Turkish Journal of Electrical Engineering and Computer Sciences

Volume 26 | Number 4 Article 7

1-1-2018

A generalized detection system to detect distributed denial of service attacks and flash events for information theory metrics

SUNNY BEHAL

KRISHAN KUMAR

MONIKA SACHDEVA

Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2018) 26: 1759 – 1770

doi:10.3906/elk-1706-340

A generalized detection system to detect distributed denial of service attacks and flash events for information theory metrics

Sunny BEHAL*, Krishan KUMAR, Monika SACHDEVA
Department of Computer Science and Engineering, Inder Kumar Gujral Punjab Technical University, Punjab, India

Received: 28.06.2017 • **Accepted/Published Online:** 03.04.2018 • **Final Version:** 27.07.2018

Abstract: Distributed denial of service (DDoS) attacks pose a severe threat to extensively used web-based services and applications. Many detection approaches have been proposed in the literature, but ensuring the security and availability of data, resources, and services to end users remains an ongoing research challenge. Nowadays, the traffic volume of legitimate users has also increased manifold. A flash event (FE) is a high-rate legitimate traffic situation wherein millions of legitimate users start accessing a particular network resource, such as a web server, simultaneously. The detection of DDoS attacks becomes more challenging when DDoS attacks are launched during behaviorally similar FEs. This research paper proposes a generalized detection system for metrics, based on information theory, capable of detecting different types of DDoS attacks and FEs. We used publically available MIT Lincoln, CAIDA, and FIFA datasets along with a synthetically generated DDoSTB dataset to validate the proposed detection algorithm in terms of various detection system evaluation metrics such as false positive rate, false negative rate, classification rate, and detection accuracy. Such a generalized detection system would be useful to researchers for validating and comparing various information theory metrics based solutions.

Key words: DDoS attacks, network security, information theory, flash event, entropy, divergence

1. Introduction

Distributed denial of service (DDoS) attacks are not a new problem for network security professionals. They have existed for many years now. Legitimate users are deprived of using web-based services and applications due to such attacks. Even a few minutes of service downtime can lead to not only loss in revenue, but also intangibles such as loss of customer faith, unfavorable media coverage, and legal actions. Usually, prominent websites are the prime victims of such attacks. Recently, DDoS attacks caused interruptions in the services of Twitter, Spotify, and Amazon for almost two hours. Such interruptions in the services lead to huge financial losses. According to a recent report (https://www.ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack/), revenue losses due to DDoS attacks reached $209 million in the first quarter of 2017, compared to $24 million for all of 2015. Based on the network traffic rate, DDoS attacks can be categorized into (a) high-rate DDoS (HR-DDoS) attacks, when the traffic rate is very different from legitimate traffic, and (b) low-rate DDoS (LR-DDoS) attacks, when the traffic rate is similar or less than legitimate traffic. However, it is comparatively easy to detect HR-DDoS attacks, as their traffic profile significantly deviates from the legitimate traffic profile.

A flash event (FE), wherein millions of legitimate users try to access a particular computing resource

*Correspondence: sunnybehal.sbs@gmail.com

such as a website simultaneously, is similar to an HR-DDoS attack [1]. This sudden surge in legitimate traffic is primarily due to some newsflash happening around the world, like the publishing of an Olympic schedule, earthquake occurrence, and election results. It causes untimely delivery of responses from a web service, and thus requires immediate action.

Both DDoS attacks and FEs cause a significant deviation in the packet header features of the network traffic. Information theory metrics such as entropy or divergence can quickly capture such variations in network traffic behavior. There are many key advantages of using solutions based on information metrics rather than other methods: (1) they require fewer packet header features to detect and characterize different types of network traffic flows, (2) they usually have small time, space, and computational complexity, and (3) they have fewer storage requirements [2,3]. The existing research has proposed several quarantine solutions to detect different types of DDoS attacks using diversified information theory metrics, but a generalized detection system to compare and contrast the effectiveness of this plethora of detection metrics is missing in the literature. The major contributions of this paper are as follows:

- This paper proposes a generalized detection system for information-theory–based metrics that are capable of detecting different types of LR-DDoS and HR-DDoS attacks along with FEs.
- The effectiveness of the proposed generalized detection system has been measured in terms of receiver operating characteristics (ROC) curves and various detection system evaluation metrics such as false positive rate (FPR), false negative rate (FNR), classification rate, and detection accuracy (also called true positive rate, TPR).
- The proposed generalized detection system has been used to compare the effectiveness of various information-theory–based detection metrics. The proposed detection system has been validated using a set of publically available real datasets and synthetically generated DDoSTB dataset.

The rest of the paper is organized as follows. Section 2 summarizes the related work, Section 3 describes the background of information theory metrics, Section 4 focuses on proposed detection algorithm, Section 5 discusses the results and performance evaluation, Section 6 compares the results with existing similar works, and, finally, the concluding remarks are given in Section 7 along with scope for future work.

