Journal of King Saud University – Computer and Information Sciences 33 (2021) 291–303

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

D-FAC: A novel ϕ-Divergence based distributed DDoS defense system

Sunny Behal [a,*], Krishan Kumar [b], Monika Sachdeva [c]

[a] I.K.G. Punjab Technical University, Kapurthala, Punjab, India
[b] Department of Information Technology, Panjab University, Punjab, India
[c] Department of CSE, I.K.G. Punjab Technical University, Kapurthala, Punjab, India

ARTICLE INFO

Article history:
Received 11 November 2017
Revised 3 February 2018
Accepted 4 March 2018
Available online 31 March 2018

Keywords:
DDoS attack
Network security
Entropy
Divergence
Flash event

ABSTRACT

A Distributed Denial of Service (DDoS) attack is an austere menace to extensively used Internet-based services and applications. Despite the presence of enormous DDoS defense solutions, the in-time detection of DDoS attacks poses a stiff challenge to network security professionals. The problem turns further crucial when such attacks are amalgamated with behaviorally similar flash events (FEs) wherein a large number of legitimate users starts accessing a particular service concurrently leading to the denial of service. This paper proposes an anomaly based distributed defense system called D-FAC that not only detect different type of DDoS attacks with efficacy but also efficiently mitigate their impact. D-FAC computes the information distance between legitimate and anomalous network traffic flows using information theory-based ϕ-Divergence metric to detect different types of DDoS attacks and efficiently discriminate them from FEs. D-FAC distribute the computational and storage complexity of computing ϕ-Divergence detection metric to the nearest point of presence (PoP) routers. D-FAC has been validated in an emulation based DDoSTB testbed using real DDoS attack tools and traffic generators. The results clearly show that D-FAC has outperformed existing Entropy and divergence based DDoS defense systems on various detection metrics like detection accuracy, classification rate, FPR, precision and F-measure.

1. Introduction

DDoS attack is not a new problem for network security professionals. It has been in existence for many years now. Thousands of organizations such as payment gateways, domain name servers, search engines (e.g. Google, Yahoo), banks, educational institutes, commercial servers (e.g. Flipkart, eBay, Amazon), social websites (e.g. Twitter, Facebook), stock trades, weather forecasting, medicine, defense, research, etc. have deployed web servers to provide Internet-based services and applications to the end users, and their usage rates have increased dramatically in recent times. The increasing usage of these interactive internet applications has also induced an exponential rise in the risks and possibilities of misuse of Internet (Arbor Network's WISR Report, 2017). A DDoS attack is such a prominent attack that poses a very critical threat to network security in general. Typically, a DDoS attack is launched in a coordinated manner by compromising millions of computer systems available freely on the Internet constituting an army of zombies called a Botnet (Wang et al., 2012). There are two categories of DDoS attacks (a) Network (Layer 3/4) DDoS attacks that targets network and transport layers. Such attacks occur when the amount of data packets and other traffic overloads a network or server and consumes all of its available resources, and (b) Application (Layer 7) DDoS attacks that exploits the breach or vulnerability in a web design of an application to overwhelm the server or database powering a web application with the aim to bring it down to its knees. Such attacks mimic legitimate user traffic, making them harder to detect (Latest DDoS attack trends Report, 2016a). Application layer DDoS attacks are more frequent nowadays wherein sophisticated attackers use Botnets to send redundant legitimate looking requests to fetch files or execute queries at the search engine databases deployed on the web servers (Singh et al., 2017a). The largest application layer attack in the year 2017 has been observed to be peaked at 173,633 RPS (requests per second).

Primarily, there are two types of DDoS attack detection methods in existence (a) signature-based detection methods which works on the basis of already stored attack signatures that match a known pattern with the pattern of incoming packets, and (b) anomaly-based detection methods which compare the pre-built network behavior model with the incoming network behavior in real-time. Anomaly-based detection has some inherent limitations. Firstly, sophisticated attackers can monitor the network traffic to train their detection systems. Secondly, the difficulty in setting

* Corresponding author.
E-mail address: sunnybehal.sbs@gmail.com (S. Behal).

https://doi.org/10.1016/j.jksuci.2018.03.005
1319-1578/

up an optimal threshold leads to an increase in false positive rate. Thirdly, it is very difficult to extract both qualitatively and precisely appropriate features of legitimate and anomalous network behavior. On the other hand, signature based detection methods require updated signatures for their efficient working. Based on the traffic rate, the DDoS attacks can be categorized into (a) high-rate DDoS (HR-DDoS) attacks, when the traffic rate is very different from the legitimate traffic, and (b) low-rate DDoS (LR-DDoS) attack, when traffic rate is similar or less than the legitimate traffic. As per Akamai Q4 DDoS 2016 report (Akamai's Q4 DoS attack report, 2016), high-rate DDoS attacks (HR-DDoS) are predominant nowadays, having traffic volume more than 900 Gbps. It is crucial to detect such attacks in time to ensure the timely delivery of the widely used Internet-based services and applications. HR-DDoS attacks are often amalgamated with several low-rate DDoS (LR-DDoS) attacks which follow the same distributed nature as that of HR-DDoS attacks but having low traffic rates (Wang et al., 2012).

Differentiating a DDoS attack from legitimate traffic pose an immense challenge to network security researchers since the attackers strike with more suave techniques to the victim every time. The prominent websites are the prime victims of such DDoS attacks. Recently Twitter, Spotify, and Amazon suffered interruptions in their services for almost two hours on Oct 21, 2016, because of DDoS attacks. Such interruptions in the services lead to huge financial losses. The revenue loss has amplified to $209 million in 2017 as compared to $24 million for all of 2015 (Recent DDoS Attacks Report, 2016). According to the recent Worldwide Infrastructure Security Report (WISR), the traffic volume of such attacks has amplified to around 1 Tbps in the year 2017. It is evident from this exponential increase in attack traffic that the attackers are continuously updating their skills, using advanced techniques to generate such huge amount of traffic and at the same time defeating the existing defense solutions. Some recent DDoS trend reports (Akamai's Q4 DoS attack report, 2016; Latest DDoS attack trends Report, 2016b) found that the frequency of DDoS attacks is up by 129 percent in the last quarter of 2017 compared with the same period last year. It means there is no indication to combat against such attacks effectively in near future too.

There is an another kind of network traffic called a flash event (FE) that also cause a denial of service. An FE is similar to a HR-DDoS attack wherein thousands of legitimate users try to access a particular computing resource such as a website simultaneously (Bhandari et al., 2016). It causes untimely delivery of responses from a web service similar to the case of a HR-DDoS attack and thus, requires immediate action. Both HR-DDoS attacks and FEs share many common behavioral characteristics like increase in the rate of traffic volume, delay in responses from the web server, etc. but still there are a few parametric differences between them. Further, the similarity of network flows, less throughput and duration of traffic per source IP are some rationales that differentiate an HR-DDoS attack from an FE (Behal et al., 2017a,b).

It is important to note that the successful DDoS defense schemes not only defined by the underlying detection algorithm but also depends on its placement (Gulisano et al., 2015). Actually DDoS attacks originates from different source networks. Every packet stream flows out of a system, through a server or router into the Internet, across one or more core routers called Autonomous Systems (AS), and finally to the target itself. A DDoS Defense solution can be deployed at some or all of these locations. Based on the deployment locations, defense solutions can be categorized into source-end, intermediate network, and victim-end (Kumar et al., 2007; Bhuyan et al., 2016). Each possible deployment location has its own strengths and weaknesses. The nodes near the victim can closely observe the complete attack traffic, model its behavior and detect anomalies efficiently whereas the mechanisms deployed elsewhere can see only a partial attack traffic and might need to take action based on incomplete attack information. However, during a typical HR-DDoS attack or an FE, various network and server resources like bandwidth, CPU cycles, memory, etc. often gets overloaded. In such cases, it may not be possible for the victim-end defense deployment to detect and characterize the legitimate and attack traffic efficiently. Due to lack of sufficient computational resources, it may start dropping legitimate packets instead of dropping attack packets, which will result in the increase of false positives (Sachdeva et al., 2016).

The conventional security methods like router access control lists, firewalls, intrusion detection and prevention systems are not able to guard against DDoS attacks and FEs effectively. That is why there is no perfect solution to this ongoing of detecting DDoS attacks and FEs till date; some of the reasons may be the decentralized nature of Internet, lack of collaboration among ISPs, infrastructure changes, collateral damage, the absence of latest real datasets and obsolete methods used for validation purpose, and deployment issues, etc. (Kumar et al., 2007; Sachdeva et al., 2016; Behal and Kumar, 2016a; Bhatia, 2016; Saravanan et al., 2016; Bhandari et al., 2016).

Many isolated solutions have been proposed in the literature to defend against LR-DDoS attacks, HR-DDoS attacks and FEs (Bhuyan et al., 2014). It has been observed that the earlier prominent research has extensively used the variations of information theory-based Shannon Entropy, Generalized Entropy, and Divergence based metrics such Kullbeck-Leibler divergence for detecting DDoS attacks and FEs. This research work proposes to use an information theory based novel generalized ϕ-Divergence metric for the distributed detection and mitigation of different types of DDoS attacks and FEs. As part of the work, a distributed, flexible, automated and collaborative (D-FAC) defense system has been proposed. The proposed detection metric is computed at all of the ingress points called PoPs and sent to a central coordinator located in the premises of a victim network which, then, aggregate the detection metric. As per our knowledge, we are the first one to use ϕ-Divergence metric based distributed approach to distribute the storage and computational overheads of a victim-end defense deployment. It has also lead to the protection of proposed distributed solution against high volume of network packets generated during DDoS attacks and FEs which most of the existing research solutions have failed to provide.

