International Journal of Security and Its Applications
Vol. 10, No. 5 (2016) pp.139-146
http://dx.doi.org/10.14257/ijsia.2016.10.5.13

Evaluation of Flow and Average Entropy Based Detection Mechanism for DDoS Attacks using NS-2

Raghav Vadehra[1], Manjit Singh[2], Butta Singh[3], Nitika Chowdhary[4]
[1,2]ECE Dept., GNDU, RC, Jalandhar
[3]CSE Dept., GNDU, RC, Jalandhar
[1]raghav.vadehra12@gmail.com
[2]manu_kml@yahoo.co.in
[3]bsl.khanna@gmail.com
[4]nitu.expert@gmail.com

Abstract

Distributed Denial of Service (DDoS) attacks has started posing a serious threat to all sorts of businesses, which have used the power of internet to their credit. DDoS attacks have put a big question mark on the capabilities and reliability of the World Wide Web. The use of supreme techniques to combat the DDoS attacks has not been substantial enough to fight the distributed nature of attacks. Hackers have been successful in blocking the services and flooding traffic to servers, in spite of a tight check on the network. Thus, in the view of personal data being present on the web and the threat to global economy worth million dollars, it becomes really important to devise some new techniques that are self-capable enough to capture, trace and nullify the dangers posed by such attacks. This term paper talks about such solutions to combat DDoS attacks. Here, the flow entropy in combination with average entropy technique is used to detect an attack. It highlights how the loop holes of one technique are covered by the other, resulting in a considerable improvisation in the methods of how we deal with these attacks.

Keywords: *DDoS attacks, Flow Entropy, Average Entropy, Botnet*

1. Introduction

DDoS attacks have proved to be one of the most disastrous means of denying and disrupting services to the legitimate users across the globe. These attacks are made possible either by flooding the server's network bandwidth or by consuming the computing resources. With the help of corrupt programs which the attackers install on different systems, they create a network of all the compromised machines called Bots. These bots are programmed to launch packets which are malicious and target the victim computer leading either to disruption of services or the flooding of the legitimate network. DDoS attacks have been able to create an atmosphere of fear globally to such an extent that sometimes it is confused with the authorised flash events, which is the sudden increase in legitimate traffic. So, here it becomes crucial to stretch a line between legitimate and illegitimate traffic sources.

This paper is divided into 6 sections; Section 2 is background of DDoS attacks and gives the brief explanation of attacks. Section 3 is the related work, which illustrates incidents and the existing countermeasures against attacks. Moreover, it explains the concept of entropy and its significance in detection mechanism of attacks. Section 4 illustrates the simulation methodology and entropy based parameters to detect attacks. Section 5 discusses results based on the simulation. Section 6 is the future work and finally, Section 7 gives concluding remarks on flow entropy based countermeasure against DDoS attacks.

ISSN: 1738-9976 IJSIA

2. Background

This section helps us to understand the basics regarding DDoS attacks and also lists various attacks worldwide in history.

How DDoS attacks occur?

First, the attacker targets the primary victims by installing malicious scripts on their systems. In this way, the victim machines become Bots or Zombies, and the network of these machines is called Botnet [1]. This network unwillingly gets attached to the Command and Control channel of the attackers. After that, these machines send illegitimate traffic to the primary victim channel on the commands received from attacker [2]. The high volume of the malicious packets blocks the victim server. As a result, the legitimate users are deprived of the services of the server. Since, this unauthorised data is being sent through the widespread network of botnets, hence it is very difficult to detect and track the source of attack [3].

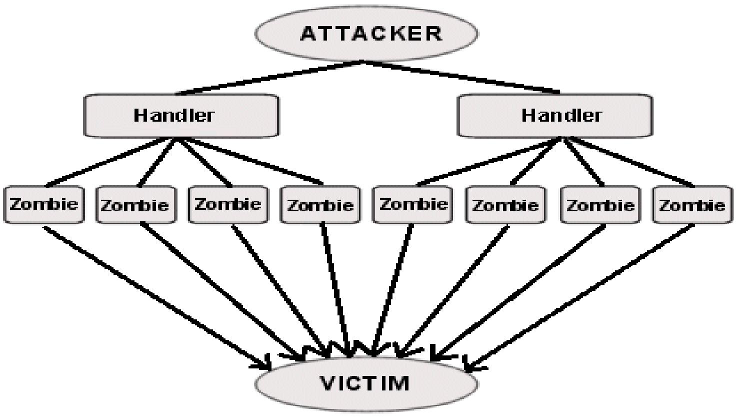


Figure 1. Agent Handler Model of DDoS Atack [1]