2. Related work

Many efficient solutions have been proposed in the literature to combat DDoS attacks using Shannon entropy, generalized entropy, and information-divergence–based metrics for detecting different types of DDoS attacks [2–6]. For example, Xiang et al. [2] used Renyi's generalized entropy (GE) and generalized information distance (GID) metrics to differentiate an LR-DDoS attack from legitimate traffic. They compute the information distance (ID) between legitimate traffic and LR-DDoS attack traffic based on packet header features such as source IP, destination IP, and type of protocol. However, they did not consider detecting and discriminating between HR-DDoS attacks and FEs, which occur frequently nowadays. Their proposed algorithm detects LR-DDoS with a reduced FPR as compared to the existing Shannon entropy and Kullbeck–Leibler (KL) divergence metrics. They validate their proposed approach using real datasets of the MIT Lincoln laboratory dataset (https://www.ll.mit.edu/ideval/data/2000data.html) and CAIDA DDoS Attack Dataset (https://www.caida.org/data/passive/ddos-20070804_dataset.xml).

This paper has extended their work to detect HR-DDoS attacks and FE traffic as well. Additionally, the effectiveness of proposed detection algorithm is validated using detection system evaluation parameters of TPR, FPR, FNR, and classification rate. Further, Bhuyan et al. [3] used the idea of ID between different sample flows as originally proposed by [2]. They compute extended entropy metric (EEM) on source IP and incoming packet rate packet header features to detect HR-DDoS attacks. They validate their approach against real datasets of MIT Lincoln and CAIDA. However, their proposed approach did not consider discriminating FEs from HR-DDoS attacks, as both types of traffic share many similar behavioral characteristics. Additionally, in this paper, the results of Renyi's GE metric have been compared with Shannon and Tsallis entropies, and the results of Renyi's generalized divergence metric have been compared with (KL) divergence, Hellinger distance, total variation distance, and Jenson–Shannon divergence metrics along with detection of FE traffic. Jun et al. [4] used traffic volume and entropies of destination IP, source port, and the number of packets received per time window to detect HR-DDoS attacks. Ma et al. [5] calculated the entropy of source and destination IPs with the Lyapunov exponent to detect HR-DDoS attacks. Nychis et al. [6] used packet header features of source and destination IPs, ports, flow sizes, and the number of distinct destination/source IPs pairs to detect DDoS attacks. They observed that there is a strong correlation between the entropies of source and destination IP addresses and the distributions of port numbers. Some authors have also used a generalized nonextensive Tsallis entropy for network anomaly detection [7,8]. Basicevic et al. [7] used Tsallis entropy to detect HR-DDoS attacks. They compared the results of a Tsallis-entropy–based detection scheme with a Shannon-entropy–based detection scheme in simulation-based experiments. They observed that the Tsallis-entropy–based detector outperformed Shannon-entropy–based detector and produced a low FPR. Tellbach et al. [8] used Tsallis entropy to find the correlation between source/destination IP addresses and port numbers. They observed a strong correlation between source/destination port numbers in the legitimate traffic, but no strong correlation between source/destination IP addresses and ports in the attack traffic. They used many real traffic traces and net flow data to validate their detection approach.

The research of DDoS attack detection cannot be complete until we discriminate them from similar-looking FEs. The problem of discrimination becomes even more crucial when DDoS attacks are launched during FEs [9]. Many researchers have proposed solutions to discriminate HR-DDoS attacks from FEs using information theory. Yu et al. [10,11] compute change in entropy rate to discriminate an HR-DDoS attack from a similar-looking FE. Their proposed method assumes a uniform packet size in attack traffic and calculates a similarity index between FEs and HR-DDoS attacks. Bhatia et al. [12] compute the correlation of source IP entropy, change in the rate of new IPs, and distribution of source IPs of incoming traffic to detect different types of HR-DDoS attacks and FEs. They validate their proposed approach using real datasets from MIT Lincoln and CAIDA. Bhandari et al. [1] used coefficients of variation to distinguish HR-DDoS attacks from FEs. They concluded that coefficients of variation among attack profiles are quite similar, but are different between FEs and legitimate traffic. They used the FIFA World Cup dataset (http://ita.ee.lbl.gov/html/contrib/WorldCup.html) dataset for representing FE traffic and the CAIDA dataset to represent DDoS attacks. Sachdeva et al. [13] used cluster entropy in combination with source IP entropy to discriminate DDoS attacks from FEs. They observed that the traffic cluster entropy drops dramatically during FEs because most of the traffic is generated from already-visited source networks, whereas the traffic cluster entropy increases in HR-DDoS attacks.

The existing research has extensively used real datasets from MIT Lincoln, CAIDA, and FIFA for the validation of their proposed solutions. Though these datasets are obsolete in the context of today's high-

rate traffic, no other benchmark datasets are available for the validation of DDoS-related research [14] to date. The lack of appropriate recent datasets has shifted the focus of the research community towards real-time experimental setups to enable the validation of DDoS research against real traffic on a large scale. Further, there are few detection methods that have collectively focused on detecting LR-DDoS attacks, HR-DDoS attacks, and FEs; rather, the existing research has used separate datasets to represent normal and attack traffic scenarios. Thus, there is a need to develop a collective detection mechanism that can detect different types of DDoS attacks and FEs and that should be validated using a single state-of-the-art dataset.

