Int. j. inf. tecnol. (February 2023) 15(2):955–964
https://doi.org/10.1007/s41870-022-01097-3

ORIGINAL RESEARCH

A behavioral model for characterizing flooding distributed denial of service attacks

Oreoluwa Tinubu[1] · **Adesina Sodiya**[1] · **Olusegun Ojesanmi**[1]

Received: 2 June 2022 / Accepted: 9 September 2022 / Published online: 23 September 2022

Abstract The availability of networks, servers, applications and websites is greatly impaired by Distributed Denial of Service (DDoS) attacks. DDoS attacks pose major threats to IT-based systems. Understanding the behaviors of the attack flows in networks is pertinent for the development of effective defense systems. This study presents a behavioral model for characterizing flows in flooding DDoS attacks. A network traffic-based analysis was carried out for the identification of anomaly behaviors of attack flows. Through the behavioral characteristics observed, three distinct features namely the Flow rate, Arrival rate and Inter-arrival time of packets were identified. A multidirectional relationship between the behavioral features and rate of exhaustion of the target's resources is thus established. Furthermore, we verified the feasibility of the features in distinguishing legitimate flows from DDoS attacks and even Flash Events. The network environment was simulated in NS2 such that attack flows, normal network flows and Flash Events were generated in the network. Finally, real-world publicly available datasets as the latest CICDDoS2019 and 1998 FIFA World Cup were used for the validation of the model through statistical comparisons.

Keywords DDoS attacks · Flash events · Characterization · Network flow · Features

✉ Oreoluwa Tinubu
tinubuco@funaab.edu.ng

1 Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria

1 Introduction

Availability is a critical issue in modern distributed systems. Distributed Denial of Service (DDoS) attacks are coordinated attacks against the availability of services in networks, being launched via several compromised computing systems [31]. DDoS attacks are launched to deplete connectivity and processing resources of the victim, causing partial or total unavailability of services to genuine users [41]. The attackers access databases, servers and network applications remotely [25]. One of the earlier launched DDoS attacks was against Yahoo in the year 2000, which caused a total unavailability of services for a significant period of time and severe financial losses [42].

A DDoS attack comprises of the Attacker, Agents, Bots and the Victim. The attacker utilizes many compromised machines (bots) through some agents to launch attacks on the target system. The use of botnets has emerged as a major approach of launching sophisticated DDoS attacks [22, 38]. A botnet comprises of a large number of malware-infected devices which are remotely controlled by a malicious user [16]. Typically, the botmaster sends commands to each bot in his botnet to commence an attack session. Often, the IP addresses of the bots are spoofed, making it extremely challenging for trace-back mechanisms.

DDoS attacks are classified into two (2) essential types; Flooding-based and Vulnerability-based attacks [19]. Flooding-based attacks use huge volumes of vague requests to exhaust vital resources of the victim [5]. They are aimed at bandwidth depletion or memory exhaustion, such that victims are incapable of providing services to authorized users [17]. On the other hand, Vulnerability-based attacks exploit one or more flaws in an application or a bug in the software that implements the target system. They exhaust excessive amount of resources of the victim using a few crafted requests [1].

Flooding-based DDoS attacks can be extremely severe, as to abruptly drain all network resources within a short time [31]. They can be executed in Network/Transport and Application layers using several protocols, such as UDP, TCP, ICMP and HTTP [30]. The most frequent DDoS attacks occur over the User Datagram Protocol (UDP) of network systems [14]. These attacks cause devastating effects such as service interruption, degradation of service, customer dissatisfaction, reputational damages, huge financial losses, security implications, breach of contracts, amongst others. Notably, severe flooding attacks have been launched against many popular organizations, including websites as Twitter, Netflix, The New York Times, CNN, Amazon, Yahoo, BBC, eBay, etc.

Understanding the trends of Distributed Denial of Service (DDoS) attacks and their attack strategies is an important phase in developing effective defenses [37]. The design of an accurate detection system for flooding attacks relies on an in-depth understanding of the behaviors of the attackers in networks. Network analytics comprises of traffic monitoring and traffic classification [12]. However, most existing detection methods cannot accurately distinguish attack flows from benign flows. Consequently, a high false positive remains a lingering challenge of current works. The use of relevant features for detecting malicious flows influences the accuracy of defense systems. Using a single flow feature results in ineffective detection while selecting too many features exhausts more network resources with high computational complexity.

In this study, a behavioral model for characterizing flows in flooding-based DDoS attacks is presented. By a network analysis, three distinct traffic features namely the flow rate, arrival rate and inter-arrival time of packets were identified for characterizing attack flows, which can distinguish flooding DDoS attacks from legitimate flows. These relevant features serve as inputs to any DDoS detection mechanism.

The remainder of this study is organized as follows: In Sect. 2, an overview of related literature is presented. Section 3 details on the behavioral model for flooding-based DDoS attacks. In Sect. 4, the experimental evaluation of the developed model is explained. Section 5 concludes and summarizes the work with suggestions for further research.

2 Background and related work

A major threat to cybersecurity is the Distributed Denial of Service (DDoS) attacks [39]. DDoS attacks are characterized by malicious behaviors which aim to deplete network and/or system resources of the victim. DDoS attacks seek to disrupt applications, web-based services or networks [11]. Flooding DDoS attacks are typically launched by a network of remotely manipulated and well-coordinated bots which are simultaneously and continuously forwarding huge amounts of traffic to the target system [39]. The packets often arrive in high quantities consuming the victim's critical resources as network bandwidth, I/O bandwidth, memory, disk space, CPU, etc.

