A VIVACIOUS APPROACH TO DETECT AND PREVENT DDoS ATTACK

Kharat J.S.[1], Radhakrishna Naik[2]

[1]Student ME (CSE), [2]Head, Computer Science and Engineering, MIT (E) Aurangabad, Maharashtra, India,
kharat.jyo@gmail.com, naikradhakrishna@gmail.com

Abstract

A serious problem on the Internet nowadays is Distributed Denial of Service (DDoS) attacks and this is coordinated attack performed by hackers to immobilize a particular Computer service through manipulation of techniques those are used to provide the Services. In this attack, normally attackers generate a huge amount of requests to victims through compromised computers. DDoS attacks are a critical threat to the internet. Packet flooding DDoS attack is a very common way to attack a victim machine by sending large amount of unwanted traffic. This paper proposes a threshold based approach to detect and prevent the DDoS attack before reaching the victim end with high detection rate and low false positive rate to achieve high performance. The result obtained from various experiments on UDP Flood attack and HTTP GET attack show the effectiveness and the efficiency of our approach.

Keywords: *Denial of Service (DoS), Distributed Denial of Service (DDoS), Entropy, flooding attack.*

----------***----------

1. INTRODUCTION

Internet Operators have been observed that DDoS attacks are increasing noticeably and individual attacks are more strong and complicated. Furthermore, the Arbor Worldwide Infrastructure Security Report highlighted important trends in distributed denial of service (DDoS) attacks. Several findings stand out, including the overall expansion of attack surface and the escalation of attack size and frequency [1].Distributed denial-of-service (DDoS) attacks consist of an overwhelming quantity of packets being sent from multiple attack sites to a victim site. These packets get there in such a high quantity that some key resource at the victim (bandwidth, buffers, CPU time to compute responses) is quickly exhausted. The victim cannot attend its real work due to spending so much time in handling the attack traffic. Thus legitimate clients are deprived of the victim's service for as long as the attack lasts.

The first large-scale appearance of distributed denial-of-service (DDoS) attacks occurred in mid-1999 and still researchers are struggling to devise an effective solution to the DDoS problem. There are many commercial and research defenses has been appeared, but none of them provide complete security from the threat. Rather, they detect a small range of attacks that either use malformed packets or create severe disturbances in the network; and they handle those attacks by non-selectively dropping a portion of the traffic destined for the victim[1]. This strategy relieves the victim from the high-volume attack, but also inflicts damage to legitimate traffic that is speciously dropped.

2. OVERVIEW OF DoS AND DDoS ATTACK

2.1 Denial of Service (Dos) Attacks

The DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. The goal of a Denial of Service (DoS) attack is to interrupt some legitimate activity, such as browsing Web pages, email functionality or net banking. It could even shutdown the whole Web server. To obstruct legitimate operations is to exploit vulnerabilities on the target machine or application, by sending specially crafted requests targeting the given vulnerabilities. Denial-of-service effect is achieved by sending messages to the target machine such that the "message" hampers with its operation and makes it hang, crash, reboot, or do useless work. Also some key resources of the target machine such as bandwidth, CPU time, memory, etc can be consumed by sending a vast number of packets. One cannot attend to legitimate clients because the target application, machine, or network spends all of its critical resources on handling the attack traffic [2].

2.2 Distributed Denial-Of-Service (DDoS) Attacks

It is simply an extension of DoS attack. DoS and DDoS attack scenario is shown in Fig-2.Making a machine or network resources unavailable to its intended user-s is the DDoS attempt. It generally consist of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the internet. DDoS attacks are able to take out an entire server in a matter of minutes. To overwhelm a service to the point where it no longer works is the goal of any DDoS attack.

In a DDoS attack, the incoming traffic flooding the victim originates from many different sources potentially hundreds of thousands or more. To saturate a target computer or device with external communications requests, such that it cannot respond to other legitimate traffic, or responds so slowly[3] is the most common method of DDoS attack. In general terms, DDoS attacks are implemented by either forcing the targeted computers to reset, or to consume their resources so that they can no longer provide services, or obstructing the communication media between communicators so that they can no longer communicate.