3. Background of information theory metrics

There are a vast number of applications of information theory in the field of mathematics, statistics, computer science, physics, neurobiology, and electrical engineering. Recently, information-theory–based metrics have been used progressively in the network anomaly detection domain of computer science research. In information theory, information entropy is a measure of the uncertainty associated with a random variable, forming the basis for distance and divergence measurements between probability densities. Alfred Renyi defined a GE of order α as follows [15]:

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

for $\alpha >= 0$ and $\alpha \neq 1$. GE highlights the different contributions of the tail and the main proportion of a probability distribution. GE measures these contributions by using a generalized α parameter called an entropic index. For $\alpha >= 0$, GE is more sensitive to frequent events, whereas for $\alpha < 0$, GE is more sensitive to less frequent events. Hence, different types of entropies can be derived based on different values of entropic index. For example, when $\alpha = 0$, the maximum value of information entropy is reached also known as Hartley entropy, i.e. $H_0(x) = \log n$. When $\alpha \to 1$, the Shannon entropy is derived as follows:

$$H_1(x) = -\sum_{i=1}^{n} p_i \log_2 p_i \tag{2}$$

When $\alpha \to \omega$, minimum information entropy $H_{\omega}(x)$ is reached. There also exists a nonextensive generalized entropy known as a Tsallis entropy [16] that has been used extensively in network anomaly detection in recent times and is defined as

$$H_{\alpha}^{'}(x) = \frac{1}{\alpha - 1}\left(1 - \sum_{i=1}^{n} p_i^{\alpha}\right) \tag{3}$$

When $\alpha \to 1$, Shannon entropy is derived. This is also a generalized form of entropy similar to GE that also focuses on different regions of a distribution with increasing value of α order.

For any two discrete probability distributions $P = (p_1, p_2, ..., p_n)$ and $Q = (q_1, q_2, ..., q_n)$ with $\sum_{i=1}^{n} p_i = \sum_{i=1}^{n} q_i$, $i = 1, 2..., n$, GID is defined as

$$D_{\alpha}(P||Q) = \frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{n} p_i^{\alpha} q_i^{1-\alpha}\right), \alpha \geq 0. \tag{4}$$

When $\alpha \to 1$, the KL divergence metric is derived.

4. Proposed methodology

We proposed a generalized detection algorithm as shown in Algorithm 1. The proposed detection algorithm works on the assumption that there is a flow similarity in the case of attack traffic, whereas legitimate network traffic is highly variable because of its dynamic nature, which causes a significant deviation in the packet header features of attack traffic from legitimate traffic. We sample the network traffic in each time window T_w and extract the relevant packet header features. Then we compute a number of information-theory–based metrics from the probability distributions of sampled network traffic. We compute the thresholds σ_1 and σ_2 from the normal baseline behavior of the network. We count the number of packets per T_w to set σ_1, and compute the ID between normal flows to set σ_2. Initially, we separate the low-rate and high-rate network flows based on n_1 in each T_w. Then we calculate the ID between different metric values of legitimate and attack traffic. If ID is more than σ_2, it is declared attack traffic; otherwise it is declared legitimate traffic.

Algorithm 1 A Proposed Generalized Detection Algorithm

1: Set f as sampling frequency, T as sampling period, T_w as time window size, σ_1, σ_2 as standard thresholds, Entropic_index = set of optimal values of α.
2: While $T_w <= T$, analyze the network traffic packets coming from upstream routers.
3: Extract the packet header features:
$F \leftarrow \{$srcIP; dstIP; proto; number of pkts $(n_1)\}$ in each T_w and classify into unique network flows.
4: Compute the probability distributions of these network flows based on srcIP in a T_w.
5: Compute $E\prime$ metric from these computed probability distributions for each Entropic_index, where $E\prime = \{$GE, Shannon entropy, Tsallis entropy, KL, GID, Hellinger, Jensen–Shannon$\}$.
6: Calculate the ID between respective $E\prime$ metric values of current network flow and normal traffic flow in each T_w, i.e. ID $= |E\prime_C - E\prime_N|$.
7: If $n_1 > \sigma_1$ then
8: Traffic may be HR-DDoS or FE.
9: If ID $> \sigma_2$ then
10: Declare the traffic HR-DDoS.
11: Else
12: Declare the traffic FE.
13: End if
14: Else
15: Traffic may be LR-DDoS or legitimate.
16: If ID $> \sigma_2$ then
17: Declare the traffic as LR-DDoS.
18: Else
19: Declare the traffic legitimate.
20: End if
21: End if
22: Increment T_w and goto Step 2.

We compute the set of $E\prime$ metrics on α-order from 1 to 15. The threshold σ_1 is the standard deviation in traffic rate and σ_2 is the standard deviation in the ID values between legitimate traffic flows computed by analyzing the baseline behavior of the network without attack. We used the calibration of FPR and FNR curves for selecting the optimal value of tolerance factor (as described in detail in next section), which are then used to compute the optimal threshold values. The value of entropic index parameter α can be adjusted according to the dynamic network behavior as per requirements to improve the detection rate using reduced FPR as described by Xiang et al. [2] or by computing the coefficients of correlation as done by Berezinski et

al. [17]. ID is defined as the difference in the detection metric values of attack and normal traffic flows. For GE metric, ID is computed as $|E\prime_C - E\prime_N|$. ID can also be computed for divergence-based metrics in a similar pattern. However, for computing divergence-based metrics, the number of source IPs in both the probability distributions need to be normalized within a T_w. The greater the ID between two network traffic flows, the higher the detection efficiency.

We have used the same packet header features for computing the detection metrics as used by [2,3]. We choose $T_w = 10$ s with a sampling period of 300 s. We have chosen a time window size where we get the minimum value of standard deviation of GE or GID metric while computing the both metrics on normal traffic, i.e. without attack.

