IJCTA, 9(22), 2016, pp. 279-292
© International Science Press

Analysis of Web Services under HTTP attack Using Real Time Testbed

Harjeet Kaur* Krishan Kumar Sunny Behal*****

Abstract : In today's fast growing world, Essential requirement of internet users is to gain high quality of service(QoS) in order to perform the routine activities viz. banking, shopping, E-commerce, trading, communication and many more. But instead they fail to achieve the best quality of service(QoS). Rather suffer with large delays and excessive losses because of immensely growing attacks DoS(denial of service) attack and DDoS(Distributed denial of service) attack. DoS(denial of service) is launched by the single source in order to cripple down all services of the target server. Whereas, DDoS(distributed denial of service) attacks are caused by exploiting unconscious victim networks which coordinately launch attack to cripple down the corporate sector. Hence, such attacks triggered an orchestrated traffic jam. It has been a solemn intimidation for all the services controlled through the internet. A well formulated solution is required to detect and compensate the impact of DDoS attacks which is possible with the synthetic traffic traces. In spite of demerits of emulators and real time testbed, this paper compare the results of emulator(DETER testbed), real time distributed environment(GENI testbed), real time testbed. Results are computed in the form of following metrics viz. goodput, badput, average response time, round trip time, number of retransmissions and number of active connections. The following comparison will take the research to the higher level.

Keywords : DoS, DDoS, Goodput, Badput, RTT, Response Time, Retransmissions, DETER, GENI, Real Time Testbed.

1. INTRODUCTION

In the present era, world is highly debased on the internet and is considered as major framework for providing services to the global information society. Therefore, the crucial and essential requirement of society is availability of internet for the growth of socio-economic sector. The availability of internet and its services means that the information, the computing systems and security controls are accessible and operable in committed state at some random point of time. Hence indispensable vulnerabilities of internet architecture procure many contingencies and paths to attack on services and infrastructure of internet [15]. DDoS(distributed denial of service) attacks is one of the major threat on the availability of internet. [1][2] DDoS(distributed denial of service) attacks may degrade and completely disrupt all the services serving the legitimate users of the target. DDoS is the expanded form of DoS and is launched by compromising precarious network which are known as zombies against a single target server. In this way, unaware compromised networks become the part of DDoS attack network. As per the research conducted over a decade, DDoS attacks has become a severe and exponentially growing problem for the E-business and government sector. These attacks follow the basic modus operandi mentioned in [5] which shows the way taken by the attacker for such attacks, in spite of this, our research is still lacking behind because the attacker community

* Department of Computer Science and Engineering SBSSTC, Ferozepur, Punjab, India harjeet.4444@gmail.com
** Department of Computer Science and Engineering SBSSTC, Ferozepur, Punjab, India k.salujasbs@gmail.com
*** Department of Computer Science and Engineering SBSSTC, Ferozepur, Punjab, India sunnybehal@rediffmail.com

is coordinated, sophisticated and well-organized. The modus operandi can be helpful in determining the magnitude, frequency and complexity of attacks. Hence, developing techniques can reliably and accurately detect the DDoS attack [3][4][5].

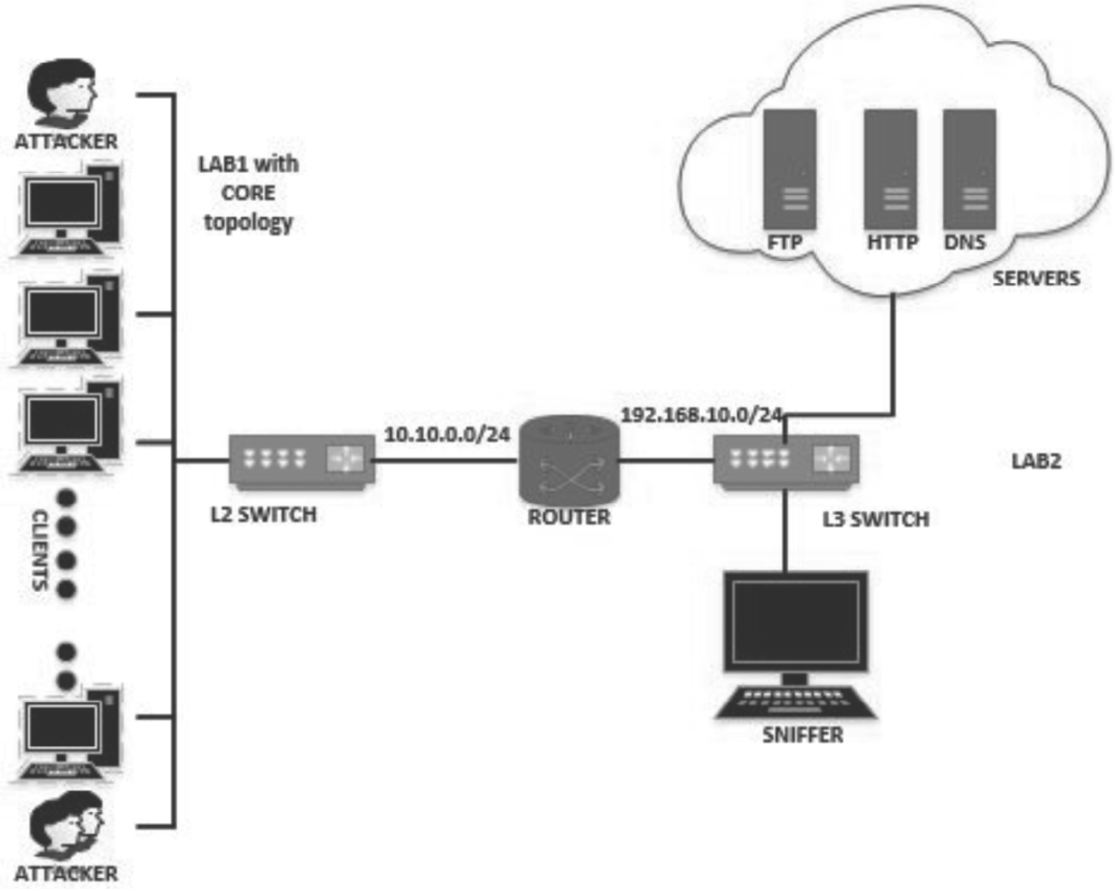


Fig. 1. Real Time Testbed.

The idiopathic goal of DDoS attacks is to prevent the access of the resources of target victim. The newly published report suggests DDoS attacks are getting bigger and more sophisticated and results tremendous business loss. The report shows more than 200 attacks reported in 2015 summoned 100 Gbps of traffic and largest of these clocked at 500 Gbps which is enough to disrupt an entire internet provider's network [37]. The Akamai report scaled that 23 percent increase in DDoS attacks and 26 percent increase in web application attacks as compared with Q4 2015. The rise in repeat DDoS attacks is seen in which average of 29 attacks per target and is repeated 283 times.[38]. A phase 3 Oplcarus(project Mayhem) is the anonymous cyber assault against worldwide stock exchange and this attack takedown the London Stock Exchange website on June 5, 2016. [39]. The 2016 U.S. presidential election has sparked a wave of cyber assaults on candidates, political parties and governmental IT networks. This reports shows that in Philippines election commission, attackers has leaked 55 million voters from the voter database [40].

In order to formulate a comprehensive solution against the DDoS attack solution, there is need to study and analyze the impact of DDoS attack in different perspectives and distinct available platforms. This paper contributes as:

1. Analyzing the behavior of legitimate and attack traffic generating tools to prepare a testing and monitoring toolkit.
2. Creating an emulated environment for performing attacks in DETER testbed.
3. Creating a real time distributed environment for performing attacks in GENI testbed.
4. Setting up the real time testing framework *i.e.* our own real time testbed which is shown in the figure 1.