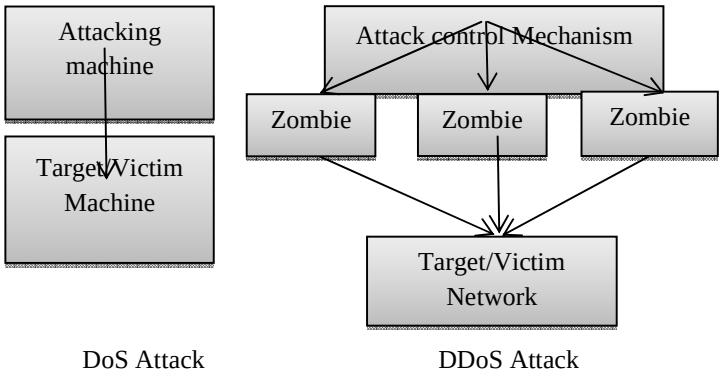

Fig-1: DoS and DDoS Attack Scenario

There are many types of DDoS attacks targeting both the network and the application layers. They could be classified upon their impact on the targeted computing resources (saturating bandwidth, consuming server's resources, shattering an application) or upon the targeted resources as well:

- Attacks targeting Network Resources: UDP Floods, ICMP Floods, IGMP Floods.
- Attacks targeting Server Resources: the TCP/IP weaknesses –TCP SYN Floods, TCP RST attacks, TCP PSH+ACK attacks – but also Low and Slow attacks as Sock stress for example and SSL-based attacks, which detection is particularly challenging.
- Attacks targeting the Application Resources: HTTP Floods, DNS Floods and other Low and Slow attacks as Slow HTTP GET requests (Slowloris) and Slow HTTP POST requests (R-U-Dead-Yet).
- A DDoS attack usually comprises more than three attack vectors thus increasing the attacker's chances to hit its target and escape basic DoS mitigation solutions[4].

In general there are two types of denial of service attacks: those that target the network layer and those that target the application layer. The server cannot simultaneously process other requests from other legitimate users, if an attacker overloads the server with many requests. Examples of DDoS attacks are discussed as follows:

A. UDP Flood Attack

UDP Flood attack is a network layer DDoS attack. UDP is a connectionless protocol and it does not require any connection setup procedure to transformation. To consume the bandwidth is the main purpose of UDP Flood type attack. In this attack, Attacker send IP packets containing UDP datagrams with the purpose of slowing down the victim to the point that the victim can no longer handle valid connections.

B. HTTP GET Flood Attack

HTTP GET flood attack is an Application layer DDoS Attack. In this, a large amount of legitimate requests(to an application)use to send by HTTP attacker. The feature of HTTP GET Flood attack is that it will establish a normal TCP Connection to Servers, and constantly submit a lot of calling requests which dramatically consume database resources. For sample, an Http Flood attack can make hundreds of thousands of page requests to a web server, which can wear out all of the servers processing capability. So that the server cannot handle the legitimate request [5]

An HTTP GET flood is as exactly as it sounds: it's a massive influx of legitimate HTTP GET requests that come from large numbers of users. These requests mimic legitimate users are nearly impossible for applications and even harder for traditional security to detect. This result of this attack is similar to the effect: server errors increasingly degraded the performance, and resource exhaustion.

3. RELATED WORK

Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS) are the most dreadful network threats in recent years. Different techniques and challenges involved in anomaly detection system [6].

Yonghua You and Zulkernine[7]introduce two distance-based DDoS detection techniques: average distance estimation and distance-based traffic separation. They detect attacks by analyzing distance values and traffic rates. The distance information of a packet can be inferred from the Time-to-Live (TTL) value of the IP header. In the average distance estimation DDoS detection technique, the prediction of mean distance value is used to define normality. The prediction of traffic arrival rates from different distances is used in the distance-based traffic separation DDoS detection technique. The mean absolute deviation (MAD)-based deviation model provides the legal scope to separate the normality from the abnormality for both the techniques. The results of the proposed techniques show that the techniques can detect attacks effectively.

Muhai and MingLi [8] propose a model for detecting DDoS attacks automatically. In order to reduce the error to identify attacks, we use discrete wavelet transform (DWT) technique.