5. Performance evaluation

We replayed the traffic traces of the MIT Lincoln, CAIDA, and FIFA datasets in an emulation-based DDoSTB testbed. Both LR-DDoS and HR-DDoS attack scenarios were taken from the CAIDA dataset, the FE traffic profile was taken from day 66 of the FIFA World Cup dataset, and a normal traffic profile was taken from the MIT Lincoln dataset. The DDoSTB testbed was composed of a hybrid of real systems and emulated systems, as shown in Figure 1. We deployed 75 physical nodes organized in three clusters, with 25 computers running Ubuntu and Windows OS instances per cluster, 3 physical routers, 3 L2 switches, 2 L3 switches, and a two-processor 8 core Linux server that acts as victim web server. We used the CORE (http://www.nrl.navy.mil/itd/ncs/products/core) emulator to increase the number of nodes. The idea is to mix normal, LR-DDoS, and HR-DDoS attack traffic profiles into a single state-of-art DDoSTB dataset. This dataset is then used to validate the proposed detection algorithm. More information about performing real experiments using DDoSTB testbed can be found in [18].

The ID values between different types of network traffic flows for CAIDA and DDoSTB datasets calculated using various entropy metrics, such as Renyi's GE, Shannon entropy, and Tsallis entropy, are shown in Tables 1 and 2, respectively, and are plotted in Figures 2 and 3, respectively. Here, ID_1, ID_2, and ID_3 represent the ID values in legitimate versus LR-DDoS attack traffic, legitimate versus HR-DDoS attack traffic, and HR-DDoS attack traffic versus FE traffic, respectively. The ID in legitimate traffic versus LR-DDoS attack traffic remains lower than the ID in HR-DDoS attack traffic versus legitimate traffic. This is due to the similarity between traffic rates of LR-DDoS attack traffic and legitimate traffic. The ID values between Shannon and Renyi's GE metric increases with increase in α-order for LR-DDoS attacks and FEs. However, no such pattern was found while computing ID values using Tsallis entropy. The ID values of legitimate versus LR-DDoS attack using Renyi's GE metric remained in the range from 0.42 to 0.56 in the CAIDA dataset and from 0.11 to 0.39 in the DDoSTB dataset. For legitimate versus HR-DDoS attack traffic, the ID values remained in the range from 2.66 to 9.03 in CAIDA dataset and from 8.39 to 11.81 in DDoSTB dataset. The ID values between HR-DDoS attack versus FE traffic remained in the range from 0.52 to 2.57 in the CAIDA dataset and from 1.97 to 4.38 in the DDoSTB dataset. The results clearly show that Renyi's GE metric is able to magnify the ID between legitimate versus attack traffic and HR-DDoS attacks versus FEs, as compared to Shannon and Tsallis entropy metrics.

The variation of ID values using information divergence metrics such as Renyi's GID and KL metrics between different types of network traffic for CAIDA and DDoSTB datasets are shown in Figures 4 and 5. The ID in legitimate traffic versus LR-DDoS attack traffic using Renyi's GID metric remained in the range of 0.89 to 13.80 in the CAIDA dataset and from 0.1 to 0.49 in the DDoSTB dataset. For legitimate traffic versus HR-DDoS attack traffic, it remained in the range from 0.41 to 2.82 in the CAIDA dataset and from

