Low-rate DDOS Attack Detection using Optimal Objective Entropy Method

Poonam N. Jadhav
Dept. of CNE
M B E Society's College of Engineering, Ambajogai
Maharashtra, India

B. M. Patil
Professor
M B E Society's College of Engineering, Ambajogai
Maharashtra, India

ABSTRACT
A Distributed Denial of Service (DDOS) attack is a type of Internet attack that disrupts the normal function of the targeted computer network (server). This kind of attacks attempts to make target host resource unavailable to its legal users. Several efforts had made in detection and computation of the DDOS attacks over network, where IDS (Intrusion detection systems) are unable to isolate the normal flow of traffic from attacks. So this paper is an introduction of the optimal objective entropy (OOE) based method to detect low-rate DDOS attacks. Minimization of objective function in entropy based method show considerable improvement over the traditional entropy based schemes.

Keywords
Optimal Objective Entropy (OOE), Intrusion Detection System (IDS).

1. INTRODUCTION
The Internet is a global network connecting millions of computers. In general, Internet network is an open and scalable in features. These characteristics have led the growth of the Internet, whereas vulnerabilities in the network has occurred simultaneously [1].Now days, the threat of Distributed Denial of Service (DDoS) attacks has become a major issue in network security. Launching a Low-DDoS attack from anywhere becomes an easier task for DDoS attackers, while the defenders have a more difficulties in detecting malicious network flow since the DDoS attacker uses normal packets flow with spoofed packet information (1, 2). A challenging task for the defenders is to process all packet information within a fraction of seconds because DDoS attacker sends a huge amount of normal packets to the victim. Although there are a good monitoring schemes against DDoS attacks, but still they are lack in detecting Low rate DDoS attacks from a normal packet flow. There are few researches which are focused on improving the traditional information entropy based method for detection of Low rate DDoS attacks. This paper mainly concentrates on designing an optimal DDoS attack detection method that can significantly detect Low-rate DDOS attack over the network and increase detection accuracy.

To detect the network traffic, conventional entropy based method is used in this paper. But for detection of Low rate attacks over the network objective function have been set. To minimize the objective function there is an upper bound and lower bound as the concept of genetic algorithm. The algorithm implemented in this paper select best optimal value from its child for next iterations and selects that value for triggering alarm.

The rest of the paper is organized in the following manner; section 2 describes related work on different DDoS detection methods, section 3 presents simulation and analysis, section 4 shows experimental results and finally the conclusion and future scope for new proposed scheme.

2. RELATED WORK

Jie Zhang and Alex X. Liu [3] proposed an advanced entropy-based system which divides DDoS attacks into different fields and treats each field with an individual method. Different schemes have been proposed to identify the attackers such as probabilistic Packet Marking (PPM), Deterministic Packet Marking (DPM). But these are not efficient because it requires injecting marks into individual packets in order to trace back the attackers. V.Sus hma Reddy, K.Damodar Rao, P.Sowmya Laks hmi have designed a method based on Entropy Variation [4] is used to overcome above drawback which is a measure changes of randomness of flows at a router for a given interval. This method identifies DDoS attacks in a wide area of network that is based on entropy variations between normal and DDoS attack traffic. Aditya Akella, Ashwin Bharambe, Mike Reiter and Srinivasan Seshan [5] designed a detection method in which each router identify attack by using normal traffic send by stream sampling algorithms. Ming Li, Jun Li & Wei Zhao [6] perform many experiments on flood attacking, and showed that bandwidth consumption for UDP packet flooding is more than TCP. In both DDoS and flash crowd packet transmission rate is more than normal flow. To increase the throughput server must have the capability to distinguish legal traffic from attacks. N. Jeyanthi and N. Ch. Sriman Narayana Iyengar [7] distinguish DDoS attacks from flash crowd.