Author use actual data to validate proposed model and obtain good results in terms of tradeoff between correct detections and false alarms. The test results shows the approach not only can be different the sudden increasing normal traffic from anomaly traffic, but also has a well detect ratio.

Sumit Kar and Bibhudatta Sahoo[9]proposed method is based upon attack detection and recovery, and uses an entropy based anomaly detection system to detect DDoS attack. Author design an anomaly detection system based on entropy and entropy rate to detect DDoS attack. They uses normalized entropy which calculates the over all probability distribution in the captured flow in algorithm to get more accurate result. Detection System is based on by analyzing the change in entropy of distribution flow header feature and behavioral features traffic distributions. The Result shows that the attack must be detected and blocked before reaching the victim with high detection rate and low false alarm rate.

Suratose Tritilanunt et al. [10] provide a detection mechanism based on a technique of entropy-based input-output traffic mode detection scheme. The experimental results demonstrate that our approach is able to detect several kinds of denial-of-service attacks, even small spike of such attacks. To minimize this false positive, we introduce a technique called entropy-based input-output traffic mode detection scheme. By combining packet content observation for identifying DoS and DDoS attacks in the system, this will help approach not only to increase the accuracy for detecting DoS attacks, but also to effectively discriminate legitimate users from suspicious traffic.

Yi Zhang and Qiang Liu[11] present a real-time DDoS attack detection and prevention system which can be deployed at the leaf router to monitor and detect DDoS attacks. The advantages of this system lie in its statelessness and low computation overhead, which makes the system itself immune to flooding attacks. A number of articles suggested entropy as a metrics to summarizing trafficdistribution for anomaly detection[12][13].

The authors of [9] use entropy rate to discriminate the DDoS attack from legitimate traffic. The use of entropy for analyze changes in traffic distribution has two benefit. i) Using entropy for anomaly detection increases the detection capability than volume based methods. ii) It provides additional information to classify among different types anomaly (worms, DoS attack. Port scanning) .We considers two classes of distribution i) flow header features (IP address, ports, and flow sizes) ii) behavioral features (the number of distinct destination / source address that a host communicates with) [14]. The anomaly detection system discussed in this paper is based on by analyzing the change in entropy of above two traffic distributions.

Our objective in this paper is to design an attack detection system based on entropy and packet rate to detect DDoS attack. We use normalized entropy which calculates the over all probability distribution in the captured flow in our algorithm to get more accurate result.

4. PROPOSED ENTROPY BASED DETECTION TECHNIQUE

Shannon's Entropy [15] based approach is used for DDoS attack detection. entropy is a measure of the uncertainty in a random variable or in this case data coming over the network. The Shannon's function is a useful tool for inspecting a similarity and distribution of traffic in the inspection time frame. When denial-of-service attacks occur in the observation window, the entropy of that traffic will drop noticeably and wecan identify that situation as DoS/DDoS attacks. The value of sample entropy lies in range $[0, \log n]$. The entropy shows its minimum value 0 when all the items (IP address or port) are same and its maximum value logn when all the items are different. The entropy of a random variable X with possible values $\{x_1, x_2 \dots \dots x_n\}$ can be calculated as

$$H(x) = -\sum_{i=1}^{n} P(x_i) \log P(x_i) \qquad (1)$$

In our proposed DDoS detection algorithm we use entropy as a principal matrix. We use change of entropy of traffic distributions (IP address, port) for DDoS detection. If we are interested in measuring the entropy of packets over unique source or destination address then maximum value of n is 2^{32} for ipv4address [9]. If we want to calculate entropy over various applications port then n is the maximum number of ports. Here $p(x_i)$ where $x_i \in X$ is the probability that X takes the value x_i. Suppose we randomly observe X for a fixed time window w, then$P(x_i) = m_i/m$, where m_i is the frequency or number of times we observe X taking the value x_ii.e. $m = \sum_{i=1}^{n} m_i$

$$H(X) = -\sum_{i=1}^{n} (m_i/m) \log(m_i/m) \quad (2)$$

If we want calculate probability of any source MAC address then,

mi = number of packets with xi as source MAC address and
m = total number of packets

$$P(x_i) = \frac{\text{Number of Packets with } x_i \text{ as source}}{\text{Total number of packets}}$$

Here total number of packets is the number of packets seen for a time window T.

