Information Metrics for Low-rate DDoS Attack Detection : A Comparative Evaluation

Monowar H. Bhuyan
Dept. of Computer Science and Engg
Kaziranga University
Koraikhowa, Jorhat 785006, Assam
monowar.tezu@gmail.com

D. K. Bhattacharyya
Dept. of Computer Science and Engg
Tezpur University
Napaam, Tezpur 784028, Assam
dkb@tezu.ernet.in

J. K. Kalita
Dept. of Computer Science
University of Colorado
Colorado Springs, CO 80918, USA
jkalita@uccs.edu

***Abstract*— Invasion by Distributed Denial of Service (DDoS) is a serious threat to services offered on the Internet. A low-rate DDoS attack allows legitimate network traffic to pass and consumes low bandwidth. So, detection of this type of attacks is very difficult in high speed networks. Information theory is popular because it allows quantifications of the difference between malicious traffic and legitimate traffic based on probability distributions. In this paper, we empirically evaluate several information metrics, namely, Hartley entropy, Shannon entropy, Renyi's entropy and Generalized entropy in their ability to detect low-rate DDoS attacks. These metrics can be used to describe characteristics of network traffic and an appropriate metric facilitates building an effective model to detect low-rate DDoS attacks. We use MIT Lincoln Laboratory and CAIDA DDoS datasets to illustrate the efficiency and effectiveness of each metric for detecting mainly low-rate DDoS attacks.**

Keywords*— *DDoS attack, information metric, network traffic, low-rate, entropy

I. Introduction

DDoS attacks use a set of compromised hosts to make Internet services unavailable. Attackers are continually improving their ability to launch future DDoS attacks by infecting unsuspecting hosts. These attacks normally consume a massive amount of resources from a server that makes the server inaccessible to legitimate users; they also consume network bandwidth by compromising network traffic. DDoS attacks are cooperative distributed large scale attacks and can spread by both wired and wireless networks. Hence, both industry and academia are interested in defending their networks from DDoS attacks, ensuring uninterrupted access by legitimate users. It is challenging to distinguish malicious traffic from legitimate traffic since they are similar based on traffic behavior alone. There are two types of traffic that can normally compromise a host or a network with DDoS attacks [1]. They are: (a) high-rate DDoS attack traffic, which is exceptional and similar to a flash crowd and (b) low-rate DDoS attack traffic, which is similar to legitimate traffic. Since both have characteristics of legitimate traffic, it is crucial to detect a DDoS attack and remit within a short time interval.

Most recent work aims to detect DDoS attacks launched by botnets. A botnet is a large network of compromised hosts (i.e., bots or slave machines) controlled by one entity (i.e., the master) [2]. The master can send malformed packets through a synchronized host (i.e., the slave) to the target host. However, detection of botnets is hard and an effective solution needs to monitor all machines that can possibly become active bots in a botnet.

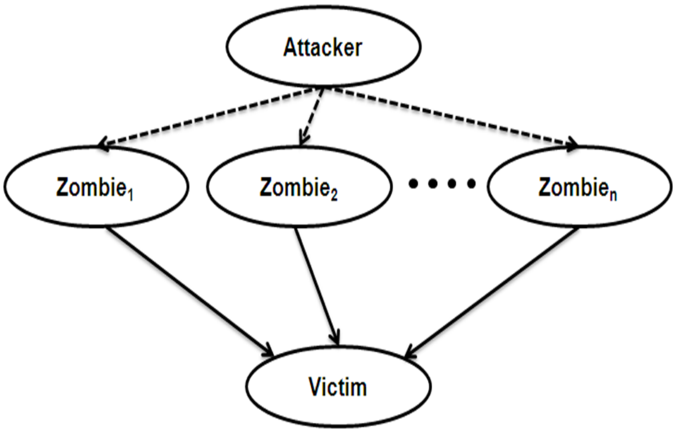

Fig.1. Direct attacks

There are two ways to launch DDoS flooding attacks: *direct* flooding attacks and *reflector*-based flooding attacks [2]. In *direct* DDoS flooding attacks, the attacker sends a massive number of packets to the victim host or server directly through multiple compromised hosts or machines as shown in Figure 1. Direct DDoS flooding attack is further classified as: Network-layer DDoS attacks and Application-layer DDoS attacks. TCP flood, UDP flood, ICMP flood and SYN flood are some common examples of network-layer DDoS attacks and HTTP flood, HTTPS flood and FTP flood are examples of application-layer DDoS attacks. In *reflector*-based DDoS flooding attacks, the attacker sends request to a reflector host to forward a massive amount of malicious traffic by spoofing IPs of victim host(s). As a result, the reflector hosts send their replies to the victim host and make the victim inaccessible by the legitimate users soon as shown in Figure 2. ICMP ECHO reply flood, SYN ACK RST flood, DNS flood and smurf flood are some well-known reflector-based attacks.