5. Impact of DDoS attacks is measured as goodput, badput, average response time, round trip time, number of active connections, No. of retransmissions.
6. Comparing the results of emulation(DETER testbed), real time distributed environment(GENI testbed) and real time testbed framework.

The experiments are performed in three platforms viz. DETER, GENI, real time testbed framework with well-organized scenarios to measure impact of DDoS(distributed denial of service) attacks. The remainder of the paper is structured as follows : Section II provides an overview of DDoS problem, section III reviews the literature of traffic generating and analyzing techniques, section IV discusses the performance metrics for measuring impact of DDoS attacks, section V discusses the proposed work used for testbed designing and impact measurement, section VI describes the experiment performed according to the scenarios, section VII highlights the results and discussions, section VIII summarizes the work, section IX directs towards the future scope.

2. DDOS OVERVIEW

DoS attack basically means denying valid Internet and Network users by using the services of the target server. It basically means, launching an attack, which will temporarily make the services offered by the network unavailable to legitimate clients.[6][9][10] A Distributed Denial of Service(DDoS) attack is the aggregation of compromised systems to attack a single target server and results to the unavailability of services for the legitimate users. A huge volume of incoming requests to the target server essentially enforce the server to shut down or even smash, thereby the services remain denied to the legitimate users. In DDoS attack, there are two victims i.e. the primary victim and the secondary victim. Primary victim are the services of server under attack and the secondary victim are the compromised systems used to launch attack. A distributed denial of service is performed in several phases. The phases are explained as follow :

1. **Enrollment Phase :** In this phase, the attacker first enroll the multiple zombie machines. This process is performed by attacker by deploying tool into the compromised machines.
2. **Accomplishment phase :** In this phase, the vulnerable machines are exploited and become the slaves of attacker.
3. **Infected Phase :** In this phase, exploited machines are get infected with attack code and such infected machines can be used for further enrollment of new agents.
4. **Engaged Phase :** In present phase, the system is under attack and agent machines are engaged in order to send the attack packets to the target victim server.

Both DoS and DDoS attacks are easy to design and operate without requiring any special skill or resource for their perpetration. The attack tools can be obtained easily online and the attack goal is attained. The main difference between DoS and DDoS attack is in scale - DoS attacks use one attack machine while DDoS attacks use large number of attack machines. The scale difference will affect the operational modes. The main requirement is to create our own tool in order to detect and protect the DoS attack. [23][24][25]

3. RELATED WORK

In recent times DDoS attacks has improved their attack launching techniques which is worldwide problem. During this span of interval there has been significant research for detection and impact measurement of DDoS attacks at distinct platforms viz. simulation, emulation, datasets, real time environments but very little has compared the results of such platforms to reach the conclusion. In the paper [17], Hussain[2013] [8], rephrased the actual datasets. The prominent datasets are KDD Cup 1999 [23], CAIDA DDoS attack 2007 [23], DARPA 2009 [23][30][31][32]. However, these datasets have their own limitations viz. IP addresses are mapped, asymmetric traffic, packets are trimmed 20bytes after the transport header, difficult to distinguish the high rate attack traffic and low rate background traffic. In the paper,[10] the impact measurement is simulation based further have some pros and cons. Jaswinder[2012] [34], Jei Wang[2011], Monika[2009][35], Massimo[2015] concluded their work in simulated environment whose results are not accurate and efficient. Most of the work has performed only on the emulated platform *i.e.* DETER testbed viz. Mirkovic[2007] [16][17], Mirkovic[2006] [7][8], Monika[2014][18], Monika[2013][10]. These performed the impact measurement and detection of DDoS attacks with DETER emulated testbed which has their own experimental conditions, real operating system and machines but still the results are not equivalent to the real time system results. Emulation lies in between the simulation and real time systems. Some of the researchers worked on real time but not on DDoS rather on DoS viz. Mirkovic and Hussain[2007][16][17][21][22], Gelenbe[2005][36] and these papers included less number of metrics.[19][20] There are the researchers developed their own testbed for the experimentation purpose but have not measure the impact of DDoS attack on numerous web services viz. Desmond[2010][3][13], Bhatia[2014][13]. Most of the researchers developed and computed their results in real time but has not compared the results with either emulation or simulation. This paper includes the development of real time testbed framework, the impact of DDoS attacks is measured in three platforms viz. Emulation(DETER), real time distributed environment(GENI), real time testbed framework and compared the results of the above mentioned three platforms.[11][12][14][15]

4. PERFORMANCE METRICS FOR MEASURING THE IMPACT OF DDOS

DDoS attack have hazardous impact on the numerous web services like HTTP, FTP,DNS which can be estimated by measuring different metrics. These metrics are Goodput, Badput, Average response time, Average round trip time, No. of active connections, No. of retransmissions .[10][18]

1. **Goodput(α) :** Goodput is defined as the number of bytes transferred per unit time from source to destination. Throughput varies according to the layers *i.e.* network layer throughput, transport layer throughput, application layer throughput. It can be measured as :

$$\alpha = \sum P_d / \sum (P_a - P_s)$$

P_d is packet delivered, P_a is the packet arrival, P_s is the packet start time.

2. **Badput(β)**: Badput can be defined as the number of bytes of attack packets which are received at the server side.

$$\beta = P_{server}$$

P_{server} are the number of packets received at server side.

3. **Average Response Time(£)**: Average response time can be defined as the total amount of elapsed time between the end of an inquiry or demand on a computer system and the beginning of a response. For example, The time taken for a packet to travel from client to server t_c + server delay t_d + time required for packet to reach to client from server t_s. It can be measured as:

$$\pounds = t_c + t_d + t_s$$

For most of applications, response time is really critical. If any application is taking more time for the particular transaction than that is considered as the failure of transaction.

4. **Average Round Trip Time(RTT)(Ω) :** Round trip time(RTT) is defined as the time required for a signal pulse or packet to travel from a specific source to a specific destination and back again.

$$\Omega = x + y$$

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

5. **Number of retransmissions (Ω) :** TCP retransmissions occurs if TCP doesn't receive the ACK within 2*RTT then it will retransmit the previously sent packet and unacknowledged segment. It can be defined as the packets which has not made its TCP connection.

$$\pi = N_{syn} + N_{ack}$$

N_{syn} are the number of synchronized packets and N_{ack} are the number of acknowledgement packets.

6. **Number of Active connections(μ) :** It can be defined as the connections that remain active before attack and after attack. The value of this metrics increases during the attack period because there will be the legitimate packets plus attack packets. Moreover, the connections which have completed the transaction are called as the active connections.

$$\mu = N_{packets} + A_{packets}$$

$N_{packets}$ are the number of legitimate packets and $A_{packets}$ are the number of attack packets.

5. PROPOSED WORK

This section proposes the work followed by adopted methodology and topology designing and testing in separate platforms viz. emulator(DETER), real time distributed testbed(GENI), real time testbed. DETER and GENI are pre-designed testbeds but the real time testbed is firstly designed and developed with the help of hardware equipment's and software tools for various purposes. The hardware used are manually configured D-LINK 2800 series router, D-LINK Layer-3 manageable switches for connecting multiple computer systems, desktop computers are installed with UBUNTU-14.04 operating system. The software attack tools and legitimate traffic generating tools are GoldenEye and Httperf respectively. The traffic generated is required to monitor with wireshark, tshark and tcpdump. CORE (common open research emulator) is used in the real time testbed so that the topology could be enhanced. The testbed constitutes two network labs in which lab1 has the traffic generating nodes either attack or legitimate traffic and lab2 is the monitoring network that further constitutes sniffer and target server. This testbed setup provides a useful prototype for performing experiments with distinct scenarios. The detailed study of methodology and topologies used in the three platforms is discussed in the coming subsections.