The major contributions of this work can be summarized as follows:

- This paper proposes a ϕ-Divergence based distributed, flexible, automated, and collaborative (D-FAC) defense system for the detection and mitigation of different types of DDoS attacks.
- The proposed D-FAC defense system has low computational and memory overhead as compared to a victim-end based deployments. We distribute the computational and memory overhead of detection metric to multiple boundary level PoPs of an ISP. The aggregated detection metric is then computed using the additive property of ϕ-Divergence at a central PoP.
- The proposed D-FAC defense system uses the same ϕ-Divergence metric for the characterization of DDoS attack and legitimate FEs traffic; and efficiently mitigate their impact with less collateral damage to legitimate traffic.
- The reporting results shows that ϕ-Divergence based D-FAC defense system is more effective in detecting different types of DDoS attacks; and has outperformed existing defense systems based on Shannon Entropy, Generalized entropy and other divergence measures. This effectiveness has been measured in terms of various detection system evaluation metrics such as detection accuracy, FPR, F-measure, classification rate, and precision.

- Design of D-FAC defense system is robust and fault tolerant as it can continue its operation even in case some of the PoPs does not send their computed detection metric in time.
- The proposed distributed detection algorithm is independent of any specific DDoS attack tool or attack pattern. So, it can be used to detect DDoS attacks of future also.
- The proposed D-FAC defense system has been validated using real network traffic generated using a set of benchmark attack tools and traffic generators in DDoSTB testbed along with trace driven simulation of prominently used real datasets in DDoS validation.

The rest of the paper is organized as follows. Section 2 describes the proposed distributed model, approach and algorithm, the working of proposed defense system is described in Section 3, the details of experimental setup is given in Section 4, results along with performance evaluation is discussed in Section 5 and finally, the proposed work is concluded in Section 6 by highlighting the scope for future work.

2. D-FAC system model

Both DDoS attacks and FEs cause significant deviations in network traffic distributions. Information theory-based detection metrics such Entropy or Divergence can quickly capture such variations in the network traffic. Out of the plethora of information theory based metrics, we have used a novel ϕ-Divergence metric to detect DDoS attacks and FEs because it is more effective and susceptible to measure even meek variations, uncertainty or randomness in a probability distribution. This section briefly describes background of ϕ-Divergence metric and proposed distributed approach to detect different types of DDoS attacks.

2.1. Background of ϕ-Divergence

There are a plethora of information theory-based divergence metrics that can be used to quantify the difference between a set of probability distributions. For any two discrete probability distributions $P = (p_1, p_2, \ldots\ldots, p_N)$ and $Q = (q_1, q_2, \ldots\ldots, q_N)$ with $\sum_{i=1}^{N} p_i = \sum_{i=1}^{N} q_i = 1, \mathrm{i} = 1, 2, \ldots, \mathrm{N}$, the generalized information divergence (GID) is defined as:

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

where N is the total number of network flows received in a time window. Here, D_α represent the divergence value computed using GID metric on entropic index parameter α. When $\alpha \to 1$, Kullbeck-Leibler (KL) divergence is derived as follows.

$$D_1(P\|Q) = \sum_{i=1}^{N} p_i log\left(\frac{p_i}{q_i}\right) \tag{2}$$

Further, we propose to use ϕ-Divergence metric which is based on Csiszar's f-divergence (Bhatia and Singh, 2013). Formerly, ϕ-Divergence is defined as:

$$D'_\alpha(P\|Q) = \sum_{i=1}^{N} \frac{p_i sinh(\alpha log \frac{p_i}{q_i})}{sinh(\alpha)}, \ \alpha \to 1. \tag{3}$$

Here D'_α represent the divergence value computed using ϕ-Divergence metric on entropic index parameter α. The divergence measure proposed above is non-symmetric in nature. The symmetric version of ϕ-Divergence is given by:

$$D_{J\alpha} = D'_\alpha(P, Q) + D'_\alpha(Q, P) \tag{4}$$

The determining function of ϕ-Divergence is given as:

$$F(x) = \frac{x sinh(\alpha log(x))}{sinh(\alpha)}, \ \alpha > 0 \tag{5}$$

The behavior of F(x) on different α-order is shown in Fig. 1. It is evident that the value of F(x) increases exponentially with minor increase in α-order.

We have exploited this property to magnify the information distance between two network traffic flows which has lead to more detection efficiency of ϕ-Divergence metric. We have empirically investigated this claim in our previous publication (Behal and Kumar, 2017a) that the ϕ-Divergence metric has a higher rate of convergence for achieving a particular solution and it produced better results as compared to other entropy based metrics. This is because a divergence metric is computed using the individual values of a probability distribution with in a time window, whereas an entropy metric merely summarize the variations in a probability distribution to a single value. So, the divergence metrics are better suited to predict the pattern of variations in a probability distribution as compared to entropy based metrics which can be easily deceived by the sophisticated attackers (Ozcelik and Brooks, 2015). Therefore, much better results can be obtained by using the ϕ-Divergence metric as compared to other existing widely used information theory metrics.

2.2. Distributed detection using ϕ-Divergence

On the Internet, all the end systems or nodes are connected to each other through a tiered hierarchy of Internet Service Providers (ISPs). Within an ISP network, the points where one ISP connects to other ISPs are known as Point of Presence (PoP). Within an ISP network, a PoP is logically a group of connected core and access routers to which core routers of the same or other ISPs (public/private peer or NAT) and ISPs customers and servers are connected. An abstract view of ISP topology is shown in Fig. 2. As shown, there are two types of PoPs. One is used to connect to other PoPs of other ISPs, and the second type is used to connect customer domain or a web server. The PoP designated as P_s aggregates the detection metric values from all other PoPs, and computes the final detection metric value.

Ideally, the computation of a detection metric should be done at the PoP, where web server is connected, as maximum attack traffic is available at this point (as shown in Fig. 2). However, the huge volume of DDoS or FE traffic, and large memory and computational overheads at this single point makes this defense deployment location implausible. To address this problem, there is a need to distribute the costs of monitoring and computation of detection metric to multiple PoPs from which traffic is arriving at the

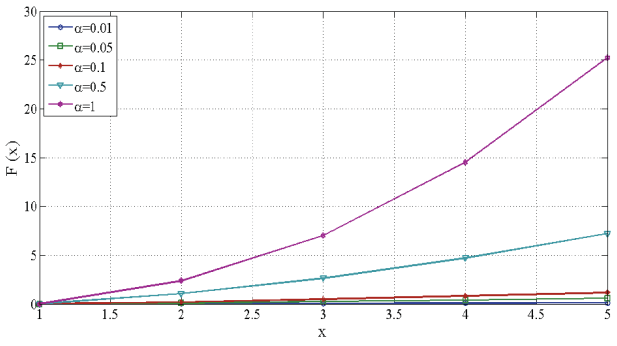


Fig. 1. Behavior of F(x) with increasing α-order.

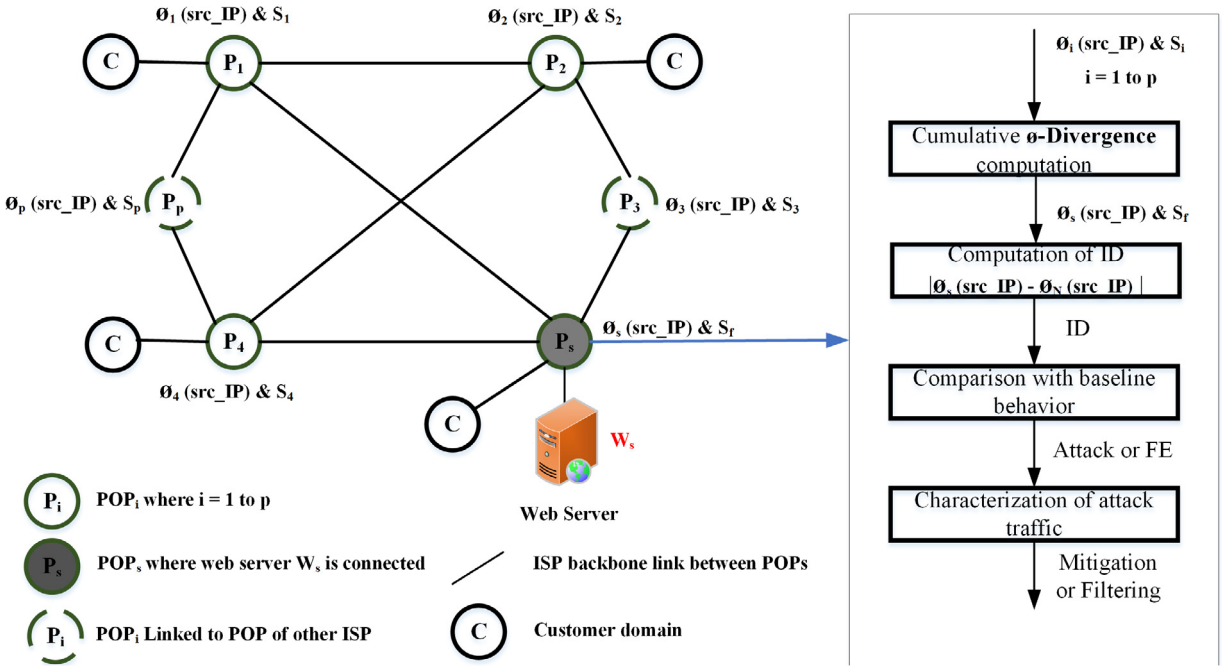


Fig. 2. Architecture of D-FAC defense system.

expense of communication overhead. Finally, the detection metric needs to be calculated at the victim site from the accumulated values of all PoPs. It makes the process analogous to existing victim-end approach in which total traffic is monitored at the victim site where all the attack or FE traffic converges.

Assuming $PoP_1, PoP_2, \ldots PoP_n$ be the n PoPs of an ISP domain. For any two discrete probability distributions $P = (p_1, p_2, \ldots\ldots, p_N)$ and $Q = (q_1, q_2, \ldots\ldots, q_N)$ with $\sum_{i=1}^{N} p_i = \sum_{i=1}^{N} q_i = 1, i = 1, 2, \ldots, N$, let $D_\alpha(P, Q)$ represents information divergence value at PoP_i. The information divergence values computed at each PoP_i are sent to P_s (PoP connecting web server to ISP) where final computation of information divergence is calculated.