History of DDoS describes the detrimental effect of these attacks on the worldwide network. First attack occurred in 2000 when university website went offline for two days. It was followed by attacks on websites yahoo and amazon. Year 2002 witnessed an attack on www.grc.com .Tools like TFN (Tribe Flood Attack); Trino which were employed, failed drastically to find an effective way out .The most devastating of all attacks happened in 2009, when 48 websites of US and Korea were taken down by the attackers [4]. This particular attack gave more courage to the attackers and since then, the web world has seen different kinds of attacks targeting different areas across. For instance, the most recent one was an attack by Cyber Bunker (Dutch web hosting company) in 2013, which led to decrease of internet speed of millions of users. DDoS attacks can be very extensive in nature as they can block the victim servers with 500 Gbps of data (as claimed by the network of new attackers, DD4BC)[5].

3. Related Work

Techniques like Deterministic Packet Marking (DPM) and Probabilistic Packet Marking (PPM) have proved to be a failure because of the cumbersome task of injecting marks in individual packets [6]. Techniques like activity profiling as suggested by Moore *et al.* in [7] have already been cracked by hackers. Next attempt was made by Yi *et al.* when he used uniformity in distribution of source IP address and thus identified DDoS attacks on the basis of chi square statistics and entropy. However, this led to confusion of increase in entropy due to flash events which led to the surge of false positive rate. Later, he attempted to detect and distinguish DDoS attacks from flash events but accuracy was not ensured in that approach [8]. Monika Sachdeva *et al.* in [8] had suggested the traffic cluster entropy based method in place of volume based approaches in order to differentiate between flash events and DDoS attacks. Gil *et al.* proposed the monitoring of packet rate both for uplink and downlink can be helpful in detection of DDoS attack. This technique assumes that a disproportionate inflow and outflow of traffic from a subnet can be taken as an indication of attack [9]. Shingang Chen *et al.* describes perimeter based defense mechanism for the internet service providers to provide anti-DDoS services to the customer that rely on edge routers to avoid stress on ISP core routers [10].

3.1. Entropy Based Approach

Entropy is defined as the measure of the uncertainty or randomness associated with the random variables which in this case are the attributes of the packets of data in the network. Randomness of a variable is directly related to entropy. Rate of distribution is higher if the class distribution is impure. It has the lowest entropy value *i.e.* 0, when all the variables belong to same class [11].

Let X= {n_i, i=1,2,......N} is the frequency distribution consisting of N features where feature ‘i’ occurs n_i times in the sample.

Let

$$S = \sum_{i=1}^{N} \mathrm{n_i} \quad ..1$$

Where ‘S’ be the total number of observations in the distribution.

Let $pi = n_i / S$ be the probability of occurrence of each feature i in the sample. The entropy H(X) is calculated as

$$H(X) = -\sum_{i=1}^{N} (p_i) \times \log_2(p_i) \quad ..2$$

Where ‘X’ gives the number of packets observed for each feature ‘i’ in the sample. Sample entropy has maximum value of $\log_2 N$ when the distribution is maximally dispersed.

Average Entropy for different Flow ID is given as:

$$H\left(F_{avg}\right) = \frac{-\sum_{i=1}^{n} H(F_i)}{N(H(F_i))} \quad ...3$$

Where, N(H(F_i)) is the total flow and H(F_i) is the entropy of the particular flow ‘i’.

4. Simulation Methodology

This section deals with the scenario based on DDoS attacks. NS-2, which is a discrete event driven simulator, is used for the purpose. First, the 20-node network is created using GT-ITM Topology generator. Then, legitimate and the illegitimate traffic sources are attached in the network. Next, awk script is used in order to analyse the trace file of the simulation scenario. After that, with the help of Microsoft Excel, entropy parameters of different nodes in different time periods are calculated and analysed. At last in analysis, the cumulative average entropy of the total traffic distribution in different time periods is considered as the threshold entropy. If the attack is suspected then, Flow Id is detected and traced using the average flow entropy during different time periods. Following figure describes the above mentioned steps in the form of flow diagram.

