Volume 2, No. 4, July-August 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Comparing Popular DDoS Defenses Using Various Attack Distributions – An Experimental Analysis

Rashpinder Pal*, Sunil Kumar and Preetinder Kaur
*M.Tech. Scholar, Department of Computer Science & Engineering,
Bhai Maha Singh College of Engineering, Sri Muktsar Sahib, Punjab, India
er.rashpinder@gmail.com
sunil.budhlada@gmail.com
inderpreet_bti@yahoo.co.in

Abstract— Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper presents comparative analysis of existing DDoS Defenses and classifies them in various scenarios, and thus provides researchers with a better understanding of the problem and the current solution space. In order to make our defenses effective, we need precise and comprehensive DDoS Defenses' comparison. In this paper, we have emulated network topology and generated Flash Event. The attack traffic is generated at different strengths using different protocols in order to effectively compare the DDoS Defenses and get a better conclusion. This paper compares COSSACK, D-WARD and FloodWatch Defenses. It shows how this comparison dictates the advantages and deficiencies of these Defense mechanisms.

Keywords— DDoS, Defenses, Comparison, Analysis.

I. INTRODUCTION

Denial of Service (DoS) attacks attempt to make a computer resource unavailable to its intended users. The attacks in DDOS Scenario become coordinated and come from multiple sources at the same time thus are even more devastating [1]. The bandwidth congestion attacks are identified as "Bulls Eye" in the communications substrate and attackers flood them with large volumes of traffic in case of web services [2].

To circumvent detection, attackers are increasingly moving away from pure bandwidth floods to stealthy DDoS attacks that mimic flash crowds. Unlike traditional single-source attacks, DDoS attacks are virtually impossible to trace due to the numerous attack paths and the multiple levels of indirection [5]. Moreover, attack tools are constantly evolving and some already incorporate defenses like encryption and "decoy" packets to sidetrack their detection.

This paper proposes a comparative analysis of defense systems. It facilitates a global view of the problem and solution space. By setting apart and emphasizing crucial features of defense mechanisms, while abstracting detailed differences, these comparisons can be used by researchers to answer many important questions:

A. Which attacks have been handled effectively by existing defense systems?
B. What attacks still remain unaddressed and why?
C. How would defense mechanisms perform if attack occurred?
D. What are defense mechanisms' vulnerabilities?
E. Can defense mechanisms complement each other and how?
F. Is there some deployment points that are better suited for defense mechanisms?
G. How can I contribute to the DDoS field?

The proposed comparisons are complete because, the defense systems' comparison covers commercial approaches that are sufficiently documented to be analyzed. We provide representative examples of existing mechanisms.

These comparisons may not be detailed as possible. Many published defense classes could have been left out. Also, new defense mechanisms are likely to appear, thus adding new comparisons to the ones we propose.

Our goal was to select several important features of defense mechanisms that might help researchers design innovative solutions, and to use these features as comparative criteria. It is our hope that our work will be further extended by other researchers.

This paper does not propose or advocate any specific DDoS defense mechanism. Even though some sections might point out vulnerabilities in certain classes of defense systems, our purpose is not to criticize, but to draw attention to these problems so that they might be solved. Following this introduction, Section 2 investigates the causes of DDoS attacks, and Section 3 discusses the DDoS defense challenge, Section 4 provides an overview of related work and Section 5 proposes metrics to measure performance of DDoS defense systems. Section 6 discusses Experimental setup. Section 7 provides detailed comparison, and Section 8 concludes the paper.

II. DDOS ATTACKS

The rapid expansion of the Internet and the proliferation of low-cost PCs are two important factors that have made DDoS feasible. In addition, the following recent trends have contributed to the rise in DDoS attacks:

A. The increase in the number of new software and the (inevitable) security vulnerabilities that accompany them, present many opportunities to hijack computers.

B. The number of computers with broadband connections has been rapidly increasing. Not only do these computers pose a danger (if hijacked) due to their high-speed connections, but their "always on" nature makes them far more susceptible to compromise.
C. The lack of automated security update of software vulnerabilities means that the user is responsible for carrying out this task manually. Since many users either lacks the time, knowledge or motivations to do so, many systems remain running software with known insecurities.
D. The availability of attack tools (along with instructions on how to use them) on several web sites, drastically expands the number of potential attackers, who no longer need to understand the operation of the tools in order to use them. Termed "script kiddies", attacker can use attack tools without understanding them.

The lack of attribution, impossibility of securing every machine on the Internet, and difficulty of performing intrusion detection, mean that host-based or highly localized solutions to neutralize DDoS attacks will not work.

III. DDOS DEFENSES CHALLENGES

Although many DDoS defenses have been developed, the problem is hardly tackled, let alone solved. Why is this so? There are several serious factors that hinder the advance of DDoS defense research [3].

A. Need for a Distributed Response at Many Points on the Internet:

It is frequently necessary to have a distributed, possibly coordinated response system. Since the Internet is administered in a distributed manner, wide deployment of any defense system or even cooperation between networks cannot be enforced or guaranteed. This discourages many researchers from even designing distributed solutions.

