"Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks"

Neha Tewari[*] , Akash Bhardwaj[**]
[*] Department of Computer Science and Engineering,
Lovely Professional University,
Jalandhar, India
[**] Department of Computer Application,
Lovely Professional University,
Jalandhar, India

Abstract- Distributed Denial of Service (DDoS) is a rapidly growing problem. DDoS attacks pose a severe security threat to the steady functioning of any network. These attacks degrade or completely disrupt services to legitimate users by eating up communication, computational, and memory resources of the target through sheer volume of useless traffic. The outcome of this fact is that legitimate users are denied service.
Based on the volume of traffic used by the attackers, DDoS attacks can be classified as Low Rate attacks and High Rate attacks. Low rate DDoS attacks consume lesser resources for long time in contrast to High Rate DDoS attacks which consume more resources for less time.
In this work "Flow Statistics Based Detection of Low Rate and High Rate DDoS Attacks", an Entropy Based Scheme is used for effective detection of both low rate and high rate DDoS attacks. In this scheme, changes in distributional aspects of packet header fields are considered for effective detection. The simulation experiments are done in ns-2 simulator. Also a rigorous study is done on MIT Lincoln Laboratory Data Sets provided for the 1999 DARPA Intrusion Detection off-line evaluation.
We detected both low rate degrading and high rate flooding DDoS attacks. In case of low rate degrading attacks, the entropy value increases than the value in case of normal behavior whereas in case of high rate bandwidth disruptive attacks, the value decreases. Also, we observed that there is a shift in the entropy distribution of individual flows in a time window.

Index Terms- DDOS; Smaller Response Time; Enhanced Throughput of Networks; Secure communication.

I. INTRODUCTION

The basic needs of human beings to live society is to exchange messages ,or information securely. The Internet has revolutionized the computer and communications world like nothing before [1]. The technological evolution began with early research on packet switching and the ARPANET. The Internet was created in 1969 to provide an open network for researchers [2]. The world is evolving towards interconnecting computers, mobile communication devices and even household appliances together. With the growth of the Internet, the attacks to the Internet have also increased incredibly fast. The widespread need and ability to connect machines across the Internet has caused the network to be more vulnerable to intrusions and has facilitated break-ins of a variety of types. According to [2], a mere 171 vulnerabilities were reported in 1995 which boomed to 7236 in the year of 2007. Apart from these, a large number of vulnerabilities go unreported each year. Secure communication has some desirable aspects such as confidentiality, authentication, message integrity and non-repudiation. Besides, people are aware of Denial of Service (DoS) attacks that render a network, host, or other piece of network infrastructure unusable by legitimate users; especially it is against the frequently visited web sites of a number of high-profile companies or governments. In Distributed Denial of Service (DDoS) attacks scenario, the attacks become coordinated and come from multiple sources at the same time, thus are even devastating.

A Denial of Service (DoS) attack is an event in which a legitimate user or organization is deprived of certain services, like e-mail or network connectivity, that they would normally expect to have. DoS attacks [3, 4] inject maliciously-designed packets into the network to deplete some or all of these resources.

The attack power of Distributed DoS (DDoS) attack [5] is based on the massive number of attack sources instead of the vulnerabilities of one particular protocol. DDoS attacks, which aim at overwhelming a target server with an immense volume of useless traffic from distributed and coordinated attack sources, are a major threat to the stability of the Internet. Distributed Denial of Service (DDoS) attacks pose an immense threat to the Internet, and many defense mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks [6].

There are four different ways to defend against DoS attacks [6]:

1) Attack prevention to fix security holes, such as insecure protocols,
2) Attack detection aims to detect DoS attacks in the process of an attack,
3) Attack source identification aims to locate the attack sources,
4) Attack reaction aims to eliminate or curtail the effects of an attack.