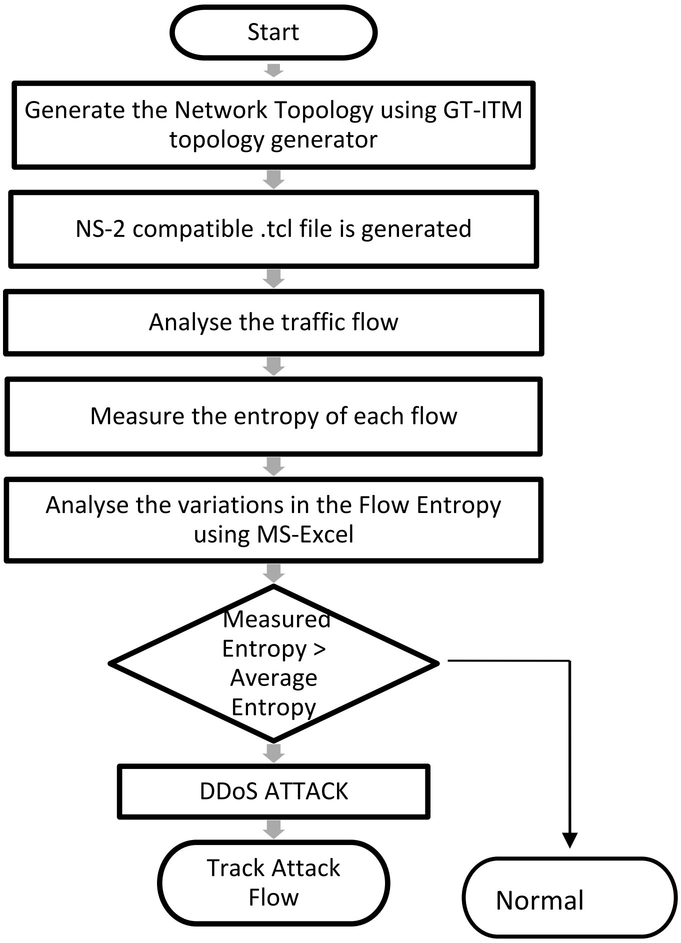

Start
Generate the Network Topology using GT-ITM topology generator
NS-2 compatible .tcl file is generated
Analyse the traffic flow
Measure the entropy of each flow
Analyse the variations in the Flow Entropy using MS-Excel
Measured Entropy > Average Entropy
DDoS ATTACK
Track Attack Flow
Normal

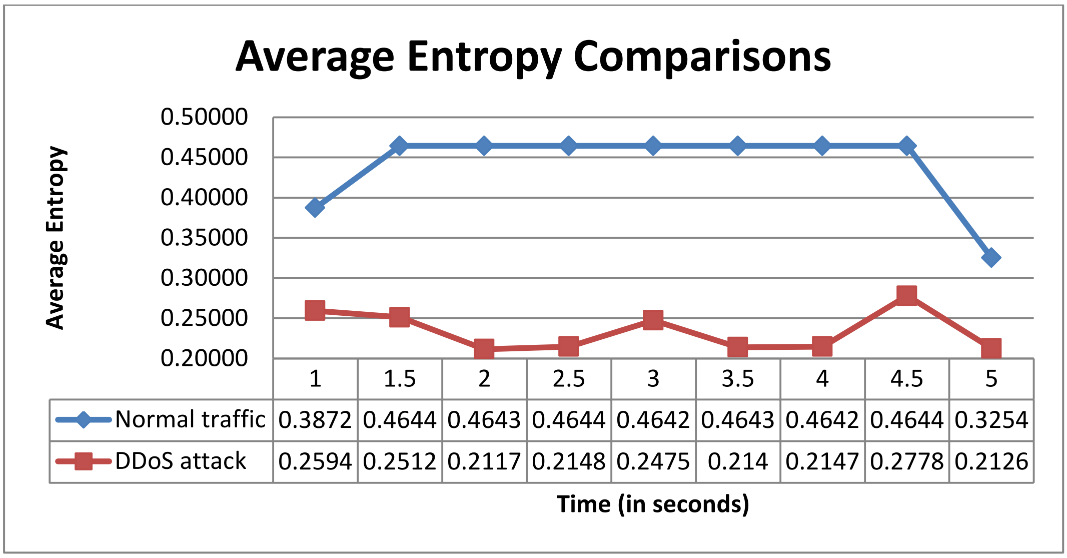
Figure 2. Simulation Methodology

4.1. Performance Metrics

In our simulation, we have used Flow Entropy as the measure to detect attacks because of the efficiency and reliability of this countermeasure. Flow entropy defines the distribution of traffic based on attributes like Source address, destination address and Flow Id. It is an important parameter to analyse the traffic. If the average entropy is less than normal then we can suspect the presence of attack because it means that the traffic distribution has been limited to few nodes only, which signifies that major portion of the traffic is sent by the attacking nodes to block the resources of the victim system. Furthermore, it is important to differentiate between authorized and unauthorized flow to identify attacks. To trace the malicious flows, flow entropy of the individual flows is calculated and analyzed. If the entropy value of the specific flow Id (based on particular source) is greater than average entropy, we classify it as attack flow; else it is classified as a legitimate flow.