B. Economic and Social Factors:

A distributed response system must be deployed by parties that do not suffer direct damage from the DDoS attack (source or intermediate networks). This implies an unusual economic model since parties that will sustain the deployment cost are not the parties that directly benefit from the system.

C. Lack of Detailed Attack Information:

It is necessary to understand DDoS attacks in order to design imaginative solutions for them. While there exist publicly available analyses of popular DDoS attack tools [27, 28, 29, 64], what is lacking is the information on frequency of various attack types (e.g., UDP floods, TCP SYN floods), and the distribution of the attack parameters such as rate, duration of the attack, packet size, number of agent machines, attempted response and its effectiveness, damages suffered, etc.

D. Lack of Defense System Benchmarks:

Many vendors and researchers make bold claims that their solution completely handles the DDoS problem. There is currently no benchmark suite of attack scenarios or established evaluation methodology that would enable comparison between defense systems. Such a situation is likely to discourage networks from investing in DDoS protection, since they cannot be assured of the quality of the product being purchased.

E. Difficulty of large-scale testing:

DDoS defenses need to be tested in a realistic environment. This is currently impossible due to the lack of large-scale test-beds, safe ways to perform live distributed experiments across the Internet, or detailed and realistic simulation tools that can support several thousands of nodes. Claims about defense system performance are thus made based on small-scale experiments and simulations, and are not credible.

F. Manual intervention:

Many DDoS Defenses require a high degree of manual intervention. Individuals highly trained in network operations and security, pour over audit data and form convincing hypotheses consistent with the audit trails. They then contact other ISPs in the Internet to confirm suspicious traffic patterns and coordinate a collective response to the attack.

IV. RELATED WORK

The D-Ward system [4] monitors outgoing traffic from a given source network and attempts to determine outgoing attack traffic. Attack traffic is identified by comparing the traffic patterns against models of reasonable congestion control behavior. For example, TCP traffic is monitored and compared to an equation approximation of the TCP congestion control model. TCP streams that are observed violating the behavior of the model is marked as an attack and is subsequently throttled back by the edge network's egress router. The amount of throttling is proportional to the flows deviation from its expected behavior. In a similar fashion, the same approach can be applied to other transport protocols. The health of destination hosts can be gleaned using ICMP echo/reply probes or other techniques that generate the necessary 2-way traffic needed to analysis the compliance of a given flow to reasonable congestion control behavior.

COSSACK [5] forms a multicast group of defense nodes which are deployed at source and victim networks. Each defense node can autonomously detect the attack and issue an attack alert to the group. Sources involved in the attack cooperate with the victim to suppress it. Cossack is a distributed approach to DDoS detection and response. Rather than observing traffic in the core of the network, Cossack adopts an approach that involves observing traffic at the egress/ingress point of individual edge networks. Observation of egress edge network traffic is also being explored in the D-Ward project [4]. The D-Ward approach of performing localized attack detection at the source edge network shows reasonable promise, but without any coordination among instances of D-Ward agents, the detection process may be error prone and penalize non-attack traffic.

Flood Watch [6], the DDoS defense system developed under this project, is an integrated detection and response system that has been shown effective against current DDoS attack tools and some stealthier variants. The detection module measures statistical properties of specified fields in packet headers, watching for anomalies that may indicate

DDoS attacks. This module computes two statistics: First, Entropy (a measure of randomness of a set of values); and second, Divergence of frequency-sorted distributions from a baseline using the chi-square statistic.

V. PERFORMANCE METRICS

The organizations do not understand the actual losses that are suffered by then due to growing number of DoS and DDOS attacks. The wastage of time caused to legitimate clients result in lost revenues as time is money in on-line business. In current work, our focus is on measuring these network performance metrics without attack, under attacks and with Defense Applied. We have measured performance using following metrics:

A. Goodput (GP):

Good-put is defined as no. of bits per second of legitimate traffic that are carried by the backbone link, whereas bad-put gives no. of bits per second of attack traffic that flow through the backbone Link.

B. Response Time (RT):

The 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 (TCS)+ server delay(TS)+ time required for packet to reach to client from server(Tsc). So RT= TCS+ TS+ TSC. For most of applications, response time is really critical.

C. No. of Active Connections (NAC):-

No. of clients which have completed three way handshake (in case of TCP) and started sending data. It clearly highlights number of live connections interacting with the server. In case of attacks due to packets drop at backbone point, even connection start up packets can be dropped causing decrease in legitimate connections and No. of active connections increase rapidly when defense is applied.

D. Backbone Link Utilization (BLU):

Backbone Link Utilization is defined as percentage of bandwidth that is being used for good put.

E. Authenticating Overhead (AO):-

Every defense requires some authenticating mechanism in order to detect the DDoS Attacks. This authentication process takes some time to validate the legitimate packets and hence precious network time is wasted, so this overhead must be as low as possible to keep the QoS requirements fulfilled by the network.

