© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

An Efficient Entropy Based Approach for the Detection of DDOS Attack

Abhilash Singh, Kausthav Pratim Kalita, Sweta Bhadra
Department of CSE, Assam Don Bosco University, Guwahati, Assam, India

ABSTRACT

Distributed Denial of Service (DDoS) attack is now a big threat to the steady functioning of any network. DDoS attack is an attempt to degrade the victim resources. The legitimate users are denied of services by eating up the communicational memory and computational resources of the victim system through sheer volume of traffic. Various schemes are developed to detect DDoS attacks. One of the schemes is the Entropy based approach. In this paper we have discussed some of the research work on entropy based DDoS attack detection. We have also analysed an efficient entropy based approach to detect the DDoS attack. The experiment is carried out on NS2 simulator. The simulation result shows that the proposed approach can detect the DDoS attack efficiently.

Keywords : DDoS, Entropy, Normalized Entropy

I. INTRODUCTION

Distributed Denial of Service (DDoS) attack is one of the most well known threats to any computer network or internet services. In DDoS attack, an attacker takes control of several computers on internet which has security issues and can be easily penetrated. The attacker then sends flux of packets using the hacked computers to a target machine on internet. The result is that the target machine looses all its resources and will be unavailable for the genuine clients. There are two types of DDoS attacks (a) Low Rate DDoS attacks: In Low Rate DDoS attack the attacker send packets in low rate for a longer duration of time. Low rate DDoS attack are hard to detect as they behave like a legitimate client (b) High Rate DDoS attacks: In High Rate DDoS attack the attacker sends packets in a high rate for a shorter duration of time.

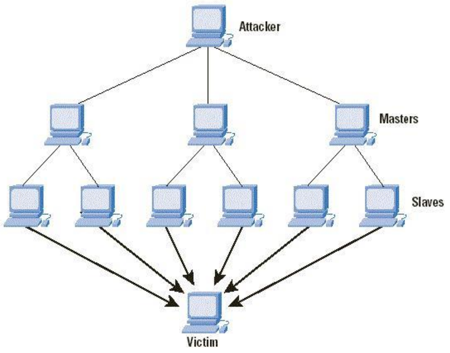

Figure 1: DDOS Attack Model [8]

1.1 SYMPTOMS OF DDoS ATTACK:

(a) Slow network Performance.
(b) Particular websites unable to access.
(c) Increase in the numbers of spam emails received.
(d) Usually the connection gets disconnected.
(e) Denial of internet services for a duration of time.

II. ENTROPY

Entropy can be defined as the measure of randomness or uncertainty of a random variable [1]. The Entropy of a random variable can be calculated as defined in [9]

$$H(x)= -\sum^{n}_{i=1} P_i * \log_2 P_i$$

where H(x) is the entropy of a random variable X with possible values ($x_1,x_2\ldots x_n$) and distribution of probabilities P=($p_1,p_2,\ldots p_n$) with n elements.

III. RELATED WORK

Abhinav et al. [1] in his paper used a traffic monitoring module for the detection of DDoS attack which keeps on monitoring the incoming traffic in the network. The module calculates the entropy of each router for a particular time window. If the value of router entropy goes below the certain threshold value the system marks it as suspicious flow. Then the system calculates the Average entropy of the router for different flows using the below equation as define in [1].

$$\text{Average Entropy} = \frac{H(x1,x2,...xn)}{n}$$

Then the system sends signal to calculate the same for the downstream router. If the both the values are exactly same or the difference is equal or less than the certain threshold value the system gives alarm of DDoS attack to the edge router.

Jaswinder et al. [2] proposed a entropy based anomaly detection algorithm. Two different approaches are used to detect ddos attack in the network. Firstly, the entropy is calculated with respect to time window and secondly, entropy is calculated with respect to packet window [2]. After the experiment they observe that, while the network is not under attack the entropy value falls in narrow range but when the network is under attack the value of entropy decreases gradually which is easily detectable.

Brajesh et al. [4] In this paper has first tries to identify the types of DoS and DDoS attack. The author has also provided the solution attacker's identification. In this paper the author tries to detect the actual attacker who has forged multiple systems for performing ddos attack.

To achieve that the author first prevented IP forgery using sender authentication process, calculation TCP flow rate the author can identify between normal packets and malicious packet. By calculating entropy and normalize entropy on receiver proxy server ddos attack is detected. The malicious packets are dropped, and the attacker is trace backed using the packets mark value. Further the actual attacker is identified by using ISP and IANA concept.

