Discriminating Flash Events from DDoS Attacks: A Comprehensive Review

Sunny Behal[1], Krishan Kumar[2], Monika Sachdeva[1]

(Corresponding author: Sunny Behal)

I. K. Gujral Punjab Technical University[1]
Kapurthala, Punjab 144603, India
(Email: sunnybehal@sbsstc.ac.in)
Information Technology Department, University Institute of Engineering and Technology[2]
Chandigarh, India

(Received June 23, 2016; revised and accepted Sept. 3 & Nov. 15, 2016)

Abstract

Millions of people across the globe access Internet-based applications and web services in their day to day activities. Distributed Denial of Service (DDoS) attack is one of the prominent attacks that cripple down the computing and communication resources of a web server hosting these services and applications. The situation turns further crucial when DDoS attacks are launch during similar looking legitimate traffic called a flash event (FE). Both DDoS attacks and FEs causes a sudden surge in the network traffic leading to delay in the responses from the web server. It often leads to massive financial losses, and thus, require timely actions. This paper presents a comprehensive review that broadly discusses the DDoS and FE problem, and recapitulates the recently published strategies in this field. As part of the work, a pragmatic list of rationales to discriminate the two has been proposed. This list can help the researcher community for better understanding the problem and can provide more effective solutions to the ongoing problem of discriminating DDoS attacks from FEs.

Keywords: DDoS Attack; Discrimination; Flash Event

1 Introduction

A DDoS attack deploys the collection of compromised hosts and results in unavailability of network resources for the intended users. Not directly or permanently damaging the data, but intentionally compromising the availability of the resources is the motive of these attacks [24]. However, the attackers keep on strengthening their proficiency for launching sophisticated DDoS attacks by compromising the freely available credulous hosts. Differentiating DDoS attacks from legitimate traffic is an immense challenge to the network security researchers since the attackers strike with more suave techniques to the victim every time. Almost all types of DDoS attacks are launched using botnets nowadays [13]. The prominent websites are the prime victims of such DDoS attacks. Recently Twitter, Spotify, and Amazon suffer 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 the first quarter of 2016, compared to $24 million for all of 2015 [8]. According to the recent Worldwide Infrastructure Security Report (WISR), the traffic volume of such attacks has amplified to around 600 Gbps in the year 2015 [14].

Apart from detecting of DDoS attacks, there is an another kind of network traffic which is gaining popularity among security researchers, and which causes a denial of service to legitimate users of a web service, is a Flash Event (FE). As per [4], an FE is similar to high-rate DDoS (HR-DDoS) attack wherein thousands of legitimate users try to access a particular computing resource such as a website simultaneously. This sudden surge in legitimate traffic is mainly due to some breaking news happening around the world like the publishing of Olympic schedule or new product launch by companies like Apple, Samsung, etc. It causes the untimely delivery of responses from web service and thus, require immediate action. As there are only a few parametric differences between DDoS attacks and FE traffic, it is very challenging to discriminate the two [6]. The typical network traffic profile of a DDoS attack and an FE is shown in Figure 1(a) and Figure 1(b) respectively.

In this paper, we have presented a comprehensive review of the recent solutions proposed by the fellow researchers to discriminate DDoS attacks from similar looking FEs. We have compared the existing work on a set of

identified attributes. A list of distinct detection metrics and rationales is also provided which has been used to prominently to discriminate the two types of traffic.

The rest of the paper is organized as follows: The Section-2 present the recent flash events, Section-3 describe the review of existing countermeasures for discriminating DDoS attacks from FEs. The Section-4 summarizes the core rationales that can discriminate the two, Section-5 highlights the key research gaps in the existing research, and finally, the last section conclude the paper by highlighting the scope for future work.

2 Recent Flash Events

Many FEs have occurred in recent times which have lead to the untimely responses to the legitimate users. Some of the famous examples of FEs are:

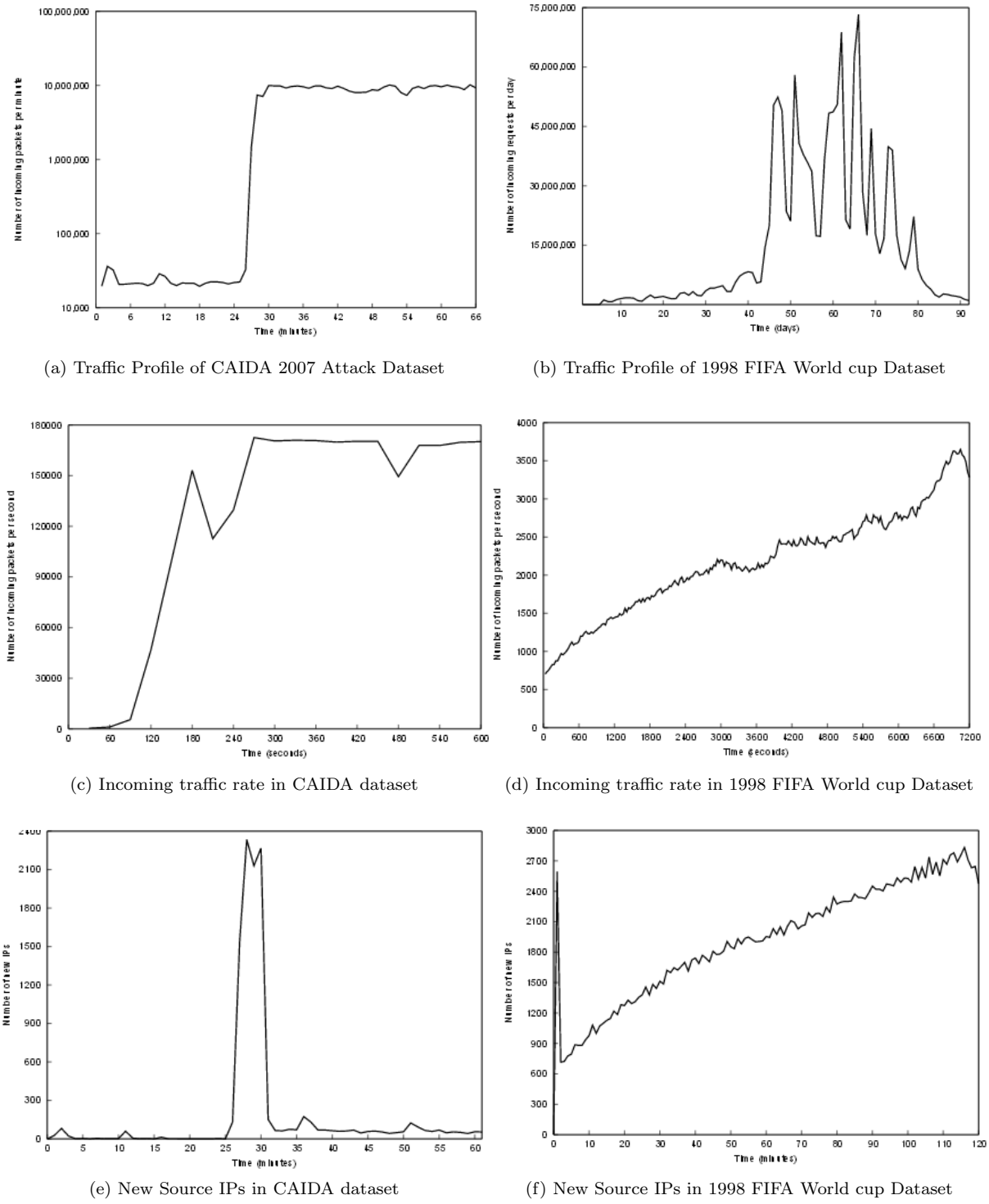
- In August 2016, millions of users simultaneously accessed the Australian census website to fill their personnel details. The lack of sufficient resources on the web server causes the website to crash down [7].
- In February 2016, a new phone was launched with a lowest ever price of INR 251 named as freedom251. It attracted millions of people in a short span of time and lead to the crash down of the web server in few hours.
- In November 2014, the announcements of attractive schemes by leading online shopping vendors like Amazon, Flipkart, Snapdeal, etc. resulted in the shutdown of their shopping website for about an hour.
- In June 2014, a unique breakdown occurred at Microsoft office, when their products like Exchange & Lync, MS Office 360 were not available online. The leading traffic peaks overwhelmed the huge amount of network elements, which results in unavailability of the functionality of Lync for a longer time.
- In September 2013, the launch of iOS7 update by Apple lead to a surge in network traffic from 1.4 Gbps to 6 Gbps when thousands of students at various universities in US began to download it simultaneously.
- In November 2012, an online shopping initiative in Australia clickfrenzy.com.au suffered unexpected surge in the network traffic leading to a dramatic reduction in the response of web server and the website failed within minutes of its launch.
- In October 2012, the news of Sandy storm in the USA result in surge of Internet traffic to around 150% in few hours [4].
- In June 2012, George Takei (the Star Trek hero) broadcast a link about the selling of 'Takei T-shirts' on his Facebook page [4]. This post engages around 2 millions of his fans directing them to a web server having limited resources in no time. High hit rate forces the website to shut down for several hours.
- From 11 June to 11 July 2012, the Twitter website suffered four times increase in tweets per second than an average day due to soccer world-cup news [4].
- In Oct. 2011, the death announcement of Apple's cofounder Steve Jobs result in a surge in the number of hits on his Twitter account, to around 42,000 tweets per second The news websites such as CNN and the Washington Post also experienced slowdowns of their mobile sites as people fascinated to get more information about him.
- In Feb. 1999, the victoria's secret webcast [16] of their first annual online fashion show attract around 1.5 million visitors in a short span of time which lead to dramatic increase in traffic to the host server.
- From 1 May to 24 July 1998, the FIFA world cup website remains overloaded due to the publishing of soccer world-cup event schedule and experience massive increase in web traffic from day 45 to 80 of the event [4].