Each PoP_i computes source IP address based ϕ-Divergence on its accumulated network flows according to the following mathematical model:

$$\phi\text{-}Divergence_i(srcIP) = \sum_{i=1}^{N} \frac{p_{srcIP_i} sinh\left(\alpha log\left(\frac{p_{srcIP_i}}{q_{srcIP_i}}\right)\right)}{sinh(\alpha)} \tag{6}$$

ϕ-Divergence value computed at each PoP_i along with number of packets received per time window i.e. S_i is then sent to P_s, i.e PoP where webserver is connected. Then, the final aggregated ϕ-cas

$$\phi\text{-}Divergence_f(srcIP) = \sum_{i=1}^{n} (\phi\text{-}Divergence_i(srcIP)) \tag{7}$$

and S_f is calculated as:

$$S_f = \sum_{i=1}^{n} S_i \tag{8}$$

Where n is the number of reporting PoPs in a time window. This mathematical model gives the same information divergence value as if whole of the network traffic is monitored and analyzed at a single PoP where web server is connected. The PoP P_s on the basis of proposed distributed detection algorithm then decides whether the system is under DDoS attack or FEs.

In the next section, we extended this idea to proposed a distributed detection algorithm.

3. Working of D-FAC

The various symbols and notations used in this section have been summarized in Table 1. For the efficient working of any defense solution, there is a need to set some design parameters according to network under analysis such as time window size, packet header features used, selection of generalized entropic index parameter α, and optimal threshold values. We chose the time window size where standard deviation value of ϕ-Divergence metric is least as it indicates the stable network behavior. We choose $T_w = 1$ second after comprehensively analyzing the baseline network behavior. We used the packet header features of source (destination) IP address, source (destination) port, protocol and incoming packet rate for computing the detection metrics. The destination IP, port field is used to filter the network traffic flows that are destined towards a specific target i.e. web server under attack. Protocol field is used to detect the type of traffic flows. The other IP packet header features like variations in the packet size, source, and destination port numbers, packet inter-arrival time, etc. can also be used for anomaly detection but authors have used only those features that are used by the existing prominent research to detect DDoS attacks and FEs (Kumar et al., 2007; Bhuyan et al., 2016; Sachdeva et al., 2016; Xiang et al., 2011).

Further, the value of generalized entropy index parameter α may also affect the detection rate of any generalized Entropy or Divergence based detection system because of the highly dynamic nature of network traffic. We compute the reduced FPR as defined by Xiang et al. (2011) to decide the appropriate value of generalized parameter α for ϕ-Divergence metric. ϕ-Divergence is equal to KL divergence when $\alpha \to 0$ (Eq. (2)), we choose the information distance value at $\alpha = 0.01$ as the basis for comparing the FPR as per the following equation.

$$\beta' = \frac{\beta_{KL} - \beta_{Phi}}{\beta_{KL}} \tag{9}$$

where Phi = ϕ-Divergence.

We empirically investigated in Behal and Kumar (2017a) that ϕ-Divergence metric has low β' values as compared to KL metric on increasing α-order which signifies the better detection efficiency

of ϕ-Divergence metric. In this work, we chose the generalized entropic index parameter $\alpha = 0.5$ having reduced FPR of more than 200% as compared to *KL* based on the results reported in Table 3 of Behal and Kumar (2017a).

3.1. Proposed detection methodology

The proposed distributed detection algorithm is given in Algorithm 1. D-FAC works on the assumption that all the attack nodes (also known as zombies) inside a botnet work in a coordinated manner with some pre-defined shared similar program logic to flush the network traffic towards the victim (Yu et al., 2009). It results in a flow similarity among attack traffic flows, whereas legitimate network traffic flows are highly variable and dynamic in nature. It causes a significant deviation in packet header features of attack traffic flows from legitimate traffic flows.

The proposed detection approach then use the difference between source IP based ϕ-Divergence values of current and normal traffic flows called an information distance (ID) as detection metric. Formerly, ID is defined as

$$ID = |\phi_{s_C} - \phi_{s_N}| \tag{10}$$

where ϕ_{s_C}, ϕ_{s_N} are the source IP address based ϕ-Divergence values of current and normal network traffic flows respectively at PoP P_s.

Algorithm 1: A distributed detection Algorithm

1. Set
   $f \leftarrow$ sampling frequency.
   $T \leftarrow$ sampling period.
   $T_w \leftarrow$ Time window size =1 s.
   $\sigma_1, \sigma_2 \leftarrow$ thresholds at PoP P_s.
2. While $T_w <= T$, analyze the network traffic coming from upstream Routers.
3. Extract packet header features :
   $F \leftarrow \{srcIP, dstIP, pktsize, no.ofpkts(S_i)\}$ in current T_w and classify into unique network flows at each PoP_i.
4. Calculate the probability distributions of network flows based on src_{IP} in the current T_w at each PoP_i.
5. Compute the srcIP based ϕ-Divergence metric between network flows using Eq. (6) at each PoP_i.
6. Send $\phi - Divergence_i$ and S_i computed at each PoP_i to PoP P_s for the final aggregation of ϕ-Divergence metric and S_f using Eq. (7) and 8 respectively.
7. Calculate the information distance (ID) between current and normal network flows using Eq. (10).
8. **if** $S_f > \sigma_1$ **then**
9. Traffic may be HR-DDoS or FE.
10. **if** $ID > \sigma_2$ **then**
11. Declare the traffic as HR-DDoS.
12. **else**
13. Declare the traffic as FE.
14. **end if**
15. **else**
16. Traffic may be LR-DDoS or Legitimate.
17. **if** $ID > \sigma_2$ **then**
18. Declare the traffic as LR-DDoS.
19. **else**
20. Declare the traffic as Legitimate.
21. **end if**
22. **end if**
23. increment T_w and goto step 2.

Actually, the motivation of using ϕ-Divergence based ID metric comes from the empirical results of our previous publication (Behal and Kumar, 2017a). We had computed the ϕ-Divergence metric on real datasets of MIT Lincoln (legitimate traffic), CAIDA (LR-DDoS and HR-DDoS traffic) and FIFA (FE traffic) in that paper. We chose these datasets as they have been used extensively by the prominent research in the field of DDoS defense. It had been observed that the ID values between attack traffic vs legitimate traffic flows, and between legitimate traffic vs FE traffic flows computed at entropic index parameter $\alpha = 0.5$ are much better as compared to Renyi's generalized information divergence metric and KL metric. So, we extended the concept of ID to propose a distributed approach in this paper. For this, we define different types of network traffic flows as follows:

Table 1
Notations and Symbols used.

Notation	Definition
T	Sampling period
T_w	Time Window
Δ	size of T_w
j	initialized to 1 and increment after each T_w
$flowid_i$	Unique flow id of i^{th} network flow
n_C	number of packets per T_w in current traffic
n_N	number of packets per T_w in baseline traffic
σ_1	threshold based on n_N computed from baseline traffic
σ_2	threshold based on ID_N computed from baseline traffic
ID_C	Information distance between current and normal traffic flows
ID_N	Information distance between normal traffic flows

Definition 1. *Network traffic flow*: For a given PoP_i in a network, a network traffic flow is defined as a 5-tuple {srcIP, dstIP, sport, dport, protocol} where srcIP (dstIP) is source (destination) IP address, sport (dport) is the source (destination) port number, protocol is the type of network flow.

Definition 2. *Legitimate traffic flow:* A network traffic flow is termed as Legitimate traffic flow iff $n_C <= n_N + x * d_n \wedge ID_C <= ID_N + k * z_{ID_N}$.

Definition 3. *LR-DDoS attack traffic flow:* A network traffic flow is termed as LR-DDoS traffic flow iff $n_C <= n_N + x * d_n \wedge ID_C > ID_N + k * z_{ID_N}$ i.e. the traffic rate is less than or equal to legitimate traffic but having more information distance than legitimate traffic.

Definition 4. *HR-DDoS attack traffic flow*: A network traffic flow is termed as HR-DDoS traffic flow iff $n_C > n_N + x * d_n \wedge ID_C > ID_N + k * z_{ID_N}$ i.e. the traffic rate is more than the legitimate traffic but having more information distance than legitimate traffic.

Definition 5. *FE Traffic Flow:* A network traffic flow is termed as FE traffic flow iff $n_C > n_N + x * d_n \wedge ID_C < ID_N + k * z_{ID_N}$ i.e. the traffic rate is more than legitimate traffic but having small information distance than legitimate traffic.

Here x, k $\in$ I where I is the set of integers. Tolerance factors x and k are design parameters. d_n is the standard deviation in traffic rate, and z_{ID_N} is standard deviation in the information distance (ID) between legitimate traffic flows computed using the normal state of the network. i.e. without attack and FEs. The factor $n_N + x * d_n$ represents the threshold σ_1, which is 320 in our case. Whereas the factor $ID_N + k * z_{ID_N}$ represents threshold σ_2 which is 0.625 in our case. Both of these thresholds are computed by analyzing the baseline behavior of the network without attack.