A.S Syed et al. [5] In this paper has proposed a system which combines Entropy based system and Anomaly Detection System which will provide multilevel DDoS detection. It is done in two phases. Firstly, Through router users are allowed to pass in network site which uses detection algorithm and identifies legitimate user. Secondly, gain the user passes through cloud site in which router is placed which uses confirmation algorithm incorporated in it and check for threshold value. If the value appears beyond threshold value it considered as legitimate user, else it is considered as intruder. The System is maintained by a third party. When attack takes place in environment, the system sends notification message to client and advisory report to Cloud Service Provider.

IV. SIMULATION

The simulation is done using NS-2 simulator to evaluate the performance of our DDoS detection algorithm with results obtained from the experiment. We tested our anomaly detection algorithm in Linux (Ubuntu 12.04 LTS) environment.

EXPERIMENTAL SETUP: Our simulation includes 6 source, 2 intermediate routers and 1 destination nodes as server as shown in figure 2. The legitimate user (Client 1,2,3,4) send packets in an interval of 0.1 second and the attacker(1,2) starts sending attack traffic after 0.001 second frequently. The experiment lasts for 4 seconds. We traced number of packets received in every 0.5 second interval from the trace file obtained after the simulation.

TABLE 1: SIMULATION PARAMETERS TABLE

Parameter	**Value**	**Description**
Simulator	NS2	Simulation Tool
No. of Nodes	9	Network Nodes
Genuine Clients	4	Clients
No. of Attackers	2	Attackers
Simulation Time	2 seconds	Duration of Simulation
Legitimate Traffic Type	TCP	Transmission Control Protocol
Attack Traffic Type	UDP	User Data Protocol/CBR
Client-Router Link-Bandwidth	2 Mbps	Bandwidth
Attacker - Router Link Bandwidth	2 Mbps	Bandwidth
Router -Server Link Bandwidth	2 Mbps	Bandwidth
No .of Intermediate Routers	2	Routers

The simulation topology created in ns2 is shown below in figure 2.

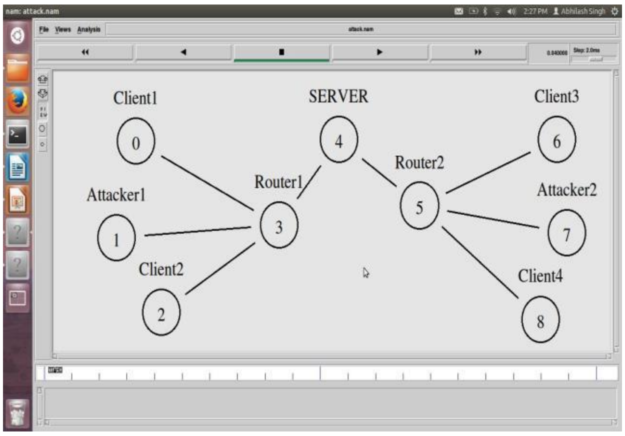

Figure 2: Simulation Topology

TABLE 2: TRACE TABLE OF NORMAL PROGRAM

Time Interval	**Normal Packets**	**Attack Packets**	**Normalized Entropy**
0.0 – 0.5	243	143	0.35
0.5 – 1.0	290	200	0.35
1.0 – 1.5	347	294	0.37
1.5 – 2.0	282	196	0.36
2.0 – 2.5	305	241	0.34
2.5 – 3.0	270	198	0.36
3.0 – 3.5	265	210	0.32
3.5 – 4.0	306	242	0.34

TABLE 3: TRACE TABLE OF ATTACK PROGRAM

Time Interval	Normal Packets	Attack Packets	Normalized Entropy
0.0 – 0.5	370	260	0.44
0.5 – 1.0	356	497	0.43
1.0 – 1.5	7	501	0.03
1.5 – 2.0	112	498	0.02
2.0 – 2.5	345	244	0.39
2.5 – 3.0	370	254	0.42
3.0 – 3.5	26	436	0.04
3.5 – 4.0	1	501	0.01

V. ENTROPY CALCULATION

$$H(x) = -\sum_{i=1}^{n} P_i * \log_2 P_i \quad \text{--------------}(1)$$

Where,

P(i) = (Number of normal packet and Number of attack packet)/ Total No. of packet.

