Computer Science and Information Systems 14(3):839–856 https://doi.org/10.2298/CSIS161230032K

Distinguishing Flooding Distributed Denial of Service from Flash Crowds Using Four Data Mining Approaches*

Bin Kong[1,2], Kun Yang[4,5], Degang Sun[4,5], Meimei Li*[3,4,5], and Zhixin Shi[4,5]

[1] School of Economics and Management, Beijing Jiaotong University
Beijing, China
pingpangfan@163.com
[2] National Secrecy Science and Technology Evaluation Center
Beijing, China
pingpangfan@163.com
[3] School of Computer and Information Technology, Beijing Jiaotong University
Beijing, China
limeimei@iie.ac.cn
[4] Institute of Information Engineering, Chinese Academy of Sciences
Beijing, China
{yangkun,sundegang,limeimei,shizhixin@iie.ac.cn}
[5] School of Cyber Security, University of Chinese Academy of Sciences
Beijing, China
{yangkun,sundegang,limeimei,shizhixin@iie.ac.cn}
Corresponding Author Email: limeimei@iie.ac.cn

Abstract. Flooding Distributed Denial of Service (DDoS) attacks can cause significant damage to Internet. These attacks have many similarities to Flash Crowds (FCs) and are always difficult to distinguish. To solve this issue, this paper first divides existing methods into two categories to clarify existing researches. Moreover, after conducting an extensive analysis, a new feature set is concluded to profile DDoS and FC. Along with this feature set, this paper proposes a new method that employs Data Mining approaches to discriminate between DDoS attacks and FCs. Experiments are conducted to evaluate the proposed method based on two real-world datasets. The results demonstrate that the proposed method could achieve a high accuracy (more than 98%). Additionally, compared with a traditional entropy method, the proposed method still demonstrates better performance.

Keywords: Flooding DDoS, Flash Crowds, Data Mining, Entropy.

1. Introduction

Distributed Denial of Service (DDoS) attacks have been wreaking havoc on the Internet, and these attacks show no signs of disappearing. In fact, attackers are constantly looking for new targets and new ways to deplete network performance [23], [21]. DDoS attacks are becoming more complex and sophisticated. Among all kinds of DDoS attacks, Flooding DDoS attacks are the most common and the most dangerous. Especially, when they

* This work is supported by the National Natural Science Foundation of China (61372062) and Major National Projects of China-The Core Electronic Components, High-end General Chips and Basic Software (CHBS) (2017ZX01045101).

happened under Flash Crowds (FCs) which have many similarities to the kind of DDoS attacks (more can be seen in Table 1) [5], [27], it usually render defense systems helpless.

FCs cause a large amount of traffic to surge simultaneously, causing dramatic stress on the server's network links and resulting in considerable loss of packets and network congestion at last. Although Flooding DDoS attacks are often launched by Botnets [33], [15], the master (attacker) in a Botnet orders compromised hosts (Bots) to simultaneously send packets to deplete the victims resources (e.g., memory, network bandwidth), eventually leaving the victim's system paralyzed [29].

Table 1. A Comparison Between DDoS And FC

Category	DDoS	FC
Network Status	Congested	Congested
Server Status	Overloaded	Overloaded
Traffic Type	Malicious	Genuine
Response to Traffic Control	Unresponsive	Responsive
Traffic Source	Any	Mostly Web
Flow Size	Any	Large Number of Flows
Predictability	Unpredictable	Mostly Predictable

Not only wired networks but also wireless networks [12] face resource constraints, such as limited bandwidth and less memory. Wireless networks also face other constraints, such as short communication ranges, less computational power, open channels, and short lifetimes. These characteristics of wireless networks make them vulnerable to anomalies. Any anomalies in a wireless ad hoc network degrade the overall performance of the network. DDoS attacks are one of these network anomalies, they are still severe attacks on wireless networks and may not be easily identifiable from FCs.