Information theory-based metrics are well established in detecting distributed DoS attacks. In information theory,

978-1-4799-5173-4/14/$31.00 ©2014 IEEE

entropy is a popular uncertainty measure unites with a random variable. Information distance computes the variation between various probability distributions. Kullback-Leibler divergence and Shannon's entropy are assumed to be the most useful methods in detecting malicious traffic based on IP address or packet size distribution statistics [3], [4].

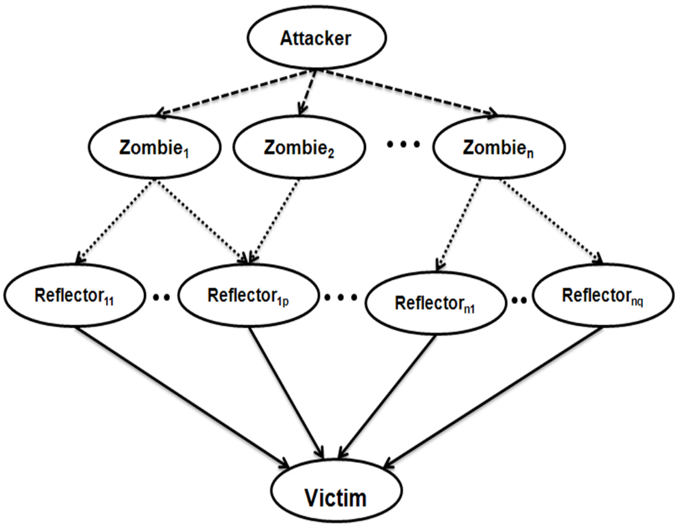

Fig. 2. Indirect attacks

In this paper, we contribute in two ways: First, we discuss the most common information metrics that are used in detecting DDoS attacks with pros and cons. Second, we analyze and evaluate each information metric from an attacker's viewpoint in the context of detecting low-rate DDoS attacks. We use victim-end architecture for analyzing information metrics in detecting low-rate DDoS attacks.

The rest of the paper is organized as follows: Section II discusses related research with a focus on the detection of low-rate DDoS attacks. Section III discusses various information metrics that are used to detect low-rate DDoS attacks within short time intervals. It also includes the complexity analysis of the detection method. However, in Section IV, we report experimental results and discussion based on the use of information metrics in detecting low-rate DDoS attacks. Finally, Section V presents conclusions with future work.

II. Related Research

Detection of attacks is crucial for infrastructure networks. So, both industry and academic researchers are constantly trying to detect network attacks with high accuracy for at least two decades. There are mainly two techniques to detect attacks: signature-based and anomaly-based. Signature-based detection mechanisms only can detect attacks, whose signatures are known. If any attack is discovered, it should be used to train the system. However, an anomaly-based detection system characterizes legitimate network behavior and reports an alarm if it deviates from it. Information metric is a statistical metric, which is increasingly being used in network anomaly detection. Sheng et al. [5] discuss a measure, designed, based on Hurst coefficient to detect low-rate DDoS attacks. Experimental results obtained and demonstrate effectiveness in detecting low-rate DDoS attack*s.* Xiang et al. [4] present two information metrics: generalized entropy and information distance to identify low-rate DDoS attacks. They measure the difference of the information metrics between normal traffic and malicious traffic. They test their metric using real-life DDoS traffic traces and show the reduction of false alarms with early stage detection.

Zhang et al. [6] present a metric for flow-level network traffic, designed based on Congestion Participation Rate (CPR) to detect and filter low-rate DDoS attacks that generate low-level congestion in the network. If the CPR value is higher than the user defined threshold, a network flow is classified as a low-rate DDoS attack and the network allows subsequently dropping all connected packets. The authors analyze the effectiveness of the CPR-based approach to quantify the average CPR difference between legitimate TCP flows and low-rate DDoS flows. It was shown that the CPR-based approach can differentiate between legitimate and attack traffic. Experiments using Internet traffic-trace analysis, ns-2 simulator and test-bed experiments establish the results. Tao and Yu [7] present a DDoS flooding attack detection method using an information theoretic measure. It can detect DDoS attacks within a short time interval and is effective when experimented on real-life datasets. Francois et al. [8] report the theoretical foundation, architecture, and algorithms to detect DDoS flooding attacks; their approach is known as FireCol. FireCol contains intrusion prevention systems (IPSs) installed by various Internet service providers (ISPs). A virtual protection ring is created by IPSs around the hosts to defend against DDoS flooding attacks by interchanging the chosen traffic information. FireCol was evaluated using both simulations and real datasets and obtains effective results. It also supports cumulative deployment in real networks.