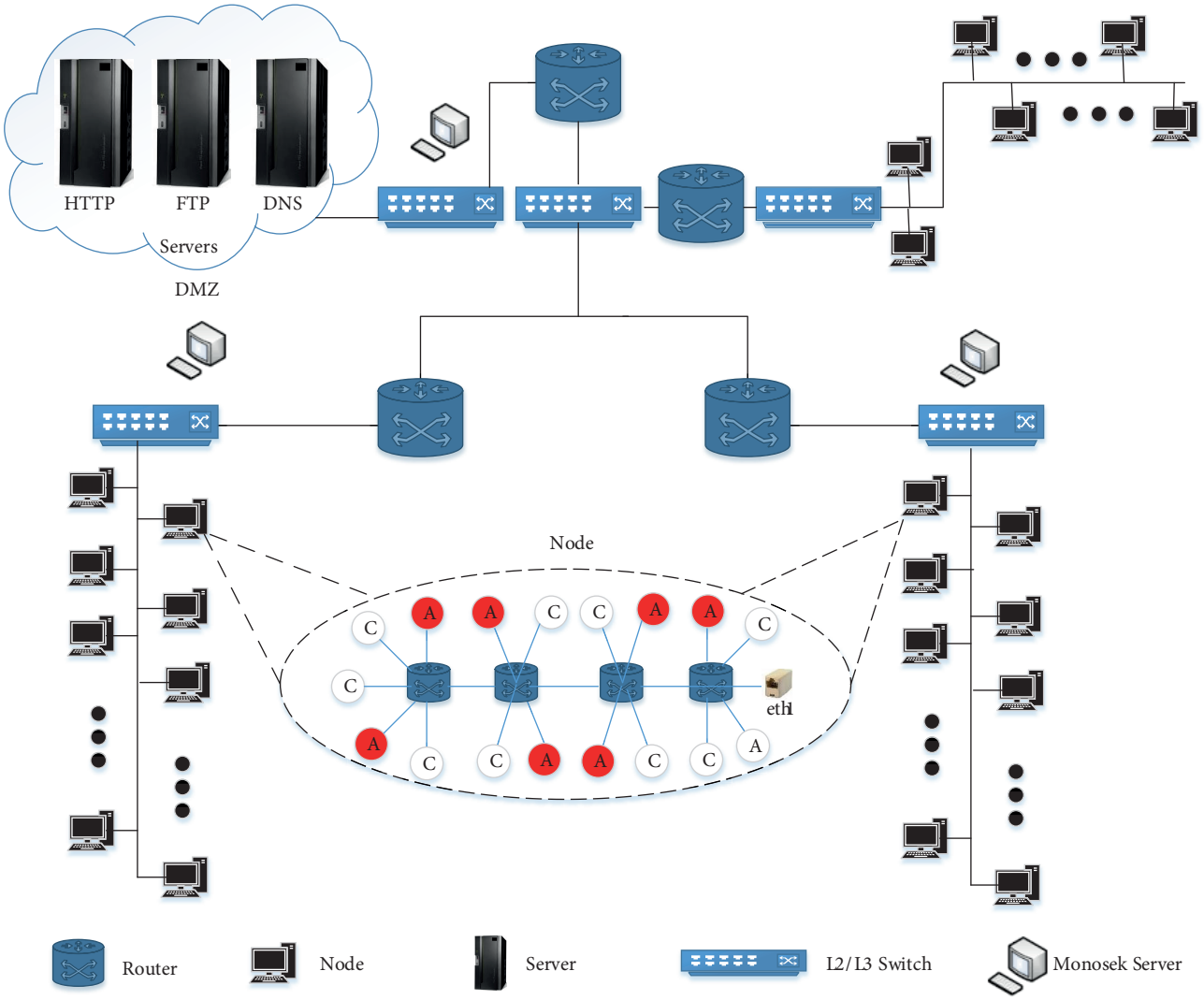

Figure 1. Distributed denial of service testbed.

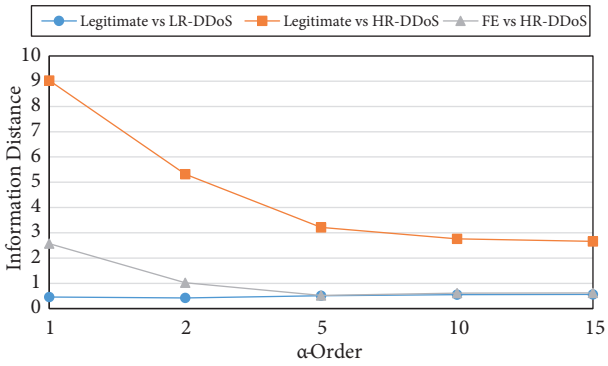

Figure 2. Temporal variation in ID values of Renyi's GE metric in the CAIDA dataset.

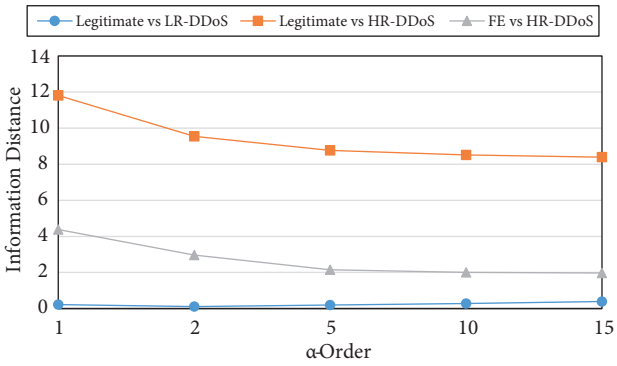

Figure 3. Temporal variation in ID values of Renyi's GE metric in the DDoSTB dataset.

Table 1. Comparison of entropy metrics in detecting DDoS attacks and FEs in the CAIDA dataset.

Entropy		Legitimate	LR-DDoS	ID_1	HR-DDoS	ID_2	FE	ID_3
Shannon	$\alpha = 1$	2.65	3.11	0.46	11.68	9.03	9.11	2.57
Renyi's GE	$\alpha = 2$	1.61	2.03	0.42	6.93	5.32	5.91	1.02
	$\alpha = 5$	1.41	1.92	0.51	4.62	3.21	5.14	0.52
	$\alpha = 10$	1.31	1.86	0.55	4.07	2.76	4.68	0.61
	$\alpha = 15$	1.29	1.85	0.56	3.95	2.66	4.57	0.62
Tsallis	$\alpha = 2$	0.79	0.84	0.06	0.96	0.17	1.00	0.04
	$\alpha = 5$	0.25	0.25	0.0	0.25	0.0	0.25	0.0
	$\alpha = 10$	0.11	0.11	0.0	0.11	0.0	0.11	0.0
	$\alpha = 15$	0.07	0.07	0.0	0.09	0.0	0.09	0.0

Table 2. Comparison of entropy metrics in detecting DDoS attacks and FEs in the DDoSTB dataset.