Due to plenty of similarities existed in DDoS and FC, all of them make the issue of discriminating DDoS and FC hardly to be tackled [29]. In the case of FCs, the high volume of traffic generated by legitimate users needs to be serviced by provisioning extra resources, whereas in the case of DDoS attacks, traffic generated by Bots needs be filtered as early as possible. Therefore, DDoS attacks and FCs should to be treated in different ways. To solve this discrimination issue, we extensively analyze these two phenomena and find that a few abnormal statistical features exist in DDoS attacks and FCs. With these features, we can translate the problem of differentiating DDoS attacks and FCs into ways to classify points in Euclidean n-spaces. As a result, we propose a method that employs Data Mining to discriminate between DDoS attacks and FCs.

This paper has been organized as follows: Section 2 reviews the currently available literatures. Section 3 concludes a new feature set and explains our proposed method in detail. Section 4 conducts experiments to evaluate this method and analyzes the results. Section 5 concludes our work.

2. Related Work

Since DDoS attacks first began in the early 2000s, considerable literatures have been published on detecting DDoS to avoid unnecessary economic loss, but little works related to the topic of distinguishing between DDoS attacks and FCs has been published [12], [31], [39]. Based on our understanding of the field, we simply divided the existing methods into two categories: Turing Test and Anomaly Behavior Analysis.

2.1. Turing Test

DDoS attacks are usually launched by Botnets, whereas FCs derive from legitimate clients; consequently, the problem of differentiating between DDoS attacks and FCs can be simplified to the problem of identifying whether the client is a human or a Bot. According to the client's responses, then distinguish whether the client is a normal user or not, that is Turing Test, which is the main and pervasive method for distinguishing DDoS attacks from FCs. The common Turing Test includes graphic puzzles, which display a slightly blurred or distorted picture or a puzzle and ask the user to type in the depicted symbols. This task is easy for humans yet hard for computers to answer.

CAPTCHAs (Completely Automated Public Turing Test to Tell Computers and Humans Apart) [36], [18] and AYAHs (Are You a Human) [1] are the most commonly used Turing tests. These methods, however, may cause some delays for normal users and usually annoy users with the increasingly difficult images employed. At the same time, various mechanisms, such as Reverse Turing Test, have also been developed by hacker communities to break these visual puzzles, which means that Turing Test will no longer completely defend against DDoS attacks or be able to distinguish DDoS attacks from FCs.

2.2. Anomaly Behavior Analysis

DDoS attacks mainly rely on Botnets, and Bots are usually executed by preprogrammed codes [14], whereas legitimate users are different individuals, and consequently, a few anomalies do exist between Bots and legitimate clients.

Jung et al. [17] first identified a few characteristics for discriminating DDoS attacks from FCs after analyzing various FC traces. The authors found that during FCs, most of the requests were generated either from those clients who had visited previously or from those clients who belonged to the same networks or administrative domains.

Xie et al. [37] proposed a novel method to detect anomaly events based on the hidden Markov model. This approach used the entropy of document popularity as the input feature to establish this model.

Ke et al. [20] proposed novel approaches using probability metrics to discriminate DDoS attacks from FCs. These methods efficiently identified the FC attacks from the DDoS attacks, reduced the number of false positives and false negatives, and also identified the attacks. Conversely, probability metric approaches failed to maintain the same accuracy for discriminating the FC attack from significant attack traffic.

Oikonomou et al. [25] tried to discriminate mimicked attacks from real FCs by modeling human behavior. The study is mainly based on the dynamic changes of requests and the semantic meaning of requests and then builds the normal behavior model, which it used to distinguish Bots from normal visitors. This model is difficult to employ, however, for large-scale dynamic web pages because of the complicated process of establishing a transfer probability matrix.

Theerasak et al. [34] proposed a discrimination method based on packet arrival patterns. Pearsons correlation coefficient was used to measure packet patterns. These patterns are defined using the repeated properties observed from the traffic flow and are also calculated by the packet delay. Defining packet patterns is difficult, however.

Bhatia et al. [4], [5] proposed a technique combining the analysis of both network traffic features (e.g., incoming traffic volume, new source IP addresses, number of source IP addresses, and incoming traffic distribution) and server load characteristics (e.g., system-level CPU utilization, user-level CPU utilization, CPU load, and real memory utilization) to distinguish DDoS from FC. The computational complexity of this approach, however, is quite high.