Reyhaneh Karimazad and Ahmad Faraahi proposed an anomaly-based DDoS detection method based on the various features of attack packets and Radial Basis Function (RBF) neural networks to analyze these features[8]. Rejo Mathew and Vijay Katkar designed a software based lightweight method to detect LDDoS in which there is no need to modify the existing infrastructure [9]. Yang Xiang, Ke Li, and Wanlei Zhou, proposed a mechanism to detect Low-rate DDoS attack by using information distance and entropy metrics by measuring difference between legal and attack traffic [10]. H. Wang [11] proposed SYN detection to detect SYN floods. This method detects DoS attacks by monitoring statistical changes. In this method parameters is chosen for incoming traffic and model it to be a random sequence during normal operation. In this detection scheme the ratio of SYN packets to FIN and RST packets is used and is based on the fact that a SYN packet will end with a FIN or RST packet during normal TCP connection. C. M. Cheng [12] proposes to use spectral analysis to identify DoS attack flows. In this approach, the packets reached to the destination in fixed time interval are identified as legitimate traffic. Attack traffic does not manage periodicity; whereas TCP flow manage strong periodicity

around its round-trip time in both flow directions. First of all, spectral analysis is only valid for TCP flows. As UDP and ICMP are connectionless protocols, the periodic traffic behavior is unexpected. A. Kulkarni and S. Bush proposed a Kolmogorov complexity based detection algorithm [13] to identify attack traffic. The assumption of the Kolmogorov test is based on the fact that multiple attack sources use the same DoS attack tool. Therefore, the resulted traffic is highly correlated.

Low-rate DDOS attack detection using optimal objective entropy method is will increase the detection rate by implementing objective function for optimization of threshold value.

3. SIMULATION AND ANALYSIS

All the work done in this paper has been implemented and validated in NS-2.34 and experimented on Linux Red hat 5.5 as Operating System. Simulation of the script includes following pre-processing and post-processing tools respectively, Network Simulator and NAM, AWK, XGRAPH.

3.1 Method and Implementation

As stated in Simulation and Analysis section, the attack is prepared in NS-2.34 and installed as extension class in NS. The DDoS application class is further included in this simulation for traffic source generation by attackers. Other nodes are implemented with normal CBR traffic and with standard parameters.

3.2 Work and Analysis

All the work done in this paper mainly focuses on Low-rate attack detection over network, for which some value have set for set of parameters as shown in below table.

Table 1. Simulation Parameters

Simulation Parameter	Value
Number of Nodes	30
Attack Source	4
Router	4
Link Bandwidth	1mb /10mb/100mb
Simulation Time	100sec
Attacker type	TCP
Attack Initialization	6 sec
Bandwidth allocation	Router 1->Target 100 mb Router 2->1 =10mb Router 3->1= 10mb Router 4 -> 10 mb
Analysis period	6sec-15 sec
Normal traffic period	2sec-5sec & 16sec- 100 sec
Upper bound	Hc
Lower Bound	Hn
Target Server	Node 0
Low- attack rate	0.5-2 mbps
Packet Size	500

Above parameters are used for the Low-rate DDoS detection over network of 30 nodes.

3.3 Algorithm

Entropy is a measure of the uncertainty associated with a random variable (1, 3, 10).Let ‘i’ denote the flow ID, ‘m’ is the max number of flows and Xi denote number of packets of that particular flow then the probability distribution Pi is calculated by the formula (1, 3, 7),

$$Pi = Xi / \sum_{i=1}^{m} Xi \quad (1)$$

Entropy ‘H’ is calculated as follow,

$$H = -\sum_{i=1}^{m} Pi * \log_2 Pi \quad (2)$$

For optimization of threshold value, objective function [14] has been implemented, which is shown in Figure 1.

.