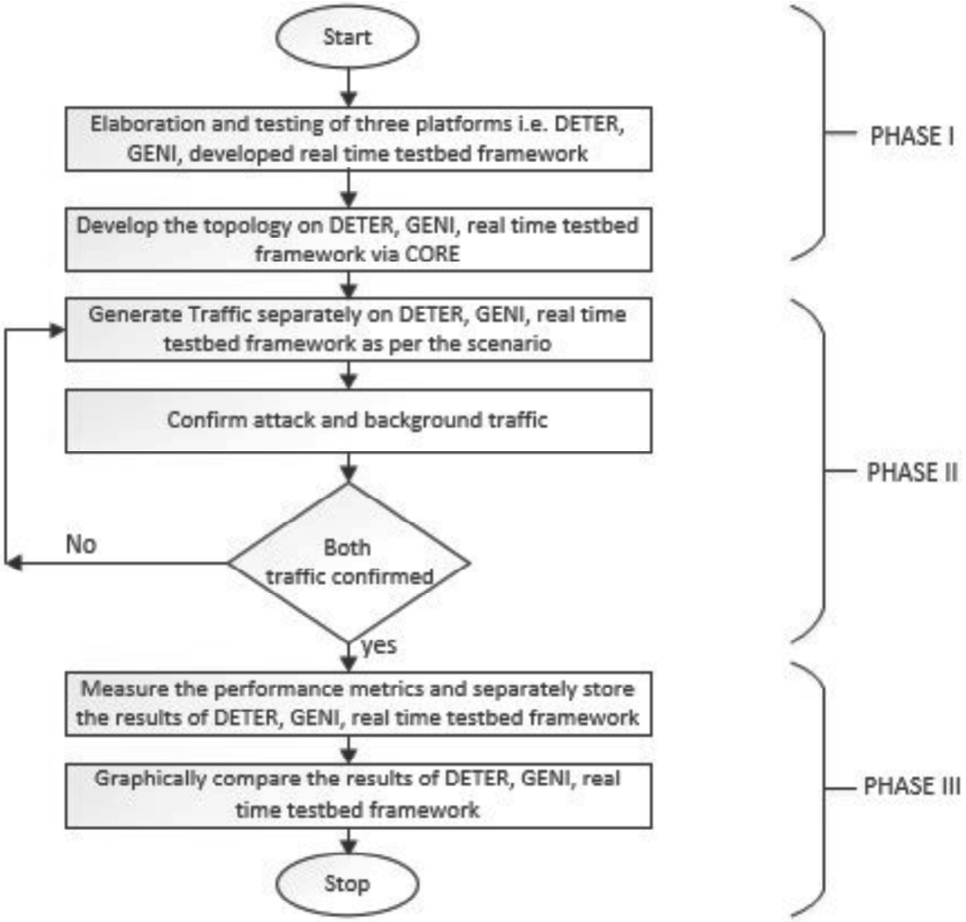

Start
Elaboration and testing of three platforms i.e. DETER, GENI, developed real time testbed framework
Develop the topology on DETER, GENI, real time testbed framework via CORE
PHASE I
Generate Traffic separately on DETER, GENI, real time testbed framework as per the scenario
Confirm attack and background traffic
No
Both traffic confirmed
yes
PHASE II
Measure the performance metrics and separately store the results of DETER, GENI, real time testbed framework
Graphically compare the results of DETER, GENI, real time testbed framework
Stop
PHASE III

Fig. 2. Proposed Methodology

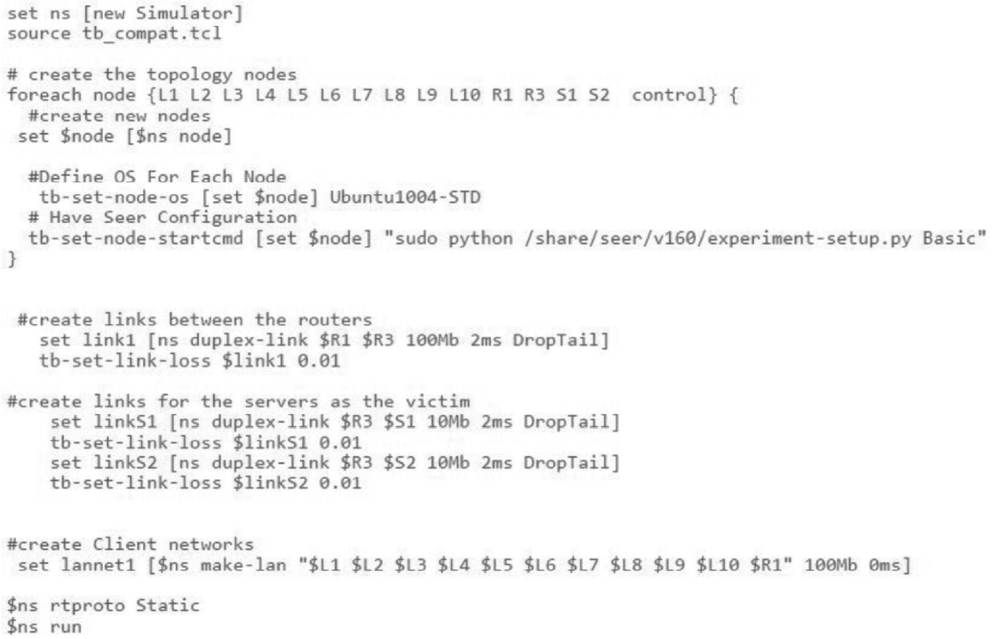
5.1. Proposed Methodology

The methodology adopted in the present work for DETER testbed, GENI testbed, and real time testbed can be elaborated by the flowchart as shown in figure 2. The respective flowchart is divided into three distinct phases. In the first phase, DETER testbed and GENI testbed are thoroughly elaborated and tested along with the testing of generated real time testbed framework. Furthermore, topologies at the three distinct platform are developed and tested to generate huge amount of traffic via large number of nodes. In the second phase, according to the scenario the traffic both attack and legitimate is generated which is monitored with the monitoring tool. When the attack and legitimate traffic is confirmed then move to the next phase otherwise, the same process is repeated. In the third phase, the captured traffic is evaluated for measuring the impact of DDoS attacks on the web services. The evaluation is done by computing the same performance metrics applied separately on the DETER testbed, GENI testbed and real time testbed. The graphical representation of the results helps in comparing the quality of service(QoS) shown by DETER testbed, GENI testbed and real time testbed.