3 Review of Existing Work

In this section, we have summarized the recent work done in the field of differentiating HR-DDoS attacks from FEs as shown in Table 1 and Table 2. The primary motive of this summary is to highlight the several rationales and detection metrics that have been used by the fellow researchers in recent times. We have compared the existing work on a set of common attributes like the type of packet header features used for detection and discrimination, detection metric, validation technique and datasets used.

Jung et al. [10] proposed a set of fundamental parameters to discriminate a DDoS attack from an FE. They analyzed the HTTP traces compiled from two engaged web servers, one from Playalong website and other from Chile website; and the log files of Code Red worm to propose parameters to distinguish an FE from a DDoS attack. They observed that the request rate per client is more in a DDoS attack than in an FE. The cluster overlapping in an FE is around 42.7% - 82.9% as compared to a DDoS attack, where it is around 0.6%-14%. It means that in the case of an FE, most of the clients have already visited the website earlier, whereas, in a DDoS attack, most of the clients are new.

They observed that the majority of the requests came from 72%-84% of the clusters in a DDoS attack, however, in case an FE, only 10% of the clusters contribute to the majority of the requests. It means that the distribution of clients among clusters is uniform in the case of a DDoS attack whereas it is highly skewed in case an FE. In the event of an FE, the number of requests for a particular requested file follows the Zipf-like distribution, whereas,



(a) Traffic Profile of CAIDA 2007 Attack Dataset

(b) Traffic Profile of 1998 FIFA World cup Dataset

(c) Incoming traffic rate in CAIDA dataset

(d) Incoming traffic rate in 1998 FIFA World cup Dataset

(e) New Source IPs in CAIDA dataset

(f) New Source IPs in 1998 FIFA World cup Dataset

Figure 1: Incoming traffic profiles of CAIDA and FIFA world cup datasets

in a DDoS attack, the requests are more concentrated towards a set of files. However, their proposed parameters did not consider different scenarios of DDoS attacks. A sophisticated attacker can easily mimic the traffic pattern of the network to elude the detection system.

Bhatia et al. [5, 6] computed many parameters like the variation in the rate of new source IPs, change in incoming traffic rate, and the number of requests per source IP to exploit the behavioral difference between an FE and a DDoS attack. They validate their approach by using two real publicly available datasets of 1998 FIFA World Cup and CAIDA DDoS attack 2007. They observe that in a DDoS attack, a sudden burst of incoming traffic is experienced by the victim server within a short time as shown in Figure 1(c) whereas, in the case an FE, there is a gradual increase in incoming traffic to the web server over the time before hitting a maximum, as shown in Figure 1(d).

They found that the victim host sees a significant number of new IPs at the start of a DDoS attack and later, it sees very few new source IP addresses during an ongoing DDOS attack as shown in Figure 1(e). But regularly new source IP addresses are observed by the web server in the case of an FE as shown in Figure 1(f). Among the distinct source IPs, the distribution of traffic is more uniform in the event of a DDoS attack whereas, a small number of requests originate per source IP in case of an FE. They observed that the coefficient of variation is greater than 1 in an FE, which indicates Erlang distribution whereas it is less than 1 in a DDoS attack which signifies hyper-exponential distribution.

They also proposed a mathematical model for an FE with growing flash Phase and declining decay phase. They classify the flash events into predictable, unpredictable and secondary types. They use an information entropy metric to measure this component and observe that the resource entropy start to decrease with the outset of FE and remain to be same for the remaining flash phase. During decay phase, it begins to increase.