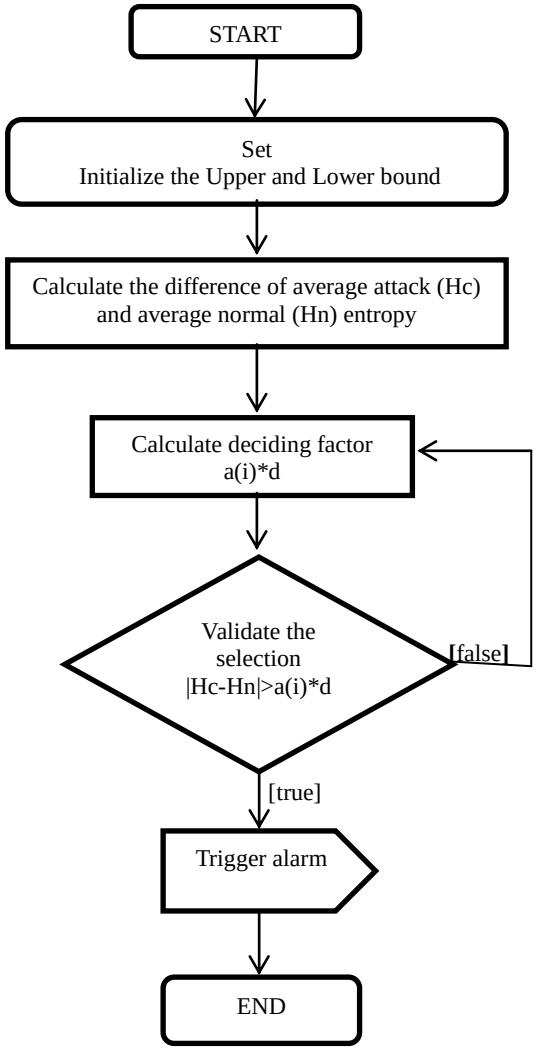

Figure 1. Optimization of threshold value

The pseudo code for optimization of threshold value is as follows,

Step 1: Set Upper bound and Lower bound.

Step 2: Calculate the difference of average normal and average attack entropy.

$$\text{Entropy diff} = Hc - Hn \quad (3)$$

Hc- average entropy when Low-DDoS attack is present.

Hn- average entropy when normal traffic is present.

Step 3: Calculate the deciding factor from absolute maximum deviation 'd' and value of 'a' set over number of iterations by,

$$\text{Deciding factor} = a[i] * d \quad (4)$$

Where i- is the index for iteration over lower bound to upper bound

Step 4: Validate the selection of value for detection using formula,

$$|Hc - Hn| > a[i] * d \quad (5)$$

If true, then return the value of current a[i] and trigger the alarm Else

Go to the step 3

4. RESULT AND DISCUSSION

The bandwidth consumption of network when low-rate attack traffic is available shown in Figure 2. And without Low-rate DDoS attack traffic graph is shown in Figure 3. Probability distribution for normal traffic and attack traffic is calculated over the simulation when no attack and attack launched as shown in Figure 4. Entropy distribution for LDDoS attack over network is calculated in time window of 6sec to 15sec as mentioned in the simulation parameter and the observed pattern for entropy values are presented in the Figure 5.