5.2. Proposed Topology

The execution of experiments related to the DDoS attacks require large number of nodes for sending huge amount of legitimate traffic and for some instant massive attack traffic also. For sending such traffic, a topology with required number of nodes must be developed. Hence, This section explain the topologies shadowed in the three platforms i.e. DETER testbed, GENI testbed and real time testbed.[6][27][28][29]

1. **Deter :** In DETER testbed, topology is developed by uploading an error free NS script. NS script is obtained by using TCL language concepts and NS simulator rules[24][25][26]. It constitutes the number of nodes, number of LANs, number of links, bandwidth of the respective link and operating system of each node. If traffic generation is by using SEER tools then add informative lines for SEER. The NS script of the current experiment is as shown in figure 3:



```
set ns [new Simulator]
source tb_compat.tcl

# create the topology nodes
foreach node {L1 L2 L3 L4 L5 L6 L7 L8 L9 L10 R1 R3 S1 S2  control} {
  #create new nodes
 set $node [$ns node]

  #Define OS For Each Node
   tb-set-node-os [set $node] Ubuntu1004-STD
  # Have Seer Configuration
  tb-set-node-startcmd [set $node] "sudo python /share/seer/v160/experiment-setup.py Basic"
}


 #create links between the routers
   set link1 [ns duplex-link $R1 $R3 100Mb 2ms DropTail]
   tb-set-link-loss $link1 0.01

#create links for the servers as the victim
    set linkS1 [ns duplex-link $R3 $S1 10Mb 2ms DropTail]
    tb-set-link-loss $linkS1 0.01
    set linkS2 [ns duplex-link $R3 $S2 10Mb 2ms DropTail]
    tb-set-link-loss $linkS2 0.01


#create Client networks
 set lannet1 [$ns make-lan "$L1 $L2 $L3 $L4 $L5 $L6 $L7 $L8 $L9 $L10 $R1" 100Mb 0ms]

$ns rtproto Static
$ns run
```

Fig. 3. NS Script.

After uploading the correct NS script, the topology can be visualized in the DETER visualization section.[31][36] The topology of above mentioned NS script is shown in the figure 4:

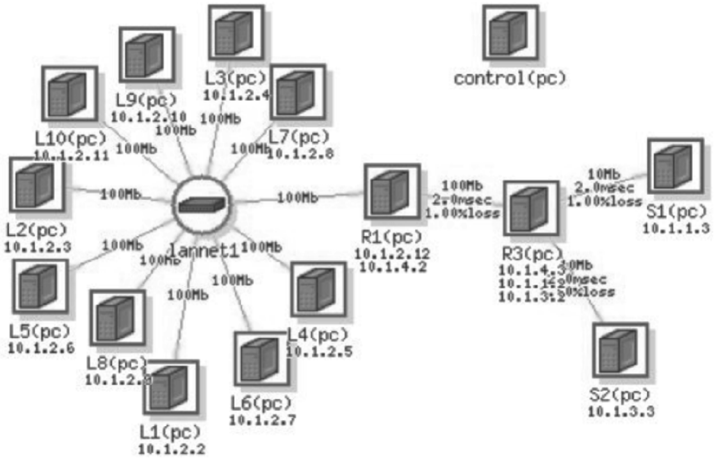


Fig. 4. DETER Topology.

2. **GENI :** In GENI testbed, topology is developed by performing drag n drop operation of the nodes, routers, links. The bandwidth of each link and operating system of each node is set manually. Once the topology is ready, it starts reserving the resources for further process and resources remain reserved for particular time duration. Since, GENI testbed is distributed in nature that has aggregates in it for reserving resources. Traffic generation is performed at GENI desktop, one of the tool of GENI testbed. The topology is shown in the figure 5

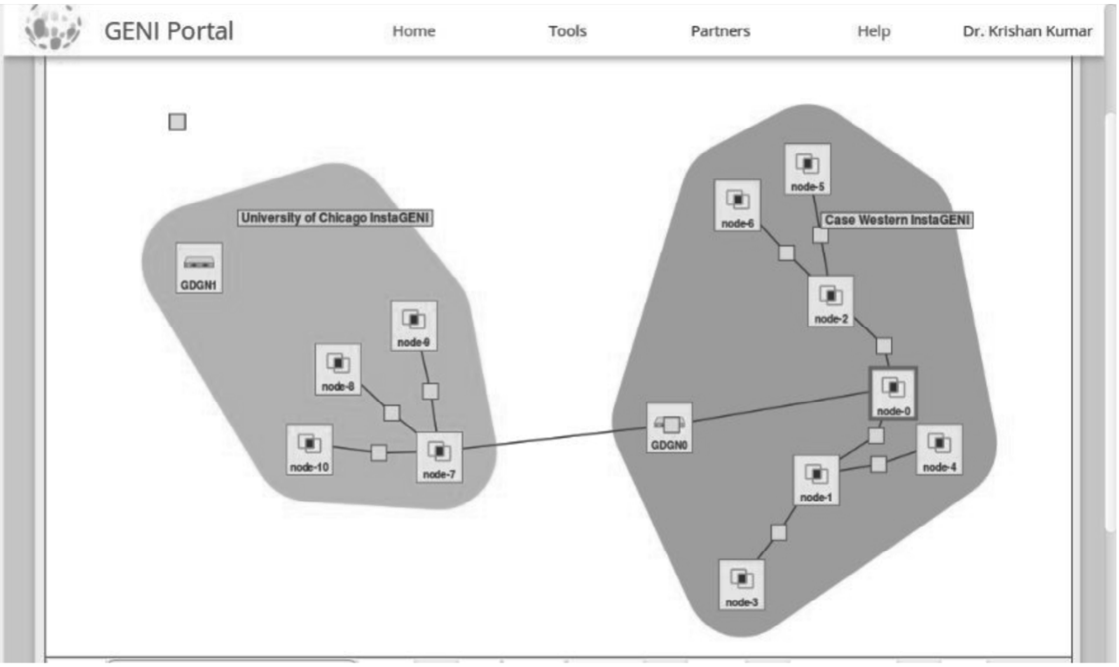
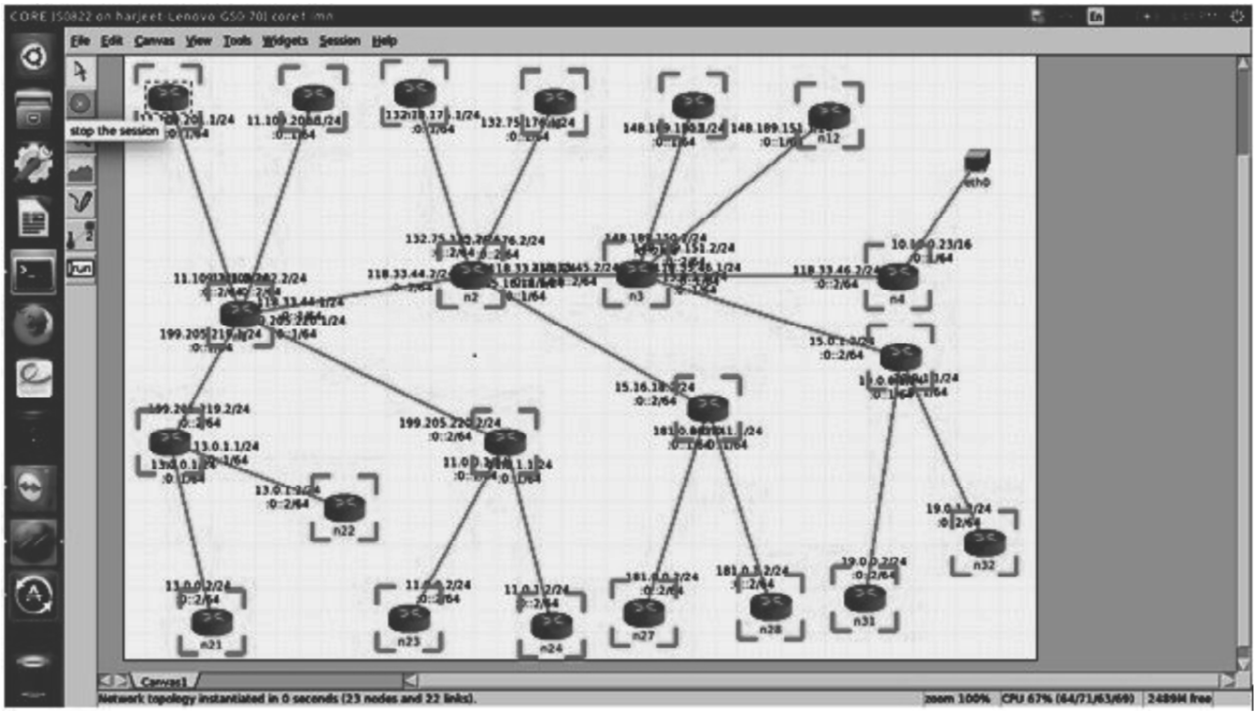


Fig. 5. GENI Topology.