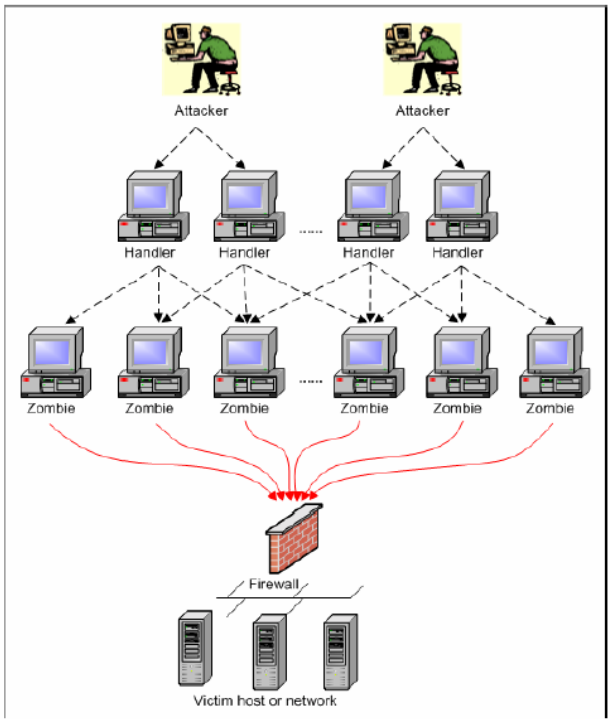

Figure 2.1 A hierarchical model of a DDoS attack

II. PROPOSED SYSTEM

We are proposing to implement the entropy-based scheme of DDoS attack detection, the simulation on a simple topology has been carried out using Network Simulator (ns-2).

A. Simulation Topology

Figure illustrates the simulated network topology. The topology considered is similar to the one used traditionally to depict a typical client-server scenario in the Internet for simulation purposes [13].

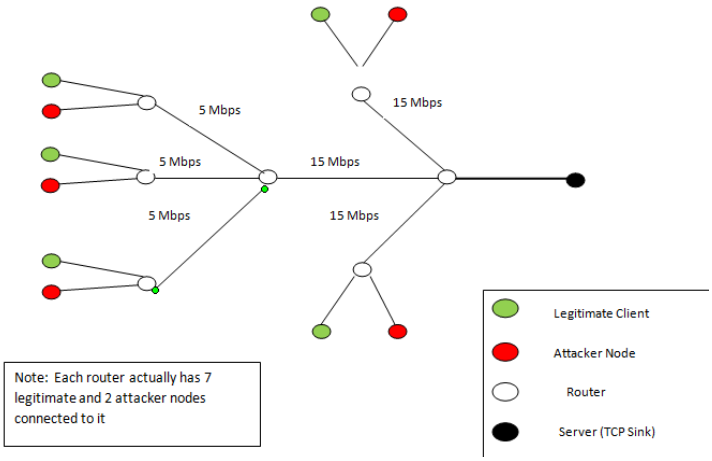

Figure. Topology used for Simulation

The legitimate clients are TCP agents which request files from the server using the FTP protocol. The attackers are modeled by UDP agents. For high rate attacks, the bit rate is kept very high (3 Mbps). The low attack bit rate is kept at 0.5 Mbps. The access bandwidth for each client node is kept at 5 Mbps. The router – router bandwidth is 5 Mbps at the first level and 15 Mbps at the second level. The bottleneck bandwidth is kept at 40 Mbps.

B. Simulation Parameters

Table 1 lists the simulation parameters, their values and description of these parameters used in the simulation.