Entropy		ID_1	ID_2	ID_3
Shannon	$\alpha = 1$	0.22	11.81	4.38
Renyi's GE	$\alpha = 2$	0.11	9.54	2.97
	$\alpha = 5$	0.19	8.76	2.15
	$\alpha = 10$	0.28	8.51	2.01
	$\alpha = 15$	0.39	8.39	1.97

4.91 to 5.93 in the DDoSTB dataset. The ID values in HR-DDoS attack versus FE traffic remained in the range from 0.54 to 3.79 in the CAIDA dataset and from 4.5 to 6.91 in the DDoSTB dataset. The entropy values are high in the case of FE traffic, similar to the situation of a HR-DDoS attack. However, in the case of divergence-based metrics, as the probability distributions of FE traffic are similar to those of legitimate traffic, it results in less divergence values in FE versus legitimate traffic. Further, as given in Table 3, Renyi's GID metric elicits a greater ID between different types of network flows than other statistical distance measures like KL divergence, Hellinger distance [19], and Jensen–Shannon distance [20] in CAIDA and DDoSTB datasets according to different entropic index parameters.

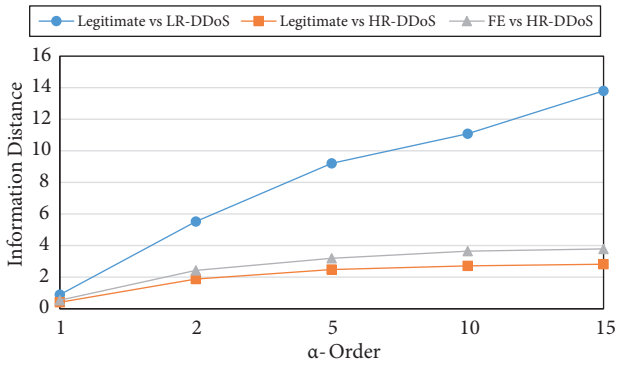

Figure 4. Temporal variation in ID values of Renyi's GID metric in the CAIDA dataset.

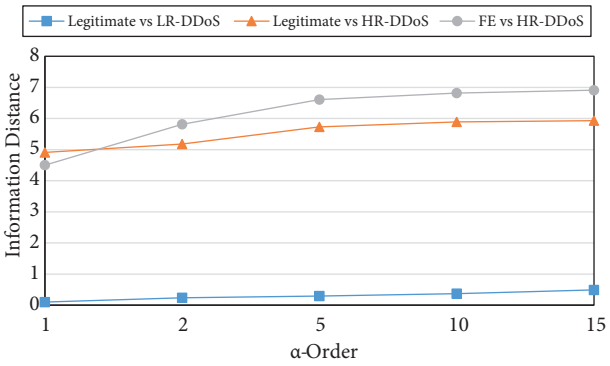

Figure 5. Temporal variation in ID values of Renyi's GID metric in the DDoSTB dataset.

Further, to validate the effectiveness of the proposed detection algorithm, we have used various detection

Table 3. Comparison of divergence metrics in detection DDoS attacks and FEs in the CAIDA and DDoSTB datasets.

Divergence Measure	CAIDA dataset			DDoSTB dataset		
	ID_1	ID_2	ID_3	ID_1	ID_2	ID_3
KL	0.89	0.41	0.54	0.1	4.91	4.5
Hellinger	0.36	0.71	0.26	0.13	2.34	1.71
Jensen–Shannon	0.09	0.32	0.25	0.01	1.74	1.34
GID at $\alpha = 2$	5.53	1.88	2.43	0.24	5.18	5.81
GID at $\alpha = 5$	9.21	2.48	3.20	0.29	5.73	6.61
GID at $\alpha = 10$	11.09	2.72	3.65	0.37	5.89	6.82
GID at $\alpha = 15$	13.80	2.82	3.79	0.49	5.93	6.91

system evaluation metrics as defined in [21], such as TPR, FPR, FNR, and classification rate, along with ROC curves. TPR measures the fraction of attack events that have been detected correctly, whereas classification rate is the ratio of truly classified events to the total occurred events. FPR measures the effectiveness of the detection system, whereas FNR measures the detection system reliability. The variation in tolerance factor k has been used to quantify FPR and FNR, which assist in making decisions on the optimal value of information distance thresholds. The point where both the curves intersect can be used to select the optimal threshold values. Figures 6a and 6b depict the ideal value of tolerance factor for Renyis' GE and GID metrics, respectively, on different α order. For $\alpha = 5$, the FPR and FNR curves intersect at tolerance factor = 1 in the case of Renyi's GE metric, whereas they intersect at tolerance factor = 5 in the case of Renyi's GID metric. The trade-off between FPR and detection rate in terms of ROC curves for Renyi's GE and Renyi's GID metrics is shown in Figures 6c and 6d, respectively. The ROC curve clearly depicts that, with an increase in FPR, TPR also increases, i.e. if we compromise on FPR, a better TPR can be achieved and vice versa. The classification rate of these metrics is shown in Figures 6e and 6f. At $\alpha = 5$, the proposed detection system produces a TPR of 80%, FPR = 0.01, and classification rate of 93% using GE metric at tolerance factor = 1, whereas it achieves a TPR of 95%, FPR = 0.01, and classification rate of 94.6% at tolerance factor = 5. The TPR and classification rate of information-theory–based generalized metrics increased with α order. The divergence-based metrics also produced better results than corresponding entropy metrics. It may be because divergence-based metrics consider the divergence between individual values of a probability distribution, whereas entropy summarizes the skewness or dispersion of a probability distribution into a single value and hence neglects changes within a time window.