A. Discussion

Based on our survey, we have made the following observations.

- Only few detection methods focus on detecting low-rate DDoS attacks.
- As discussed, low-rate DDoS traffic is similar to legitimate traffic. So, detection of such attacks is difficult and challenging.
- Detection methods are more concentrated on packet-level datasets.

III. Information Metrics for DDoS Detection

An information metric measure may be used to overcome the limitations of existing DDoS attack detection methods. In this paper, we attempt to evaluate information metrics for detecting low-rate DDoS attacks. The following assumptions have been made during experimentation.

- Routers have full control on in-and-out traffic flow.

- We collect packet and flow level traffic at the victim-end after various types of flooding attacks are launched.
- During processing, we sample the network traffic at 5 minute intervals and also further sample into 10 seconds time intervals.
- All malicious traffic follows Poisson distribution and normal traffic follows Gaussian distribution.

The symbols used to describe the information metrics for detecting low-rate DDoS attacks are given in Table 1.

TABLE I. SYMBOLS USED

Term	*Definition*
x	network traffic data
P	total probability
T	time interval taken for processing
t_i	ith time interval within T
H	the entropy metric
α	entropy metric of order α
x_i	ith instance within x
δ	threshold for attack detection
S	sample traffic
E	information distance metric
E_i	difference of entropy metric values between two samples, s_i and s_j
N	total number of packets within full time interval T
n	represents the smaller time interval t within T

In information theory, larger values of entropy are expected when the information variable is more random. In contrast, the entropy value is expected to be small when the amount of uncertainty in the information variable is small [3]. To quantify the randomness of a system, Renyi [9] introduced an entropy metric of order α as a mathematical generalization of Shannon entropy [10]. Let us consider a discrete probability distribution, P = {p_1, p_2, p_3, … p_n}, i.e., $\sum_{i=1}^{n} p_i = 1$, $p_i \geq 0$. Then the Renyi's entropy of order α is defined as

$$H_\alpha(x) = \frac{1}{1-\alpha} \log_2 \left(\sum_{i=1}^{n} p_i^\alpha \right) \tag{1}$$

where $\alpha \geq 0$, $\alpha \neq 1$, $p_i \geq 0$. If the values of the p_i's are the same, the maximum entropy value known as *Hartley entropy* [10] is achieved:

$$H_0(x) = \log_2 n \tag{2}$$

When $\alpha \to 1$, H_α converges to *Shannon entropy* [10]:

$$H_1(x) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{3}$$

If $\alpha = 2$, it is known as *collision entropy* or *Renyi's quadratic entropy* [9].

$$H_2(x) = -\log_2 \sum_{i=1}^{n} p_i^2 \tag{4}$$

Finally, when $\alpha \to \infty$, $H_\infty(x)$ reaches the minimum information entropy value. Hence, we say that the generalization of information entropy is a non-increasing function of order α, i.e., $H_{\alpha 1}(x) \geq H_{\alpha 2}(x)$, for $\alpha_1 < \alpha_2$, $\alpha > 0$.

Based on this analysis of information entropy metric, we consider different probability distributions for legitimate network traffic and malicious traffic when detecting low-rate DDoS attacks. We find the difference between legitimate and malicious traffic in low-rate attack situations. The major steps are given in Algorithm 1.

Algorithm 1 The low-rate DDoS attacks detection

Input: network traffic x with respect to time window, T and threshold, δ

Output: alarm information (attack or normal)

```
1: initialization: Probability $p(x_i)$, sample period, T=0, where i=1,2,3, … n, T= $t_1$, $t_2$, $t_3$, …, $t_N$, N is the full time interval.
2: sample the network traffic x received from upstream router R based on sampling period T
3: compute probability distribution $p_i$ based on traffic features (i.e., sIP, dIP and protocol) for each sample within T sampling period of $i^{th}$ sample.
4: compute entropy metric $H_\alpha(x)$ using Equation(1) for each sample within sampling period T
       $E_i = | H_\alpha(s_i) - H_\alpha(s_j) |$        (5)
5: check against variation threshold $E_i \geq \delta$, if so generate alarm; otherwise, router send ahead the packet to the next-level routers.
6: go to step 2.
```

A. Complexity Analysis

This analysis mechanism takes O(Tn) time for each sample in detecting low-rate DDoS attacks, where T is the time interval and n is the number of instances within a sample. Thus, for each individual order of information metric, the time complexity of the method is linear for each sample with respect to the size of the dataset and the number of attributes.