A Flash Event (FE) behaves similarly to a Distributed Denial of Service (DDoS) attack. Behal and Kumar [2] likened an FE to a high-rate DDoS (HR-DDoS) attack. In Flash Events, several genuine users concurrently access a particular service, resulting in a reduced performance of the server and unavailability of services [4]. Often, the surge in legitimate traffic results from popular events as the Olympics, new product launch, breaking news and unpredicted events such as natural disasters. However, as an FE originates from an overload by genuine users, it can be resolved through adequate load balancing and provisioning to accommodate more legitimate requests.

Meanwhile, some sophisticated DDoS attackers mimic the patterns of Flash Events to evade detection. As only a few differences exist between the traffics of DDoS and FE, differentiating them is challenging [36]. Several research efforts have been made towards distinguishing FE from DDoS attacks. Some works have employed entropy-based methods to differentiate the traffics of FE and DDoS attacks [2–4, 7, 8, 14, 18, 26, 27]. Besides, information theory-based metrics have been proposed in literatures for the detection of DDoS attacks [6, 10, 13, 21, 23, 28, 32]. However, these information-theory approaches suffer low detection accuracy with high computational overheads.

As DDoS attack sources are being programmed and the bots operate according to specified attack functions, detection based on the traffic's anomaly behaviors is feasible. In literature, several features have been employed for characterizing the flows of DDoS attacks. For instance, a study by Tan et al. [33] used the stream duration and average byte stream rate as primary features to differentiate normal flows from attack flows. In [29], the similarity of flows, page referred and legitimacy were used to differentiate FE from DDoS attacks. Zhou et al. [43] used changes in the number of packets for identifying malicious flows. In a study by [16], the source IP and packet rates were utilized. Also, Nugraha et al. [24] characterized SYN flood attacks by the number of packets.

In Lopez et al. [20], three features such as the total length of backward packets, total length of forward packets and average packet size, were proposed for the identification of compromised network flows. The packet's arrival patterns were used in [34] to differentiate DDoS attack traffic from flash crowd. Yu et al. [40] utilized the flow correlation coefficient to classify DDoS attacks and FE. Tinubu et al. [35] employed features as the session rate, rate of requests, frequency of requests on a web page and time interval between successive requests to analyze user's behaviors in HTTP GET flood attacks. In [15], the average duration of flow, average byte of flow and change in speed of flow were utilized for the identification of Flash Events and DDoS attacks in SDN. In [36], the flow features selected to distinguish between DDoS attacks and FE are the new source IPs, number of source IPs and packets inter-arrival time. Similarly, Dayal and Srivastava [9] used features such as the number of flows, flow rate, entropy of protocol, entropy of source IP and entropy of destination IP to identify and categorize possibilities of flooding DDoS attacks in SDN.

From prior researches, it has been observed that a high false positive rate is a consistent occurrence in behavioral detection systems for DDoS attacks. Most of the existing works focus majorly on the number of packets and some other irrelevant features, without considering the time-related behavioral characteristics of packets in the attack flows. This results in misclassifications with high false positives and negatives. Thus, this work is geared towards addressing limitations in research by identifying the relevant features for the classification of flooding DDoS attacks.

3 Behavioral model

Attacker's behaviors can be established through monitoring different attack traffic launched by various botnet families on networks. Network flows are the basic data structures that can be used to analyze botnet traffic. A flow is a stream of packets passing through the same router with common source and destination IP addresses, source and destination ports and protocol. While the source IPs can be spoofed, the network flows cannot be altered by attackers.

By the analysis of attack traffic from several botnets, the following important behavioral characteristics are established:

(1) An aggressive behavior is typical of flooding-based Distributed Denial of Service Attacks (DDoS) traffic. Attack sources continuously flood the victim with useless flows, without awaiting corresponding responses from the target server. A sudden surge occurs in the traffic flow over a relatively short period, as the attacker simultaneously generates traffic through its compromised bots.

(2) The distribution of source IP addresses of attackers differs from those of the legitimate users. Legitimate users originate randomly from an Internet community with a dispersive distribution of IP addresses. These IP addresses when aggregated are subject to a Normal distribution. Contrarily, for attackers, the distribution of source IP addresses is concentrated relatively according to the number of bots, with huge number of packets per IP address. These IP addresses when aggregated are subject to a Poisson distribution.

(3) Attack flows are similar to one another, as its nodes execute a common program logic to launch an automated attack. These flows possess very close values of standard deviation when aggregated, compared to those of legitimate traffic.

3.1 Feature set selection

From the behavioral characteristics observed of the attack flows, three (3) unique features are identified for the detection of flooding-based DDoS attacks. These features are considered as the most important for detecting the attack flows. The features are the Flow rate, Arrival rate and Inter-arrival time of packets. The flow rate of packets is its sending rate, measured in bits/seconds. The arrival rate is the number of arrivals per unit time, measured in packet/seconds. The packets inter-arrival time represents the difference in time in the arrival of any two successive packets. This time ranges from milliseconds to minutes. The packet's time interval feature allows for a time prediction of the next anticipated attack.

Figure 1 depicts the behavioral framework of flooding DDoS attacks. The prevalent behavioral characteristics of attack flows are presented, with their corresponding flow features. Also, the proposed characterization Algorithm 1 shows the behaviors of the flow features.