VI. EVALUATION IN TESTBED EXPERIMENTS

The cost of building a real distributed testing defense environment is high. Simulation is an important method in network research, but sometimes simulations are unable to show the realistic traffic parameters and actual attack parameters, So Experiments on Test-beds is a better approach in network research as Experiments can be used to analyse Network-related problems with much less cost and in a more efficient and realistic way.

We evaluate our metrics in experiments on the DETER test-bed using SEER GUI environment [7] [8]. 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. Following subsections deals with experimental methodology [9] and parameters.

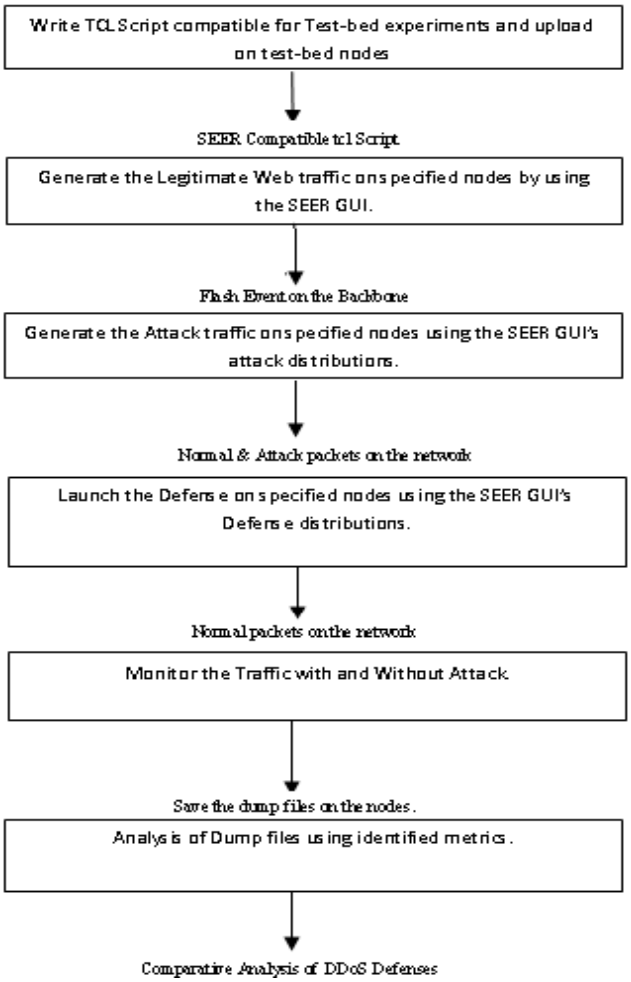


Figure 1: Procedure of Experimental methodology

A. Topology:

One legitimate network, one attack network and one Servers network are connected via two core routers. Legitimate network has 20 legitimate client nodes, and is connected to the core via an access router. Links between the access router and the core have 100 Mbps bandwidth; the backbone is chosen to mimic high bandwidth.

B. Background Traffic:

Each client generates Web traffic. We have generated realistic traffic. Clients talk with Web server 'V' in server network. All attacks target the server 'S' and cross its backbone link, so the web traffic coming at Server 'V' should be impacted by the attacks.

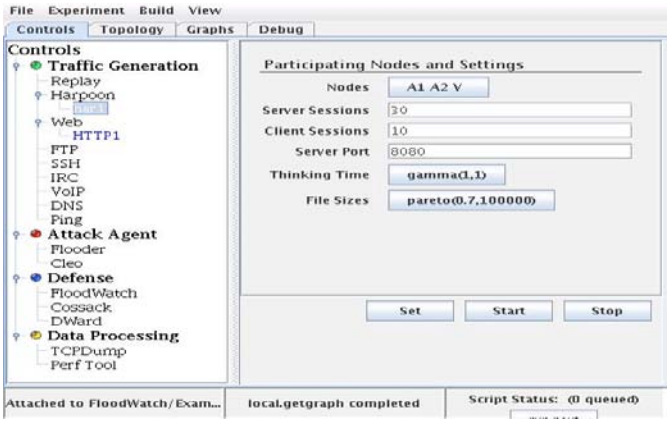


Figure 2: SEER GUI Main Window Frame

C. Attack Traffic:

We have used UDP, TCP, and ICMP traffic for generating DDoS flood. In this experiment, we have generated UDP, TCP and ICMP bandwidth flood with PULSE distribution to achieve attacks in different scenarios which are very similar to the realistic conditions.

D. Defences:

We have performed our comparative analysis on three defenses provided in older versions of SEER as third party applications i.e. D-WARD, COSSACK and Flood Watch, These defenses are required to be installed manually on the nodes to support the newer versions of SEER. After launching the attack for some time, each defense is applied to measure its efficiency on various attack distributions.