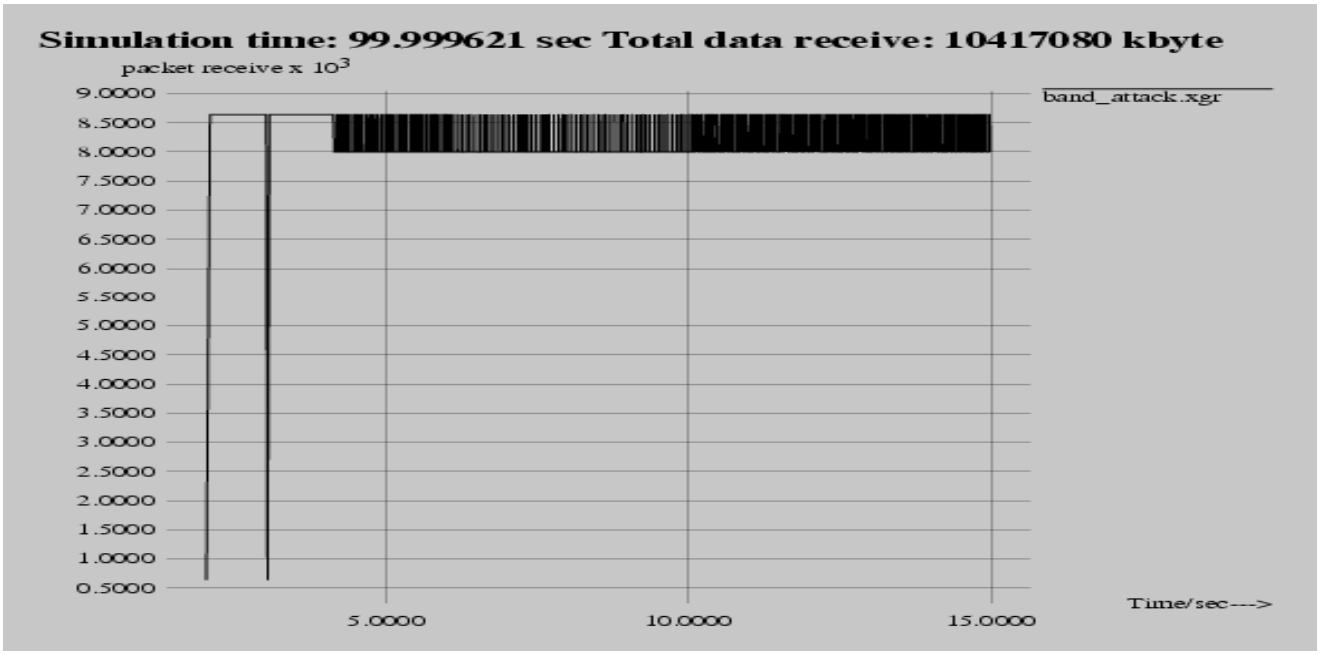

Figure 2: Packet received over Low-rate DDoS attack

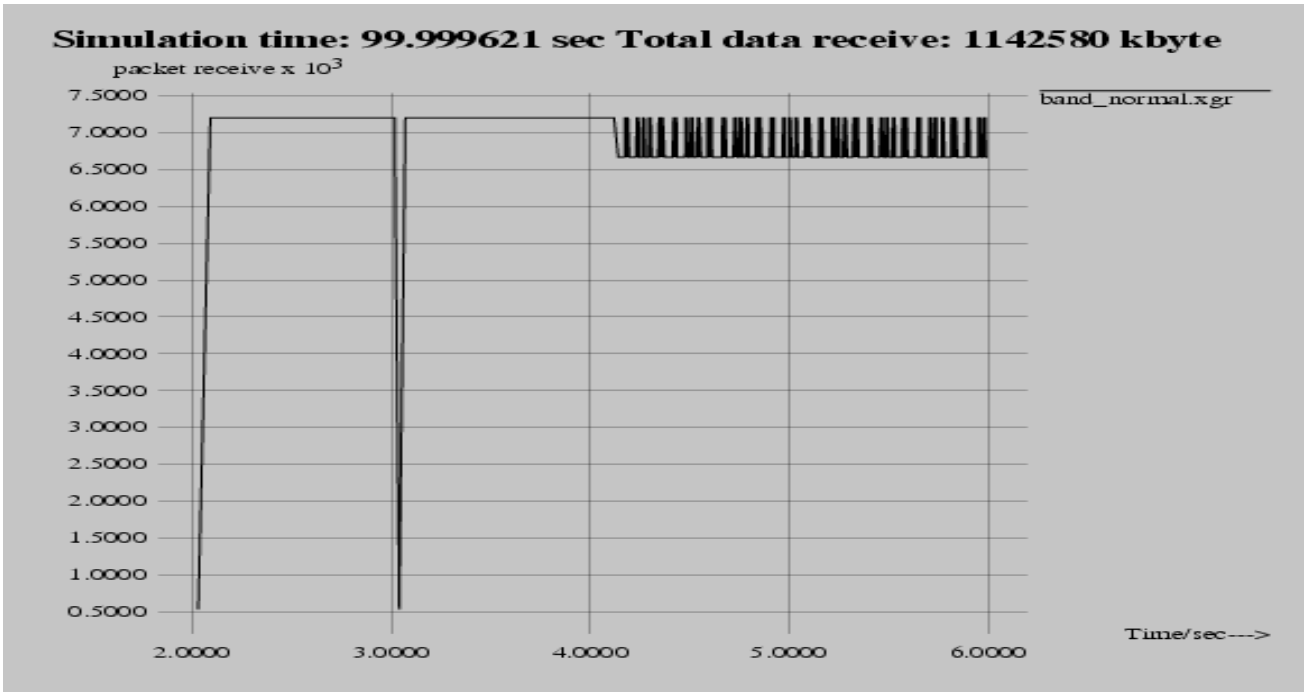

Figure 3: Packet received