Initially, we separated the low-rate and high-rate traffic flows by comparing the current incoming traffic rate in each time

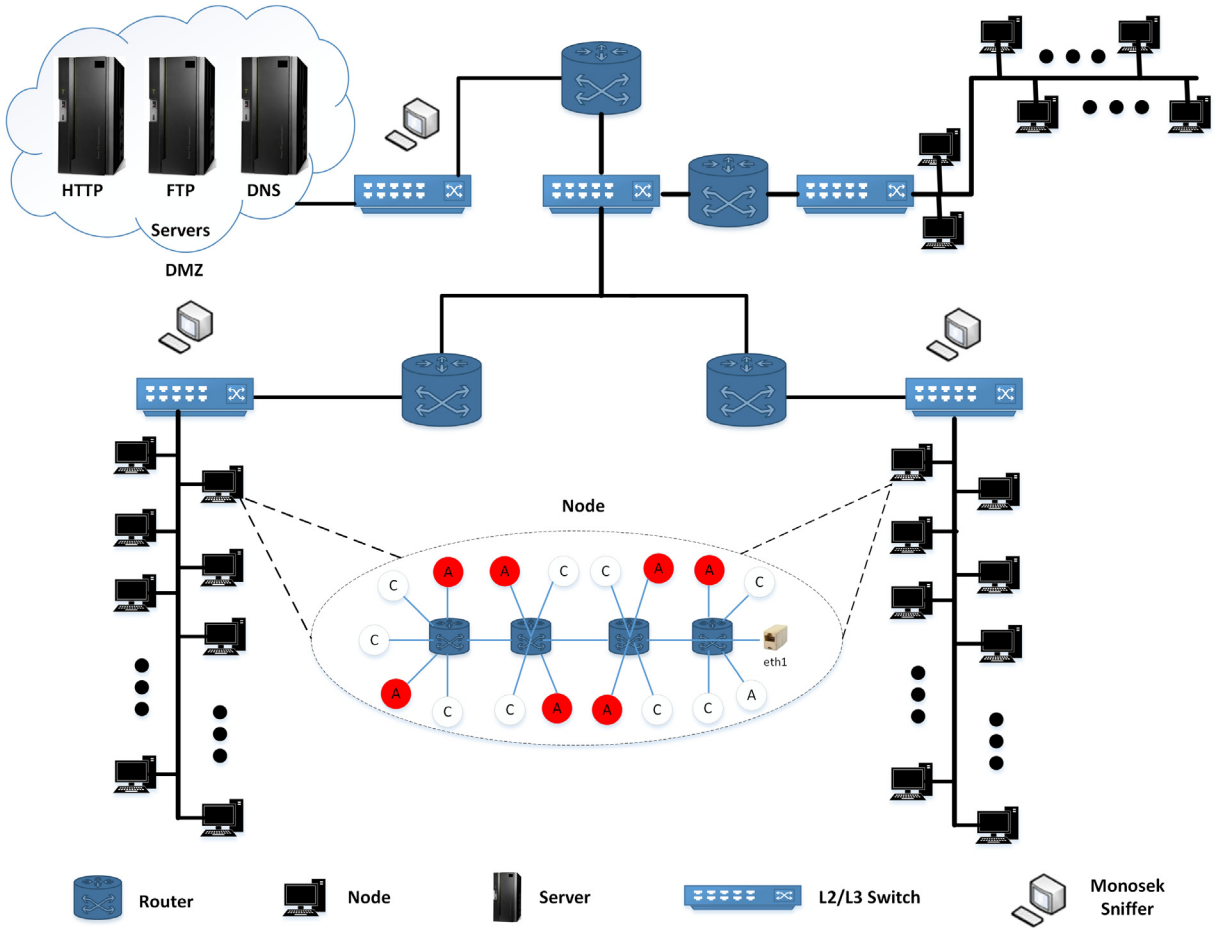


Fig. 3. Design of DDoSTB Testbed.

window (T_w) i.e. by computing current number of incoming packets (n_C) and comparing with threshold σ_1. Whenever there is a significant deviation of information distance (ID) value of current monitored traffic flow (ID_C) from σ_2, the attack is said to be detected. If ID value is more than the threshold value, we declare it as an attack traffic; otherwise as a legitimate traffic. The high rate traffic can also be declared as legitimate traffic. This high rate can be due to a sudden burst of the network traffic, or due to some newsworthy event happening around the world because of which a large number of users start accessing the particular website or a network resource simultaneously. Such a situation is called a flash event (FE) (Sachdeva et al., 2016).

All the PoPs route their traffic towards PoP P_s where webserver W_s is attached. In each time window T_w, we continuously send the calculated ϕ-Divergence values and number of packets received per time window i.e. S_i at each PoP_i to PoP P_s. The PoP P_s then decides whether the system is under LR-DDoS (HR-DDoS) DDoS attack or FEs. In either case, it activates the characterization and mitigation module as shown in Fig. 4.

If the system is under DDoS attack, D-FAC defense system excludes the corresponding malicious PoP from the list of PoPs to be monitored and continue its working without further collateral damage. The PoP P_s continuously keep on comparing the recently computed information distance (ID) value with the baseline behavior and excluding the malicious PoPs from the list of monitored PoPs. If the system is under FEs, D-FAC send signal to each PoP to activate a text-based captcha module so as to limit the traffic rate destined towards web server W_s. The captcha module restrict the number of new connection requests and at the same time ensures fair allocation of web server resources to the existing connections. In this way, our proposed D-FAC system continue to work in case of FEs.

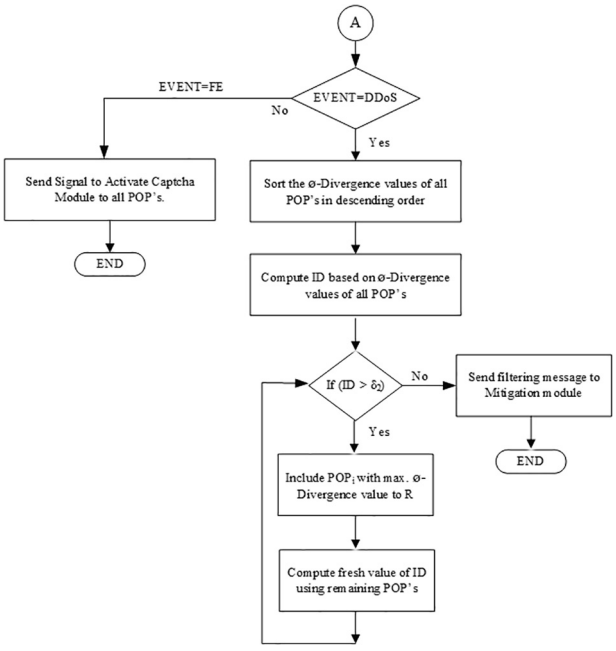


Fig. 4. Flowchart of characterization and mitigation module.

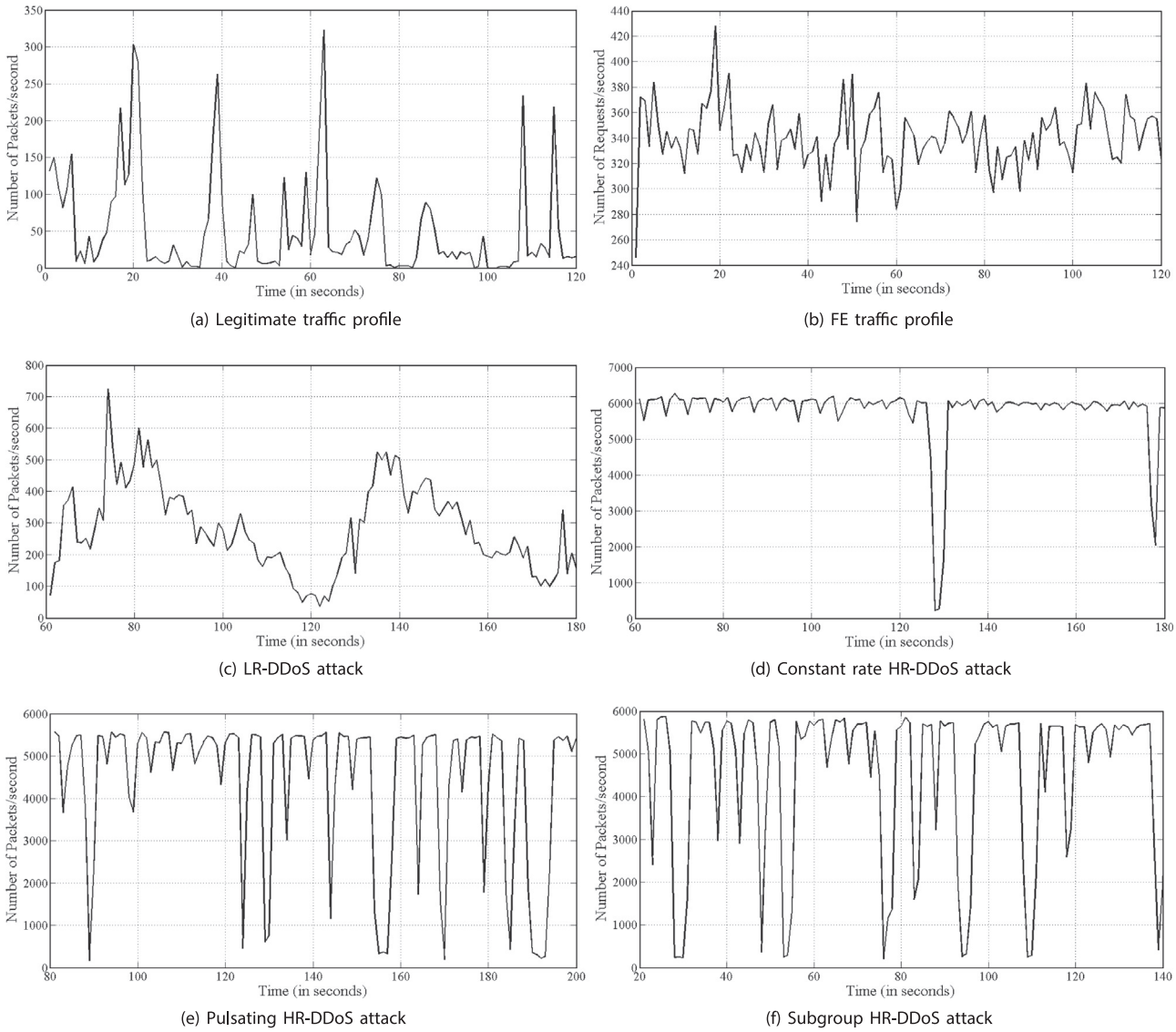
4. Experimental setup

We implemented the proposed D-FAC defense system in a DDoSTB testbed. DDoSTB testbed is a multipurpose emulation-based real testbed that has been designed as part of the research work as shown in Fig. 3. It is a hybrid of real systems and emulated systems to design and develop large scale topologies. This testbed has been used to synthetically generating datasets for different types of DDoS attacks and FEs, for measuring the impact of DDoS attacks on web services and for user behavior modeling. We have used this testbed to generate real network traffic through benchmark DDoS attacks tools and traffic generators to validate the proposed D-FAC defense system. The testbed is composed of 75 physical nodes organized into three clusters of 25 computers each, which runs Linux and Windows OS instances, 4 D-Link physical routers that act as PoPs and a 2-processor 8-core Linux server that act as the victim web server W_s connected to PoP P_s. CORE emulator (CORE Emulator, 2016) has been used to increase the number of virtual nodes in the testbed. As shown in Fig. 3, one CORE node is composed of 16 virtual clients and 4 soft routers. For generating the synthetic network traffic, the legitimate clients and attackers are randomly distributed with in each node. We have used this testbed to replay the traffic traces, for user behavior modeling to detect application layer attacks, for measuring the impact of DDoS attacks on web services (Behal and Kumar, 2016b), and for generating near to real datasets for validation purpose.