VII. RESULTS AND DISCUSSIONS

We conducted our experiments using parameters listed in previous sections. In The Experiment

a. First 20 seconds are allocated for Legitimate traffic only,
b. Next 20 seconds (20-40 sec) are allocated for performing various attacks, Both legitimate and attack traffic flows through the network
c. In the last part of the experiment (40-60 sec) Different Defenses have been applied and their results are compared to show their effect on Pulsing Attacks.

This experiment has been performed several times to launch different parameters of attacks and defenses. Log files have been analysed using PERL scripts to get average values and then using them for graphs. The effect of DDoS attacks on the performance of web service is analysed below:-

A. Good put:

During a DDoS attack, bottleneck link is attacked to force the edge router at the ISP of victim end to drop most legitimate packets. In the following explanations, we concentrate on the Goodput Line to get the measure of actual loss during attack and after applying the defense.

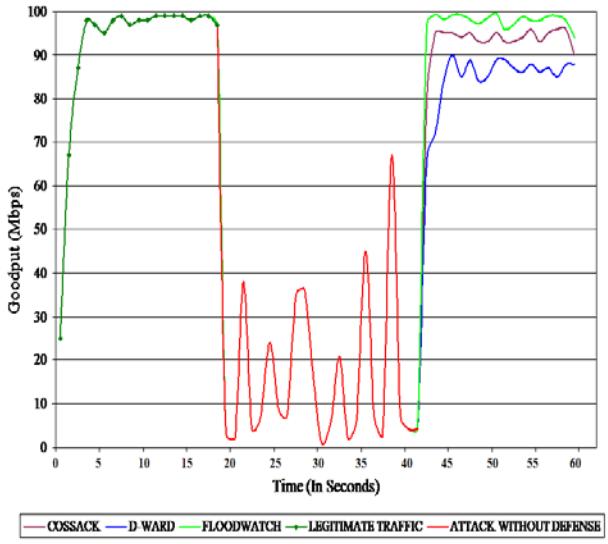


Figure 3: Comparison of Goodput With TCP Pulse Attack

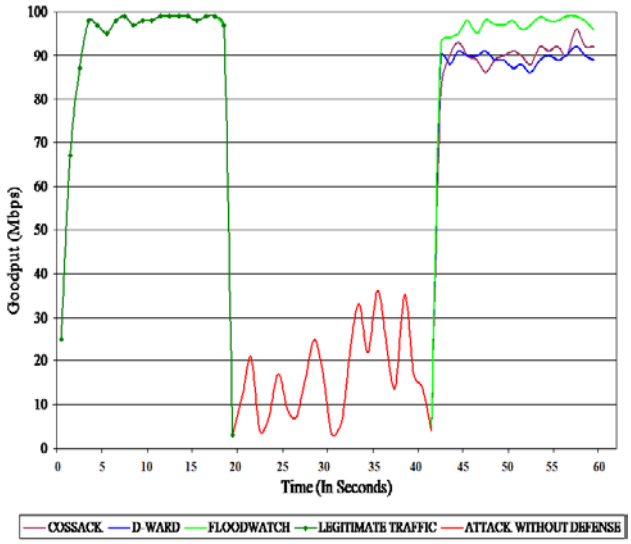


Figure 4: Comparison of Goodput With UDP Pulse Attack

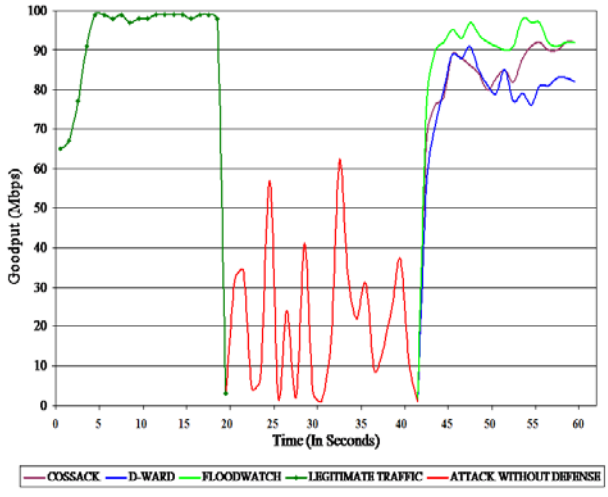


Figure 5: Comparison of Goodput with ICMP Pulse Attack

B. Average Response Time:

Web services need minimum response time to finish an HTTP transaction. HTTP transaction is considered a successful one it is completed in less than 10 seconds Calvin

et. Al. [10] Therefore, we calculate the average Response Time based on HTTP transactions which finish in 10 seconds. The average Response Time is increased almost 3 to 5 times during the attack as compared to legitimate.