Algorithm 1: DDoS Characterization Algorithm

Input: *Malicious network flows from several botnets M*
Output: *Flow features F*

```
Initialize Threshold Values = V_f
Number of packets of the network flow = n
Number of source IP addresses = s
Number of packets per IP address = p
Number of bytes per IP address = b
Total time of analysis = T
Time interval of received packets = t_i
  for (n = 0, n < T, n++)
      s = count(IP_address)
      p = count(packets per IP_address)
      b = count (bytes per IP_address)
          if (b > V_f)
              if (p > V_f) then
                  set arrival rate = high;
              else
                  set arrival rate = low;
              end if;
          set flow rate = high;
          else
              set flow rate = low;
          end if;
          if (t_i > V_f) then
              set packet interarrival time = high;
          else
              set packet interarrival time = low;
          end if;
  end for;
```

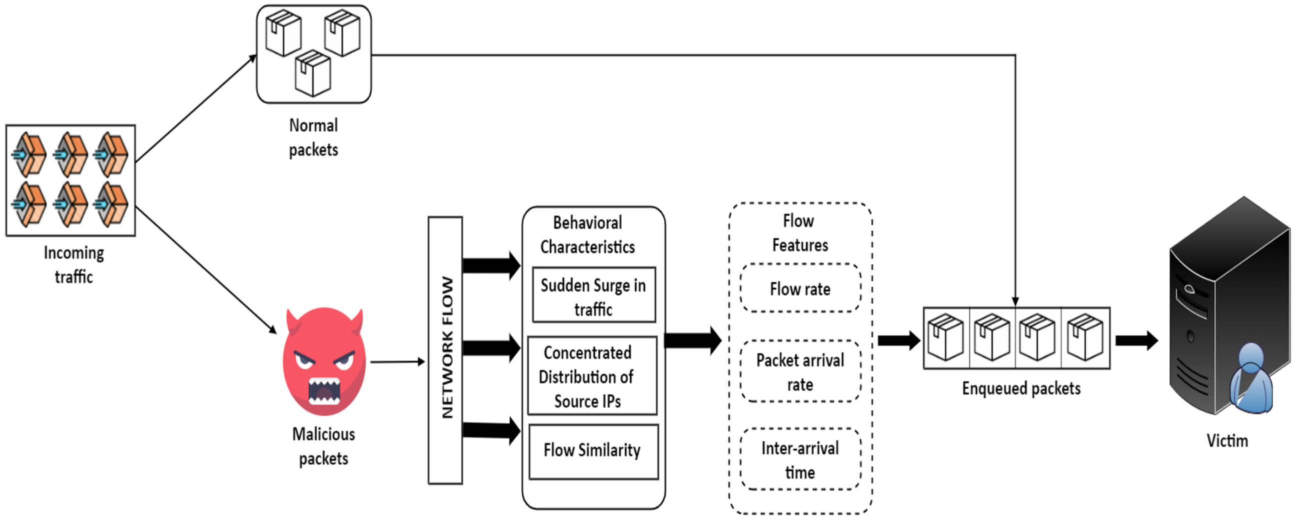


Fig. 1 Behavioral framework of flooding-based DDoS attacks

3.2 Impact of the features on the victim

Equations 1–5 establish the relationship between the features in the behavioral model and the rate of exhaustion of the victim's resources.

Considering the number of packets arriving at the victim as a random process.

Based on the similarity of attack flows, the packet arrivals are modeled as a Poisson process with rate λ.

Let $N(t)$ represent the active network flows at time t,

$$N(t) = \{F_1(t), F_2(t), F_3(t), \dots, F_n(t)\}. \quad (1)$$

Let $p(t)$ represent the number of packets of the network flow $F_n(t)$,

Let A represent a sample set of arrival rates of packets,

$$A = (\{\lambda_p\} : p \in \mathbb{Z}). \quad (2)$$

Table 1 Details of the relevant features in attack and normal scenarios

DDoS traffic			Normal traffic			Flash Event traffic		
Inter-arrival time	Arrival rate	Flow rate	Inter-arrival time	Arrival rate	Flow rate	Inter-arrival time	Arrival rate	Flow rate
0.00098759	925561.0807	90844432368.84	4.8019	97.063	4845.9444	1.9516515	84.6765	8313.0424
0.00103688	1071896.145	94225516020.96	6.7414	37.9894	7564.8417	1.01795849	85.237	8455.5672
0.00106611	1070978.789	90905422970.41	0.9014	5.6011	2230.0658	2.33875001	78.7204	7975.3932
0.0010505	1050347.99	91450977035.60	2.7841	57.6817	2857.4568	2.5881653	79.4212	8484.5881
0.00098693	1095264.532	108710695214.89	6.7423	70.9529	4835.4306	1.61015836	81.7716	8650.3109
0.00109792	1054021.517	100435207061.46	1.2118	52.2668	2468.0526	1.42547176	77.4437	8954.2954
0.00107845	997020.5468	90689852077.63	6.3561	30.5092	1770.7781	1.13762808	74.6567	8219.641
0.00095963	985054.415	104749358939.79	5.8572	25.9264	2583.8513	2.37217723	85.9485	8536.7633
0.00106273	909689.6957	106653840986.50	2.6061	78.5904	3887.2859	1.76270567	78.6657	8994.9512
0.00106516	950600.1128	109564834779.92	8.0954	40.1344	7078.5266	1.3061699	77.1328	8417.7725
0.00104391	990198.4642	103588810527.71	7.0414	19.5184	9131.4724	1.78331786	86.0062	8114.5683
0.00101665	1016336.57	106643614412.33	5.2129	44.7179	8032.1902	2.26245161	88.2999	8937.785
0.00092009	1094709.955	99687784555.38	1.9922	50.4533	7054.1259	2.4780667	77.1822	8416.5843
0.00107667	904042.8749	104601839043.07	9.1866	27.7428	1553.5361	1.97723651	86.0423	7501.2026
0.00097778	1000435.599	90606126457.17	4.2177	14.8792	5615.8218	2.48237799	87.0527	7605.9863
0.00105194	1003229.059	95601104241.08	0.802	80.5871	982.4578	1.62456301	81.8351	8240.0181
0.00107184	985162.426	98438928131.74	0.2996	32.6172	9572.3338	2.49329992	82.8931	7965.319
0.00099459	902928.0913	109834532393.04	9.3339	54.1019	9064.2625	2.36575549	89.5509	7823.8094
0.0009732	1031694.591	106371020252.75	3.8912	78.5805	4869.5138	2.61899105	79.9257	8606.8979