Parameter	Value	Description
Simulator	Ns-2	Simulation tool
Number of Nodes	53	Network Nodes
Client Load	0.1-0.4	Relative load issued by client requests
Attack load	0-0.9	Relative load due to attack traffic
Simulation time	0-15 sec	Simulation duration
Attack time	2-7 sec	Attack duration
Legitimate Traffic type	TCP	File Transfer Protocol
Attack Traffic Type	UDP	Constant Bit Rate
Client-Router Link Bandwidth	5 Mbps	Bandwidth
Attacker-Router Link Bandwidth	5 Mbps	Bandwidth
Router-Router Link Bandwidth	5 Mbps	BW at 1st level
Router-Router Link Bandwidth	15 Mbps	BW at 2nd level
Router-Server Link Bandwidth	30 Mbps	Bandwidth

Table 1: Simulation Parameters

C. Application procedure of the detection approach

The simulation is carried out on the topology in Figure 1 using the parameters specified in Table 1. The entropy-based detection methodology is then applied for attack detection. A flow is defined by the flow id assigned during simulation setup.

- The simulation is run for the specified duration and the trace file for the packet flows is obtained.
- The packets received at the bottleneck router (the one connected directly to the server) are filtered out from the trace file.
- The packets are divided into windows of time duration 0.2 sec each (This size is chosen to be just greater than the Internet round trip time which is around 120 msec).

For each window, the entropy of individual flows are calculated and added up to get entropy of the window.

For observing the distribution of various entropy values over the flows i.e., frequency of entropy values of individual flows, the analysis is carried out over a number of consecutive windows of the same size and separate curves constructed for each window.

It's the foremost preliminary step for proceeding with any research work writing. While doing this go through a complete thought process of your Journal subject and research for it's viability by following means:

1) Read already published work in the same field.
2) Goggling on the topic of your research work.
3) Attend conferences, workshops and symposiums on the same fields or on related counterparts.
4) Understand the scientific terms and jargon related to your research work.

III. RESULTS

The results obtained for simulation carried out on the topology in Figure 1 are presented next.

A. Results obtained using simulated topology

A normal entropy profile has been created for our topology by disabling all attackers. Subsequently, high rate and low rate attackers are started to get the entropy profiles of the topology under high rate and low rate DDoS attacks.

B. High Rate DDoS Attacks

Figure 3.1 shows the decrease in entropy values of the windows under high rate attack.

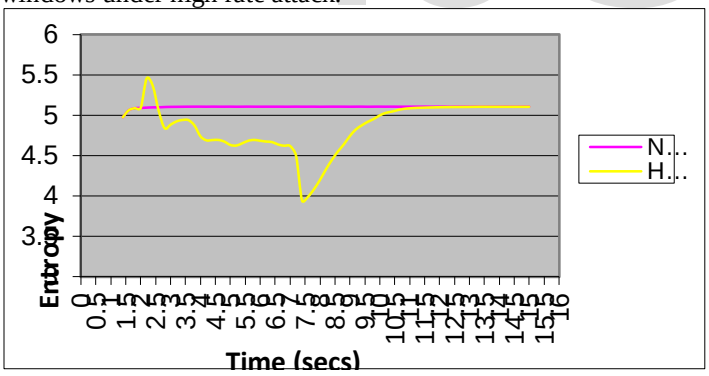

Figure 3.1 Entropy under high rate DDoS attack

C. Low Rate DDoS Attacks

Figure 3.2 shows the increase in entropy values of the windows under low rate attack. Under low rate attack, the distribution of packets flowing in the network becomes concentrated in a large numbers of flows. Hence, the entropy of each window would increase.

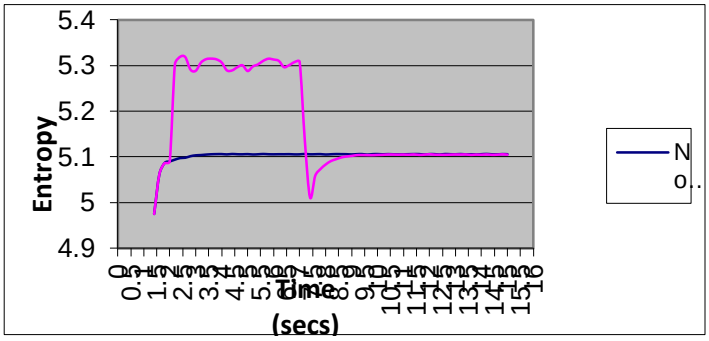

Figure 3.2 Entropy under low rate DDoS attack

Figure3.3 shows the variation in entropy values of the windows under differing attack strengths.