Sheng et al. [25] proposed a CALD system to protect the web server against DDoS attacks. They predict HTTP request rate & use a Kalman filter for calibrating the forecast results. They use the assumption that the rapid variation of traffic leads to the markable presence of abnormal traffic. They use entropy as the detection metric. They observe that the mess extent for DDoS is more as compared to FE. They validated their approach using real-time logs from two websites namely www.sina.com and www.taobao.com.

Saravanan et al. [22] proposed a behavioral detection system based on the rationale of flow similarity, client legitimacy and page referred to distinguish between FE and high rate application layer DDoS attacks. They use Hellinger Distance as the detection metric. They observed that the distance metric value is close to zero in the case of a DDoS attack, whereas it is close to one in case the of an FE as shown in Figure 2. They validate their proposed approach by simulating the CAIDA dataset & FIFA world-cup dataset for DDoS attack and FE respectively. Their proposed work results in a small number of false positives and false negatives, with the detection accuracy of around 91%.

Thapngam et al. [23] proposed a behavior-based detection system. They use the rationale of packet arrival rate to discriminate DDoS attack from FE. They compute Pearson's correlation coefficient. They found that in the case of a DDoS attack, there is a high degree of automation along with predictable transmission rate, leading to correlation value close to 0 or 1. They observed that the request rate is unpredictable in the case of an FE which results in correlation value less than 1. For the evaluation of their proposed method, they use the data from 1998 FIFA world cup dataset and project mstream attack.

Prasad et al. [18] proposed three rationales namely the distribution of source IP addresses, access intent and speed of increased-decreased traffic to observe the traffic behavior of FE and DDoS attacks. They proposed an information theoretic Internet threat monitoring (ITM) system consisting of centralized data center and a group of monitors for the modeling and discrimination of FE attack from a DDoS attack.

Their proposed system work in two phases. In the first phase, they detect the ongoing attack by computing the entropy values and in the second phase, they discriminate the FE and DDoS attack using variation in entropy values. They deploy their proposed system on the Internet with the botnet.

Shui et al. [28] observed that the attack tools are usually similar for one botnet with the same pre-built program. In a single botnet, all the bots follow a single command by the bot master to start an attack session. In a botnet, the number of active bots is usually less than the number of legitimate users. So, to mimic a flash event, the active bots generate a significant number of packets which result in small standard deviation among attack flows than flash flows.

They found that the flow similarity in DDoS is much more than an FE. They propose a discrimination algorithm which computes flow correlation coefficient among suspicious flows. They validate their approach using a real dataset of 1998 FIFA World Cup for FE. A real DDoS attack tool called mstream is used to generate DDoS attack data.

Hakem et al. [3] proposed a connection-score scheme to detect application layer DDoS attacks. Their proposed system computes the statistical attributes such as download rate, request rate, uptime, downtime, classification of the page type, page popularity, hyperlink click rate, and hyperlink depth. They compute the values of these attributes to set the baseline behavior of the network, and scores are assigned to the various connections accordingly. The connections which get the lowest score are the malicious connections, and bottleneck resources are taken back from them by the server. They perform the experiment using Emulab using real traces of ClarkNet server. They observed that the Connection-Score scheme could tackle the application layer DDoS attacks efficiently as