As most of the DDoS attacks are launched nowadays using Botnets (Wang et al., 2012), we installed multiple instances of BONESi (Alcorn and Chow, 2014) botnet simulator tool to generate DDoS attack traffic. For the generation of real background and normal network traffic, we used httperf and D-ITG traffic generators. The traffic profiles of different types of traffic generated using DDoSTB testbed are shown in Fig. 5(a)–(f). Further, we have also used the forensics capabilities of a network based monosek software tool to compute various detection and performance metrics in realtime. For this, we installed a Monosek client module at each PoP_i and Monosek server module (Monosek Network analysis tool, 2016) at PoP P_s.

5. Results and discussion

For validating D-FAC defense system, we distributed the traffic analysis monitors at PoP_1, PoP_2, PoP_4 and PoP P_s. The ID values



(a) Legitimate traffic profile

(b) FE traffic profile

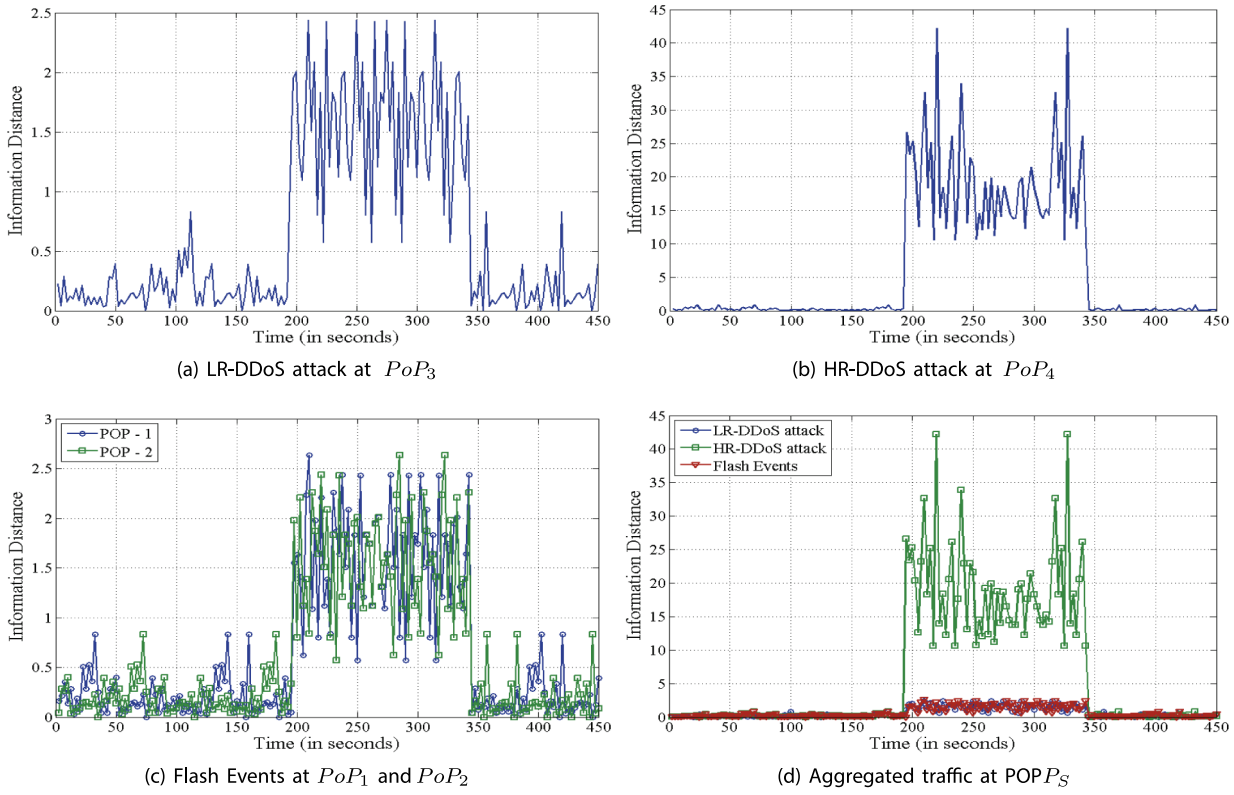
(c) LR-DDoS attack

(d) Constant rate HR-DDoS attack

(e) Pulsating HR-DDoS attack

(f) Subgroup HR-DDoS attack

Fig. 5. Profiles of various traffic scenarios in DDoSTB testbed.



(a) LR-DDoS attack at PoP_3

(b) HR-DDoS attack at PoP_4

(c) Flash Events at PoP_1 and PoP_2

(d) Aggregated traffic at POP P_S

Fig. 6. Temporal Variation in information distance (ID) values at various PoPs.

computed using Eq. (6) and number of packets received i.e. S_i at each PoP_i are sent to PoP P_S in each time window T_w. Then, the PoP P_S compute the aggregated value of information distance using Eq. (10), and classify the ongoing traffic flows in to one of the categories as per the Definitions 1–5 described in previous section. It has been observed that when there is no attack, ID values remain in range from 0 to 0.85. Then, LR-DDoS attack is launched from the source network attached to PoP_3, HR-DDoS attack is launched from the source network attached to PoP_4 and FE traffic i.e. high rate legitimate HTTP traffic is generated through source networks attached to PoP_1 and PoP_2. The ID values at all of these PoPs are shown in Fig. 6(a), (b) and (c) respectively. It has been observed that the ID values of legitimate vs LR-DDoS attack traffic remain in the range from 0.6 to 2.4, ID values of legitimate vs HR-DDoS attack traffic remain in range from 11 to 43, and ID values of legitimate vs FE traffic remain in range from 0.01 to 2.6. Now, as whole of this traffic also reached out at the victim server which is attached to PoP P_S, the corresponding ID values at PoP P_S are shown in Fig. 6(d).

5.1. Performance evaluation

To evaluate the efficiency of D-FAC defense system comprehensively, we used a number of performance evaluation metrics as described in Sachdeva et al. (2016), Ghorbani et al. (2010), Bhandari et al. (2014).

5.2. Threshold calibration

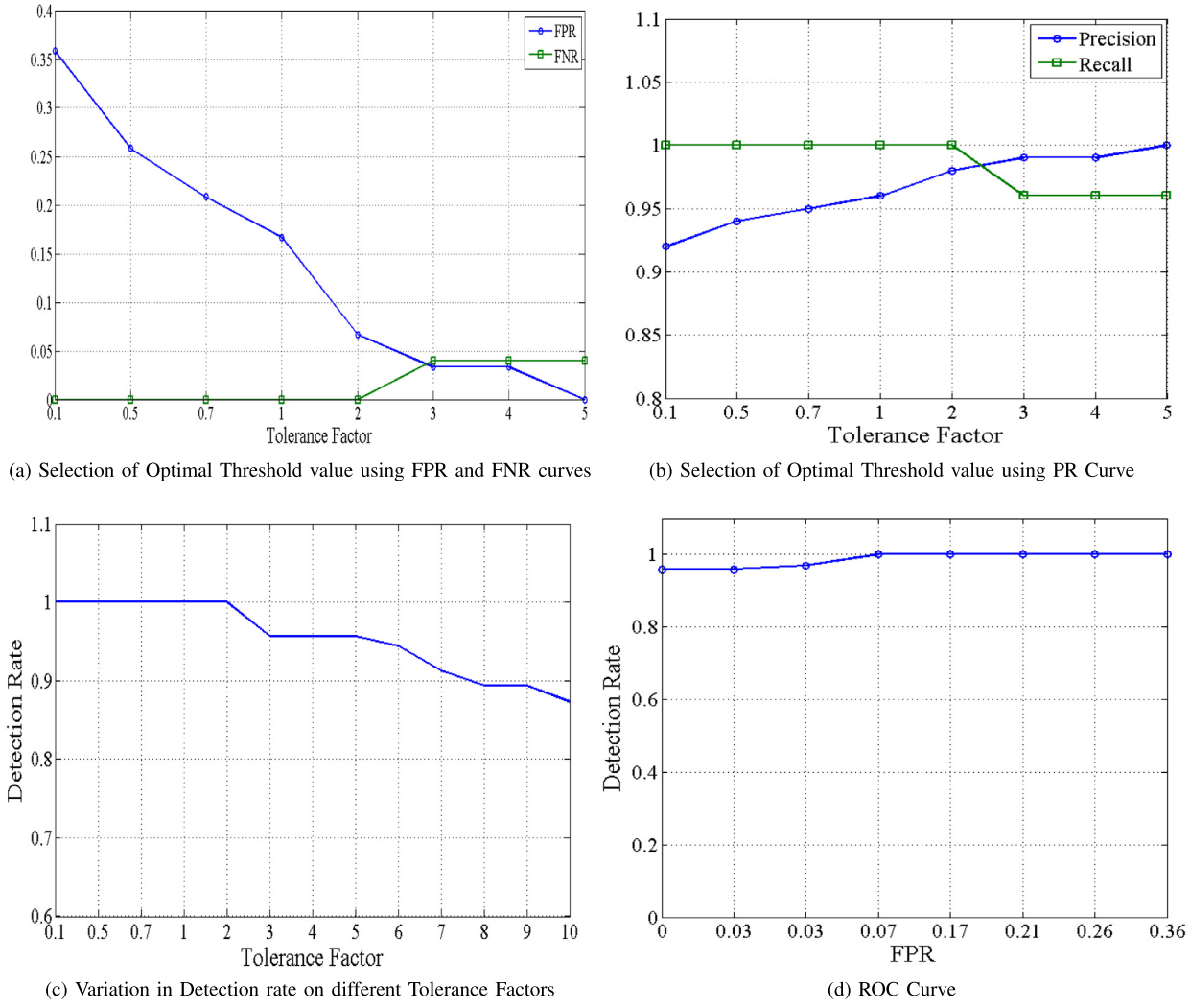
We performed a comprehensive analysis of normal traffic profiles of MIT Lincoln, FIFA, DDoSTB and OC-Link of CAIDA datasets to set the baseline network behavior. Further, we used the tradeoff between FPR and FNR curves to select the appropriate threshold limits range. Actually, an FPR measures the effectiveness of a detection system whereas FNR (1-detection rate) gives a measure of the system reliability. There are two ways to select an optimal threshold value. We can chose the threshold value where both FPR and FNR curves intersect each other as shown in Fig. 7(a) or alternatively, a Precision-Recall (PR) curve can also be used for the same purpose. We can chose the threshold value where both Precision and Recall curves intersect each other as shown in Fig. 7(b).