Rabia et al. [19] reviewed the state-of-the-art detection mechanisms for the identified DDoS attacks in wireless body area networks (WBANs). The most serious threat to data availability is a DDoS attack that directly affects the all-time availability of a patients data. The existing solutions for standalone WBANs and sensor networks are not applicable in the cloud. Therefore, the purpose of this review was to identify the most threatening types of DDoS attacks affecting the availability of a cloud-assisted WBAN and review existing mechanisms to detect DDoS attacks.

Yu et al. [40], [42] employed flow similarities to discriminate DDoS attacks from FCs and achieved better results. The authors mainly used fixed thresholds, which required craft design and professional field knowledge.

Somani et al. [32] surveyed new environments for DDoS. The authors presented developments related to DDoS attack mitigation solutions in the cloud. In particular, this paper presented a comprehensive survey with detailed insights into the characterization, prevention, detection, and mitigation of these attacks. Additionally, it presented a comprehensive taxonomy to classify DDoS attack solutions.

Sachdeva et al. [29] combined multiclusters of source address entropy not only to detect various types of DDoS attacks against web services but also to distinguish DDoS attacks from FCs. Optimal thresholds for traffic cluster entropy were calibrated through receiver operating characteristic curves.

Saravanan et al. [30] found that during FCs, human users always tried to access hot pages, but Bots accessed pages randomly. To some extent, this finding could be helpful for differentiating between DDoS and FCs. The approach combined multiparameters with weights to discriminate DDoS from FC and achieved better results than when using a single parameter. The weights, however, were fixed and could not be updated automatically.

Gupta et al. [12] reviewed the researches on DDoS attacks on wireless networks and outlined various types of DDoS attacks. The impact of the attack occurs at various points along the network, most significantly on the routing mechanism, security goals, and protocol stack layer. The genuine nodes are kept busy by the malicious node while processing a large number of route requests or sending large data packets to other nodes. An ad hoc network must have a secured mechanism to evade the attacks.

DDoS is a spy-on-spy game between attackers and detectors, and these attacks have caused huge losses [2]. In particular, these attacks can mimic normal users, which look like FCs, and can often evade the existing defense systems. As far as we know, Turing Test is the most popular and pervasive method used to distinguish between DDoS and FC; however, with the development of Reverse Turing Test [22], increasingly distorted and obscure images have been employed to defend against the reverse Turing test, which usually causes user annoyance and helplessness. Additionally, the existing anomaly analysis approaches are too sensitive to detect the thresholds needed to elaborate on the design and are usually not flexible. In this paper, we propose a Data Mining method to solve this problem, which may act as a complementary mechanism of existing defence systems.

3. Proposed Method

To solve this issue of discriminating between DDoS attacks and FCs, we conducted an extensive analysis of these two phenomena and identified a few abnormal statistical features in DDoS attacks and FCs, such as the number of packets sent by Bots and legitimate users is different, the number of new IPs appeared in DDoS and FC is different. With these features, we were able to translate the differentiating problem into a method for classifying points in Euclidean n-spaces. As a result, we propose a method to employ Data Mining to discriminate between DDoS attacks and FCs.

3.1. The Concluded Feature Set

Based on our understanding and analysis of Flooding DDoS attacks and FCs, we conclude the following:

1) Unique Source IPs' Or Clients' Number In Each Interval ($uniqueSrcIPs$): In FCs, users are interested in specified events only, such as flash news or interesting information. These users usually come from the whole Internet, so the distribution of source IP addresses in FCs may be largely dispersive. In DDoS, however, the attacker collects hosts that are vulnerable, so the distribution of IP addresses is relatively concentrated because the availability of Bots or zombies is limited. As a result, in each interval Δt, the unique source IPs' or clients' numbers for DDoS and FC is different, and this feature can be formally represented as follows:

$$uniqueSrcIPs = \{uniClients|\ different\ IPs\ number\ in\ each\ interval.\} \tag{1}$$

where, $uniClients$ is the number of different source IPs or clients in an interval.

2) New Increased IPs' Number In Adjacent Interval ($newIncresedSrcIPs$): In FCs, many more individuals care about a specific event than during a DDoS attack, and these individuals are usually more evenly distributed geographically than Bots in DDoS. Therefore, in the adjacent interval, the number of source IPs or clients in the FC has increased more than that of IPs or clients in DDoS.

$$\begin{aligned} newIncresedSrcIPs = \{x|x \in uniClients,\\ x \notin uniClientsPrevious\} \end{aligned} \tag{2}$$

where, $uniClientsPrevious$ is the number of different source IPs or clients in the previous interval, which is adjacent to the current interval.