Table 1: Comparison of related work for discriminating DDoS attacks and an FE

Sr. No.	Author/Year	Parameters	Detection Metric	Validation Technique	Datasets Used
1.	Saravanan et al. [22] / 2016	1. Flow Similarity 2. Page Referred 3. Client Legitimacy	Hellinger Distance	Simulation	1998 FIFA world-cup for FE CAIDA 2007 for DDoS attack
2.	Abhinav et.al[4] /2016	1. Page Access Order 2. Number of Source IPs 3. Flow Similarity 4. No. of Requests per IP 5. Unique Source IPs	Entropy	Simulation	1998 FIFA world-cup for FE CAIDA 2007 for DDoS attack
3.	Sachdeva et.al [21] /2014	1. Source IPs 2. Traffic Clusters	Entropy	Simulation Emulation	1998 FIFA world-cup for FE CAIDA 2007 for DDoS attack
4.	Prasad et.al [18] / 2013	1. Source IP Distribution 2. Access Intents 3. Change in Traffic Rate	Entropy	Realtime	–
5.	Tongguang et.al [15] /2013	1. HTTP-GET requests per Source IP	Entropy	Simulation	1998 FIFA world-cup for FE myDOOM botnet for DDoS attack
6.	Katiyar et.al[11] /2013	1. Source IP and port 2. Destination IP and port	Entropy	Simulation	–
7.	Yu et.al [28] /2012	1. Flow Similarity	Correlation coefficient	Simulation	1998 FIFA world-cup for FE mstream attack tool for DDoS attack
8.	Beitollahi et.al [3] /2012	1. Uptime and Downtime 2. Request rate and Download rate 3. Page popularity and Classification 4. Hyperlink depth and Click rate	Entropy	Emulation	Clarknet server logs
9.	Bhatia et.al [5] /2012	1. Volume of Incoming traffic 2. Number of Source IPs 3. Resource accessed	Entropy	Emulation	1998 FIFA world-cup for FE CAIDA 2007 for DDoS attack
10.	Thapngam et al. [23] /2011	1. Packet arrival rate	Correlation coefficient	Simulation	1998 FIFA world-cup for FE mstream attack tool for DDoS attack
11.	Wen et.al [25] /2010	1. Distribution of Source IPs 2. Page access order	Entropy	Realtime	NLANR Auckland VIII for FE www.sina.com for DDoS attack www.taobao.com for DDoS attack
12.	Yu et.al [27] /2009	1. Flow Similarity	Jefrrey Distance Sibson Distance Hellinger Distance	Simulation	NLANR Auckland VIII for FE MIT Lincoln for DDoS attack
13.	Li et.al[12] /2009	1. Source IPs Distribution 2. Access Intent 3. Traffic Rate	Total Variation Correlation coefficient		HTTP logs for FE MIT Lincoln for DDoS attack
14.	Oikonomou et.al[17] /2009	1. Access Content 2. Request Dynamics 3. Ability to ignore invisible content	Probability matrix	Simulation	Synthetically generated logs for FE Web server logs for DDoS
15.	Yatagai et.al [26] /2007	1. Page Access Order 2. Browsing Time 3. Page information	correlation metric	Realtime	–
16.	J.Jung et al. [10] / 2002	1. Traffic pattern 2. Cluster characteristics 3. File References	Entropy	Realtime	–

compared to existing methods.

Shui Yu et al. [27] proposed a detection algorithm for the discrimination of a DDoS and an FE. They compute information distance between different kinds of network flows, with the idea that the DDoS flows are strongly alike as compared to an FE because of similar pre-built programs executed by the attackers. They validate their approach by simulating the real datasets of NLANR PMA Auckland dataset for FE and MIT LLS DDOS 1.0 intrusion dataset for a DDoS attack.

They count the number of packets destined to a web server. Their proposed detection algorithm gives detection accuracy of 65% while discriminating DDoS and FE flows. They compute Sibson distance, Jeffrey distance, and the Hellinger distance and prove that the Sibson distance metric is better as compared to the other detection metrics for discriminating a DDoS attack from an FE.

Yatagai et al. [26] modeled an HTTP-GET flood detection technique by taking into account the page access behavior. They propose two detection algorithms. The first algorithm deals with the web page browsing order. If there are some IP addresses with the same browsing order, then, the GET requests from those IP addresses are dropped. Because it is assumed that in case a DDoS attack, all the participated attackers will generate an equal number of GET requests. The second algorithm computes the correlation between browsing time and page information size.

They found that in the case of regular clients, the browsing time increases in proportion to the information size. They deployed the proposed detection technique at the network gateway to computing the number of false positives and false negatives. They observed that when we give high priority to client services, then the first algorithm provides better results whereas, when the detection rate of HTTP-GET flood attack is given more priority, then the second algorithm is more appropriate.

Tongguang et al. [15] proposed a novel concept based on the entropy of HTTP-GET requests per source IP (HRPI) for the discrimination of AL-DDoS attack from legitimate traffic. They found that the HRPI value dramatically drops in case of a DDoS attack, however, in the event of an FE, there is an abnormal increase in HRPI of the network.

They proposed a two-step detection scheme. In the first step, the approximation of the Adaptive AutoRegressive(AAR) model to transform the HRPI time series to multidimensional vector series (MVS). Then, the support vector machine (SVM) is applied to classify AAR parameters to identify the attack. To validate the proposed approach, they simulate the MyDoom worm for application layer DDoS attack and use FIFA world-cup dataset for FE traffic. They observed that their approach could identify the DDoS attack traffic and FE with high precision, efficiency, and flexibility.

Li et al. [12] proposed a detection method using proba-

bility metrics for the discrimination of an FE and a DDoS attack. They compute a composite probability metric of total variation and similarity coefficient. The detection mechanism comprises a flow anomaly detector that identifies the specified router for observing the anomalies in incoming network flows. The flow distribution estimator estimates the distribution of sampled flows using pre-defined characteristics and calculates the total variation and similarity coefficient values in parallel of the two flows. The decision device makes the distinction between FE, DDoS, and a legitimate flow based on the value of detection metric and decides the type of anomaly.