3. **Real Time Testbed :** In real time testbed, topology is developed for the generation of attack and background traffic. In the testbed, emulator based topology is used with the help of CORE(common



Network topology instantiated in 0 seconds (23 nodes and 22 links).

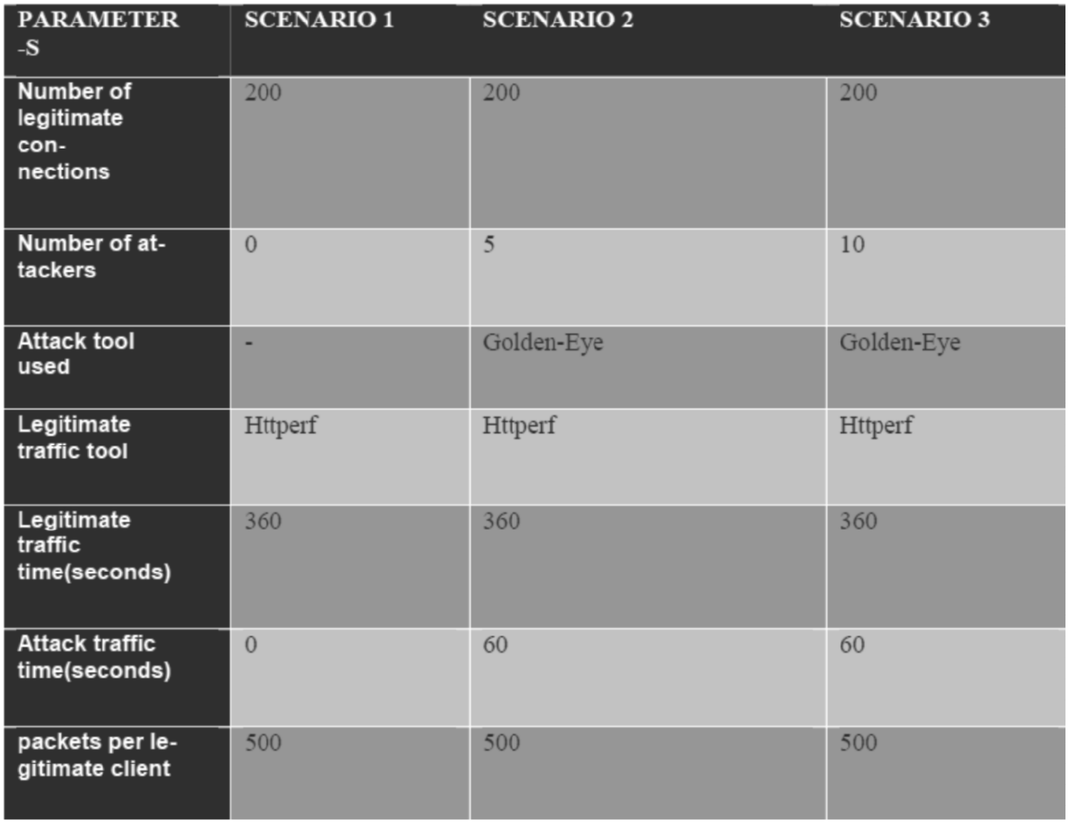
Fig. 6. CORE Topology in Real Time Testbed.

open research emulator).CORE is a tool for building virtual networks and as an emulator, CORE builds a representation of a real computer network that runs in real time network, that opposed to simulation, where abstract models are used. The live-running emulation can be connected to physical networks and routers. It provides an environment for running real applications and protocols, taking advantage of virtualization provided by the Linux or FreeBSD operating systems. Hence, CORE can run on a virtual machine and it uses full size file which is very large almost 600 megabytes. Some of the features of CORE are efficient, scalable, runs applications and protocols without modification, easy to use as it provides a GUI platform and highly customizable also. CORE is typically used for network and protocol research work, demonstrations, application and platform testing, evaluating number of networking scenarios, security studies, and increasing the size of physical test networks. In the present experiment, the topology is build by CORE which has two networks *i.e.* one for generating legitimate traffic and other for generating attack traffic. Traffic generated via CORE topology will pass through the real computers, router, switches and finally reach to the real target victim. The topology is shown in the figure 6.

6. IMPLEMENTATION OF PROPOSED WORK

This section explains the traffic generation scenarios for generating legitimate and attack traffic and parameters used in the experiment which is same for the three platforms i.e. DETER testbed, GENI testbed and real time testbed. In the present experiment, 200 legitimate clients generates the legitimate traffic with steady rate via httperf legitimate traffic generator and varied number of attacker as per scenarios for generating attack traffic via goldeneye as attack traffic generator.[2][37][41] In the first scenario, the legitimate traffic is generated for 360secs from 200 legitimate clients. In the second scenario, same legitimate traffic is generated from 200 clients for 360 seconds along with attack traffic from 5 attackers for the duration of 60 seconds. In the third scenario, the strength of attack traffic has been increased by introducing 5 more attackers which further leads to the increased attack traffic impact on the legitimate requests. Legitimate traffic is generated from 200 clients for 360 seconds but number of attackers are increased from 5 to 10 that intensified the strength of attack traffic. The experimental parameters used in the experiment are shown in the table:

Table 1. Parameters Used.



PARAMETER -S	SCENARIO 1	SCENARIO 2	SCENARIO 3
Number of legitimate connections	200	200	200
Number of attackers	0	5	10
Attack tool used	-	Golden-Eye	Golden-Eye
Legitimate traffic tool	Httperf	Httperf	Httperf
Legitimate traffic time(seconds)	360	360	360
Attack traffic time(seconds)	0	60	60
packets per legitimate client	500	500	500

7. RESULTS AND DISCUSSIONS

Experimental results are computed in the form of following metrics i.e. goodput, badput, average response time, average round trip time, number of active connections and number of retransmissions. The results of three platforms i.e. DETER testbed, GENI testbed, real time testbed are compared in the present section.

Goodput : Goodput is defined as the number of bytes transferred per unit time from source to destination. Throughput varies according to the layers i.e. network layer throughput, transport layer throughput, application layer throughput. During a DDoS attack, attack traffic fills the bottleneck link to force the router to drop most of the legitimate packets and increase the number of retransmissions. In the following figure 7. comparison is done which shows decrease in goodput at the time of attack period starting from 120sec and stopped at 180secs. As we increased the strength of attack from 5 attackers to 10 attackers in each of the three platform, the goodput curve decreased more.