3) The Average Of The Number Of Packets Sent By Source IPs or Clients In Each Interval ($uSrcIPsSendPkts$): To attain the expected attack effect, such as network congestion, Bots usually have to send as many packets as possible, so the average number of packets sent by each Bot and legitimate client is different. In general, the average number of packets sent by Bots is larger than that of normal users in each interval.

$$uSrcIPsSendPkts = \left\{ \frac{\sum\limits_{i=1}^{n} numPackets_i}{n} \right\} \tag{3}$$

where, $numPackets_i$ is the packets number sent by the i-th client, n is the unique number of clients in each interval Δt.

4) The Standard Of The Number Of Packets Sent By Source IPs In Each Interval ($stdSrcIPsSendPkts$): DDoS mainly rely on Botnets, and Bots are usually executed by preprogrammed codes. Each bot exhibits similar traffic behavior, whereas legitimate users are different individuals who exhibit varied behavior. Thus, the standard of the number of packets sent by each user in a DDoS attack is lower than that of in a FC.

$$stdSrcIPsSendPkts = \left\{ \sqrt[2]{\frac{\sum\limits_{i=1}^{n} (numPackets_i - u)^2}{n-1}} \right\} \tag{4}$$

where, u is the uSrcIPsSendPkts.

To demonstrate our feature set, it is useful to distinguish between DDoS and FC. The following section will discuss some experiments we conducted.

3.2. Proposed Idea

In general, different datasets are created in different situations, such as different topologies and network bandwidths. For these reasons, different datasets cannot be mixed without any preprocessing. To address this problem and obtain the new feature set, we conducted the following preprocessing tasks:

1) Difference Topology: Different IP masks and different IP addresses exist in each dataset, so we apply relevant statistical features instead of using IPs directly, such as adopting the number of packets sent by each IP, the average packet size sent by each IP, and the standard deviation of the packet size sent by each source IP. With these preprocessing tasks, we believe that we could eliminate the effect caused by network topology.

2) Network Bandwidth: For various reasons, datasets are usually created at different bandwidths. To address this issue, we scaled the interval to ensure that different datasets have the same network bandwidth at each interval. For example, assume that the bandwidth of the first dataset is 10 M/s, and the second dataset is 100 M/s. To achieve the same traffic volume in each interval (2s), we enlarged the first dataset to be 100 M/s, which was an increase 100/10 (ten) times that of the interval. In this way, the impact of the network bandwidth was minimized.

With the new feature set, we proposed a method to employ several common Data Mining methods [13] [24], including logistic, multilayer perception, J48, and PART, to distinguish between DDoS attacks and FCs. The entire procedure is given in Algorithm 1. We labeled each interval with one class label: DDoS or FC.

Algorithm 1 Proposed Idea.

```
Input:
    DDoS and FC dataset
Output:
    The discriminating results of DDoS or FC
1: Calculate each feature with default interval $\Delta t$ for each data separately, then label the class-DDoS or FC, and we could obtain 5 dimensional row vectors:
       $(uniqueSrcIPs, newIncresedSrcIPs, uSrcIPs-SendPkts, stdSrcIPsSendPkts, Class)$
   These vectors can be used as input. Consequently, we can translate the differentiating problem into a method to classify points in Euclidean n-spaces.
2: Mix the results in Step 1 and normalize the mixed results.
3: Take the mixed and normalized results in Step 2 as input for Data Mining methods, such as, Logistic, MultilayerPerceptron, J48 and PART, and estimate these results on public datasets.
4: return the final distinguishing results.
```

4. Experiments

In this section, we conducted additional experiments to verify our method on two public real-world datasets: CAIDA DDoS Attack 2007 Dataset (CAIDA2007) [7] used as the DDoS data and the World Cup 1998 Dataset (WorldCup1998) [11] used as the FC data.