Table 3.1 shows the detection rate and the false positive rates for high rate and low rate DDoS attacks obtained on the topology.

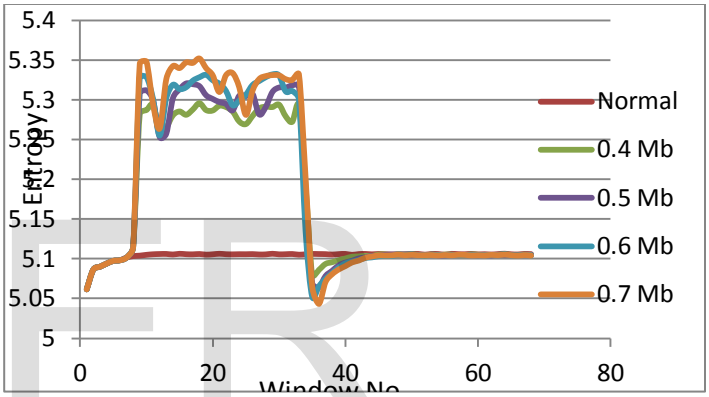

Figure 3.3 Entropy variations under varying strengths of low rate DDoS attacks

Attack Type	Detection Rate	False Positive Rate
High Rate	99.97%	23.7%
Low Rate	99.99%	2%

Table 3.1 Detection rate and False Positive Rates with a = 6

D. Throughput of Bottleneck Link

Figure 3.4 shows the throughput of the bottleneck link for the whole duration of simulation time, i.e., 15 seconds.

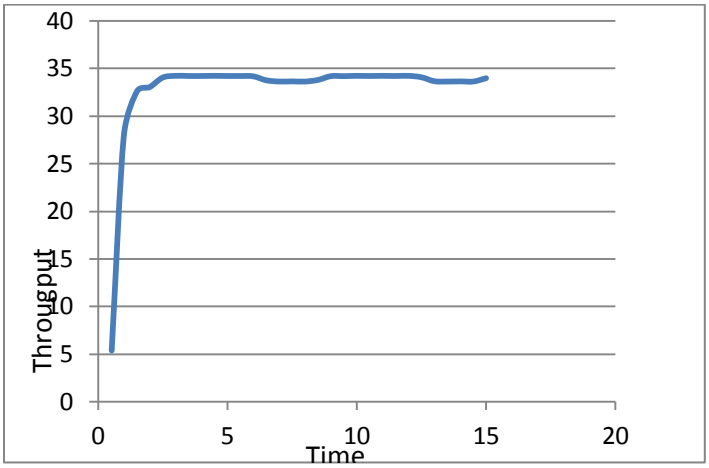

Figure 3.4 Throughput of bottleneck link under no attack conditions

Figure 3.5 shows the variation in throughput of the bottleneck link under a high rate attack. The throughput is found to decrease dramatically during the attack duration. This shows the disruptive effect of a high rate attack on bottleneck bandwidth utilization.

Figure 3.6 shows the variation in throughput under a low rate attack. The decline in throughput is still significant but it is not as large as that for a high rate attack. This shows the degrading effect of a low rate DDoS attack on bottleneck bandwidth utilization.