6. Comparison with existing work

The results of our proposed generalized detection system are compared with existing prominent work in this domain. Xiang et al. [2] also used information-theory–based Renyi's GE and GID metrics to detect LR-DDoS attacks with low FPR, whereas our proposed detection system can detect different types of DDoS attack scenarios along with the detection of FEs traffic. Further, Bhuyan et al. [3] extended the idea of [2] to formulate EEM to compute the difference between legitimate and HR-DDoS attacks. They proposed a lightweight detection system that is capable of detecting HR-DDoS attacks, but they did not consider detecting FEs and LR-DDoS attacks. Our proposed detection algorithm can detect FEs and HR-DDoS attacks with 100% TPR, more than in the proposed scheme (99%). Ma et al. [5] used Lyapunov exponents between legitimate and attack traffic

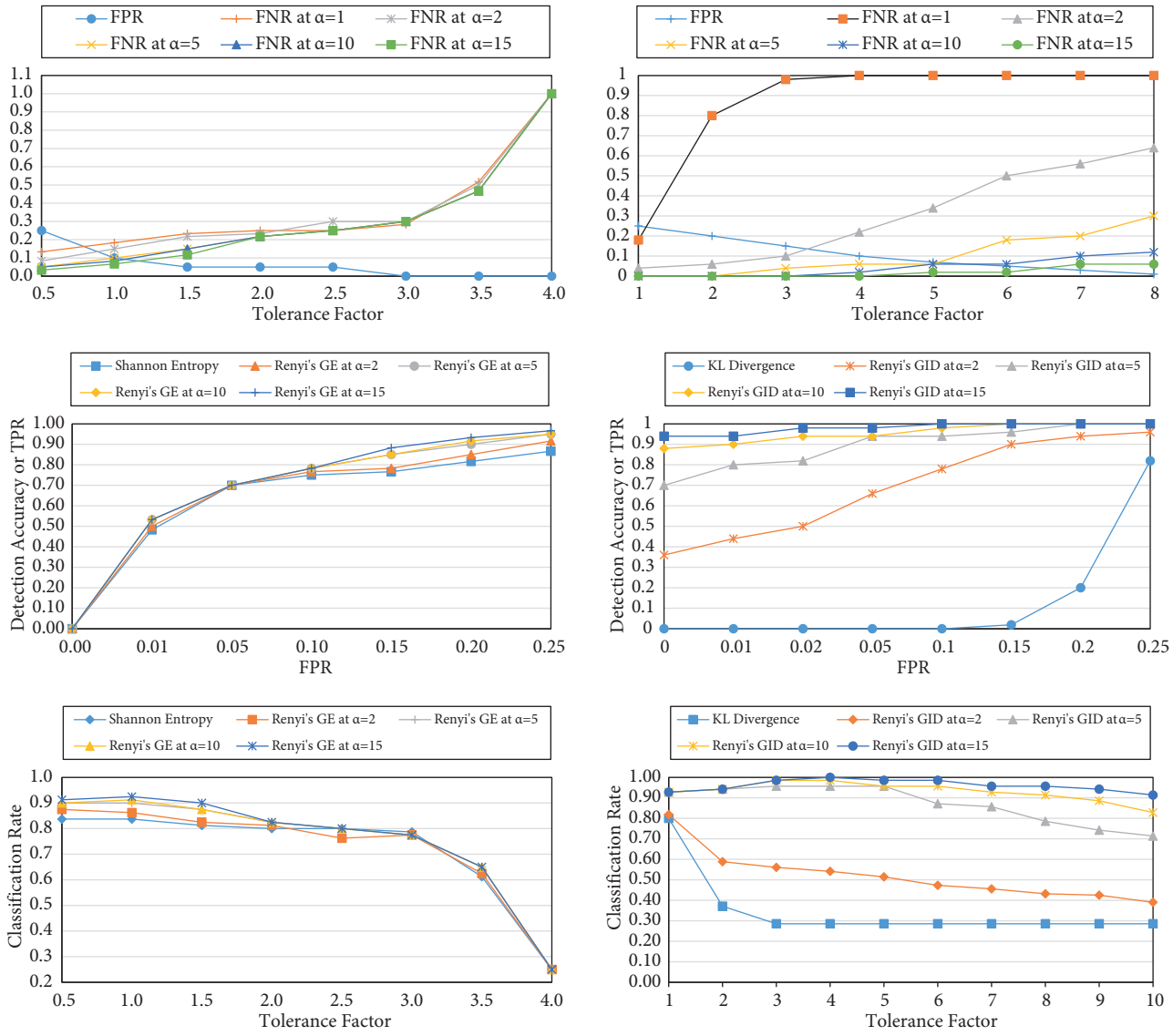

Figure 6. a. Tradeoffs between FNR and FPR of Renyi's GE metric. b. Tradeoffs between FNR and FPR of Renyi's GID metric. c. ROC curve of Renyi's GE metric. d. ROC curve of Renyi's GID metric. e. Classification rate of Renyi's GE metric. f. Classification rate of Renyi's GID metric.

to compute the ID between the two. Our proposed generalized detection system achieves higher TPR (100%) in detecting HR-DDoS attacks than in the proposed scheme (98.56%). Yu et al. [10,11] used Shannon entropy to detect HR-DDoS attacks and FEs based on packet size and ID, but their proposed system did not consider the detection of different types of DDoS attacks. Sachdeva et al. [13] computed Shannon's entropy metric to detect FEs and HR-DDoS attack traffic. However, we obtained a better TPR (95%) in case of GID metric than in their proposed scheme (82%). Further, Behal et al. [22] proposed using novel, highly convergent generalized φ-entropy and φ-divergence metrics for detecting DDoS attacks and FEs, but these metrics are computationally expensive. These metrics produced high TPR, but with high FPR values.