Fig. 2 Flow rate of DDoS attacks from CICDDoS2019 dataset

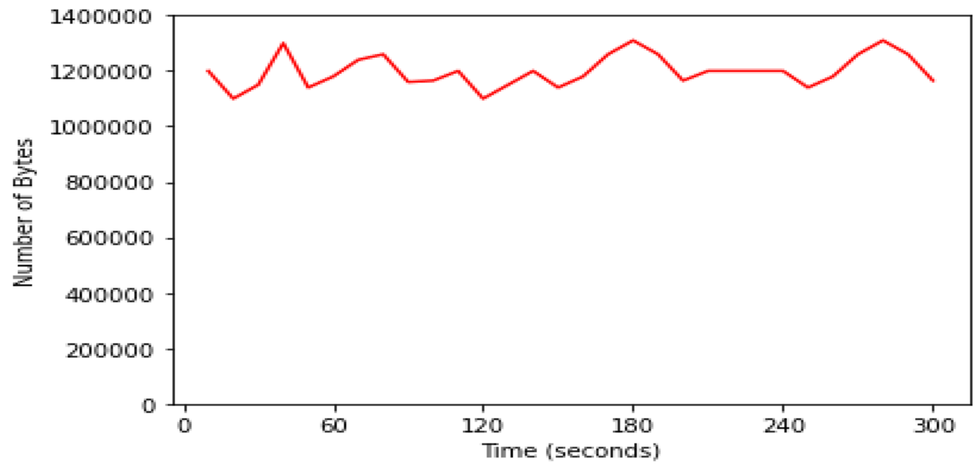


Fig. 3 Flow rate of normal traffic from CICDDoS2019 dataset

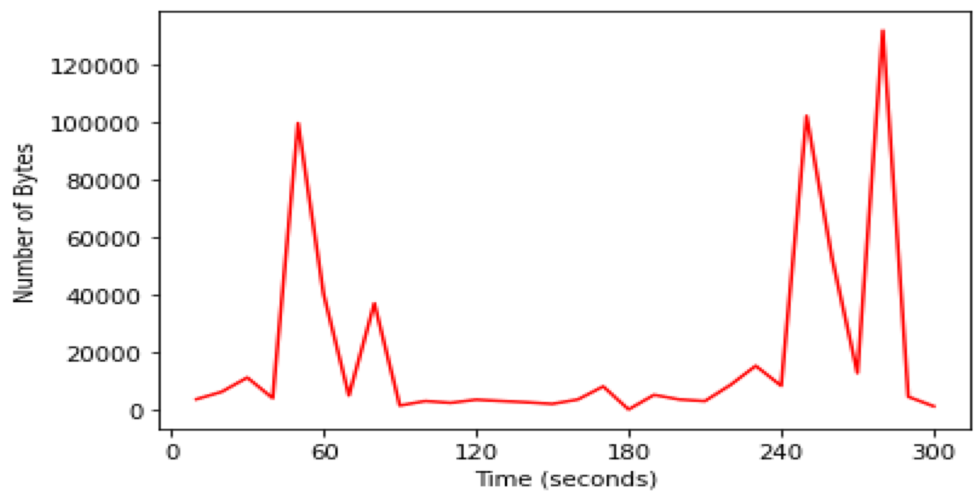
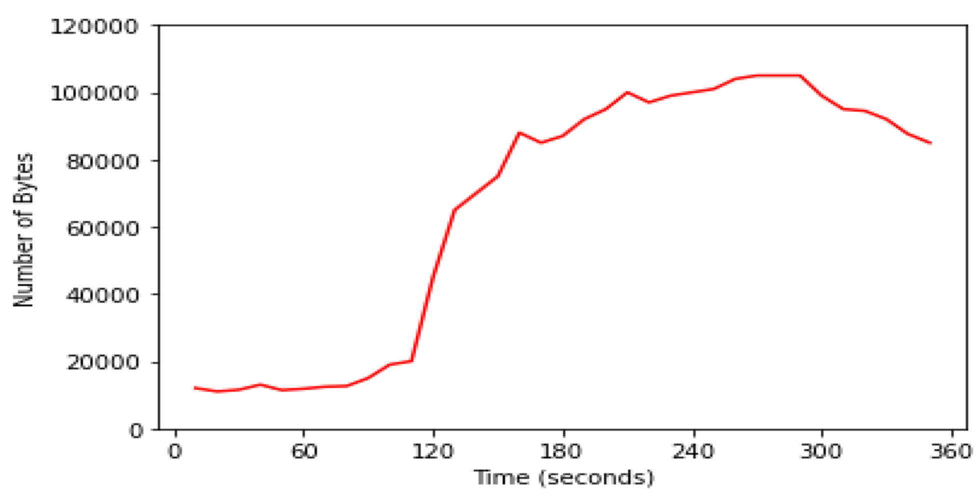