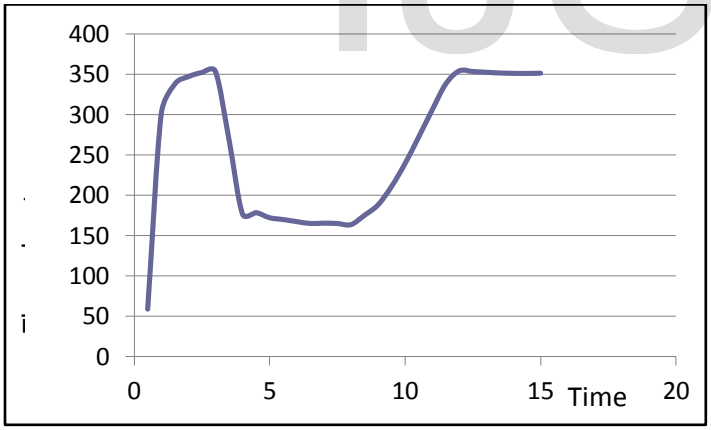

Figure 3.5 Throughput of bottleneck link under high attack conditions

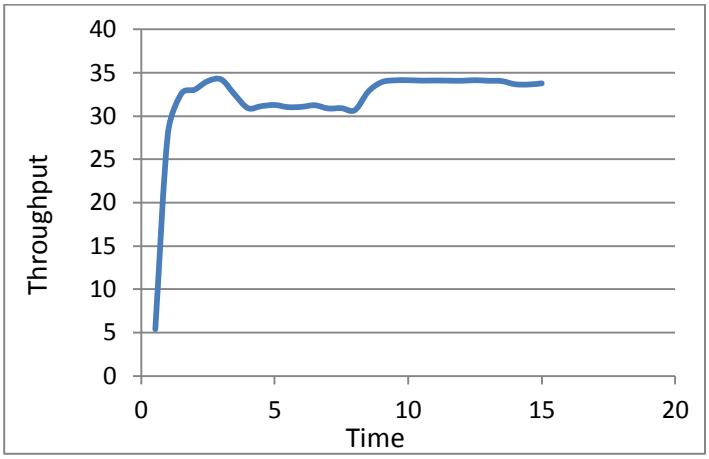

Figure 3.6 Throughput of bottleneck link under low attack conditions

E. Distribution of individual flow entropies

The function used for calculation of entropy flow is given by:

$F(p) = (-1)*p*\log(p), \quad 0 \le p \le 1$

Figure 3.7 shows the variation in F (p) for different values of p.

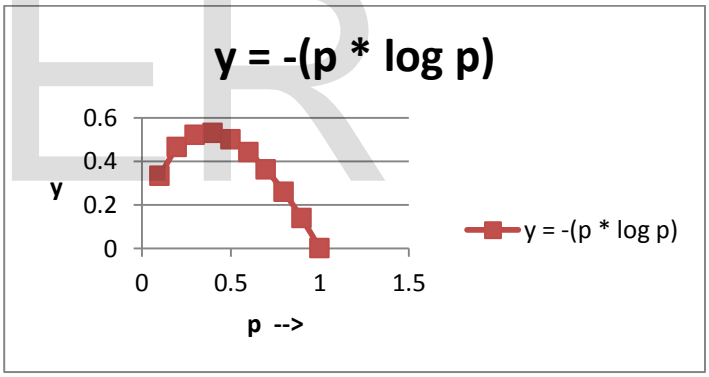

Figure 3.7 Variation of entropy with probabilities

According to the figure, the peak of the curve occurs corresponding to a probability of 0.5. The function is an increasing function for values of 'p' between 0 and 0.5 and it is decreasing for 'p' between 0.5 and 1.

$0 \le p \le 0.5$	Increasing function
$0.5 \le p \le 1$	Decreasing function

Figure 3.8 shows the distribution of individual values of entropies over the flows present in the topology. The curve is drawn under normal flow conditions, i.e., when all attackers are absent and for a single window of size 0.2 seconds. Most of the flows are found to be concentrated around a single entropy value. These observations have been taken over flows in a series of windows of size 0.2 seconds with a separate curve for each window.