5. Results and Discussion

Entropy measurements help us to detect and find the sources of attacks. Different topologies in the presence and absence of attacks have been simulated in NS-2. In the following section we will discuss the results we have obtained from two different scenarios.



	1	1.5	2	2.5	3	3.5	4	4.5	5
Normal traffic	0.3872	0.4644	0.4643	0.4644	0.4642	0.4643	0.4642	0.4644	0.3254
DDoS attack	0.2594	0.2512	0.2117	0.2148	0.2475	0.214	0.2147	0.2778	0.2126

Figure 3. Graph of Average Entropy of the Traffic Distribution

From figure 3, it is evident that there is a decrease in average entropy, which indicates that only few nodes are responsible for sending majority of packets. Hence, we can consider it as illegitimate traffic. Moreover, average entropy varies more in case of DDoS traffic, which is evident from the graph. After this, we consider individual flows based on Flow Id, those flows which have entropy greater than the average entropy are considered as malicious flows.

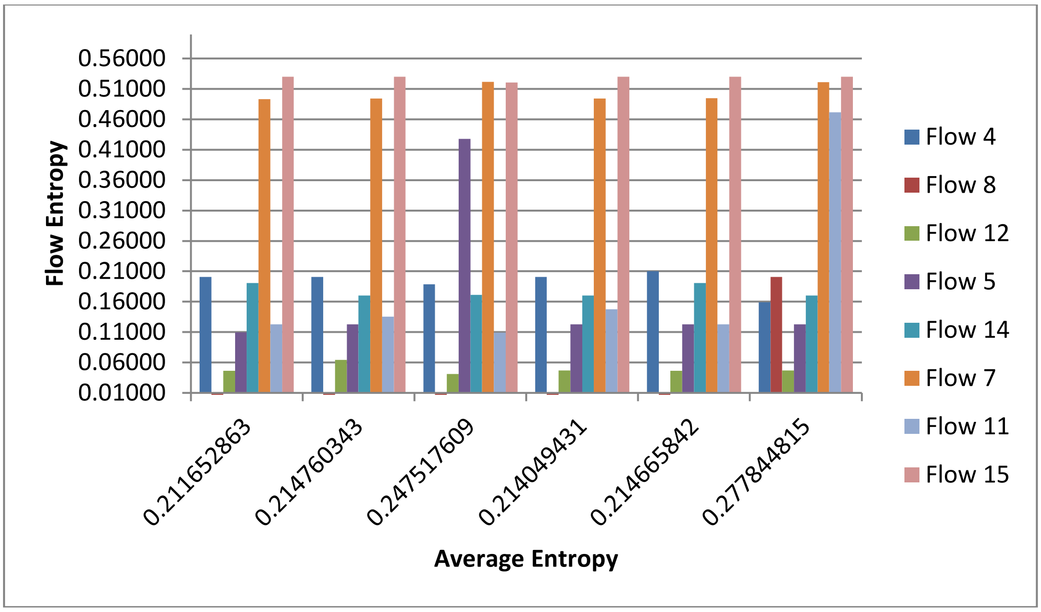


Figure 4. Graph Showing Flow Entropy of Different Flows

From figure 4, it is clear that Flow 7 and 15 are definitely attacking flows. Since, the value of Flow entropy for these flows is greater than the average entropy during specific time periods. However, Flow11 is under the suspicion of being the illegitimate flow. Other flows with Flow Ids as 4, 8, 12, 5 and 14 have the entropy much less than the average entropy. Hence, they are categorized as the legitimate flows.

5.1. Outcome

Average entropy of the network hit by DDoS attack is smaller than entropy of normal network. It is evident of the fact that only illegitimate users are sending the majority of traffic to the victim server in order to deprive its resources to the legitimate users. Moreover, the entropy of the attack flows is greater than the normal legitimate flows which signify that the packets from malicious sources are being sent at a much larger frequency than the legitimate users.

6. Future Work

Our overall objective is to find the most efficient and reliable mechanism to detect DDoS attacks. Different entropy based countermeasures are effective to combat the attacks. We have used the combination of average and flow entropy parameters for detection in this paper. In our future work, we will propose a more comprehensive and reliable hybrid model to detect DDoS attacks using different types of entropy variations of other network parameters like port address, packet transmission *etc*., which could help to find the best suitable measure to block the sources of these attacks.