CAIDA2007 contains approximately 1 hour of anonymized traffic traces from a DDoS attack on August 4, 2007 (Universal Time Coordinated, UTC). This attack attempted to block access to the targeted server. The 1-hour trace is split up into 5-minute pcap files. The total size of the dataset is 5.3 GB (compressed; 21 GB uncompressed). Only attack traffic directed to the victim and responses to the attack from the victim are included in the traces. We have removed as much of the nonattack traffic as possible. Traces in this dataset were anonymized using CryptoPAn prefix-preserving anonymization using a single key. The payload has been removed from all packets [7].

WorldCup1998 includes all requests made to the 1998 World Cup website between April 30, 1998, and July 26, 1998. During this 88-day period, the World Cup site received 1,352,804,107 requests. No information is available regarding how many requests were not logged, although it is believed no system outages occurred during the collection period [11].

We selected 1-minute of DDoS data (2007-08-05 05:30:00 to 2007-08-05 05:31:00) from CAIDA2007 and 1-hour of FC data (1998-06-10 16:00:00 to 1998-06-10 17:00:00) from WorldCup1998 for analysis (see Fig. 1). We ensured that different datasets would produce the same traffic volume in each interval by scaling the interval to reduce the effects of bandwidth. After analyzing the selected data, we selected a scale interval rate of 1:100, which meant that the traffic produced in 1 DDoS interval was nearly equal to the traffic produced in 100 FCs intervals. After this process, we achieved the scaled traffic shown in Fig. 2. We found that the average amounts of traffic were almost the same, which significantly eliminated the effect of different bandwidths.

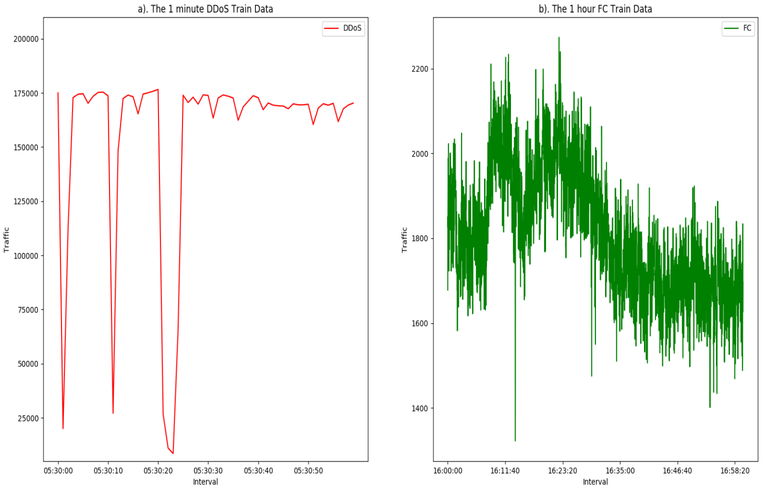

Fig. 1. a). The 1 minute DDoS Data with the interval-1s from 2007-08-05 05:30:00 to 2007-08-05 05:31:00. b). The 1 hour FC Data with the interval-1s from 1998-06-10 16:00:00 to 1998-06-10 17:00:00.

4.1. New Feature Set Evaluation

To evaluate the importance of each feature of our feature set, Correlation (Pearsons) based Method (CorrelationAttributeEval), Gain Ratio Method (GainRatioAttributeEval) and Information Gain Method (InfoGainAttributeEval) have been selected to do features

Tab. 2 shows the estimated results of the new features in detail. The results reveal that all three feature selection methods gave $uniqueSrcIPs$ the greatest priority; the second most important feature was $stdSrcIPsSendPkts$ and the next most important feature was $newIncresedSrcIPs$; the least vital feature was $uSrcIPsSendPkts$. These results are basically consistent with our expectation of real data.