To validate their approach, they use the legitimate and attack profile from the real dataset of MIT Lincoln Laboratory. For FE traffic, they use the HTTP log dataset from a busy server.

Oikonomou et al. [17] analyzed the human behavior for the discrimination of DDoS bots from human users. Their proposed detection scheme is based on three models. A request dynamic model for capturing the human's interaction with the server to detect bot aggressiveness. A request semantic model for capturing the common human request pattern to mark the bots that make different sequences. A deception model that model human invisible attributes into server replies. The addresses that request for these items are marked blacklisted. To validate their proposed approach, they use a collection of web server logs, and synthetically generated logs of FE bots. Their proposed approach gives detection accuracy of 95%.

Katiyar et al. [11] proposed a novel traceback mechanism based on entropy variations to discriminate a DDoS attack from an FE. They compute entropies of source IP, source port, destination IP and destination port. It is assumed that the router stores the entropy values of each flow during the non-attack period. Once a DDoS or an FE is identified, it starts to trace the source of the attack. They perform a simulation based experiment to validate their proposed approach. They evaluate traceback time, packet delivery ratio (PDR), and throughput based on entropy. They observed that the PDR under attack is small in comparison to an FE or a non-attack case. Throughput is maximum in case of non-attack case, nearly the same in an FE but it decreases in a DDoS attack.

Abhinav et al. [4] proposed a taxonomy of FEs based on the nature of events occurred, traffic generated, geographical distribution, the signature of the network, duration, and the shock level. They discriminate DDoS attacks from FEs by computing a set of packet header features like new source IPs, change in request rate, the number of distinct source IPs, page access entropy, the similarity between flows, and distribution of request rate among source IPs. They used FIFA World Cup 1998 dataset for FE, CAIDA dataset for simulating application-layer DDoS attack for validating their approach. They used curl-loader and Bonesi DDoS attack tool to simulate different scenarios of DDoS attacks.

Sachdeva et al. [19] used cluster entropy to discriminate FEs from DDoS attacks. Their detection approach is based on the idea that during an FE, most of the requests comes from the already visited clients. They calculate the entropy of traffic clusters and source IPs. They observed that there is the significant increase in source IP entropy and minor variation in traffic cluster entropy in the case of an FE whereas in a DDoS attack, there is a substantial increase in source IP entropy as well as traffic cluster entropy. They perform emulation based experiments on DETER testbed, CAIDA dataset, and FIFA world-cup dataset to validate their approach.

4 Key Rationales to Discriminate DDoS Attacks from FEs

After the extensive review of existing research, we have derived a list of rationales that can be used to distinguish DDoS attacks from FEs as shown in Table 2.

5 Research Gaps

Today, the major thrust area in the field of DDoS attack detection is to distinguish the attack traffic from similar looking FEs. An FE occurs when a server experiences a sudden surge in the number of requests from legitimate clients. The FEs share many common characteristics with DDoS attacks such as a substantial increase in the incoming network traffic, the overloading of the servers providing the services, and degradation in the delivery of services. We have been able to find the following research gaps after the extensive review of existing research in discriminating DDoS attacks from FEs.

- Most of the researchers have validated their proposed approaches using publically available real datasets. They have mostly used 1998 FIFA world-cup dataset for FE traffic. This dataset seems to be obsolete if we consider the high-rate network traffic of nowadays fast growing networks but still, the pattern of GET requests towards a web server is still the same. However, the lack of availability of other related real datasets makes the validation a nightmare for the researchers.

- Most of the proposed solutions have used separate datasets for DDoS attacks and FE traffic. However, in reality, the DDoS attacks are often launched during FEs which makes the problem of discrimination very challenging. There are no real datasets available which contain the mixture of two types of traffic.