Normalized entropy calculates the over all probability distribution in the captured flow for the time window T.

$$\text{Normalized entropy} = (H/\log n_0) \quad (3)$$

Where n_0 is the number of distinct $x_i$values in the given time window.

In a DDoS attack from the captured traffic in time window T, the attack flow dominates the whole traffic, as a result the normalized entropy of the traffic decreased in a detectable manner. But it is also possible in a case of massive legitimate network accessing. To confirm the attack we have to again calculate the packet rate (P_{Rt}) of suspected flow. Here flow is packages which share the same destination address/port. In this mechanism we have taken one assumption that the attacker uses same function to generate attack packets at "zombies".

$$P_{Rt}(x) = \frac{\text{Total No. of packets coming from same MAC address}(T_x)}{\text{Total number of packets (T)}} \quad (4)$$

The steps in our proposed DDoS detection algorithm are described below.

Algorithm 1 : DDoS Detection Algorithm
1: Collect sample flows for a time window T on the edge routers. 2:Calculate router entropy $H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$ 3: Calculate NE $= (H/\log n_0)$where, NE = normalized router entropy. 4: If NE $< threshold(\delta_1)$, identify the suspected attack flow. 5: Calculate the packet rate $P_{Rt}(x) = \frac{(T_x)}{(T)}$ of the suspected flow inthat router 6:If $P_{Rt}(x) \leq$ threshold(δ_2), it is a DDoS attack. Else legitimate traffics. 7: Generate alarm and Discard the attack flow.

5. EXPERIMENT AND RESULT

Section 5 provides the experiment and results of our approach to detect distributed denial-of-service attacks. The system can detect the attack by using an entropy detection method because the value drops significantly from the stored profile once the DoS/DDoS attacks occur in the system. We observe that most DoS attacks immediately decrease the entropy of the overall system. A prototype of the proposed system has been implemented and evaluated on an real base system.

Experimental Setup: Fig-2 shows the experimental setup. experiment includes 3 source, 1 intermediate routers and 1 destination node. Out of which 3 source nodes 2 nodes are legitimate users and 1 node is attacker. The bandwidth of legitimate traffic is set constant.

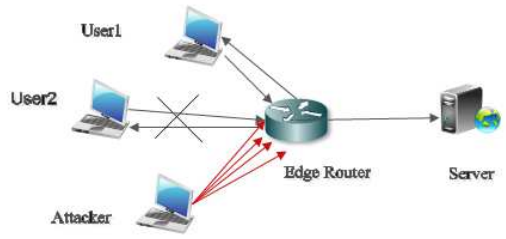

Fig-2: Experimental setup

The goal of our experiments is to assess the scalability of our approach and the performance of the protection system.

5.1 UDP Attack:

UDP is a bandwidth depletion attack. Attacker consumes the network bandwidth with unwanted UDP traffic so that legitimate user cannot send packets to destination.We traced no of packets received in every 1 second interval. Performance metrics used is Network Utilization.

Experiment 1: UDP attack with 2 legitimate user and 1 attacker: Suppose node A3 is the attack source and node A1 and A2 are legitimate users and node D_1 is the victim. All the three users sending packets to specified destination Experiment lasts at 6 second. We traced number of packets received in a fixed time window T.Table-1 shows the traced data in 6 seconds. The router entropy is calculated according to Eq. (2), and the normalized router entropy is being calculated using Eq. (3). Table-2 shows the normalized entropy calculation for experiments.

Table 1: Traced data

Times in Second	Number of attack packets received	Number of legitimate packets received
0-1	80	63
1-2	80	65
2-3	699	150
3-4	766	125
4-5	700	100
5-6	615	80

Table-2: Normalized entropy calculations

Time in Second	Normalized Router Entropy
0-1	0.98
1-2	0.99
2-3	0.535
3-4	0.45
4-5	0.51
5-6	0.76

Captured flow for every source is shown in Table-3 when NE=0.535.