Fig. 4 Flow rate of FE traffic from '98 FIFA World Cup dataset



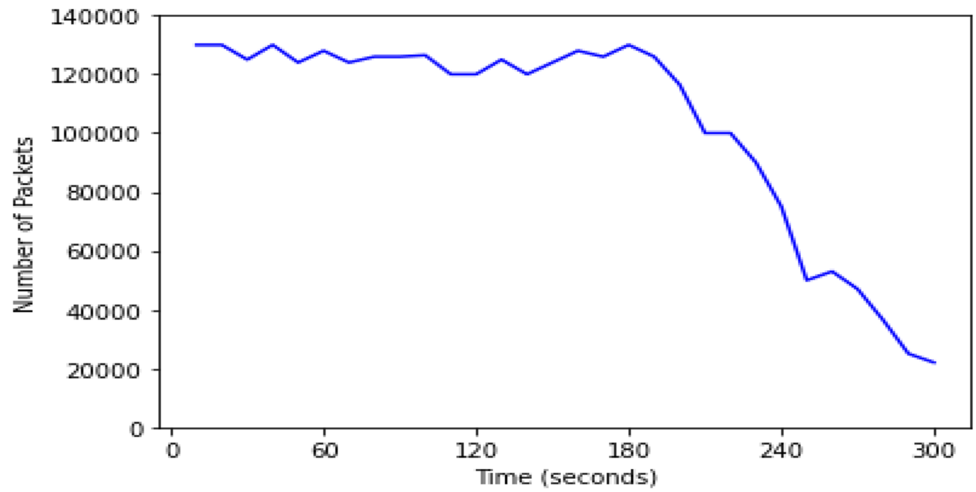


Fig. 5 Arrival rate of DDoS attacks from CICDDoS2019 dataset

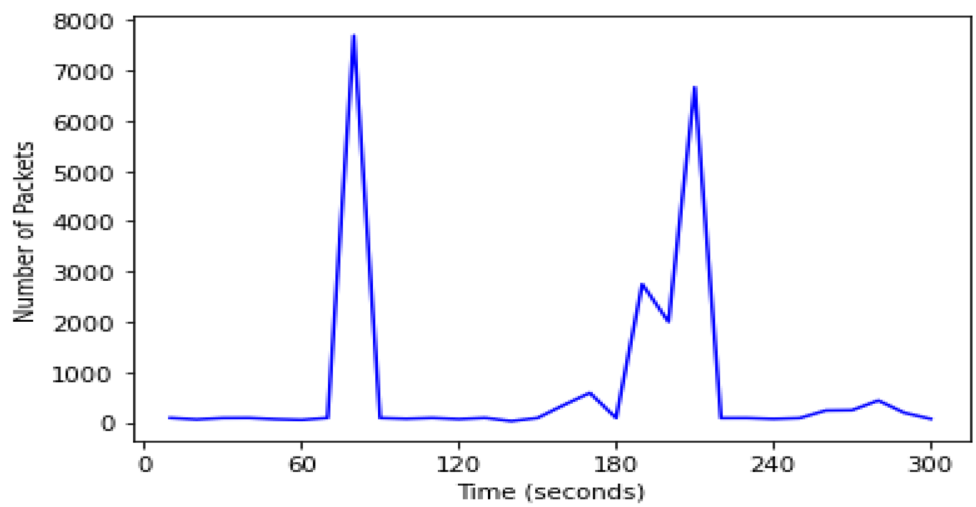


Fig. 6 Arrival rate of normal traffic from CICDDoS2019 dataset

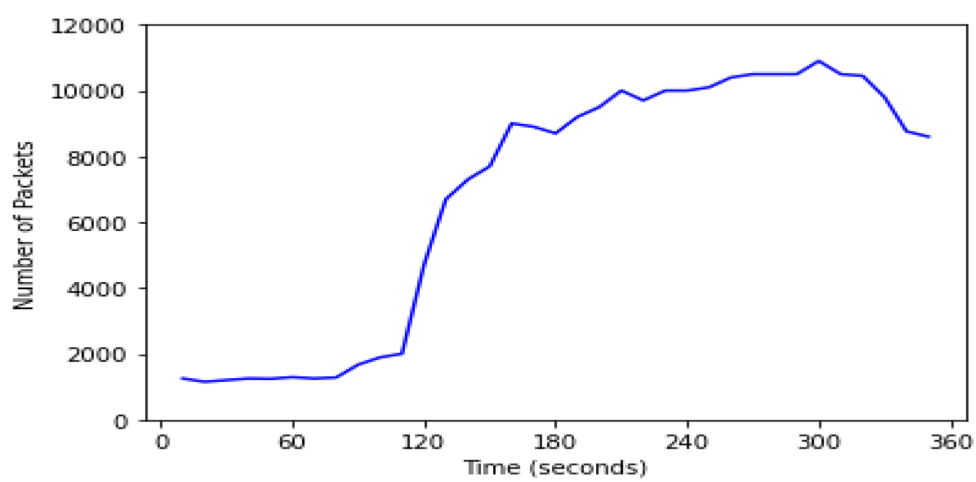


Fig. 7 Arrival rate of FE traffic from '98 FIFA World Cup dataset

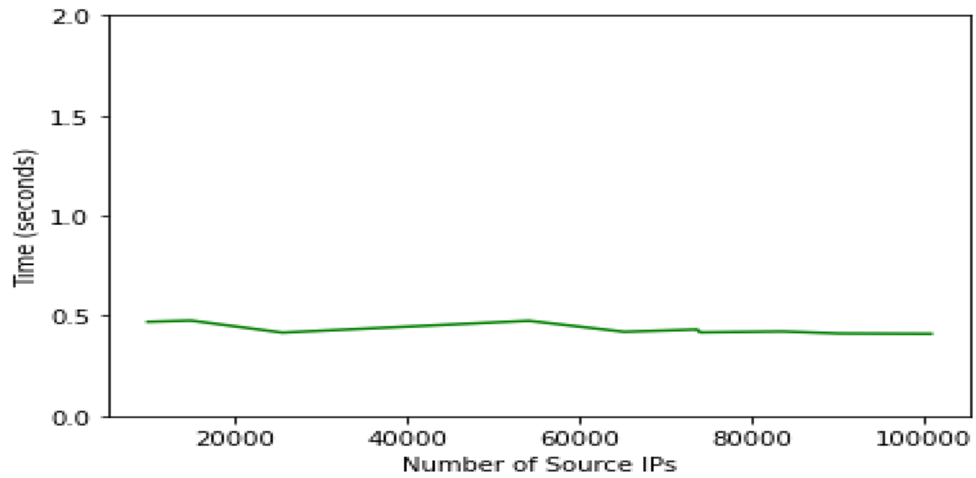


Fig. 8 Packet Inter-arrival time of DDoS attacks from CICD-DoS2019 dataset

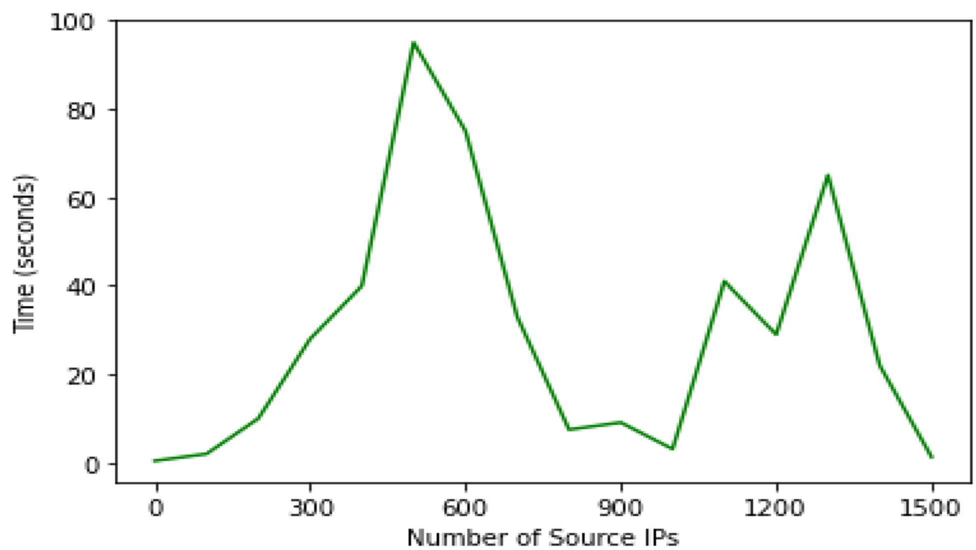


Fig. 9 Packet Inter-arrival time of normal traffic from CICD-DoS2019 dataset

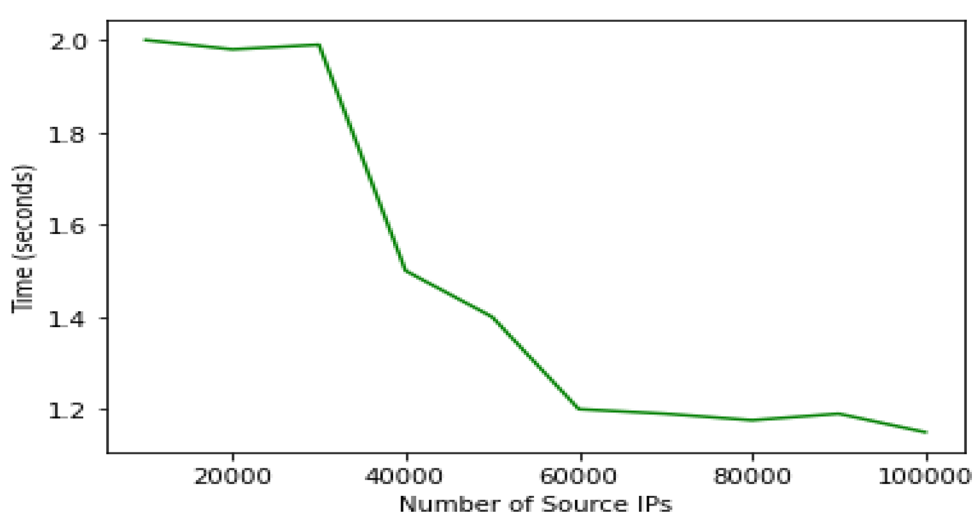


Fig. 10 Packet Inter-arrival time of FE traffic from '98 FIFA World Cup dataset

λ_p follows the Poisson process with probability density function (pdf):

$$\text{Poisson}\,(p) = \frac{\lambda^p e^{\lambda}}{p!}, \tag{3}$$

where λ is the arrival rate (packet/s).

For an attack packet with flow rate R_F(bits/s), the attack arrives at a time t and progresses at a time $t + \delta$, where δ is the inter-arrival time. The network is in a usual state at any time $t' < t$.

$$\delta = \frac{1}{\lambda}. \tag{4}$$

Packet inter-arrival times δ follow exponential distribution and are independent and identically distributed.

Hence, it follows that the Probability of exhaustion of resources P_E of the victim directly depends on the flow rate R_F and inversely on the inter-arrival time δ of attack packets.

$$P_E \propto \frac{R_F}{\delta}. \tag{5}$$

4 Implementation and results

The network environment is set up using NS2, a network simulator. Attack flows, Normal flows and Flash Events (FE) are generated in the network using the Scapy tool. The Distributed Denial of Service (DDoS) traffic generated forwards UDP and TCP packets to the victim server. Wireshark is employed for monitoring and capturing the network traffic. The details of the flow features of the three (3) traffics as captured from Wireshark are shown in Table 1.