- Some researchers have tried to synthetically generate datasets using simulation and emulation based experiments [3, 4, 6, 17, 20] using a set of benchmark DDoS attack tools [2] but these datasets lack the capturing of relevant traffic features. Ideally, the captured network trace should contain the mixture of realistic background traffic and attack traffic in

Table 2: Summary of rationales to discriminate DDoS & FEs

Sr. No.	Rationales	DDoS	FE
1.	Flow Similarity	High	Low
2.	Web Pages Referred	Random	Hot pages only
3.	Client Legitimacy	unknown or new	Mostly well known
4.	Network Traffic Volume	Sharp increase and decrease	Gradual increase and decrease
5.	Change in Rate of New Source IPs	High in initial stage	High
6.	Distribution of clients	Uniform	Skewed
7.	Number of Distinct Clusters	Less and overlapped	Relatively more and new clusters
8.	Request-rate per source IP	More	Low
9.	Access Intents	To crash the server	Legitimate
10.	Distribution of source IPs	Limited with the availability of bots	Dispersive
11.	Correlation between browsing time & information size on web page	No effect	Increase
12.	Packet Delivery Ratio(PDR)	Low	High
13.	Throughput	Decreases	Maximum
14.	Web page browsing order	Same	Random
15.	Ratio of Entropy of source IPs and URL accessed	High	Low
16.	Duration of Traffic per Client	Long	Short
17.	Two way traffic	Low	High
18.	Coefficient of Variation	less than 1	greater than 1

appropriate proportion, and should not be biased towards a particular type of traffic. It is tough to ensure a proper mixture of normal and attack traffic in a real experiment driven dataset because there is no known formula to model Internet traffic correctly [9].

These research gaps clearly shows that it is very challenging to validate the proposed solutions to discriminate HR-DDoS attacks from FEs in the absence of latest publically available real datasets. The availability of such realistic datasets that possesses the mixture of an appropriate attack traffic, non-attack traffic, and normal background traffic, is the need of the hour [1].

6 Conclusion

The detection of DDoS attacks is a challenging issue in the network security research. The problem is further magnified when such attacks are launched during a similar looking flash events (FEs). In this paper, we have comprehensively reviewed the prominent existing work done by the fellow researchers in the domain of discriminating DDoS attacks from FEs. We have also summarized a list of core rationales which have been used as detection metrics. This pragmatic list can further be extended and used for the future research in this domain to provide better practical solutions. As part of the future work, we shall propose an efficient detection and mitigation framework which would discriminate the DDoS attacks from FEs with a low false positive rate.

References

[1] S. Behal and K. Kumar, "Trends in validation of DDoS research," *Procedia Computer Science*, vol. 85, pp. 7–15, 2016.

[2] S. Behal and K. Kumar, "Characterization and comparison of DDoS attack tools and traffic generators- a review," *International Journal of Network Security*, vol. 19, pp. 383–393, May 2017.

[3] H. Beitollahi and G. Deconinck, "Tackling application-layer DDoS attacks," *Procedia Computer Science*, vol. 10, pp. 432–441, 2012.

[4] A. Bhandari, A. L. Sangal, and K. Kumar, "Characterizing flash events and distributed denial-of-service attacks: an empirical investigation," *Security and Communication Networks*, 2016.

[5] S. Bhatia, G. Mohay, D. Schmidt, and A. Tickle, "Modelling web-server flash events," in *11th IEEE international symposium on Network computing and applications (NCA'12)*, pp. 79–86, 2012.

[6] S. Bhatia, G. Mohay, A. Tickle, and E. Ahmed, "Parametric differences between a real-world distributed denial-of-service attack and a flash event," in *Sixth IEEE International Conference on Availability, Reliability and Security (ARES'11)*, pp. 210–217, 2011.

[7] D. Braue, *Attack on Australian Census Site Didn't Register on Global DDoS Sensors*, Aug. 11, 2016. (`http://www.cso.com.au/article/604910/attack-australian-census-site`)

[8] DDoS Attacks Net, *Recent DDoS Attacks*, Oct. 21, 2016. (`https://www.ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack/`)

[9] S. Floyd and V. Paxson, "Difficulties in simulating the internet," *IEEE/ACM Transactions on Networking*, vol. 9, no. 4, pp. 392–403, 2001.

[10] J. Jung, B. Krishnamurthy, and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for cdns and web sites," in *Proceedings of the 11th International Conference on World Wide Web*, pp. 293–304, 2002.

[11] P. Katiyar, U. Kumarn, and S. Balakrishanan, "Detection and discrimination of DDoS attacks from flash crowd using entropy variations," *International Journal of Engineering and Technology*, vol. 5, no. 4, pp. 3514–3519, 2013.

[12] K. Li, W. Zhou, P. Li, J. Hai, and J. Liu, "Distinguishing DDoS attacks from flash crowds using probability metrics," in *Third International Conference on Network and System Security (NSS'09)*, pp. 9–17, 2009.

[13] M. Mahmoud, M. Nir, and A. Matrawy, "A survey on botnet architectures, detection and defences.," *International Journal of Network Security*, vol. 17, no. 3, pp. 264–281, 2015.