In a normal traffic case (i.e. without attack), a defense system always strive for minimum FPR but if a network is more vulnerable to attacks, then, high detection rate can be the priority. A low tolerance factor or threshold value always results in high detection rate, minimum FNR and high FPR. On the other hand, if tolerance factor or threshold value is set to high, then it may lead to low FPR but with low detection rate. In such case, almost no normal state will be signaled as attack state but the detection system may miss some of the attacks resulting in low detection rate. If tolerance factor or threshold value is set in between low and high bounds, then such detection system has balanced FPR and FNR. The temporal variation of tolerance factor has been used to quantify the FPR and FNR which assist in making decisions on the optimal value of thresholds. Fig. 7(c) depicts the performance of D-FAC on different tolerance factors. The Receiver Operating Characteristics (ROC) of D-FAC is shown in Fig. 7(d). The values of other defense system evaluation metrics are shown in Table 2.

It has been observed that the detection rate of D-FAC defense system decreases as tolerance factor is increased because the ability of D-FAC to classify different traffic flows also decreases as clear from values of classification rate in Table 2. Detection rate of D-FAC remains around 98% for tolerance factor = 3 and threshold value=0.625.

5.3. Measuring the impact of DDoS attacks on a web server

Further, we measure the impact of DDoS attacks on the victim web server with D-FAC defense system installed in terms of normal



(a) Selection of Optimal Threshold value using FPR and FNR curves

(b) Selection of Optimal Threshold value using PR Curve

(c) Variation in Detection rate on different Tolerance Factors

(d) ROC Curve

Fig. 7. Performance Evaluation of D-FAC defense.

Table 2
Performance of D-FAC defense on various detection system evaluation metrics.

Tolerance Factor	Threshold Value	Precision	Detection Rate	False Positive Rate	F-Measure	Classification Rate	False Negative Rate
0.1	0.201	0.92	1.00	0.36	0.96	0.93	0.00
0.5	0.259	0.94	1.00	0.26	0.97	0.95	0.00
0.7	0.288	0.95	1.00	0.21	0.97	0.96	0.00
1	0.332	0.96	1.00	0.17	0.98	0.97	0.00
2	0.479	0.98	1.00	0.07	0.99	0.99	0.00
3	0.625	0.99	0.98	0.03	0.97	0.96	0.04
4	0.772	0.99	0.96	0.03	0.97	0.96	0.04
5	0.919	1.00	0.96	0.00	0.98	0.97	0.04

packet survival ratio (NPSR), average response time of web server and %age of failed transactions metrics (Behal and Kumar, 2016b; Sachdeva et al., 2010; Singh et al., 2017b). Such a comprehensive evaluation of the proposed defense solutions is missing in the existing research. A NPSR value represents the ratio of goodput to the sum of goodput and badput; and can be used to measure the impact of attack as percentage of legitimate packets being delivered to the target during attack period. The high value of NPSR indicates the survival power of a defense solution against ongoing attacks. D-FAC starts its working when attack is launched at 190th s, it takes around 2 time windows i.e 2 s to communicate the first outcome of proposed distributed detection algorithm to each PoP_i. This delay is due to the computation of detection metric values at each PoP and communication to PoP P_S for making the final decision and sent back the decision to each PoP. That's why mitigation process is triggered after 2 s, once attack has started. It has been depicted from Fig. 8 that D-FAC defense system is able to stabilize the NPSR value of the monitored network under different types of DDoS attacks and FEs to around 91% in our case.

The performance of every application on the Internet is evaluated in terms of average response time it takes to complete. For normal network traffic scenario, the average response of the web

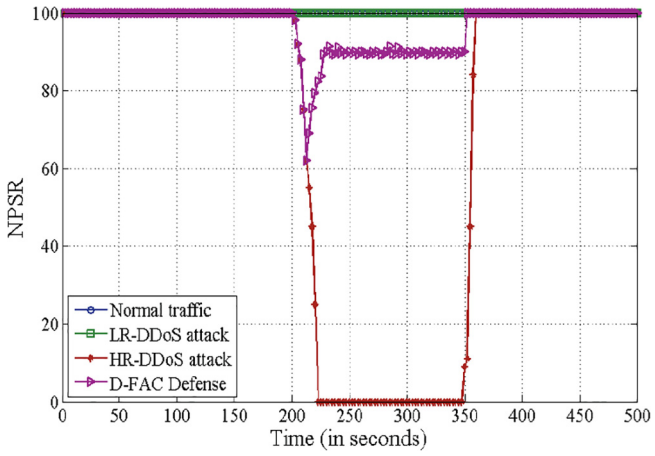


Fig. 8. NPSR of the web server under DDoS attacks with D-FAC defense installed.

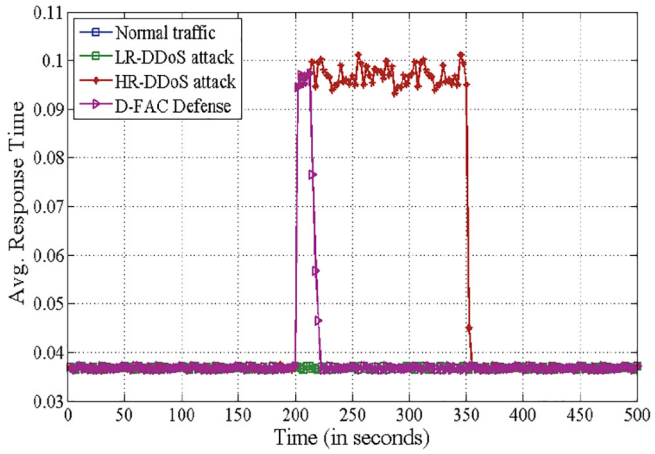


Fig. 9. Response Time of the web server under DDoS attacks with D-FAC defense installed.

server remains in the range of 0.036–0.039 s. However, in the case a HR-DDoS attack, average response time shoots up to around 30 times as shown in Fig. 9. In our case, it increases to 0.1 s which results in increase in the delay of responses from the web server.

Further, the %age of failed transactions can also indicate the occurrence of an on-going DDoS attack. Under normal circumstances i.e. without attack, all the transactions are completed within the time constraints, so, the %age of failed transactions is zero in this case. But in the case of a HR-DDoS attack, this value keeps on increasing up to 80% as shown in Fig. 10 that causes drop in NPSR value. It results in denial of service from the web server's perspective. It has been observed that in the case of a LR-DDoS attack, there is no effect on this parameter.

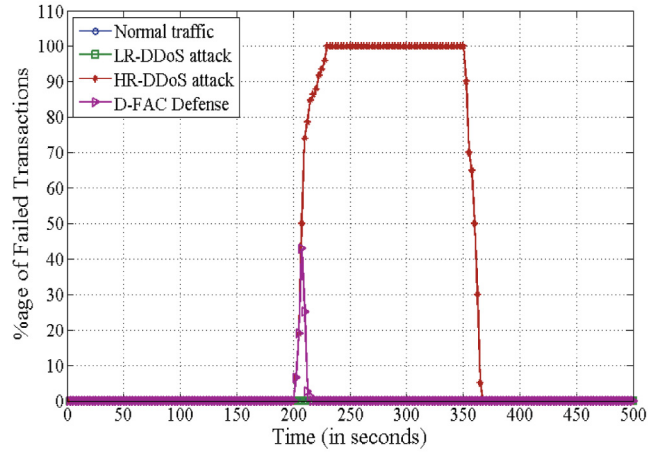


Fig. 10. %age of failed transactions under DDoS attacks with D-FAC defense installed.

5.4. Complexity analysis

Since the proposed D-FAC defense system distributes the memory and computational overheads to all PoPs, it is important to analyze its computational complexity. As per Brent and Zimmermann (2010), the computational complexity of sinh, exp and log functions is equivalent to O (M(N)log(N)), where M(n) is the cost of multiplication factor. It is evident from Eqs.(6) and (7) that high values of the α parameter in p_i^{α} factor would lead to increase in computational complexity. So, it is advisable to choose an optimal value of generalized entropic index parameter α. So, the computational complexity of a victim-end based defense system designed using Eq. (9) where whole of the network traffic is monitored at a single point is equal to $O(M(N)log(N))$, where N is the total number of traffic flows monitored at this central point and M(N) is the cost of multiplication factor. On the other hand, in the case of distributed approach with n number of PoPs, the computational overheads are distributed among n ingress PoPs and PoP P_s. Let the time complexities of each PoP_i is $O(M(N_i)log(N_i))$ where N_i is the number of traffic flows monitored at POP_i. The computational complexity of computing Eq. (7) at PoP P_s is $O(n)$ where n is the number of PoPs. So, the total computational complexity (T) of the distributed approach is $T = O(n) + (M(N_1)log(N_1)) + (M(N_2)log(N_2)) + \ldots\ldots\ldots + (M(N_n)log(N_n))$ which is equivalent to $O(n) + O(N)$ where $N = N_1 + N_2 + N_3 + \ldots.. + N_n$. As the number of traffic flows monitored in an ISP is very large as compared to the number of PoPs i.e. $N \gg n$, so T can be further reduced to $O(N)$ which is same as that of the computational complexity of a victim-end defense system as mentioned earlier. The another factor that can affect the final computational complexity is communication cost (C_c). It includes cost of communication among PoPs, average queueing delay at each PoP and other types of network delays.