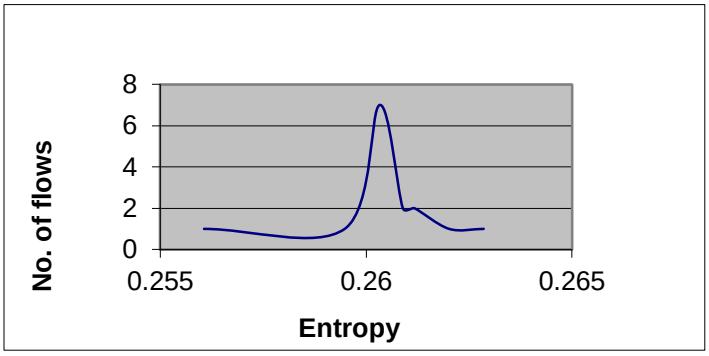

Figure 3.8 Distribution of Entropy over individual flows under no attack

Topology Specifications for Fig. 3.8

35 legitimate users, all of them TCP clients requesting file transfer service from the server. No attack flows in the network.

Analysis of Fig. 3.8

Most of the flows are concentrated around a single entropy value. The area under the curve represents the entropy of the window under no attack conditions.

Low Rate Attacks

Figure 3.9 shows the distribution in entropy values under low rate attack conditions for a single window of size 0.2 seconds. As in Figure 3.8, most of the entropy values are concentrated around a single entropy value. However, this value is left shifted i.e., less than the corresponding value under no attack.

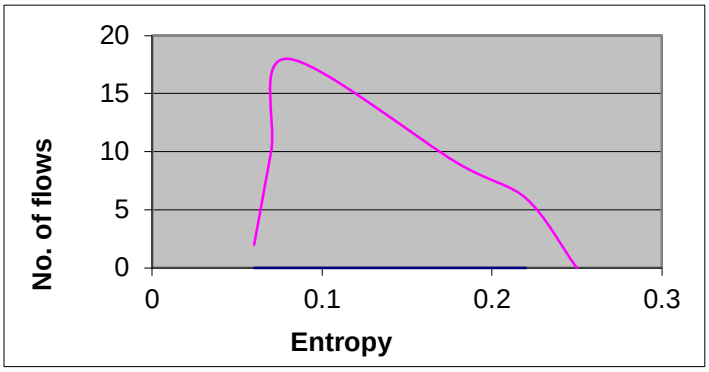

Figure 3.9 Distribution of Entropy over individual flows under low rate attack

Topology Specifications for Fig. 3.9

35 legitimate users, each one a legitimate user requesting FTP service from the server. 10 attackers are taken, with an attack rate of 0.4 Mbps for each. This corresponds to a distributed low rate attack.

Analysis of Fig. 3.9

Compared to Fig. 3.8, the curve peak has shifted to the left, the height of the peak has increased, and the area under the curve has increased. The left shift in the peak is because of the decrease in entropies of all individual flows. This is because probability of an individual flow decreases on increase in the number of flows, and according to Fig. 3.7, entropy decreases with decrease in p, for $p < 0.5$

The increase in height is also due to the increase in the number of flows in the system. However, the total area under the curve increases which explains the increase in total entropy of a window observed under low rate attacks.

High Rate Attacks

Figure 3.10 shows the distribution in entropy values under high rate attack conditions for a single window of size 0.2 seconds. Most of the flows are concentrated around two entropy values.

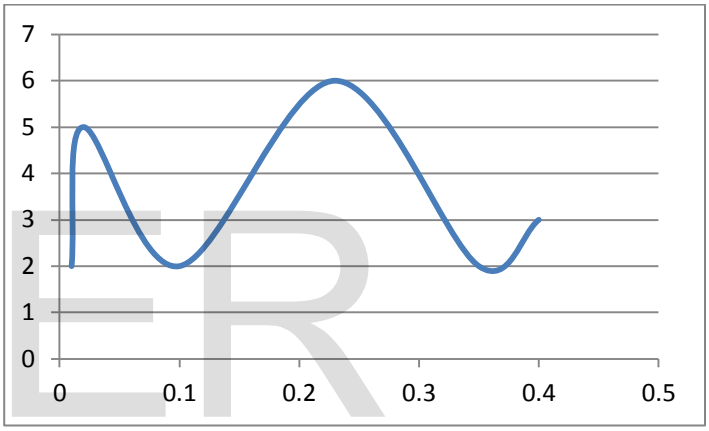

Figure 3.10 Distribution of Entropy over individual flows under high rate attack

Topology Specifications for Fig. 3.10

35 legitimate users, each one a legitimate user requesting FTP service from the server. 10 attackers are taken, with an attack rate of 4 Mbps for each. This corresponds to a distributed high rate attack.

