodes), so as to get more accurate results of DDoS attacks influence on web services.

REFERENCES

[1] D. Kaur and M. Sachdeva, “Study of flooding based ddos attacks and their effect using deter testbed.”

[2] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, “Reducing unwanted traffic in a backbone network.” SRUTI, vol. 5, pp. 8–14, 2005.

[3] D. Kaur and M. Sachdeva, “Impact analysis of ddos attacks on ftp services,” 2014.

[4] S. Behal, A. S. Brar, and K. Kumar, “Signature-based botnet detection and prevention,” http://www. rimtengg. com/iscet/proceedings/pdfs/advcom p/148. pdf, 2010.

[5] A. D. Keromytis, V. Misra, and D. Rubenstein, “Sos: Secure overlay services,” in ACM SIGCOMM Computer Communication Review, vol. 32, no. 4. ACM, 2002, pp. 61–72.

[6] S. Behal and K. Kumar, “Trends in validation of ddos research,” Procedia Computer Science, vol. 85, pp. 7–15, 2016.

[7] D. Kim, J. Kim, G. Wang, J.-H. Park, and S.-H. Kim, “K-geni testbed deployment and federated meta operations experiment over geni and kreonet,” Computer Networks, vol. 61, pp. 39–50, 2014.

[8] M. Berman, J. S. Chase, L. Landweber, A. Nakao, M. Ott, D. Raychaudhuri, R. Ricci, and I. Seskar, “Geni: A federated testbed for innovative network experiments,” Computer Networks, vol. 61, pp. 5–23, 2014.

[9] J. Mirkovic and P. Reiher, “A university of delaware subcontract to ucla.”

[10] H. Kaur, S. Behal, and K. Kumar, “Characterization and comparison of distributed denial of service attack tools,” in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on. IEEE, 2015, pp. 1139–1145.

[11] J. Mirkovic, E. Arikan, S. Wei, R. Thomas, S. Fahmy, and P. Reiher, “Benchmarks for ddos defense evaluation,” in MILCOM 2006-2006 IEEE Military Communications conference. IEEE, 2006, pp. 1–10.

[12] Y. You, “A defense framework for flooding-based ddos attacks,” 2007.

[13] 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 Cyber Security Experimentation, 2006.

[14] J. Mirkovic, A. Hussain, S. Fahmy, P. Reiher, and R. K. Thomas, “Accurately measuring denial of service in simulation and testbed experiments,” IEEE Transactions on Dependable and Secure Computing, vol. 6, no. 2, pp. 81–95, 2009.

[15] S. Kumar, M. Singh, M. Sachdeva, and K. Kumar, “Flooding based ddos attacks and their influence on web services,” IJCSIT) International Journal of Computer Science and Information Technologies, vol. 2, no. 3, pp. 1131–1136, 2011.

[16] K. Kumar, “Protection from distributed denial of service (ddos) attacks in isp domain,” Ph.D. dissertation, 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, and S. Schwab, “Towards user-centric metrics for denialof-service measurement,” in Proceedings of the 2007 workshop on Experimental computer science. ACM, 2007, p. 8.

[18] C. Ko, A. Hussain, S. Schwab, R. Thomas, and B. Wilson, “Towards systematic ids evaluation,” in Proceedings of DETER Community Workshop, 2006, pp. 20–23.

[19] A. Sardana and R. 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), vol. 3, no. 1, pp. 1–15, 2008.

[20] M. Aamir and M. A. Zaidi, “Ddos attack and defense: Review of some traditional and current techniques,” CoRR abs/1401.6317, 2014.

[21] D. Kaur and M. Sachdeva, “Study of recent ddos attacks and defense evaluation approaches,” the International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 1, pp. 332–336, 2013.

[22] J. Mirkovic, S. Wei, A. Hussain, B. Wilson, R. Thomas, S. Schwab, S. Fahmy, R. Chertov, and P. Reiher, “Ddos benchmarks and experimenter’s workbench for the deter testbed,” in Testbeds and Research Infrastructure for the Development of Networks and Communities, 2007. TridentCom 2007. 3rd International Conference on. IEEE, 2007, pp. 1–7.

[23] T. Benzel, R. Braden, D. Kim, C. Neuman, A. Joseph, K. Sklower, R. Ostrenga, and S. Schwab, “Experience with deter: a testbed for security research,” in 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. IEEE, 2006, pp. 10–pp.