7. Conclusion and future scope

DDoS attacks pose a critical threat to web-based services and applications. It is crucial to detect such attacks in time to ensure timely delivery of these web services and applications to potential users. This paper has proposed a generalized detection system for the collective detection of LR-DDoS and HR-DDoS attacks along with FEs for analyzing the behavior and performance of various information theory metrics. Divergence-based metrics produced greater ID than entropy-based metrics, which led to the higher TPR and classification rate of these metrics. ID-based detection systems also outperformed entropy-based detection systems. As part of future work, the authors shall (1) propose a state-of-art DDoS defense framework that would be able to mitigate the impact of ongoing DDoS attacks and FEs with minimum collateral damage and (2) impart more efforts to generate near to real synthetic datasets.

Acknowledgment

This research work has been supported by All India Council for Technical Education (AICTE), New Delhi, India, under a grant from the Research Promotion Scheme (RPS), Grant no. 8023/RID/RPS-93/2011-12.

References

[1] Bhandari A, Sangal AL, Kumar K. Characterizing flash events and distributed denial-of-service attacks: an empirical investigation. J Sec Comm Net 2016; 9: 2222-2239.

[2] Xiang Y, Li K, Zhou W. Low-rate DDoS attacks detection and traceback by using new information metrics. J Info Fore Sec 2011; 6: 426-437.

[3] Bhuyan MH, Bhattacharyya DK, Kalita JK. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. J Pat Rec Letters 2015; 51:1-7.

[4] Jun JH, Lee D, Ahn CW, Kim SH. DDoS attack detection using flow entropy and packet sampling on huge networks. In: ICN Networks Conference; 2014. pp. 185-190.

[5] Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy. J Comm Let 2014; 18: 114-117.

[6] Nychis G, Sekar V, Andersen DG, Kim H, Zhang H. An empirical evaluation of entropy-based traffic anomaly detection. In: SIGCOMM Internet measurement conference; 20–22 October 2008; New York, NY, USA: ACM. pp. 151-156.

[7] Basicevic I, Ocovaj S, Popovic M. Use of Tsallis entropy in detection of SYN flood DoS attacks. J Sec Comm Net 2015; 8: 3634-3640.

[8] Tellenbach B, Burkhart M, Schatzmann D, Gugelmann D, Sornette D. Accurate network anomaly classification with generalized entropy metrics. J Comp Net 2015; 55: 3485-3502.

[9] Sarvanan RD, Shanmuganathan S, Palanichamy Y. Behavior-based detection of application layer distributed denial of service attacks during flash events. Turk J Elec Eng & Comp Sci 2016; 24: 510-523.

[10] Yu S, Thapngam T, Liu J, Wei S, Zhou W. Discriminating DDoS flows from flash crowds using information distance. In: Network and System Security Conference; 19–21 October 2009; Gold Coast, QLD, Australia: IEEE. pp. 351-356.

[11] Yu S, Zhou W, Doss R. Information theory based detection against network behavior mimicking DDoS attacks. J Comm Let 2008; 12: 318-321.

[12] Bhatia S, Schmidt D, Mohay G. Ensemble-based DDoS detection and mitigation model. In: ACM Security of Information and Networks Conference; 25–27 October 2012; Jaipur, India: ACM. pp. 79-86.

[13] Sachdeva M, Kumar K, Singh G. A comprehensive approach to discriminate DDoS attacks from flash events. J Info Sec App 2016; 26: 8-22.

[14] Mirkovic J, Arikan E, Wei S, Fahmy S, Thomas R, Reiher P. Benchmarks for DDoS defense evaluation. In: MILCOM Military Communications Conference, 23–25 October 2006; Washington, DC, USA: IEEE. pp. 1-10.

[15] Renyi A. On the foundations of information theory. J Revue d'Inst Stat 1965; 1-14.

[16] Plastino A, Plastino A. Stellar polytropes and Tsallis' entropy. J Phy Let 1993; 174: 384-386.

[17] Berezinski P, Jasiul B, Szpyrka M. An entropy-based network anomaly detection method. J Ent 2015; 17: 2367-2408.

[18] Behal S, Kumar K. Measuring impact of DDoS attacks on web services - a realtime experimentation. IJ Comp Sci Info Security 2016; 14: 323-330.

[19] Cha S. Comprehensive survey on distance/similarity measures between probability density functions. IJ Math Mod Meth in App Sci 2007; 4: 300-307.

[20] Lin J. Divergence measures based on Shannon Entropy. J Trans Info Theo 1991; 37: 145-151.

[21] Ghorbani, Ali A. Network attacks. In: Ghorbani, Ali A, Lu W, Tavallaee M, editors. Network Intrusion Detection and Prevention - Concepts and Techniques. Berlin, Germany: Springer, 2010. pp. 1-25.

[22] Behal S, Kumar K. Detection of DDoS attacks and FEs using novel information theory metrics. J Comp Net 2017; 116: 96-110.