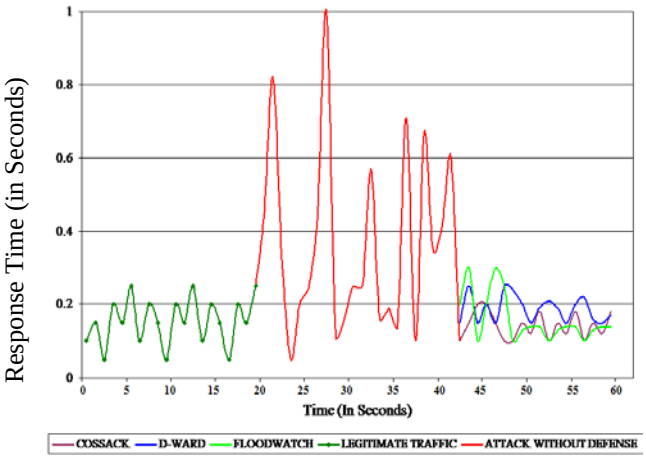


Figure 6: Comparison of Response Time (TCP Pulse Attack)

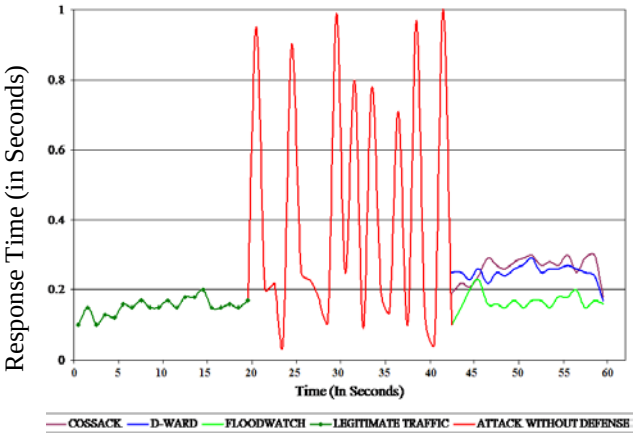
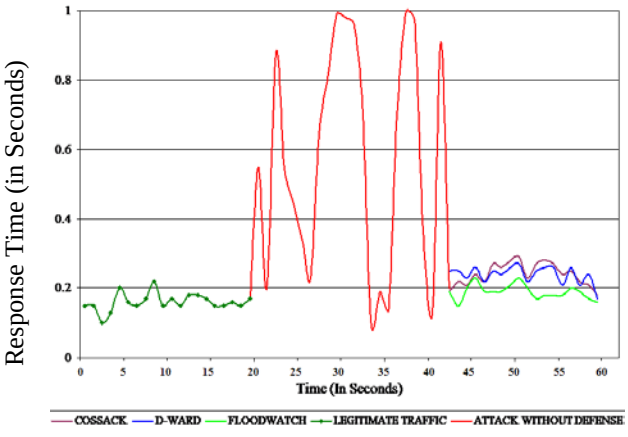


Figure 7: Comparison of Response Time (UDP Pulse Attack)



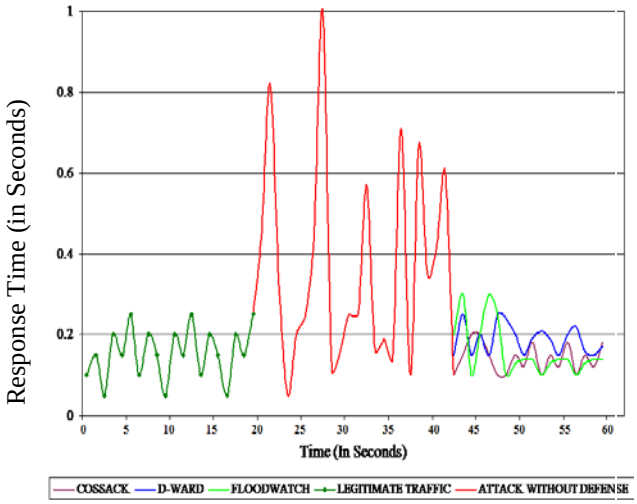


Figure 6: Comparison of Response Time (TCP Pulse Attack)

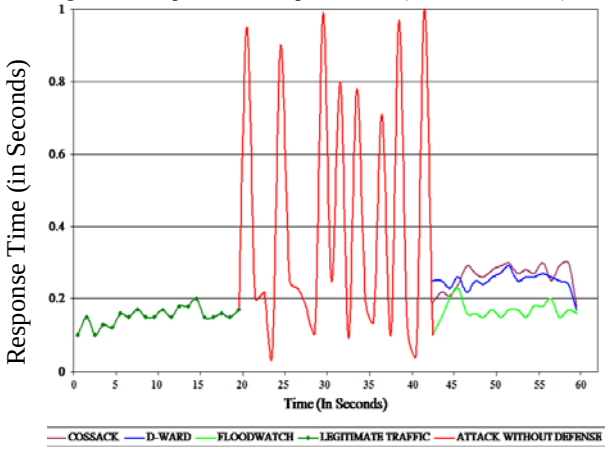


Figure 7: Comparison of Response Time (UDP Pulse Attack)