IV. EXPERIMENTAL RESULTS

Performance evaluation is important for any attack defense system. Performance for detecting DDoS attacks is mainly dependent on (i) the approach, (ii) deployment point and (iii) whether it is possible to dynamically update attack traffic information [11], [12]. When designing a DDoS attack defense mechanism, these issues should be taken into concentration to design a better defense mechanism.

In our experiments, two different datasets, viz., MIT Lincoln Laboratory [13] and CAIDA DDoS 2007 [14] datasets are used to detect low-rate DDoS attacks. The MIT Lincoln Laboratory tcpdump data is real-time pure normal data; it does not contain any attack traffic. The CAIDA dataset contains 5 minutes (i.e., 300 seconds) of annonymized traffic of a DDoS attack on August 4, 2007. These traffic traces store only attack traffic to the victim and response from the victim; non-attack traffic has been removed as much as possible. According to Moore et al. [15], it is a high-rate attack if there are more than 10,000 packets per second over the network. If 1,000 attack packets per second over the network covering 60% of the attack traffic then it is known as low-rate attack.

A. Results

We initially sample the network traffic every 10 seconds for 5 minutes, for analysis. We apply the generalized entropy measure of order α, where α is varied from 0 to 15 for our experiment. We also evaluate the generalized information distance of order α, where α is varied from 1 to 14 for detecting low-rate DDoS attacks. All features in network traffic may not play role in the detection of malicious traffic. Therefore, we consider only three features: source IP, destination IP, and protocol, for our experiments. The generalized entropy values of order α and spacing between normal traffic and malicious traffic for the CAIDA dataset are shown in Figure 3.

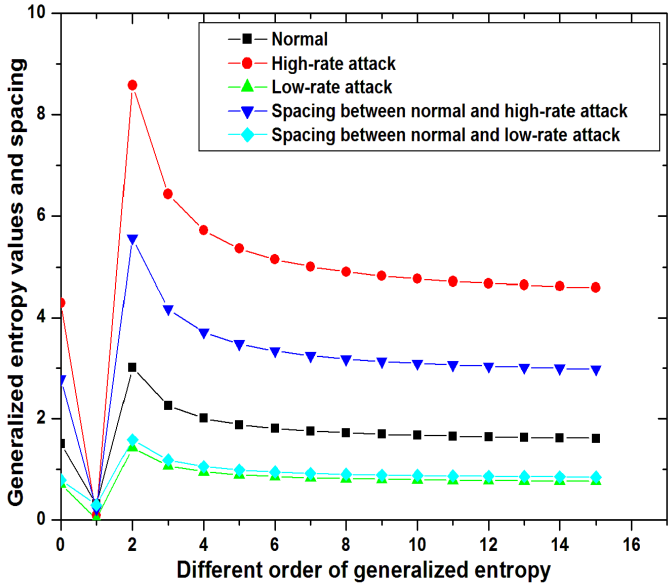

Fig. 3. Spacing between normal and malicious traffic in CAIDA dataset

In the figure, we see that spacing between normal and low-rate attack traffic is lower than the spacing in high-rate attack traffic. This is because low-rate attack traffic is similar to legitimate traffic. The spacing between legitimate or normal traffic and low-rate attack traffic using the generalized entropy metric of order α for the CAIDA DDoS dataset is given in Figure 4. The threshold δ value is varied from 0.10649 to 1.87868 when detecting low-rate DDoS attacks using CAIDA datasets.