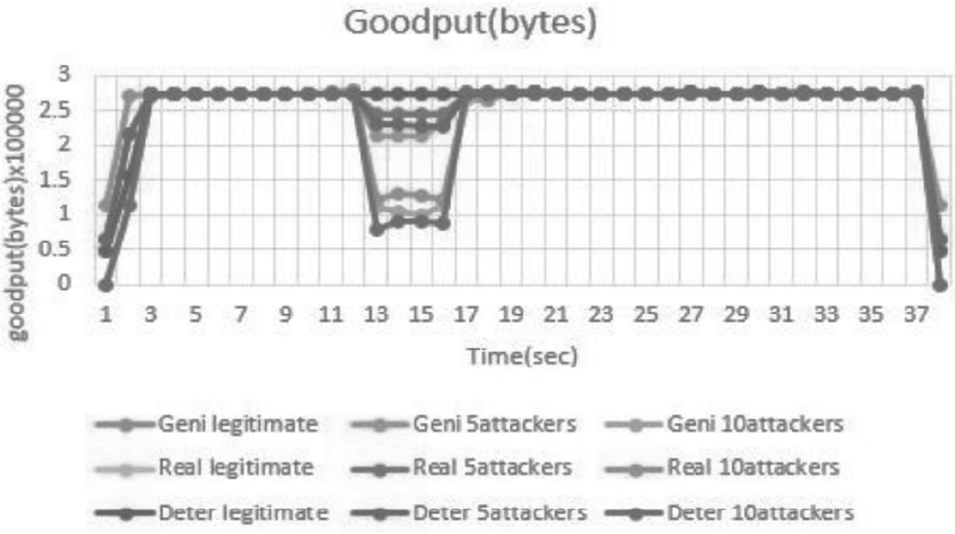


Fig. 7. Goodput.

Badput: During a DDoS attack period between 120secs and 190secs, badput increased with the increase in the strength of attack from 5 attackers to 10 attackers at each of the three platforms which is given in figure 8.

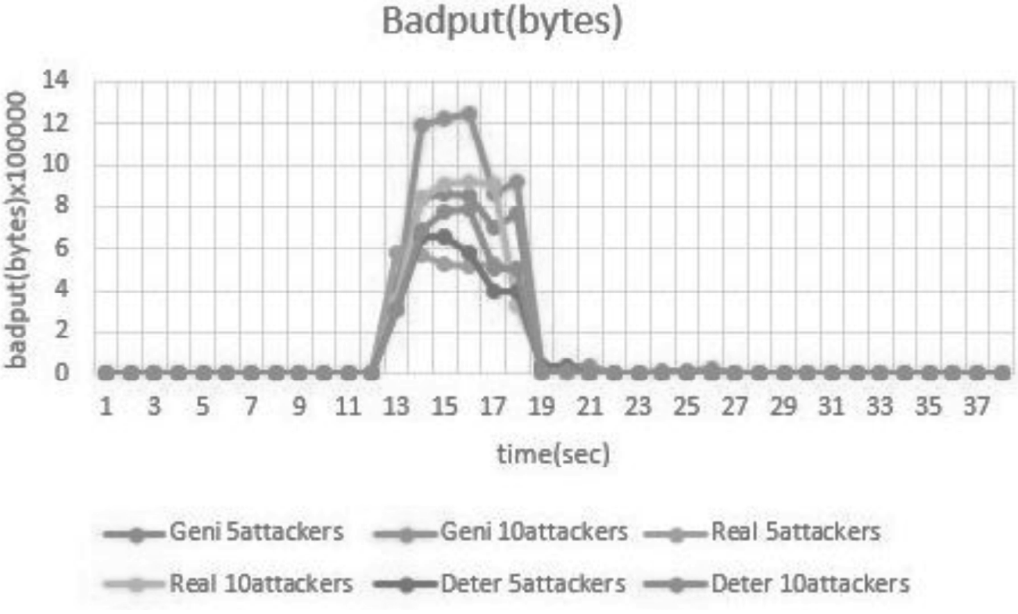


Fig. 8. Badput.

Average Response time : Quality of service required by each application is distinct as for HTTP applications, there is the need to minimize the delay of HTTP transaction. Each application has its own quality of service needs. According to the research in (ref of monika mam paper), if overall transaction completes in less than 10 seconds then it is successful transaction. Therefore, average delay must be based on the transaction finished in 10 seconds. It is shown in figure 9. that without attack average delay is 0.000946 *i.e.* zero but during a DDoS attack period between 120seconds to 160 seconds the average delay increased with the increasing strength of attack from 5 attackers to 10 attackers. Response time depends upon topology, network load and traffic parameters. Hence for measuring impact of DDoS attacks fixing threshold have no meaning.

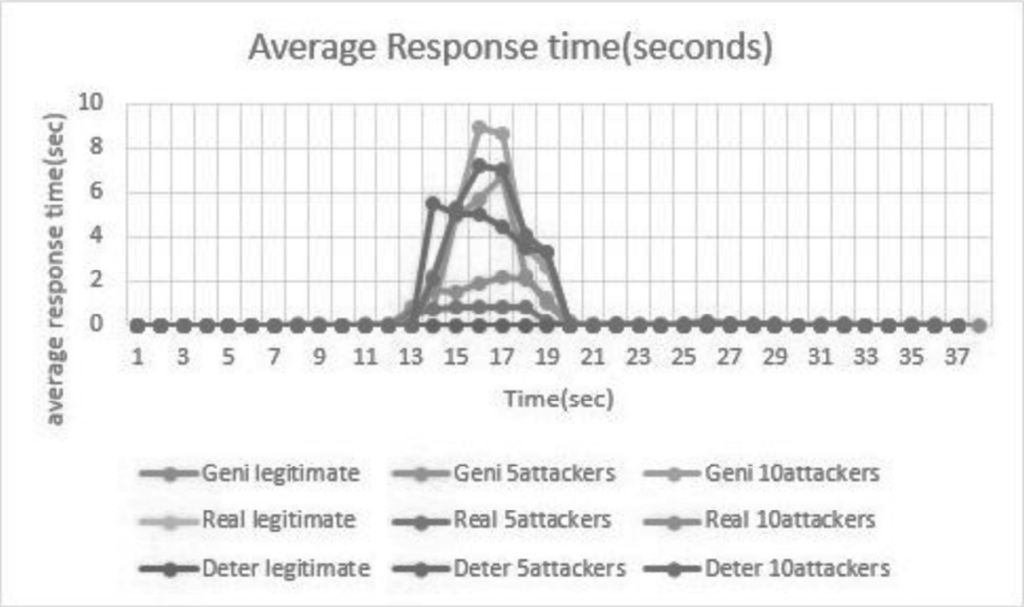


Fig. 9. Average Response Time.

Average Round Trip Time(RTT): During a DDoS attack period between 120seconds to 180 seconds, average round trip time has increased from 1sec in GENI testbed, 0.4 sec in DETER testbed, 0.2sec in real time testbed framework with 5 attackers to 2sec in GENI testbed, 0.6 in DETER testbed and 0.3 in real time testbed with 10 attackers. Therefore, increasing strength of attack traffic has major impact on the performance of victim server which is shown in figure 10.