[14] Arbor Networks, *DDoS Attack Report*, 2015.

[15] T. Ni, X. Gu, H. Wang, and Y. Li, "Real-time detection of application-layer DDoS attack using time series analysis," *Journal of Control Science and Engineering*, vol. 2013, pp. 4, 2013.

[16] K. Ohlson, *Victoria Secret Webcast of Their First Annual Online Show*, Feb. 5, 1999. (`http://edition.cnn.com/TECH/computing/9902/05/vicweb.idg/`)

[17] G. Oikonomou and J. Mirkovic, "Modeling human behavior for defense against flash-crowd attacks," in *IEEE International Conference on Communications (ICC'09)*, pp. 1–6, 2009.

[18] K. Prasad, A. Reddy, and K. Rao, "Discriminating DDoS attack traffic from flash crowds on internet threat monitors (ITM) using entropy variations," *African Journal of Computing & ICT*, vol. 6, no. 2, 2013.

[19] M. Sachdeva and K. Kumar, "A traffic cluster entropy based approach to distinguish DDoS attacks from flash event using deter testbed," *ISRN Communications and Networking*, vol. 2014, 2014.

[20] M. Sachdeva, K. Kumar, and G. Singh, "A comprehensive approach to discriminate DDoS attacks from flash events," *Journal of Information Security and Applications*, vol. 26, pp. 8–22, 2016.

[21] M. Sachdeva, G. Singh, and K. Kumar, "An emulation based impact analysis of DDoS attacks on web services during flash events," in *2nd International Conference on Computer and Communication Technology (ICCCT'11)*, pp. 479–484, 2011.

[22] R. Saravanan, S. Shanmuganathan, and Y. Palanichamy, "Behavior based detection of application layer distributed denial of service attacks during flash events," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 24, no. 12, pp. 510–523, 2016.

[23] T. Thapngam, S. Yu, W. Zhou, and G. Beliakov, "Discriminating ddos attack traffic from flash crowd through packet arrival patterns," in *IEEE International Conference on Computer Communications Workshops*, pp. 952–957, 2011.

[24] M. Uma and G. Padmavathi, "A survey on various cyber attacks and their classification.," *International Journal of Network Security*, vol. 15, no. 5, pp. 390–396, 2013.

[25] S. Wen, W. Jia, W. Zhou, W. Zhou, and C. Xu, "Cald: Surviving various application-layer DDoS attacks that mimic flash crowd," in *4th International Conference on Network and System Security (NSS'10)*, pp. 247–254, 2010.

[26] T. Yatagai, T. Isohara, and I. Sasase, "Detection of http-get flood attack based on analysis of page access behavior," in *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PacRim'07)*, pp. 232–235, 2007.

[27] S. Yu, T. Thapngam, J. Liu, S. Wei, and W. Zhou, "Discriminating DDoS flows from flash crowds using information distance," in *Proceedings of the third International Conference on Network and System Security (NSS'09)*, pp. 351–356, 2009.

[28] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1073–1080, 2012.

Biography

Sunny Behal has done Bachelor of Technology in Computer Science and Engineering from SBS State Technical Campus, Ferozepur, Punjab, India in 2002. He finished his Masters in Computer Science and Engineering from Guru Nanak Dev Engineering College, Ludhiana, Punjab, India in 2010. Currently, He is full time Ph.D. Research Scholar at SBS State Technical Campus, Ferozepur. His research interests includes Botnet detection, DDoS attacks, Information and Network Security. He has published more than 40 Research papers in different International Journals and Conferences of repute.

Krishan Kumar has done Bachelor of Technology in Computer Science and Engineering from National Institute of Technology, Hamirpur in 1995. He finished his Masters in Software Systems from BITS Pilani in 2001. He finished his Ph. D. from Department of Electronics and Computer Engineering at Indian Institute of Technology, Roorkee in 2008. His general research interests are in the areas of Information Security and Computer Networks. He has published around 200+ research papers in different International Journals and Conferences of Repute including more than 500 citations.

Monika Sachdeva has done Bachelor of Technology in Computer Science and Engineering from National Institute of Technology, Jalandhar in 1997. She finished her Masters in Software Systems from BITS Pilani in 2002. She finished her Ph. D. from Department of Computer Science and Engineering at Guru Nanak Dev University, Amritsar, Punjab, India in 2012. Currently, she is working as Associate Professor in CSE Department at I.K.G. Punjab Technical University, Kapurthala, Punjab, India. His general research Interests are in the areas of Network Security and distributed computing. She has published more than 100 Research papers in different International Journals and Conferences.