7. Conclusion

DDoS attacks pose a serious threat to the present day networks. These can lead to enormous economic losses by crashing the victim servers. Therefore, it is the need of the hour to develop comprehensive solutions against such attacks. This paper provides a good understanding of the entropy based countermeasure against DDoS attacks. Moreover, it also reviews different defense mechanisms and their drawbacks. In this paper, we have implemented the DDoS attack detection method using average and flow entropy, which is an effective means to find the attack sources. It is an efficient way to diagnose an anomaly in the traffic distribution of the network as it gives less false positives as compared to other mechanisms of detection.

References

[1] E.Alomari, S.Manickam, B.B Gupta, S.Karupayyah and R.Alfaris, "Botnet based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art", *IJCA*, vol. 49, no.7, **(2012),** pp. 24-32.

[2] A.Tyagi and G.Aghilla, "A Wide Scale Survey on Botnet", *IJCA*, vol. 34, no.9, **(2011),** pp. 9-22

[3] J.Yuan and K.Mills, " Monitoring the Macroscopic Effect of DDoS Flooding Attacks", *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no.4, **(2005),** pp. 324-335.

[4] J H Jun, D Lee, CW Ahn and S H Kim, "DDoS Attack Detection Using Flow Entropy and Packet Sampling on Huge Networks", ICN, **(2014),** pp.185-190.

[5] R Cox, "5 Notorious DDoS attacks in **2013**: Big Problem for the Internet of Things". Available at: http://siliconangle.com/blog/2013/08/26/5-notorious-DDoS-attacks-in-2013-big-problem-for-the-internet-of-things/

[6] Poonam N. Jhadhav and B.M. Patil, "Low rate DDoS Detection method using Optimal Objective Entropy Method", *IJCA*, vol. 78, no.3, **(2013),** pp. 33-38.

[7] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Transactions on Computer Systems*, vol. 24, no. 2, **(2006),** pp. 115–139.

[8] M.Sachdeva and K.Kumar, "A Traffic Cluster based Entropy approach to Distinguish DDoS attacks from Flash Events using DETER Method", *ISRN Communications and Networking*, (**2014),** Article Id-259831, Hindawi Publishing Corporation, pp. 1-15.

[9] B.B. Gupta, R.C Joshi and M.Mishra, "Dynamic and Auto Responsive Solution for Distributed Denial of Service Attacks Detection in ISP Network", *IJCTE*, vol. 1, no.1, **(2009),** pp. 71-80.

[10] ShigangChen,"Perimeter based Defense against High Bandwidth DDoS Attacks", *IEEE Transactions on Parallel and Distributed Systems*, vol. 16, no.6, **(2005),** pp. 526-537.

[11] A.S Syed Navaz, V. Sangeetha and C. Prabhadevi, "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud", *IJCA,* vol. 62, no.15, **(2013),** pp. 42-47.

Authors

Raghav Vadehra, (BTech) he received the Bachelor's degree in Electronics and Communication Engineering, in 2013. He worked as Associate System Engineer in Tata Consultancy Services Limited for one year. Currently, he is a student of MTech in Electronics and Communication Department at Guru Nanak Dev University, Regional Campus, Jalandhar (INDIA). His research area of interest is network security.

Manjit Singh received his bachelor degree in Electronics Engineering from Baba Banda Singh College of Engineering Fatehgarh Sahib, Punjab, India in 1998, and Masters Degree in Electronics and communication Engineering from National Institute of Technical Teacher Training and Research, Chandigarh, India in 2010. Currently he is pursuing his Ph.D. degree from Punjab Technical University Jalandhar, Punjab, India. He is working as Assistant Professor at Guru Nanak Dev University Regional Campus Jalandhar, Punjab, India. His research interest is in the area of biomedical signal processing.

Butta Singh received his Bachelor's degree in Electronics and Communication Engineering from Guru Nanak Dev Engineering College, Ludhiana, Punjab, India in 2002, Master's degree in In strumentation and Control Engineering from Sant Longowal Institute of Engineering and Technology, Longowal, Sangrur, Punjab, India in 2005 and Ph.D. degree in Engineering from National Institute of Technology, Jalandhar, Punjab, India. He is serving as Assistant Professor in the Department of Electronics and Communication Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab, India. His professional research interests are in signal processing, in particular, applied to biomedical applications. He has published over 50 research articles in internationally reputed journals and conference proceedings

Nitika Chowdhary, (BTech, MTech) she received the masters's degree in computer science and engineering, in 2013 and the bachelor's degree in information technology, in 2011 from Punjab Technical University, India. She is currently pursuing Ph.D. in Computer Science and Engineering Department at Guru Nanak Dev University, Regional Campus Jalandhar. Her research interests include security, distributed networks, and cloud computing.