Table-3: Traced Data when NE=0.535(UDP attack)

Source Node with MAC address	Destination IP	No. of pac kets	entropy
38-60-77-50-b0-92	192.168.0.45	70	0.29
00-1c-c0-83-b7-f8	192.168.0.45	80	0.32
70-71-BC-BE-11-9B	192.168.0.45	699	0.23

Here router entropy = 0.29+0.32+0.23= 0.84

$$n_0 = 3$$

Normalized router entropy NE = 0.84/ log2 3 = 0.535

The above data are taken practically for Edge Router. In the above case one flow dominates the whole traffic as a result the normalized entropy decreases. If the threshold δ_1 is perfect, suppose 0.94 for the above example, it will treat flow coming from node A_3 with MAC (70-71-BC-BE-11-9B) as suspected flow. After which the packet rate is being calculated for every suspected flow. While the packet rates of different flows exceed the thresholdδ_2 i.e.150 packets/second, the attack is confirmed and attack flow is discarded. All the above calculations are based on $\log_2$.

We consider 2 situations in our experiment to evaluate the performance of our proposed algorithm. In the first situation, we start with 2 legitimate users and 1 attacker and study how the system performance is being degraded. In the second situation we examine the system for 2 legitimate users and two attackers.

The graph in Fig-3 depicts the effect of DDoS attack with 2 legitimate users and 1 attacker. It shows numbers of attack packets as well as legitimate packets with respect totime. The graph in Figure 4 shows the network utilization of 3senders with 1 attacker. It shows number of packets/second with respect to network utilization.

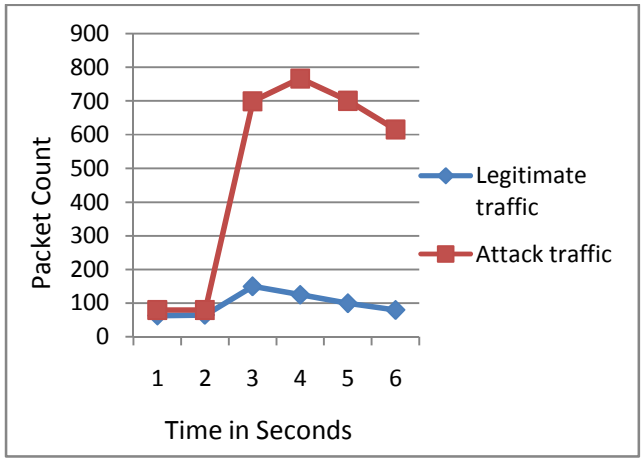

Fig-3: Effect of UDP attack

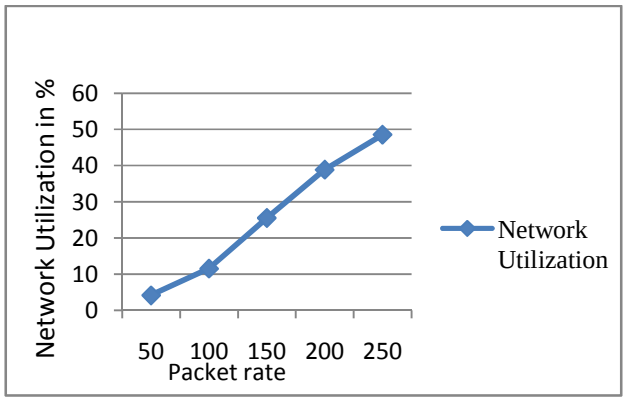

Fig-4: Threesenders with 1 attacker

The graph in Fig-4 shows the Network utilization of 4 senders with 2 attackers. It shows the packet rate with respect to network utilization.