The behavioral model is validated with two (2) real-world publicly available datasets; the latest CICDDoS2019 and the '98 FIFA World Cup dataset. The CICDDoS2019 dataset consists of a mixture of legitimate traffic and the most recent DDoS attacks. The '98 FIFA World Cup dataset represents the traffic of Flash Events (FE), and it is the only publicly accessible dataset that represents a Flash Event. The FE traffic was captured from the 66$^{\text{th}}$ day of the dataset as it contains the highest number of requests. The effects of the selected flow features (flow rate, arrival rate and inter-arrival time of packets) are compared in Attack, Normal and FE scenarios as obtained from the datasets, and shown in Figs. 2, 3, 4, 5, 6, 7, 8, 9 and 10.

The traffics of DDoS attack, Normal flows and Flash Event as seen from the employed datasets have distinct characteristics and patterns. It can be observed from Figs. 2, 3, 4, 5, 6, 7, 8, 9 and 10 that the selected features clearly show the variance in the behavioral patterns of the three (3) traffics. The features are highly sensitive towards identifying the variations in the traffics. Thus, DDoS attacks can be detected and differentiated from normal network traffic and Flash Events using relevant features as the flow rate, arrival rate and the packets inter-arrival time.

5 Conclusion and future scope

The characterization and mitigation of flooding Distributed Denial of Service (DDoS) attacks go hand-in-hand. An in-depth understanding of the behaviors of attack flows is essential for accurate detections. Notably, a high false positive remains a prominent challenge of existing detection methods. Therefore, in this study through a network analysis, we characterized attack flows using three distinct features namely the flow rate, arrival rate and inter-arrival time of packets. The relationship between the behavioral features and the rate of exhaustion of the victim's resources was established. The effects of the features were compared in DDoS attack, Normal and Flash Event scenarios, and proved to distinguish attack traffic from legitimate traffic and Flash Events. Thus, the behavioral model lays a good foundation for the mitigation of flooding DDoS attacks.

Further work will make use of the behavioral features for the detection of attack flows using several machine-learning models.

Author contributions The first author was responsible for the conception and design of the system. The research was supervised by the second and third authors, wherein they contributed immensely to the success of the research. All authors read and approved the final manuscript.

Data availability Two benchmark datasets have been used to support this research. They are: 1. The CICDDoS2019 dataset, which is provided by the Canadian Institute for Cybersecurity, and publicly available at: https://www.unb.ca/cic/datasets/ddos-2019.html. 2. The '98 FIFA World Cup website access logs are accessible at ftp://ita.ee.lbl.gov/html/contrib/WorldCup.html.

Declarations

Conflict of interest The authors declare that there are no competing interests as regards this study.

References

1. Abliz M (2011) Internet denial of service attacks and defense mechanisms. University of Pittsburgh Department of Computer Science Technical Report 1–50