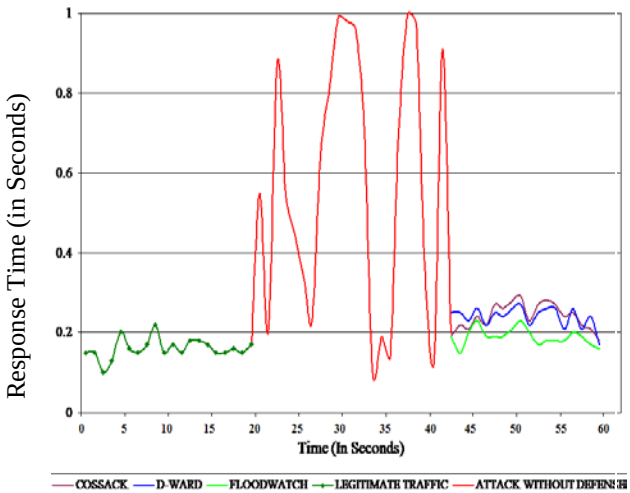


Figure 8: Comparison of Response Time (ICMP Pulse Attack)

C. Average No. of Active Connections:

Average No. of Active Connections is no of clients which have completed three way handshakes and started sending requests. Hence legitimate clients are denied services once attack is launched.

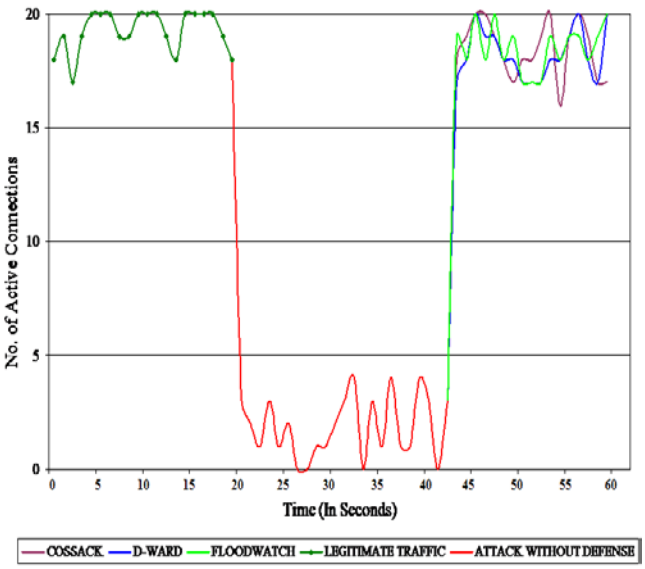


Figure 9: Comparison of Active Connections with TCP Pulse Attack

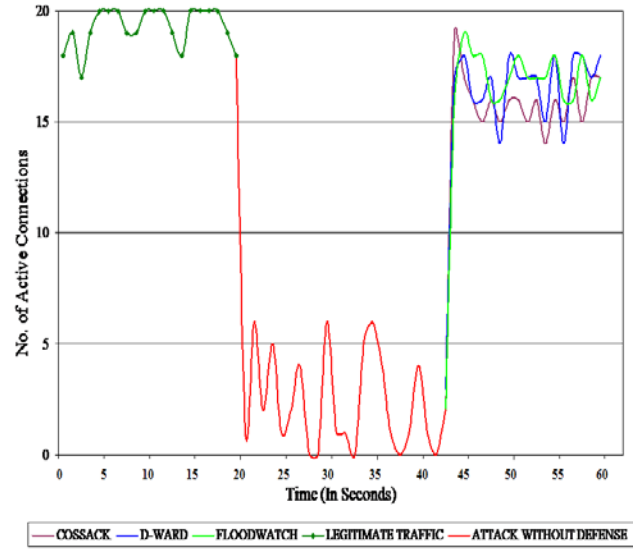


Figure 10: Comparison of Active Connections with UDP Pulse Attack

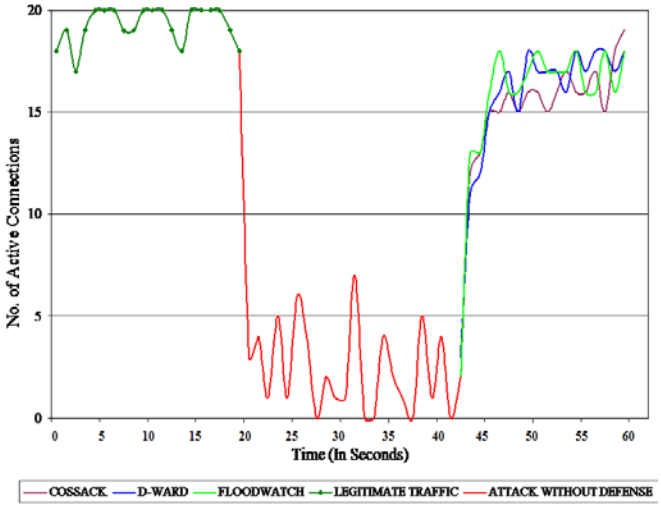


Figure 11: Comparison of Active Connections with ICMP Pulse Attack

D. Bottleneck Bandwidth Utilization:

Bottleneck bandwidth utilization is defined as percentage of bandwidth that is carrying legitimate traffic. As shown in figure 12, Bottleneck bandwidth utilization is nearly 100% without attack. During Attack, Bottleneck bandwidth utilization drops more than 50%. As normal TCP traffic follows congestion control signals [11], [12] so when a TCP packet is dropped, it further drops the rate of traffic originating at TCP source. But attack traffic does not follow these signals, so legitimate traffic sharply declines whereas attack traffic grows heavily.