Technically, $C_c = K[d_t rans + d_p rop + d_p roc + d_q ueue]$, where K is the number of links which are to be traversed by a packet and is equal to (number of PoPs + 1), $d_t rans$ is transmission delay, $d_p rop$ is propagation delay, $d_p roc$ is processing delay and $d_q ueue$ is queueing delay at the PoP. In the our DDoSTB testbed with 5 PoPs, the value of C_c comes out to be 0.2 ms approx. As this value is small as compared to total computational complexity, it can be neglected.

Hence, it is concluded that the computational complexity of the proposed D-FAC defense system is linear and is same as that of a victim-end defense system.

5.5. Comparison with related works

In this paper, we have proposed a distributed defense solution called D-FAC for the detection and mitigation of DDoS attacks and FEs. The proposed D-FAC defense system detects different types of DDoS attacks and FEs in general with low false positive rate and having low computational overhead. However, the proposed work differs from other similar work in some ways as mentioned below:

- Wang et al. (2018) proposed a sketch based novel anomaly detection and mitigation system called SkyShield for detecting application layer DDoS attacks. They used computationally

expensive sketch data structure along with Bloom filter for the efficient storage and processing of large number of network flows. They validated their proposed SkyShield defense system using off-line analysis of three real datasets at detection accuracy of 61% with reduced FPR = 4% whereas the detection accuracy of D-FAC is around 98% with FPR of 3%. SkyShield uses the modified Hellinger (HL) distance metric to compute the divergence between two sketches whereas D-FAC uses ϕ-Divergence metric which produces much better results (Behal and Kumar, 2017a,b). D-FAC distributes the computational complexity to nearby PoPs whereas SkyShield is deployed at the victim-end which has the obvious limitations as mentioned before. Furthermore, both SkyShield and D-FAC are capable of detecting HR-DDoS attacks launched during FEs with efficacy but D-FAC is capable of characterizing the attack traffic from FEs traffic by using the proposed information distance based approach which the authors of Wang et al. (2018) did not considered. SkyShield mitigate the impact of HR-DDoS attacks and FEs by making use of whitelists and blacklists of user profiles along with the annoying Captcha module at the initial stage of their framework whereas captcha module in D-FAC is activated only during DDoS attacks and FEs.

- Joldzic et al. (2016) proposed a distributed, scalable solution called TIDS (transparent intrusion detection system) for detecting network layer flooding based DoS attacks. The computational complexity is distributed to multiple traffic processors dynamically inside a protected webserver zone similar to our approach. Our proposed D-FAC defense system also uses the same IP address prefixes and traffic volume packet header features as used by TIDS for detecting malicious traffic flows but D-FAC system differs from TIDS in a number of ways. TIDS uses Shannon entropy metric for the detection of malicious traffic whereas D-FAC uses generalized ϕ-Divergence metric which produces much better results as compared to Shannon entropy metric. D-FAC distributes the computational overheads to the multiple edge router PoPs instead of layer-2 switches as done in TIDS that lead to early detection and response of D-FAC as compared to TIDS. Further, D-FAC is capable of detecting LR-DDoS attacks, HR-DDoS attacks and FEs collectively whereas TIDS is capable of detecting only network layer HR-DDoS attacks. Moreover, the validation of D-FAC defense system has been done using an emulation based real DDoSTB testbed with near to real network traffic which is more robust technique as compared to the dataset based validation technique as used by TIDS. Further, we have comprehensively evaluated the efficiency of D-FAC on a set of benchmarked defense system evaluation parameters which TIDS has not considered. Even the scope of TIDS is up to the detection of flooding based network layer DDoS attacks only whereas the methodology of D-FAC is generalized enough to detect different types of DDoS attacks and FEs.
- Bhuyan et al. (2016) used extended entropy metric (EEM) based on GE metric to compute the information distance between legitimate and HR-DDoS attacks. They proposed a light-weight detection system (E-LDAT) which is capable of detecting HR-DDoS attacks with increased information distance as compared to Xiang et al. (2011) whereas our proposed system can elicit even more information distance at low α-order as compared to both the solutions with much more reduced FPR and high detection accuracy.
- Sachdeva et al. (2016) proposed a distributed defense framework called DDF that can detect HR-DDoS attacks and FEs using a combination of Shannon entropy and cluster entropy. However, the detection accuracy of DDF is around 82% with FPR of 20% as compared to detection accuracy of D-FAC which is around 98% with FPR of 3%. Moreover, they validate their proposed approach using simulations in NS2, and emulation based experiments using DETER testbed whereas we have used publically available real datasets along with synthetically generated datasets in DDoSTB.
- Cui et al. (2016) proposed a neural networks based DDoS mitigation system called a SD-Anti-DDoS to reduce the response time of the network under DDoS attacks. They evaluated their proposed detection algorithm in a simulation based Mininet platform. They used TFN2k attack tool to generate attack traffic which is obsolete nowadays as attackers have shift their modus operandi to more sophisticated DDoS attacks.
- Gulisano et al. (2015) proposed a distributed DDoS defense framework called STONE. Their proposed system computes the deviation of source IP based cluster groups made during normal operation of network with the cluster groups computed during attack period. Based on the deviation value, their proposed system can effectively detect HR-DDoS attacks and FEs. However, D-FAC is able to detect different types of LR-DDoS and HR-DDoS attacks along with FEs. STONE framework has been validated using real legitimate traces of Swedish university computer network dataset and CAIDA attack dataset whereas D-FAC has been validated in a realtime in an emulation based DDoSTB testbed. However, the computational complexity of STONE is high as compared to D-FAC. It takes around 18 s to detect an attack in STONE framework whereas D-FAC requires only 2–3 s for the same.
- Ma et al. (2014) used Lyapunov exponents between legitimate and attack traffic to compute the information distance between the two. Whereas, D-FAC defense system can magnify this information distance even more with low computational overhead and high detection accuracy. D-FAC achieves higher detection accuracy i.e. 100% in detecting HR-DDoS attacks than 98.56% in the proposed scheme.
- Ranjan et al. (2009) proposed an anomaly based counter-mechanism against DDoS attacks called DDoS Shield. In the first step, their proposed approach assigns a unique value to each client session, and then, in the second step, a scheduler determines to schedule the session requests based on this value. They conducted a number of real testbed experiments to measure the impact of application layer HR-DDoS attacks on a webserver. The authors compute Hellinger distance metric to detect anomalies in the network traffic. However, DDoS-Shield produced the detection rate of around 61% whereas our proposed D-FAC defense system has detection accuracy of around 98%.
- Yu and Zhou (2008) used Shannon entropy to detect HR-DDoS attacks and FEs based on packet size header feature. But their proposed system did not consider the detection of different types of LR-DDoS and HR-DDoS attacks. Whereas, D-FAC considers all types of DDoS attacks in general and can efficiently highlight the type of attack with high detection accuracy and classification rate.
- Kumar et al. (2007) proposed an ISP level distributed detection, characterization and filtering system (D-DCFI) using Shannon entropy to detect flooding DDoS attacks. The authors validated their proposed approach using simulations in NS2. However, D-FAC defense system uses ϕ-Divergence as detection metric. We have empirically investigated in Behal and Kumar (2017a) that the results of ϕ-Divergence metric are much better as compared to Shannon entropy metric in detecting DDoS attacks. Moreover, the detection rate of D-FAC can be performance tuned and configured according to the dynamic network behavior that D-DCFI did not considered. Besides, D-FAC can also detect and discriminate FEs from similar looking HR-DDoS attacks and LR-DDoS attacks. Further, D-FAC produced detection accuracy of 98% with reduced FPR of 3% as compared to 86% detection accuracy of D-DCFI with FPR of 18%.

Table 3
Mathematical models of some popular Information theory measures.

Detection Measure	Victim-end Model	Distributed Model
ϕ-Divergence	$\sum_{i=1}^{N} \frac{p_i sinh(\alpha log(\frac{p_i}{q_i}))}{sinh(\alpha)}$	$\sum_{i=1}^{n}\left(\sum_{i=1}^{N} \frac{p_i sinh(\alpha log(\frac{p_i}{q_i}))}{sinh(\alpha)}\right)$
Generalized Information Divergence (GID)	$\frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{N} p_i^{\alpha} q_i^{1-\alpha}\right)$	$\sum_{i=1}^{n}\left(\frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{N} p_i^{\alpha} q_i^{1-\alpha}\right)\right)$
Generalized Entropy (GE)	$\frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{N} p_i^{\alpha}\right)$	$\frac{1}{1-\alpha} log_2\left(\sum_{i=1}^{n}\left(\frac{S_i}{S_f}\right)^{\alpha}(2^{E_i(x)(1-\alpha)})\right)$
Shannon Entropy	$-\sum_{i=1}^{N} p_i log_2 p_i$	$\frac{1}{S_f}\left(\sum_{i=1}^{n} S_i(E_i - log_2(S_i))\right) + log(S_f)$