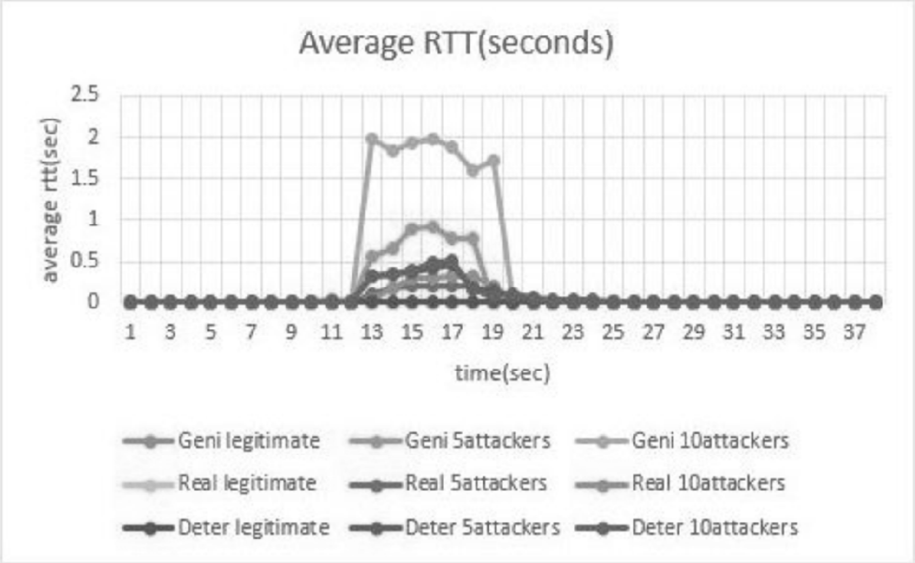


Fig. 10. Average RTT.

Number of retransmissions : TCP retransmissions occurs if TCP doesn't receive the ACK within 2*RTT then it will retransmit the packet. In this paper, the retransmissions are increased by increasing the attack traffic from 5 attackers to 10 attackers during attack period between 120seconds to 180seconds which is examined at each platform viz. DETER testbed, GENI testbed and real time testbed as shown in figure 11.

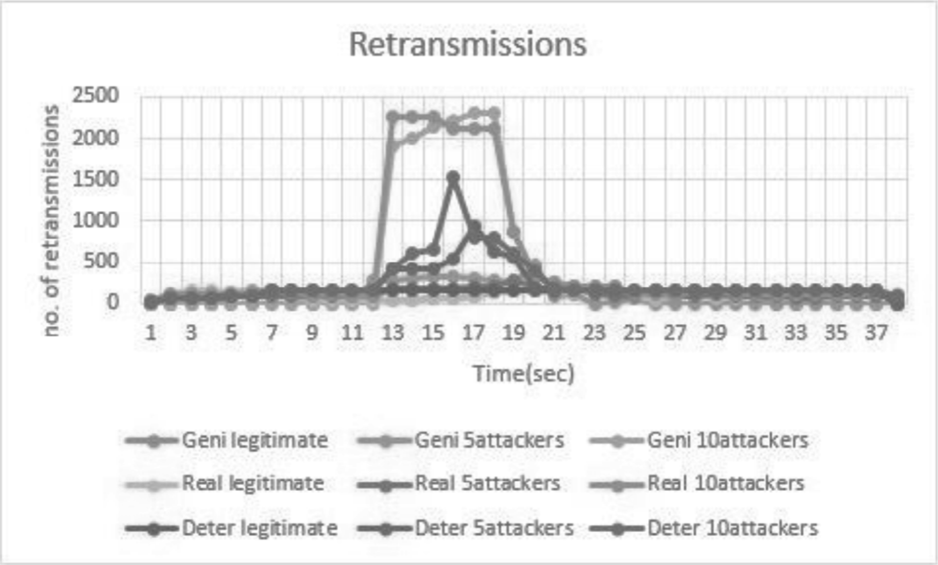


Fig. 11. No. of Retransmissions.

Number of active connections : During a DDoS attack, attack traffic increased the number of active connections measured at DETER testbed, GENI testbed and. With the increase in attack traffic i.e. from 5 attackers to 10 attackers, a tremendous increase has seen of connections in GENI testbed and real time testbed framework but not in DETER testbed which is shown in figure 12.

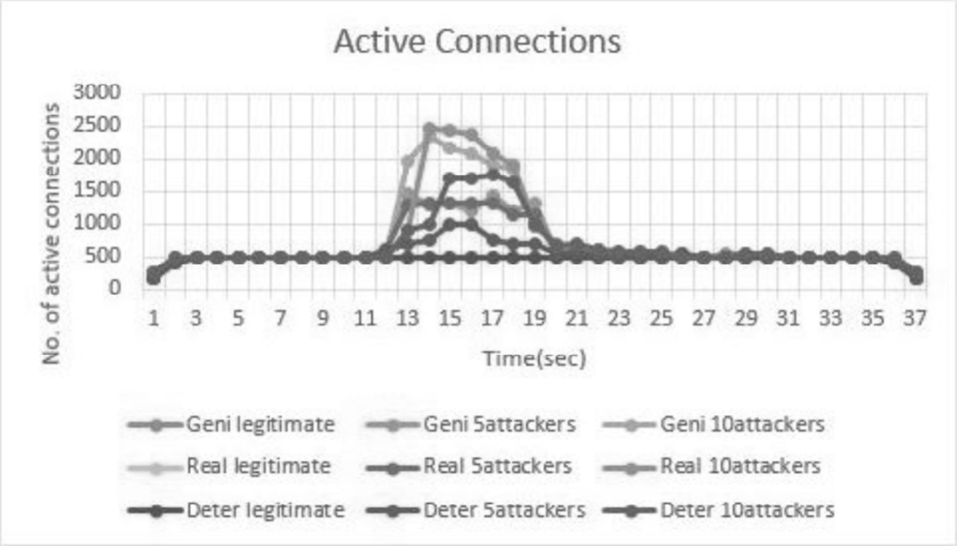


Fig. 12. No. of Active Connections

8. CONCLUSION

Distributed Denial of service attacks are the serious problem in the today's networking era and is constantly increasing with innovative attack techniques. In response to the attackers, our research community is working in the field of defense of DDoS attacks which needs to be very effectively elaborated. Research associated with DDoS defense field is lacking in many sections viz.

1. Lack of accurate evaluation i.e. attack traffic characterization is not enough to differentiate it from the normal traffic.
2. Scarcity in availability of recent and realistic datasets in public domain i.e. due to the legal policy of the cooperates, datasets are not publicly available further our research cannot proceed towards defensive approaches.
3. Datasets available are either too old or too long to meet the current trends of DDoS attacks which does not provide appropriate information about the traffic contents or origins.
4. Off-the-shelf software traffic generators have their own limitations for generating traffic either attack traffic or the legitimate traffic.
5. Lack of benchmarks in the field of DDoS defense mechanisms that leads to strike up the DDoS attacks.

In this paper, the comparison is made between the platforms i.e. DETER testbed, GENI testbed and real time testbed by measuring the impact of DDoS attacks via metrics viz. goodput, badput, number of active connection, number of retransmissions, average round trip time and average response time. The better result are shown in Real Time Testbed Framework and GENI testbed because it is real time distributed testbed but as DETER testbed is emulator the results are not accurate. Since GENI testbed is distributed in nature so average response time and average round trip time is much higher than DETER testbed and real time testbed. The major requirement of the research is to define a threshold model in order to defend against DDoS attack.

9. FUTURE SCOPE

Future development is associated with increase in flexibility and scalability of the current setup that is possible by deep investigation of the anomaly detection techniques. Enhancement in testbed by deploying more hardware devices viz. routers, switches, computers. In the present testbed, single router is used which will be advanced with five more routers, layer 2 switches will be replaced by the layer 3 switches and more desktop computers will be used with highly maintained servers. Currently, all three servers FTP, HTTP, DNS are configured on the single machine but in future these servers will be configured on the distinct three machines.