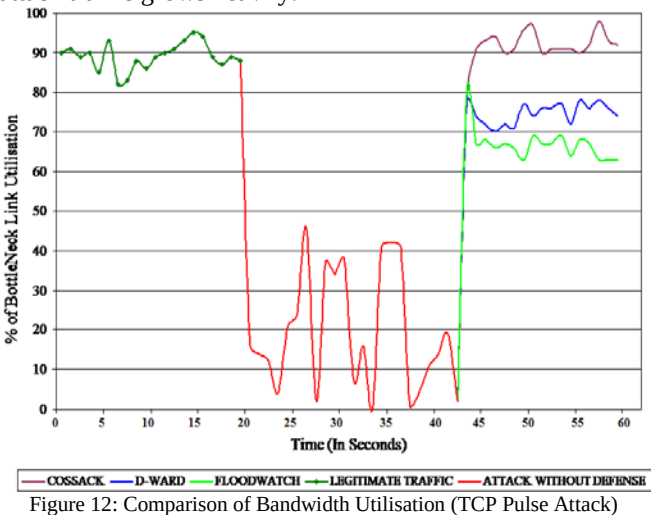


Figure 12: Comparison of Bandwidth Utilisation (TCP Pulse Attack)

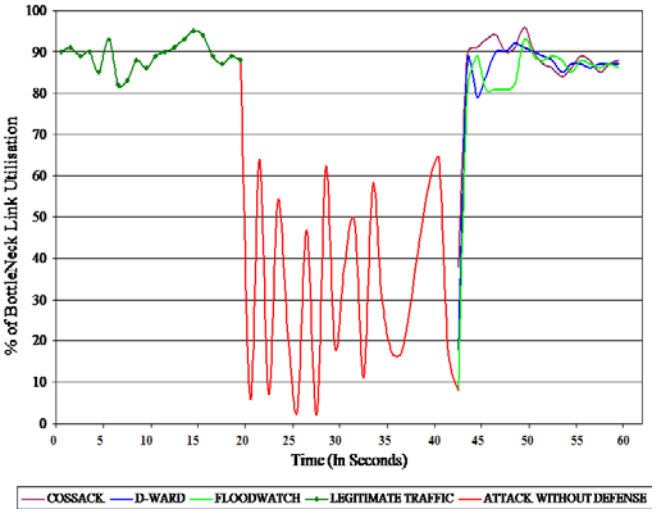


Figure 13: Comparison of Bandwidth Utilisation (UDP Pulse Attack)

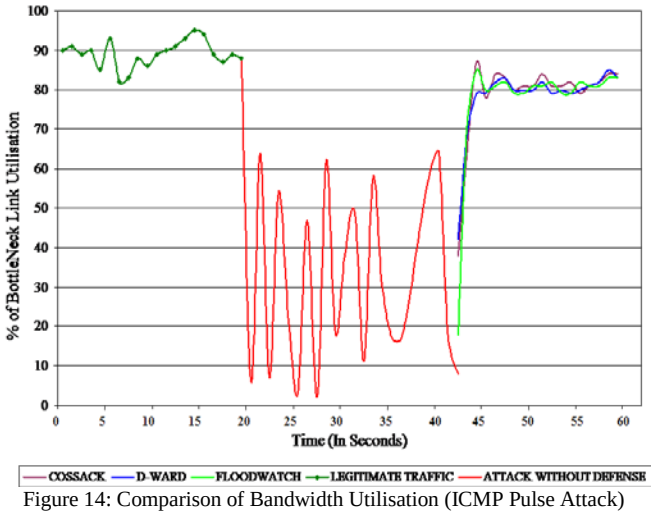


Figure 14: Comparison of Bandwidth Utilisation (ICMP Pulse Attack)

E. Authentication Overhead:

The overhead of applying the defense in the intermediate, source or Victim End is called authentication overhead, due to which the Network devices are influenced because they get busy in blocking the attacks rather then

fulfilling the QoS requirements. It is an important metric to consider for the efficiency of the Defense.