Table 4
Comparison of D-FAC with other existing Defense systems

Defense System	Mode of Operation	Detection Metric	Parameter	Detection Rate	Traffic Type Detected		
					LR-DDoS	HR-DDoS	FE
D-FAC	Distributed	ϕ-Divergence	ID	98	√	√	√
D-FAC-1	Distributed	GID	ID	75	√	√	√
D-FAC-2	Distributed	GE	ID	93	√	√	√
SkyShield (2018)	Centralized	HL	Request rate	61	√	√	√
DDF (2016)	Distributed	Shannon Entropy	srcIP	82	–	√	√
E-LDAT (2016)	Centralized	EEM	srcIP	91	–	√	–
TIDS (2016)	Distributed	Shannon	srcIP	84	–	√	–
SD-Anti-DDoS (2016)	Distributed	Shannon Entropy	srcIP	–	–	√	–
STONE (2015)	Distributed	difference of cluster groups	srcIP based cluster Request rate	–	–	√	√
DDoS-Shield (2009)	Centralized	Hellinger distance	Request rate	61	√	√	√
D-DCFI (2007)	Distributed	Shannon Entropy	srcIP	86	–	√	–

- We also implemented the proposed distributed approach using generalized information divergence (GID) measure denoted by D-FAC-1 and using Generalized Entropy (GE) measure denoted by D-FAC-2 as shown in Table 4. The corresponding victim-end (centralized) and distributed mathematical models derived using these measures are given in Table 3. It has been observed that the results of ϕ-Divergence based D-FAC defense system are better as compared to D-FAC-1. D-FAC-1 produced the detection accuracy of 75% at entropic index parameter $\alpha = 15$ as compared to D-FAC that produced the detection accuracy of 98% at entropic index parameter $\alpha = 0.5$. Further, D-FAC is more capable of detecting patterns of ongoing DDoS attacks as compared to D-FAC-1 and D-FAC-2. Detection accuracy of D-FAC-2 is around 93% with FPR of 10% whereas detection accuracy of D-FAC is around 98% with FPR of 3%. It is worth mentioning here that the computational complexity of D-FAC-2 is also more as it produced the detection accuracy of 93% at entropic index parameter $\alpha = 15$ as compared to D-FAC that produced the detection accuracy of 98% at entropic index parameter $\alpha = 0.5$.

6. Conclusion

DDoS attack is an austere menace to network security. This paper has proposed an anomaly based distributed, flexible, automated and collaborative (D-FAC) DDoS defense system. The proposed comprehensive detection approach uses the idea of computing source IP address based generalized ϕ-Divergence between network traffic flows to detect different types of DDoS attacks and FEs. D-FAC is deployed at multiple boundary level PoPs of a victim network to distribute the computational and memory overheads among these PoPs. D-FAC defense system (a) detect different types of DDoS attacks and FEs, (b) collaborate and filters attack traffic at each of the ingress PoPs, (c) generate an automated response during the occurrence of these events, (d) react to DDoS attacks and FEs without any manual intervention, and (e) characterize different types of network traffic with efficacy. Besides these features, the proposed D-FAC defense solution is flexible in nature. It mitigates the impact of FEs gradually, while blocking the DDoS attacks immediately, and (f) is robust as it can continue to work even some of the PoPs fail to report in time. Further, D-FAC has been validated in real time using a set of publically available real datasets and synthetically generated dataset in an emulation based DDoSTB testbed.

The reporting results clearly show that D-FAC has outperformed existing generalized Entropy and divergence based defense systems in terms of high values of detection rate, precision, f-measure, reduced FPR, and classification rate. As part of the future work, more applications of the proposed ϕ-Divergence metric can be explored in other research domains, the proposed distributed model can be implemented using software defined networking (SDN) technique to reduce the overall implementation cost and the communications between different PoPs can be secured using some robust encryption technique.

Acknowledgments

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

References

Akamai's Q4 DoS attack report 2016.https://www.akamai.com/us/en//q4-2016-state-of-the-internet-security-report.pdf, 2016.
Alcorn, J.A., Chow, C.E., 2014. A framework for large-scale modeling and simulation of attacks on an OpenFlow network, 2014 23rd International Conference on Computer Communication and Networks (ICCCN). IEEE, pp. 1–6.
Arbor Network's WISR Report.https://www.arbornetworks.com/images/documents/wisr2016enweb.pdf, 2017.
Behal, S., Kumar, K., 2016a. Trends in validation of DDoS research. Elsevier Proc. Comput. Sci. 85, 7–15.
Behal, S., Kumar, K., 2016b. Measuring the impact of DDoS attacks on web services – a realtime experimentation. Int. J. Comput. Sci. Inf. Secur. 14 (9), 323–330.
Behal, S., Kumar, K., 2017a. Detection of DDoS attacks and flash events using novel information theory metrics. Comput. Netw. 116, 96–110.
Behal, S., Kumar, K., 2017b. Detection of DDoS attacks and flash events using information theory metrics-an empirical investigation. Comput. Commun. 103, 18–28.

Behal, S., Kumar, K., Sachdeva, M., 2017a. Discriminating flash events from DDoS attacks: a comprehensive review. IJ Network Secur. 19 (5), 734–741.
Behal, S., Kumar, K., Sachdeva, M., 2017b. Characterizing DDoS attacks and flash events: review, research gaps and future directions. Comput. Sci. Rev.
Bhandari, A., Sangal, A.L., Kumar, K., 2014. Performance metrics for defense framework against distributed denial of service attacks. Int. J. Netw. Secur. 5 (2), 38–47.
Bhandari, A., Sangal, A.L., Kumar, K., 2016. Characterizing flash events and distributed denial-of-service attacks: an empirical investigation. Secur. Commun. Networks.
Bhatia, S., 2016. Ensemble-based model for DDoS attack detection and flash event separation, Future Technologies Conference (FTC). IEEE, pp. 958–967.
Bhatia, P., Singh, S., 2013. On a new csiszar's f-divergence measure. Cybern. Inf. Technol. 13 (2), 43–57.
Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K., 2014. Network anomaly detection: methods, systems and tools. Commun. Surv. Tutorials, IEEE 16 (1), 303–336.
Bhuyan, M.H., Bhattacharyya, D., Kalita, J., 2016. E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric. Secur. Commun. Networks 9 (16), 3251–3270.
Brent, R.P., Zimmermann, P., 2010. Modern Computer Arithmetic, vol. 18. Cambridge University Press.
CORE Emulator.http://www.nrl.navy.mil/itd/ncs/products/core, 2016.
Cui, Y., Yan, L., Li, S., Xing, H., Pan, W., Zhu, J., Zheng, X., 2016. SD-Anti-DDoS: Fast and efficient ddos defense in software-defined networks. J. Netw. Comput. Appl. 68, 65–79.
Ghorbani, A.A., Lu, W., Tavallaee, M., 2010. Network attacks. In: Network Intrusion Detection and Prevention. Springer, pp. 1–25.
Gulisano, V., Callau-Zori, M., Fu, Z., Jiménez-Peris, R., Papatriantafilou, M., Patiño-Martínez, M., 2015. Stone: a streaming DDoS defense framework. Exp. Syst. Appl. 42 (24), 9620–9633.
Joldzic, O., Djuric, Z., Vuletic, P., 2016. A transparent and scalable anomaly-based DoS detection method. Comput. Netw. 104, 27–42.
Kumar, K., Joshi, R., Singh, K., 2007. An ISP level distributed approach to detect DDoS attacks. In: Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications. Springer, pp. 235–240.
Latest DDoS attack trends Report.https://www.imperva.com/docs/DSIncapsulaTheTop10DDoSAttackTrendsebook.pdf, 2016.
Latest DDoS attack trends Report.http://www.darkreading.com/vulnerabilities-and-threats/2016-ddos-attack-trends-by-the-numbers/d/d-id/1326754?image-number=3, 2016
Ma, X., Chen, Y., 2014. DDoS detection method based on chaos analysis of network traffic entropy. Commun. Lett., IEEE 18 (1), 114–117.
Monosek Network analysis tool.http://www.ncs-in.com, 2016.
Ozcelik, Brooks, R.R., 2015. Deceiving entropy based DoS detection. Comput. Secur. 48, 234–245.
Ranjan, S., Swaminathan, R., Uysal, M., Nucci, A., Knightly, E., 2009. DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. IEEE/ACM Trans. Netw. 17 (1), 26–39.
Recent DDoS Attacks Report,https://www.ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack/, 2016.
Sachdeva, M., Singh, G., Kumar, K., Singh, K., 2010. Measuring the impact of DDoS attacks on web services, Citeseer.
Sachdeva, M., Kumar, K., Singh, G., 2016. A comprehensive approach to discriminate DDoS attacks from flash events. J. Inf. Secur. Appl. 26, 8–22.
Saravanan, R., Shanmuganathan, S., Palanichamy, Y., 2016. Behavior-based detection of application layer distributed denial of service attacks during flash events. Turk. J. Electr. Eng. Comput. Sci. 24 (2), 510–523.
Singh, K., Singh, P., Kumar, K., 2017a. Application layer http-get flood DDoS attacks: research landscape and challenges. Comput. Secur. 65, 344–372.
Singh, K., Singh, P., Kumar, K., 2017b. Impact analysis of application layer ddos attacks on web services: a simulation study. Int. J. Intell. Eng. Inf. 5 (1), 80–100.
Wang, F., Wang, H., Wang, X., Su, J., 2012. A new multistage approach to detect subtle DDoS attacks. Math. Comput. Modell. 55 (1), 198–213.
Wang, C., Miu, T.T., Luo, X., Wang, J., 2018. Skyshield: A sketch-based defense system against application layer DDoS attacks. IEEE Trans. Inf. Forensics Secur. 13 (3), 559–573.
Xiang, Y., Li, K., Zhou, W., 2011. Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans. Inf. Forensics Secur. 6 (2), 426–437.
Yu, S., Zhou, W., 2008. Entropy-based collaborative detection of DDoS attacks on community networks,, Pervasive Computing and Communications, 2008. Sixth Annual IEEE International Conference on PerCom 2008. IEEE, pp. 566–571.
Yu, S., Thapngam, T., Liu, J., Wei, S., Zhou, W., 2009. Discriminating DDoS flows from flash crowds using information distance, NSS'09. Third International Conference on Network and System Security, 2009. IEEE, pp. 351–356.