Analysis of Fig. 3.10

The two peaks in the curve correspond to entropies of legitimate flows and the attack flows. Under high rate attack, the probability of normal flows will decrease and hence their entropy would also decrease as entropy function is increasing function for $p < 0.5$. Thus, the peak corresponding to low entropy value represents the concentration of legitimate flow around that entropy value. The probability of high rate attacks increases and hence their entropy would have higher values. The peak corresponding to the higher entropy values corresponds to the entropy value around which the high rate attack flows are concentrated. The area under the

curve decreases which explains the decrease in total entropy of a window observed under high rate attack conditions.

IV. CONCLUSION

We detected both low rate degrading and high rate flooding DDoS attacks. It is found that traffic feature distributions are better measures as compared to volume to find signs of attack. Even very meek rate DDoS attacks are detected reliably.

In case of low rate degrading attacks, the entropy value increases than the value in case of normal behaviour whereas in case of high rate bandwidth disruptive attacks, the value decreases.

Also, we observed that there is a shift in the entropy distribution of individual flows in a time window. In case of low rate degrading attacks, the distribution curve shifts leftwards and in case of high rate attacks, two peaks are observed. The left peak corresponds to the legitimate flows and the other peak corresponds to attack flows. The experiments on simulated topology yielded very high detection rates and acceptable false positive rates.

The paper can be extended to incorporate mixed rate attacks in which the varying rate attack flows cancel out each other effects on entropy value. So some other measures can be clubbed with this methodology to get better detection rates. The entropy distribution curves can be used in effective identification of attack flows and for their subsequent characterization.

REFERENCES

[1] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, "Internet Society: Histories of the Internet – A Brief History Of the Internet", version 3.32, available at, http://www.isoc.org/internet/history/brief.shtml

[2] CERT Statistics, available at, http://www.cert.org/stats/cert_stats.html

[3] CERT. Denial of Service Attacks, available at, http://www.cert.org/tech_tips/denial_of_service.html, 1997.

[4] K. J. Houle, G. M. Weaver, N. Long, and R. Thomas, "Trends in denial of service attack technology", *Technical Report Version 1.0*, CERT Coordination Center, Carnegie Mellon University (2001), available at, http://www.cert.org/archive/pdf/DoS trends.pdf.

[5] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajkovi, "Distributed denial of service Attacks", *In Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, vol. 3, Nashville, TN, USA, Oct. 2000, pp. 2275-2280.

[6] J. Mirkovic, J. Martin and P. Reiher, "A Taxonomy of DDoS Attack and DDoS defense Mechanisms," *ACM SIGCOMM Computer Communications Review*, Volume 34, Number 2, April 2004, pp. 39-53

[7] V. Paxcon, "An analysis of using reflectors for distributed denial-of-service attacks" , *ACM SIGCOMM Computer Communications Review (CCR)*, Volume 31, Number 2, July 2001, pp. 38-47

[8] L. Garber, "Denial-of-Service attacks rip the Internet", *IEEE Computer*, Vol. 33, No. 4, April 2000, pp. 12-17.

AUTHORS

First Author – Neha Tewari, M.tech, Department of Computer Science and Engineering, Lovely Professional University, Jalandhar, India; er.neha2k4@gmail.com

Second Author – Akash Bhardwaj, MCA, Department of Computer Application, Lovely Professional University, Jalandhar, India; Akash.Bhardwaj.6373@gmail.com.