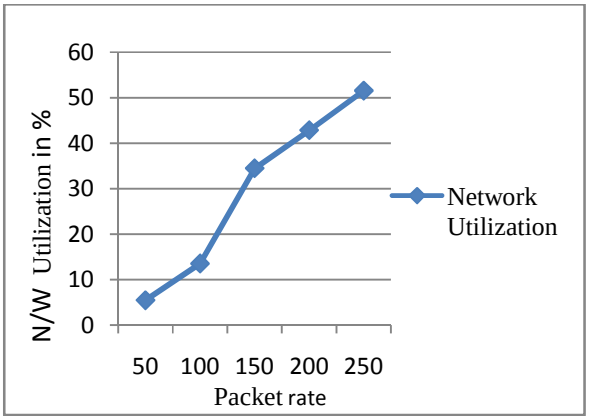

Fig-5: Foursenders with 2 attackers

5.2 HTTP GET Flood Attack

We traced no of HTTP GET request received in every 1 second interval.We have taken two examples using Fig. 2 how the detection scheme works. Suppose node A1 is the attack source and node A2and A3 are legitimate users and node D1 is the victim. Based on the DDoS detection algorithm flows coming from all the client nodes will first captured by router 1 Suppose at router 1, we have captured flows as given in Fig-6 which shows the legitimate traffic as well as attack traffic with respect to time in a fixed time window T. The router entropy is calculated according to Eq. (2) and the normalized router entropy is being calculated using Eq. (3).Table-4 shows the Normalized entropy calculations and Table-5 shows the traced data when NE=0.81

Table-4: Normalized entropy calculation

Times in Second	Normalized Router Entropy
0-1	0.71
1-2	0.86
2-3	0.63
3-4	0.67
4-5	0.81

Table-5 Traced Data when NE=0.81

Source Node with MAC address	Destination IP	No.of request	entropy
38-60-77-50-b0-92	192.168.0.45	217	0.41
00-1c-c0-83-b7-f8	192.168.0.45	74	0.47
70-71-BC-BE-11-9B	192.168.0.45	49	0.40

Here router entropy = 0.41+0.47+0.40= 1.28 and $n_0 = 3$

Normalized router entropy $NE = 0.84/\log_2 3 = 0.811$

The above data are taken practically for Router1. In the above case one flow dominates the whole traffic as a result the normalized entropy decreases. If the threshold is perfect, suppose 0.94 for the above example, it will treat flow coming from node A3 with MAC(70-71-BC-BE-11-9B) as suspected flow. After which the packet rate is being calculated for every suspected flow. While the packet rates of different flows exceed the threshold δ_2 i.e. 150 p/s, the attack is confirmed and attack flow is discarded.

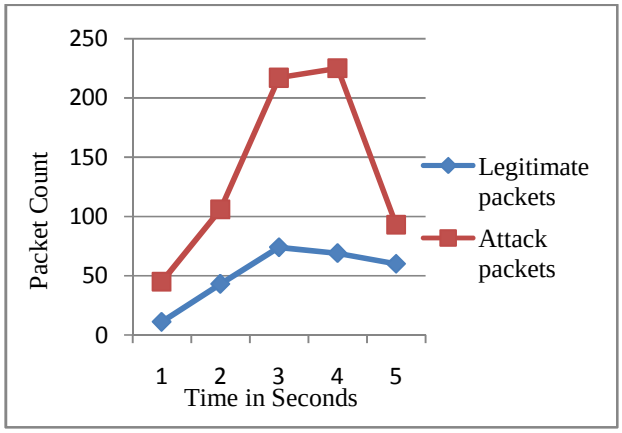

Fig-6: Traced data

The graph in Fig-7 shows the Heap utilization of 3 senders with 1 attacker. It shows packet rate with respect to Heap Memory utilization in %.The graph in Fig-8 shows the Heap utilization of 4 senders with 2attacker. It shows packet rate with respect to Heap Memory utilization.