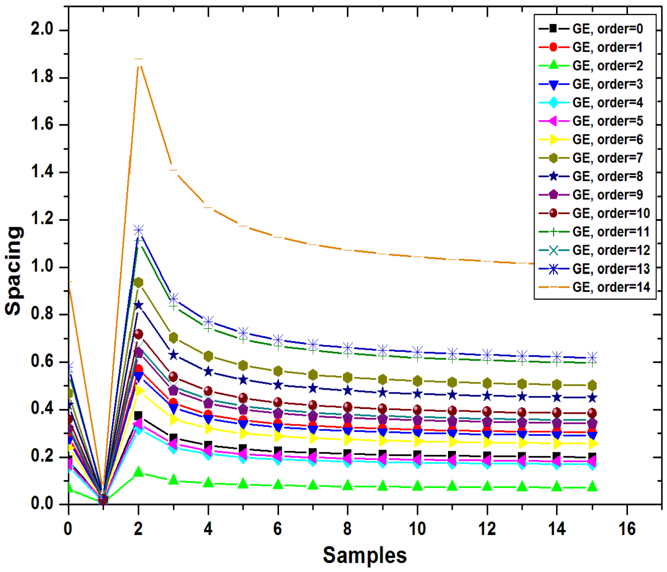

Fig. 4. Spacing between normal and low-rate DDoS traffic when using generalized entropy measure in the CAIDA dataset

B. Discussion

To detect low-rate DDoS attack traffic, it is important to use a minimum number of traffic features. Several detection mechanisms use either distribution of IP addresses or packet sizes. In this paper, we evaluate information metric measures to detect low-rate DDoS attacks in real-life DDoS dataset. The following are some observations.

- Information entropy provides better result when increasing the order of generalized entropy in detecting low-rate DDoS attacks.
- Information metric produces better result in terms of complexity because it uses a minimum number of parameters during detection.
- For generalized entropy, the value of α can be adjusted easily for better spacing between normal and attack traffic.

V. Conclusion

This work presents an empirical evaluation of information metrics when detecting low-rate DDoS attacks. We include several information entropy measures: Hartley entropy, Shannon entropy, Renyi's entropy and Renyi's generalized entropy. The use of information metric magnifies the spacing between legitimate and malicious traffic for low-rate DDoS attack detection in real world network traffic. Moreover, these measures take minimum time to find the spacing between the malicious and legitimate traffic.

ACKNOWLEDGMENT

This work is supported by Council of Scientific and Industrial Research (CSIR) and Department of Information Technology, Government of India.

REFERENCES

[1] W. Wei, F. Chen, Y. Xia, and G. Jin, "A Rank Correlation Based Detection against Distributed Reflection DoS Attacks," IEEE Communications Letters, vol. 17, no. 1, pp. 173–175, 2013.

[2] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions," The Computer Journal, vol. 57, no. 4, pp. 537–556, 2014.

[3] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDoS Attacks Using Entropy Variations," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 3, pp. 412–425, March 2011.

[4] Y. Xiang, K. Li, and W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 426–437, 2011.

[5] Z. Sheng, Z. Qifei, P. Xuezeng, and Z. Xuhui, "Detection of Low-rate DDoS Attack Based on Self-Similarity," in 2nd International Workshop on Education Technology and Computer Science (ETCS), vol. 1, March 2010, pp. 333–336.

[6] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, "Flow Level Detection and Filtering of Low-rate DDoS," Comput. Netw., vol. 56, no. 15, pp. 3417–3431, October 2012.

[7] Y. Tao and S. Yu, "DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics," in 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013, pp. 233–240.

[8] J. Francois, I. Aib, and R. Boutaba, "FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," IEEE/ACM Transactions on Networking, vol. 20, no. 6, pp. 1828–1841, 2012.

[9] A. R´enyi, "On Measures of Entropy And Information," in Proc. of the 4th Berkeley Symposium on Mathematics, Statistics and Probability, 1960, pp. 547–561.

[10] C. E. Shannon, "A Mathematical Theory of Communication," Bell system technical journal, vol. 27, pp. 397–423, 1948.

[11] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "AOCD: An Adaptive Outlier Based Coordinated Scan Detection Approach," International Journal of Network Security, vol. 14, no. 6, pp. 339–351, 2012.

[12] ——, "Network Anomaly Detection: Methods, Systems and Tools," IEEE Communications Surveys Tutorials, vol. 16, no. 1, pp. 303–336, 2014.

[13] MIT Lincoln Laboratory Datasets, "MIT LLS DDOS 0.2.2," http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/2000data.html, 2000, Massachusetts Institute of Technology, Cambridge,MA.

[14] CAIDA, "The Cooperative Analysis for Internet Data Analysis," http://www.caida.org, 2011.

[15] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-service Activity," ACM Trans. Computer System, vol. 24, no. 2, pp. 115–139, May 2006.