Vs time at absence of LDDoS attack

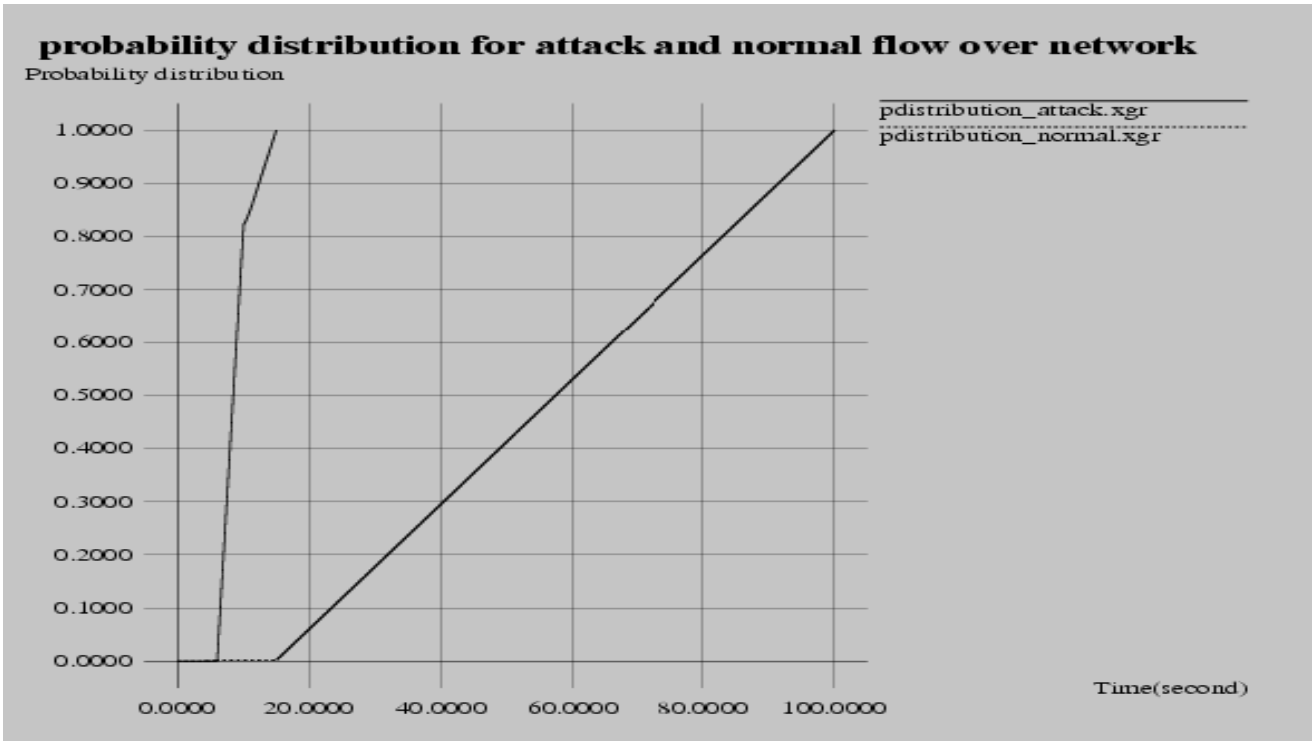

Figure 4: Probability distribution for normal and attack traffic over simulation time