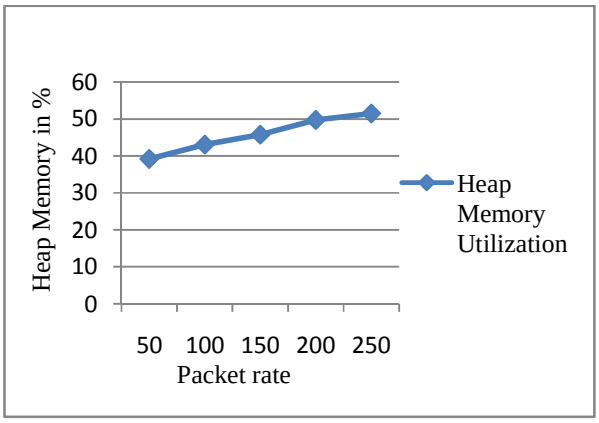

Fig-7: three senders with 1 attacker

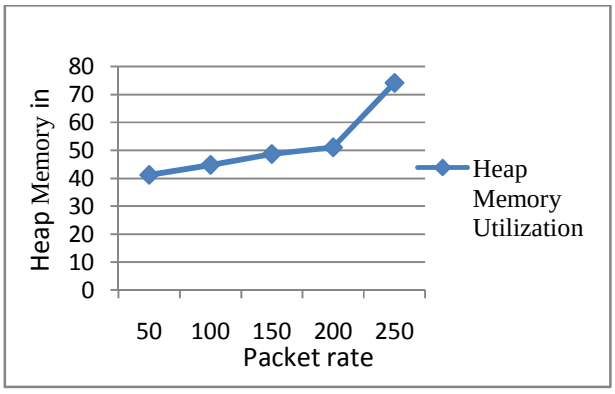

Fig-8: four senders with 2 attackers

CONCLUSIONS

In this paper we discussed different types of DDoS attacks that could exploit network and related detection strategies and introduces an alternative technique to detect denial-of-service and distributed denial-of-service attacks by using packet rates and packet address entropy-based technique. As we will take the detection threshold δ_1 as0.94 then, the proposed anomaly detection system can detect DDoS attack traffics with high detection rate and without any false positive before reaching the victim and taking threshold δ_2 as 150 p/s then, proposed system can achieve the efficient use of Network utilization in case of UDP attack and Heap Memory utilization in case of HTTP Get flood attack. we plan to test our approach with other kinds of DoS/DDoS attacks in the future work.

REFERENCES

[1]. http://blogs.ixiacom.com/ixia-blog/application-layer-ddos-attacks-growing.

[2]. http://www.linuxforu.com/2011/04/securing-apache-part-8-dos-ddos-attacks.

[3]. http://en.wikipedia.org/wiki/Denial-of-service_attack.

[4]. http://security.radware.com/knowledge-center/DDoSPedia/ddos-attack/

[5]. Saman Taghavi Zargar, James Joshi, David Tipper," Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks",ieee communications surveys & tutorials 2009.

[6]. P. G. Teodoro, J. D.Verdejo, G. M.Fernandez, E.Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", computer & security, Volume 28, Issues 1-2, pp.18-28, 2008.

[7]. Yonghua You and Zulkernine,"A Distributed Defense Framework for Flooding-Based DDoS Attacks", ICC Proceeding, 2007

[8]. Muhai Li and Ming Li," A New Approach for Detecting DDoS Attacks Based on Wavelet Analysis",ieeeconference, 2009.

[9]. Sumit Kar and Bibhudatta Sahoo," An Anomaly Detection System for DDoS Attack",ijca-se 2009.

[10]. Suratose Tritilanunt et al," Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks",2010 .

[11]. Yi Zhang and Qiang Liu," A Real-Time DDoS Attack Detection and Prevention System Based on per-ITraffic Behavioral Analysis",2010.

[12]. Suratose Tritilanunt, SuphanneeSivakorn, ChoochernJuengjincharoen, AusaneeSiripornpisan," Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks", ISCIT 2010

[13]. Wonjun Lee and Squicciarini,"Detection and Protection against Distributed Denial of Service Attacks in Accountable Grid Computing Systems",IEEEJournel 2011.

[14]. G. Nychis, V. Sekar, D. G Andersen, H. Kim and H.Zhang, "An Empirical Evaluation of Entropy-Based Traffic Anomaly Detection". Tech. Rep. CMU-CS-08-145, Computer Science Department, Carnegie Mellon University, 2008

[15]. Thomas M. Cover and Joy A. Thomas, "Elements of Information Theory", second edition, 2007

BIOGRAPHIES

Ms. Kharat J.S. obtained her Bachelor's Degree in Computer Science from BAMU University during 2008 and currently pursuing Masters Degree from the same university. She is working in Computer Dept. of Shreeyash Polytechnic Aurangabad as Lecturer from last 5 years. Her research area includes Network Security.

Dr. Radhakrishna Naik is working as professor and Head in CSE Department of MIT (E) Aurangabad. He did his PhD in Real Time Systems and his subjects of interest are Real Time systems, Real Time database management and Network security.