Using eqn. (1), we calculated

For Time Interval: 0.0 - 0.5 seconds (Table 2)

$$H(X) = -\sum_{i=1}^{n} \left(\frac{243}{380}\right)\log\left(\frac{243}{380}\right) + \left(\frac{143}{380}\right)\log\left(\frac{143}{380}\right)$$

$$= 0.29$$

Normalized Entropy:

$$NE = H(X)/\log_n$$

$$= 0.29/\log 6 \text{ (source node are 6)}$$

$$= 0.35$$

Now calculating all the remaining values in the same way, we got the normalized entropy value in Table 2 & table 3 of both the attack and the Normal program. Now we plot the normalized entropy values of Attack program and Normal program on the Y axis and the time interval on the X axis using gnuplot, we got the Entropy Graph.

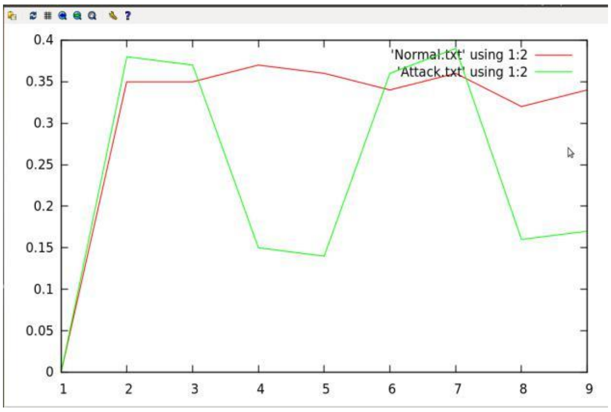

FIGURE 3: ENTROPY GRAPH OF NORMAL & ATTACK PROGRAM

ANALYSIS OF GRAPH & RESULTS

In the above graph, red line denotes the normal network without ddos attack and the green lines denotes the network under attack. We can observe that the red line maintains a steady flow whereas the green line fluctuates due to the sudden drop and increase of entropy. By analyzing the graph we can easily detect ddos attack in a network using entropy.

VI. CONCLUSION AND FUTURE SCOPE

DDoS attack has become a big threat for the world of internet. Therefore proper attention must be given to DDoS attack. To prevent a DDoS attack first we need to detect DDoS attack. Identifying illegal packets among thousands and thousands of packets is not an easy task. We must keep in mind that in order to detect illegal packets we should not barred legitimate users from service.

The concept of Entropy can be very useful in detecting DDoS attacks. In this survey paper we have introduced works of various authors who have successfully applied Entropy based approach for detecting DDoS attacks. We also performed an experiment to detect DDoS attack in a network using entropy based approach. The result we obtained was satisfactory. In our future work we will try to enhance our work and also we will come up with an approach to prevent DDoS attack in a network. If implemented properly Entropy based approach could be the most efficient way in detecting DDoS attacks in a network.

VII. REFERENCES

[1]. Abhinav Bhandari, Krishan Kumar “Destination Address Entropy based Detection and Traceback Approach against Distributed Denial of Service Attacks” I. J. Computer Network and Information Security, 2015, 8, 9-20

[2]. Jaswinder singh, Monika sachdeva & Krishan kumar “detection of ddos attacks using source ip based entropy” International Journal of Computer Science Engineering and Information Technology Research(IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 1, Mar 2013

[3]. Jie Zhang, Zheng Qin, Lu Ou, Pei Jiang , JianRong , Alex X. Liu “An Advanced Entropy-Based DDOS Detection Scheme” 20IO International Conference on Information, Networking and Automation (ICINA).

[4]. Brajesh Kashyap, S.K.Jena “ DDoS Attack Detection and Attacker Identification” International Journal of Computer Applications (0975 – 8887) Volume 42– No.1, March 2012.

[5]. A.S.Syed Navaz, V.Sangeetha, C.Prabhadevi “ Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud” International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013.

[6]. Surender Singh, Sandeep Jain, “A Review Of Detection of DDOS Attack Using Entropy Based Approach” IJCST Vol. 4, Iss ue 2, April - June 2013 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print).

[7]. Poonam Jadhav, B.M Patilm, “Low-rate DDOS Attack Detection using Optimal Objective Entropy Method”. International Journal of Computer Applications (0975 – 8887) Volume 78 – No.3, September 2013

[8]. https://www.cisco.com/c/en/us/about/press/internet protocol-journal/back-issues/table-contents-30/dos attacks.html

[9]. K. Kumar, R. Joshi and K. Singh, "A Distributed Approach using Entropy to Detect DDoS Attacks in ISP Domain," in Signal Processing, Communications and Networking, 2007. ICSCN '07. International Conference, 2007.