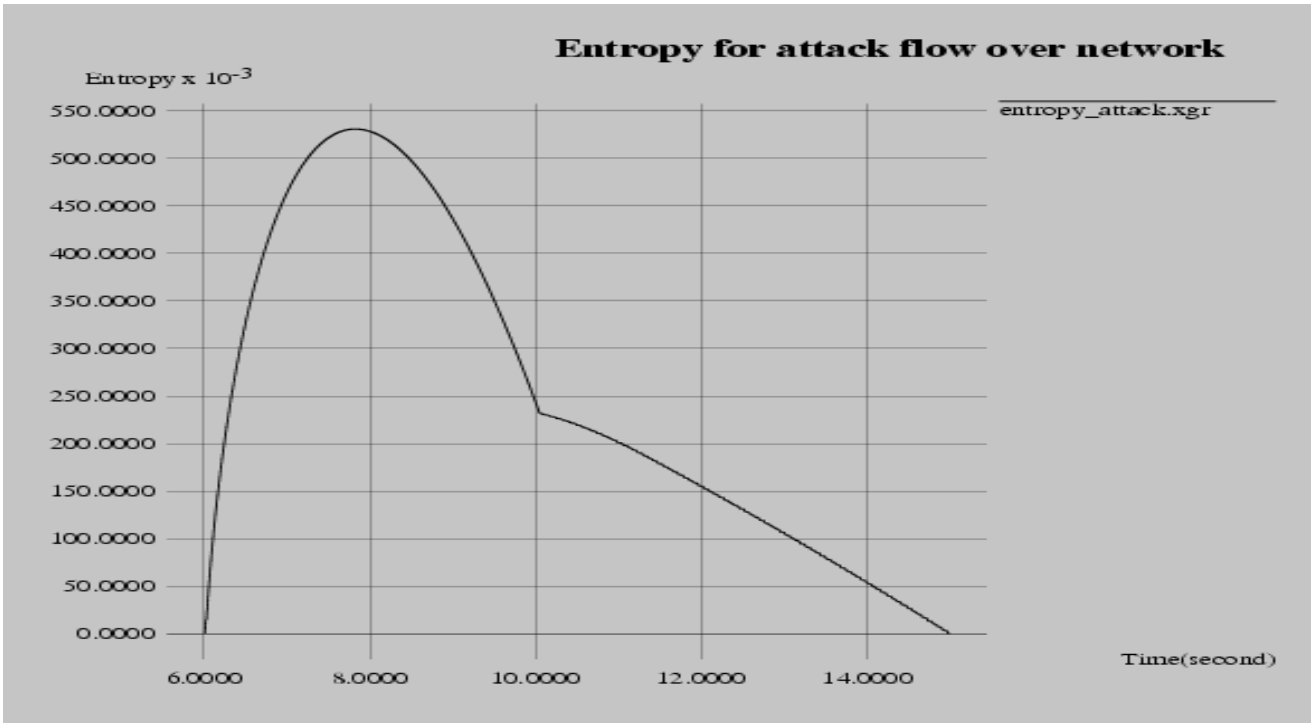

Figure 5: Entropy variations for LDDOS attack traffic

Simulation has been executed for 100sec and the final output result of the simulation with optimized value for multiplying factor, average normal entropy, average attacker entropy, maximum deviation is as follows,

Hc=0.360693
Hn=0.360674
d=0.000019
Entropy Difference=0.000019
Factor=0.000017
Attack detected for the value of a=0.900000

From the above values it can be conclude that the values of entropy are very nearer to each other hence it is always critical to isolate Low rate DDoS from normal traffic flow using simple thresholds, so for that in the above section it was explained that the optimization function for selection of multiplying factor here the value of 'a' for which attack detected is 0.9.

The method explained here is optimal for detection of Low-DDoS traffic over network as compared to previous Advance entropy based detection scheme where the values of 'a' are fixed for specific network traffic and unable to detect precise Low-rate attack because of the adaptive nature of the traffic.
Consider 'v' is max packet sequence number and 's' denote total packets received then detection rate (q) for OOE is defined by formula,

$$q=(v/(v+s)) * 100 \quad (6)$$

Detection rate over the previous detection scheme and our experiment is shown in Figure 6.