Depending upon the coming scenarios and experimentation, attack traffic and background traffic generating tools require intensive exploration to tackle down the extremely growing DDoS attacks. Hence, future work will be directed towards further investigation and testing of such tools which will improvise previously maintained toolkit. Impact measurement tools used in the present and future research could be added to the toolkit for appropriate results of detection metrics.

Our future work is worldwide establishment can be done so that researchers around the world can reliably perform their experiments and accurately compute their results through this testing framework. This sort of enlargement of testbed requires the conversion of the off-line real time testbed into online real time testbed. Our future work is to enhance the performance of our Real Time Testbed.

10. REFERENCES

1. Abhinav Bhandari,A.L. Sangal and Krishan Kumar,”Performance metrics for defence framework against Distributed Denial of Services Attacks”,ACEEE,2014.
2. Sunny Behal and Krishan Kumar,”Characterization and Comparison of DDoS attack Tools and Traffic Generators - A Review”, International journal of Network Security,2016
3. Desmond Schmidt,Suriadi Suriadi, Alan Tickle, Andrew Clark, George Mohay, Ejaz Ahmed, James Mackie, “A Distributed Denial of Service Testbed”,
4. Lam, H.-Y., Li, C.-P., Chanson, S.T. and Yeung, D.-y., A Coordinated Detection and Response Scheme for Distributed Denial of Service attacks. In: IEEE International Conference on Communications, 2006. ICC ’06. Vol. 5, pp. 2165-2170(2006).
5. Mirkovic, J. Fahmy, S., Reiher, P., Thomas, R.K.: How to Test DoS Defences, (2009)
6. Benzel, T., Brader., R., Kim, D., Neuman, C., Joseph, A., Sklower, K.: Experiment with DETER: A Testbed for Security

Research. In Proceedings of Teridentcom(International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities), March 2006.

7. Mirkovic, J., Reiher, P., Thomas, R., Schwab, S.: Automating DDoS Experimentation.Proceedings of the DETER workshop, August(2007).
8. Mirkovic, J., Hussain, A., Fahmy, S., Reiher, P., Thomas, R.k.,: Accurately Measuring Denial of Service in Simulation and Testbedexperiments. IEEE Transactions on dependable and Secure Computing, Vol. 6.2,81-95(2009).
9. Botta A, Dainotti A, Pescape A. A tool for the generation of realistic network workload for emerging networking scenarios. Computer Networks 2012,56(15):3531-47.
10. Sachdeva M, singh G, Kumar K, Singh K. Measuring impact of DDoS attacks on web services ICCC(2010).
11. Sommers J, Kim H, Barford P.,Harpoon: a flow-level traffic generator for routter and network tests. In: ACM SIGMETRICS performance evaluatonreview, vol. 32(1). ACM;June 2004.392-392.
12. White B, Lepreau J, Stroller L, Ricci R, Guruprasad S, Newbold M, et al. An integrated eperimental environment for distributed systems and networks. AZM SIGOPS Operar Syst Rev 2002; 36(SI):255-70.
13. Sajal Bhatia, Desmond Schmidt, George Mohay, Alan Tickle: a framework for generating realistic traffic for Distributed Denial of Service attacks and Flash events. Computers and Security 40(2014)95-107.
14. Aversa R, Di Martino B, Ficco M, venticinque S. A simulation model for localization of pervasive objects using heterogeneous wireless networks. Simulation modelling practice and theory 2011: 19(8):1758-1772.
15. IIk D, Volf,Jakpob M, Agents for games and simulation. Distributed platform for large scale agent based Simulation, Lecture Notes in Computer Science LNCS 2009;5920:16-32.
16. Jelena Mirkovic, Peter Reiher,"Taxonomy of DDoS Attacks",2004.
17. Jelena Mirkovic, Alfefiya Hussain, Brett Wilson and Sonia Fahmy,"Towards user Centric Metrics for Denial of Service Measurement", ACM,june2007.
18. Monika Sachdeva, Krishan Kumar, Gurwinder Singh and Kuldip Singh,"measuring the impact of DDoS attacks on Web services", Journal of information Assurance and Security,2010,392-400.
19. Krishan kumar,A.L. Sangal,Abhinav Bhandari,"Traceback Techniques Against DDoS attack: A comprehensive Review",in the proceedings of 2nd international Congerence Computer and Communications Technologies organised by MNLR,NIT Allahbad.Sept. 2011.
20. Behal, K Kumar,"An Experimental analysis for malware detection using extrusion", IEEE Conference of Computer and Communication Technology,2011.
21. S. Schwab, B. Wilson, C. Ko, and A. Hussain. SEER:A Security Experimentation Environment for DETER. InProceedings of the DETER Community Workshop on Cyber Security Experimentation and Test on DETER Community Workshop on Cyber Security Experimentation and Test 2007, 2007.
22. D. Schmidt, S. Suriadi, A. Tickle, A. Clark, G. Mohay,E. Ahmed, and J. Mackie. A Distributed Denial of Service Testbed. IFIP Advances in Information and Communication Technology, 2010.
23. Sunny Behal and Krishan Kumar,"Trends in Validation of DDoS Research", International Conference on Computational Modeling and Security,2015.
24. NS2,. The network simulator 2 http://www.isi.edu/nsnam/ns/. 2015. URL: http://www.isi.edu/nsnam/ns/.
25. NS3,. The network simulator 3 http://www.nsnam.org/. 2015. URL: http://www.nsnam.org/.
26. OMNET++,. The network simulator http://omnetpp.org/. 2015. URL: http://www.omnetpp.org/.
27. Ahrenholz, J., Danilov, C., Henderson, T.R., Kim, J.H.. Core: A real-time network emulator. In: Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE; 2008.
28. DETER,. The deter testbed http://www.deter-project.org/. 2015.
29. Bhatia, S., Mohay, G., Tickle, A., Ahmed, E.. Parametric di erences between a real-world distributed denial-of-service attack and a flash event. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. IEEE; 2011.
30. CAIDA,.The caida ddos attack dataset http://www.caida.org/data/passive/ddos-20070804dataset.xml. 2007.
31. DARPA,. The darpa ddos attack dataset. 2009. URL: http://www.isi.edu/ant/traces/DARPA\\2009DDoSattack-20091105.README.txt.

32. FIFA, . The fifa world cup dataset http:// ita.ee.lbl.gov/html/contrib/worldcup.html. 1988.

33. Bhuyan, M.H., Bhattacharyya, D., Kalita, J.. An empirical evaluation of information metrics for low-rate and high-rate ddos attack detection. Pattern Recognition Letters 2015.

34. Jaswinder Singh,Krishan Saluja, Monika Sachdeva,Navjot Sidhu,.DDoS attack Simulation Using Legitimate and attack Real Data Sets. International journal of Science and Engineering Research, Vol 3,june-2012,2229-5518.

35. Monika Sachdeva, gurvinder Singh, Krishan Kumar,."An Emulation Based Impact Analysis of DDoS attacks on Web services during Flash Events", International Conference on Computer and Commmunication Technology(ICCCT)-2011.

36. Erol Gelenbe, Michael Gellman, and George Loukas,"An Autonomic Approach to Denial of Service Defence"

37. ATTACk1,:http://www.bbc.com/news/technology-35376327.

38. AKAMAI,:https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp.

39. ATTACK2,:https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/project-mayhem/.

40. ATTACK3,:https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/hactivism-us-presidential-election/.

41. H Kaur, S Behal, K Kumar,"Characterization and comparison of Distributed Denial of Service attack tools", IEEE Conference on Green Computing and Internet of Things,2015.