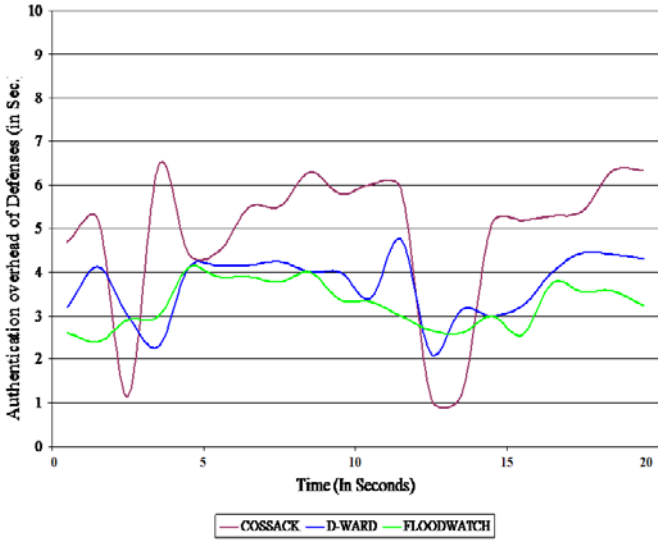


Figure 15: Comparison of Authentication overhead of given defenses

VIII. CONCLUSION AND FUTURE SCOPE

There are various defense mechanisms available in related work for reducing impact of DDoS Attacks; existing defenses are implemented at Source or Destination network. Each technique has some limitations due to openness and vulnerabilities in the architecture of internet and they are unable to defend the bandwidth floods [13] [14] [15] [16] that mimic flash crowds. Few defense mechanisms have been employed at intermediate networks also, but those mechanisms increase the job of routers, because of their complex implementation, which is not acceptable due to high QoS requirements.

Measurement of Service during DDoS attacks and defenses are quantified in terms of Good-put, Response Time, Active Connections, Bottleneck Bandwidth Utilization and Authentication Overhead in this work. We evaluate our metrics in experiments on the DETER test-bed [7] [8]. We generated attacks at different strengths so that DDoS defenses' efficiency can be compared at different scenarios of attack. Moreover the quantitative measurements clearly indicated degradation of web service with and without attacks. The future scope of this work is summarized as below: -

A. Computing the cumulative comparison of DDoS defenses by combining weight of all the metrics.
B. Building a new Secure-Protocol based defense by introducing all the good features of existing defenses.

IX. REFERENCES

[1]. P.G Neumann, "Denial-of-Service Attacks", Communications of the ACM, Volume 43, no. 4, pp. 136-136.

[2]. D.L Cook, W. G. Morein, A.D. Keromytis, V. Misra, and D. Rubenstein, "WebSOS: protecting web servers from DDoS attacks". 11th IEEE International Conference on networks (ICON), pp. 461 – 466, 2003.

[3]. J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April, 2004.

[4]. J. Mirkovic, "D-WARD: Source-End Defense Against Distributed Denial-of-service Attacks", Ph.D. Thesis, University of California, Los Angeles, 2003.

[5]. C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, R. Govindan, "COSSACK: Coordinated Suppression of Simultaneous Attacks".

[6]. SPARTA Inc. FloodWatch: Distributed Denial-of-Service Detection and Response.

[7]. 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", 2nd IEEE TridentCom Conference, March 2006.

[8]. 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", Proceedings of Tridentcom, 2007.

[9]. Monika Sachdeva, Gurvinder Singh, Krishan Kumar and Kuldip Singh, "Measuring Impact of DDOS Attacks on Web Services", Journal of Information Assurance and Security 5, p.p 392-400, January 2010.

[10]. C. Ko, A. Hussain, S. Schwab, R. Thomas, and B. Wilson. "Towards systematic IDS evaluation", Proceedings of DETER Community Workshop, pp. 20-23, June 2006.

[11]. M. Kisimoto. Studies on Congestion Control Mechanisms in the Internet – AIMD-based Window Flow Control Mechanism and Active Queue Management Mechanism, Master Thesis, Osaka University, 2003

[12]. S. Floyd and K. Fall. "Router Mechanisms to Support End-to-End Congestion Control," Lawrence Berkeley Laboratories Technical Report, 1997.

[13]. H. Jamjoom, and K. G. Shin, "Persistent Dropping: An Efficient Control of Traffic", In *ACM SIGCOMM*, 2003.

[14]. T. Anderson. T. Roscoe, and D. Wetherall, "Preventing Internet Denial-of-Service with Capabilities", In *HotNets*, 2003.

[15]. T. Gil and M. Poletto, "MULTOPS: A Data-Structure for Bandwidth Attack Detection", In *USENIX Security*, 2001.

[16]. A. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services", In *ACM SIGCOMM*, 2002.

AUTHOR'S PROFILE

Rashpinder Pal is an M. Tech student in Department of CSE at BMSCE, Sri Muktsar Sahib Punjab, India.He has done his B. Tech. CSE from GZSCET, Bathinda in 2008. His research interest include Network Security.

Sunil Kumar is an M. Tech in CSE from BMSCE, Sri Muktsar Sahib Punjab, India. He has done his B.E.in CSE from C I TM, Faridabad in 2008. His research interest include DDoS Defenses.

Preetinder Kaur is an M. Tech in CSE from Punjabi University, Patiala Punjab, India. Her research interests include Databases, DDoS Attack Impact Measurement and Defenses.