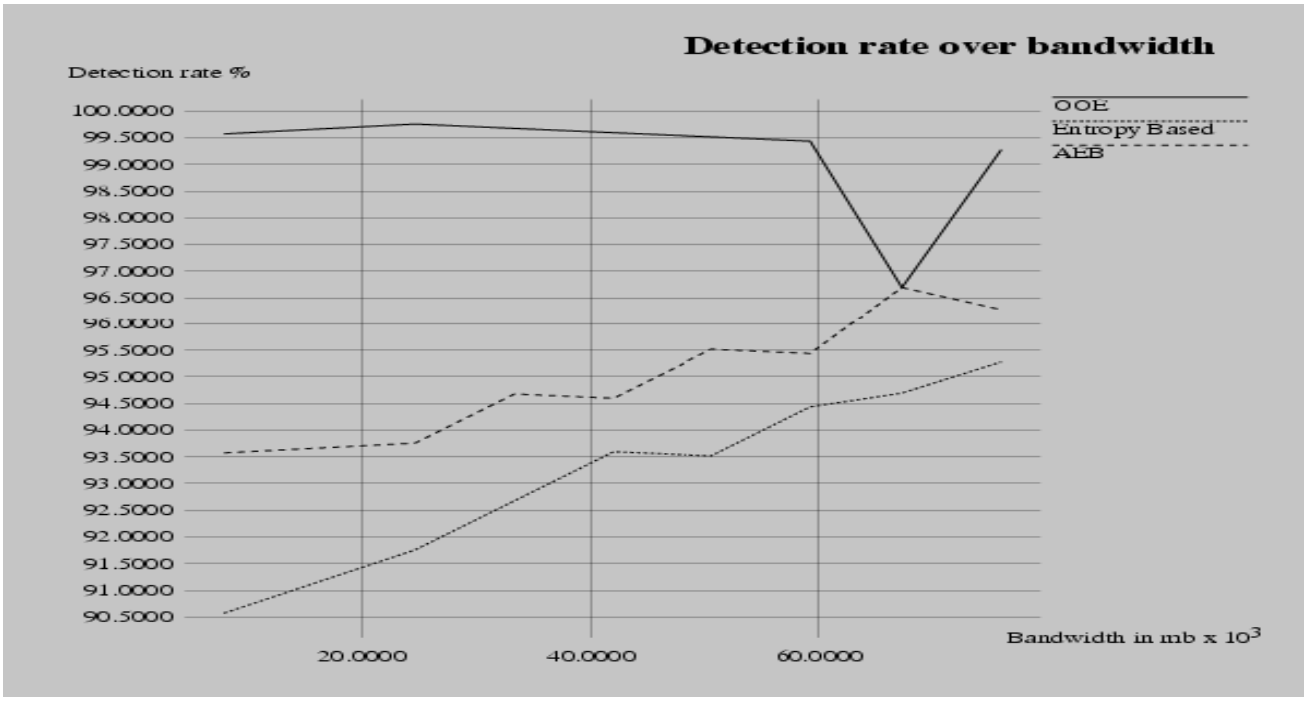

Figure 6: Detection rate comparison over OOE, AEB and Traditional Entropy-based method

5. CONCLUSION AND FUTURE SCOPE

DDoS attack prevents legitimate users from using their resources. Many solutions have been suggested for DDoS attack detection. This paper implements Optimal Objective Entropy (OOE) based method for detection of Low-rate DDoS attack, which is hard to detect than high-rate DDoS attack. For optimization of threshold value the objective function is derived by using Genetic algorithm, which will increase detection accuracy than the Advanced Entropy-based (AEB) and traditional Entropy-based method. The values derived by objective function can be tuned according to different traffic conditions.

7. REFERENCES

[1]Suratose Tritilanunt, Suphannee Sivakorn, Choochern Juengjincharoen, Ausanee Siripornpisan, "Entropy-based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks," Mahidol University, Thailand

[2]Aleksandar Kuzmanovic and Edward W. Knightly, "Low-Rate TCP-Targeted Denial of Service Attacks and Counter Strategies"

[3]Jie Zhang, Zheng Qin, Lu Ou, Pei Jiang , JianRong Liu and Alex X. Liu, "An Advanced Entropy-Based DDOS Detection Scheme," 2010 International Conference on Information, Networking and Automation (ICINA)

[4]V.Sus hma Reddy, K.Damodar Rao, P.Sowmya Laks hmi, "Efficient Detection of DDoS Attacks by Entropy Variation," IOSR Journal of Computer Engineering (IOSRJCE), ISSN: 2278-0661, ISBN: 2278-8727 Volume 7, Issue 1 (Nov-Dec. 2012), PP 13-18

[5]Aditya Akella, Ashwin Bharambe, Mike Reiter, Srinivasan Seshan,"Detecting DDoS Attacks on ISP Networks," Carnegie Mellon University

[6] Ming Li, Jun Li and Wei Zhao, "Experimental Study of DDoS Attacking of Flood Type Based on NS2," International Journal of Electronics and Computers, 1(2) December 2009, pp. 143-152

[7]N. Jeyanthi and N. Ch. Sriman Narayana Iyengar, "An Entropy Based Approach to Detect and Distinguish DDoS Attacks from Flash Crowds in VoIP Networks," International Journal of Network Security, Vol.14, No.5, PP.257-269, Sept. 2012

[8]Reyhaneh Karimazad and Ahmad Faraahi," An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks" 2011 International Conference on Network and Electronics Engineering IPCSIT vol.11 (2011) © (2011) IACSIT Press, Singapore

[9]Rejo Mathew and Vijay Katkar,"Software based Low Rate DDoS Attack Detection Mechanism," International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011

[10] Yang Xiang, Ke Li, and Wanlei Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011

[11]H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in *Proc. IEEE INFOCOM*, pp. 1530-1539, 2002.

[12] C. M. Cheng, H. T. Kung, and K. S. Tan, "Use of spectral analysis in defense against DoS attacks," in *Proc. IEEE GLOBECOM*, pp. 2143-2148, 2002.

[13]A. Kulkarni and S. Bush, "Detecting distributed denial-of-service attacks using kolmogorov complexity metrics," *Journal of Network and Systems Management*, vol. 14, pp. 69-80, 2006.

[14]U. Deepak, "Optimization of Milling Operation Using Genetic and PSO Algorithm," Bonfring International Journal of Software Engineering and Soft Computing, Vol. 1, Special Issue, December 2011