2. Behal S, Kumar K (2017) Detection of DDoS attacks and flash events using novel information theory metrics. Comput Netw 116(4):96–110. https://doi.org/10.1016/j.comnet.2017.02.015
3. Behal S, Kumar K, Sachdeva M (2021) D-FAC: A novel ϕ-Divergence based distributed DDoS defense system. J King Saud Univ-Comput Inform Sci 33(3):291–303. https://doi.org/10.1016/j.jksuci.2018.03.005
4. Bhandari A, Sangal AL, Kumar K (2016) Characterizing flash events and distributed denial-of-service attacks: an empirical investigation. Security Commun Netw 9(13):2222–2239. https://doi.org/10.1002/sec.1472
5. Bhardwaj A, Subrahmanyam G, Avasthi V, Sastry H, Goundar S (2016) DDoS Attacks, New DDoS Taxonomy and Mitigation Solutions- A Survey. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) 793–798 IEEE. https://doi.org/10.1109/SCOPES.2016.7955549
6. Bhuyan M, Bhattacharyya K, Kalita J (2015) An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recogn Lett 51(1):1–7. https://doi.org/10.1016/j.patrec.2014.07.019
7. Chawla S, Sachdeva M, Behal S (2016) Discrimination of DDoS attacks and flash events using Pearson's product moment correlation method. Int J Comput Sci Inform Security 14(10):382
8. Daneshgadeh S, Ahmed T, Kemmerich T, Baykal N (2019) Detection of DDoS attacks and flash events using Shannon entropy, KOAD and Mahalanobis distance. In 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN) 222–229 IEEE. https://doi.org/10.1109/ICIN.2019.8685891
9. Dayal N, Srivastava S (2017) Analyzing behavior of DDoS attacks to identify DDoS detection features in SDN. In 2017 9th International Conference on Communication Systems and Networks (COMSNETS) 274–281 IEEE
10. Devi S, Yogesh P (2012) Detection of application layer DDoS attacks using information theory based metrics. CS & IT-CSCP 10:213–223. https://doi.org/10.5121/csit.2012.2223
11. Dhingra A, Sachdeva M (2018) DDoS detection and discrimination from Flash Events: a compendious review. In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) 518–524 IEEE
12. Fowdur TP, Baulum BN, Beeharry Y (2020) Performance analysis of network traffic capture tools and machine learning algorithms for the classification of applications, states and anomalies. Int J Inf Technol 12(3):805–824. https://doi.org/10.1007/s41870-020-00458-0
13. François J, Aib I, Boutaba R (2012) FireCol: a collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans Networking 20(6):1828–1841
14. Furfaro A, Pace P, Parise A (2020) Facing DDoS bandwidth flooding attacks. Simulation Model Practice Theory 98:101984. https://doi.org/10.1016/j.simpat.2019.101984
15. Guozi S.U.N, Jiang W, Yu G.U, Danni R.E.N, Huakang L.I (2018) DDoS attacks and flash event detection based on flow characteristics in SDN. In 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) 1–6
16. Hogue N, Bhattacharyya D, Kalita J (2015) Botnet in DDoS attacks: Trends and challenges. IEEE Commun Surveys 14(4):2242–2270. https://doi.org/10.1109/COMST.2015.2457491
17. Hogue N, Kashyap H, Bhattacharyya D (2017) Real-time DDoS attack detection using FPGA. Comput Commun 110(5):48–58. https://doi.org/10.1016/j.comcom.2017.05.015
18. Kaur G, Behal S (2017) An information divergence based approach to detect flooding DDoS attacks and Flash Crowds. In 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) 251–258
19. Kumar B, Bhuyan B (2019) Using game theory to model DoS attack and defence. Sādhanā 44:1–12. https://doi.org/10.1007/s12046-019-1228-4
20. Lopez A, Mohan A, Nair S (2019) Network traffic behavioral analytics for detection of DDoS attacks. SMU Data Sci Rev 2(1):14
21. Manimaran A, Durairaj M (2016) The conjectural framework for detecting DDoS attack using enhanced entropy based threshold technique (EEB-TT) in cloud environment. Int J Adv Comput Res 6(27):230. https://doi.org/10.1910/IJACR2016.626020
22. Najar AA, Manohar Naik S (2022) DDoS attack detection using MLP and random forest algorithms. Int J Inf Technol. https://doi.org/10.1007/s41870-022-01003-x
23. Navaz A. S, Sangeetha V, Prabhadevi C (2013) Entropy based anomaly detection system to prevent DDoS attacks in cloud. arXiv preprint arXiv:1308.6745. https://doi.org/10.48550/arXiv.1308.6745
24. Nugraha M, Paramita I, Musa A, Choi D, Cho B (2014) Utilizing OpenFlow and sFlow to detect and mitigate SYN flooding attack. J Korea Multimedia Soc 17(8):988–994. https://doi.org/10.9717/kmms.2014.17.8.988
25. Ray S, Mishra KN, Dutta S (2022) Detection and prevention of DDoS attacks on M-healthcare sensitive data: a novel approach. Int J Inf Technol 14(3):1333–1341. https://doi.org/10.1007/s41870-022-00869-1
26. Sachdeva M, Kumar K, Singh G (2016) A comprehensive approach to discriminate DDoS attacks from flash events. J Inform Security Appl 26:8–22. https://doi.org/10.1016/j.jisa.2015.11.001
27. Sachdeva M, Kumar K (2014) A traffic cluster entropy based approach to distinguish DDoS attacks from flash event using DETER testbed. Int Scholarly Res Notices. https://doi.org/10.1155/2014/259831
28. Sahoo K.S, Tiwary M, Sahoo B (2018) Detection Of High Rate DDoS Attack From Flash Events Using Information Metrics In Software Defined Networks. In 2018 10th International Conference on Communication Systems & Networks (COMSNETS) 421–424. https://doi.org/10.1109/COMSNETS.2018.8328233
29. 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(12):510–523. https://doi.org/10.3906/elk-1308-188
30. Sharafaldin I, Lashkari A, Hakak S, Ghorbani A (2019) Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In 2019 International Carnahan Conference on Security Technology (ICCST) 1–8 IEEE
31. Singh G, Gupta M (2016) Distributed Denial-of-Service. Int J Innovative Res Sci Eng 2(4):301–309
32. Singh J, Behal S (2021) A Novel Approach for the Detection of DDoS Attacks in SDN using Information Theory Metric. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) 512–516 IEEE
33. Tan L, Pan Y, Wu J, Zho J, Jiang H, Deng Y (2020) A new framework for DDoS attack detection and defense in SDN environment. IEEE Access 8:161908–161919. https://doi.org/10.1109/ACCESS.2020.3021435
34. Thapngam T, Yu S, Zhou W, Beliakov G (2011) Discriminating DDoS attack traffic from flash crowd through packet arrival patterns. In 2011 IEEE conference on computer communications workshops (INFOCOM WKSHPS) 952–957

35. Tinubu CO, Falana OJ, Aborisade DO, Adejimi OA, Akinmusire CB (2021) DDoSDetect: a behavioral detection system for HTTP GET flood attacks. J Appl Sci Technol 1(1):102–114 (**Published by Mountain Top University Nigeria**)
36. Tinubu CO, Sodiya AS, Ojesanmi OA, Adeleke EO, Adebowale AO (2022) DT-model: a classification model for distributed denial of service attacks and flash events. Int J Inf Technol. https://doi.org/10.1007/s41870-022-00946-5
37. Wang A, Chang W, Chen S, Mohaisen A (2018) Delving into internet DDoS attacks by botnets: characterization and analysis. IEEE/ACM Trans Networking 26(6):2843–2855
38. Wang Y, Ma J, Zhang L, Ji W, Lu D, Hei X (2016) Dynamic game model of botnet DDoS attack and defense. Security Commun Netw 9(16):3127–3140. https://doi.org/10.1002/sec.1518
39. Yang G, Hespanha, J (2021) Modeling and mitigating link-flooding Distributed Denial-of-Service attacks via learning in Stackelberg games. Handb. Reinf. Learn. Control Springer. https://doi.org/10.1007/978-3-030-60990-0_15
40. Yu S, Zhou W, Jia W, Guo S, Xiang Y, Tang F (2012) Discriminating DDoS attacks from flash crowds using flow correlation coefficient. IEEE Trans Parallel Distrib Syst 23(6):1073–1080
41. Yusof A, Udzir N, Selamat A (2019) Systematic literature review and taxonomy for DDoS attack detection and prediction. Int J Digital Enterprise Technol 1(3):292–315
42. Zargar S, Joshi J, Tipper D (2013) A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun Surveys Tutorials 15(4):2046–2069
43. Zhou Z, Xie D, Xiong W (2009) A novel distributed detection scheme against DDoS attack. J Netw 4(9):921–928