Consequently, the importance of the entire feature set in descending order is as follows:

$$\begin{aligned} &uniqueSrcIPs > stdSrcIPsSendPkts \\ &> newIncresedSrcIPs > uSrcIPsSendPkts \end{aligned}$$

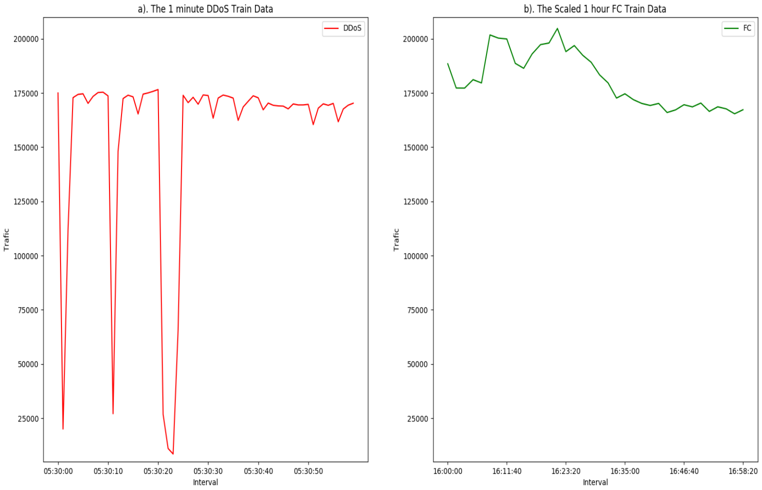

Fig. 2. a). The 1 minute DDoS Data with the interval-1s from 2007-08-05 05:30:00 to 2007-08-05 05:31:00. b). The scaled 1 hour FC Data with the intervel-100s from 1998-06-10 16:00:00 to 1998-06-10 17:00:00.

Table 2. Features Selection Estimated By 3 Common Features Selection Methods

Attribute Evaluator	GainRatio Attribute Eval		Correlation Attribute Eval		InfoGain Attribute Eval	
Search Method	Ranker					
Features	Rank	Average	Rank	Average	Rank	Average
unique SrcIPs	1	1.000	1	0.962	1	0.954
newIncreased SrcIPs	3	0.922	3	0.837	4	0.877
uSrcIPs SendPkts	4	0.747	4	0.387	3	0.954
stdSrcIPs SendPkts	2	1.000	2	0.890	2	0.954

4.2. Proposed Idea

In this section, we employ several common Data Mining methods included Logistic, MultilayerPerceptron, J48 and PART to distinguish DDoS and FC, combining with Confusion Matrix, Relative absolute error (RAE), Root relative squared error (RRSE), Accuracy, False Positive Rate (FPR) and False Negative Rate (FNR) all together as measurement standards.

The results are shown in Tab. 3. With these new features, we could distinguish between DDoS attacks and FCs with high accuracy, less than 5% RAE, no more than 30% RRSE, nearly 100% Accuracy, no more than 0.04% FNR, and nearly 0% FPR with 10-fold cross-validation for those 96 train samples. We found that different Data Mining methods have almost the same accuracy, and Logistic method may be the best discrimination method, with the lowest RAE and FNR and the highest Accuracy (98.9583%).

Table 3. Distinguished Results With 4 Data Mining Methods on Train Sets.

Methods		Logistic		Multilayer Perceptron		J48		PART	
Confusion Matrix		DDoS	FC	DDoS	FC	DDoS	FC	DDoS	FC
	DDoS	59	1	59	1	58	2	58	2
	FC	0	36	0	36	0	36	0	36
Relative Absolute Error (RAE)		2.2181 %		3.911 %		4.4361 %		4.4361 %	
Root Relative Squared Error (RRSE)		21.0712 %		20.9248 %		29.7991 %		29.7991 %	
Accuracy		98.9583%		98.9583 %		97.9167 %		97.9167 %	
False Positive Rate (FPR)		0%		0 %		0%		0 %	
False Negative Rate (FNR)		0.017%		0.017%		0.033%		0.033%	

To further verify the proposed idea, we conducted additional experiments on the test data. We selected another 1-minute DDoS data (2007-08-05 05:34:00 to 2007-08-05 05:35:00) from CAIDA2007 and a 1-hour FC data (1998-07-03 16:00:00 to 1998-07-03 17:00:00) from WorldCup1998 for analysis. Other than the scale rate, all of the processes used were the same as those used in the previous test. In this case, the scale interval rate was 1:80. After this process, we achieved the scaled traffic in each new interval (see Fig. 3). It was evident that the average traffic was basically the same, which could reduce the bandwidth effect of different datasets.

After completing the preprocessing tasks on the test data, we achieved the features and employed the trained models to estimate the new test set. The results in Tab. 4 show that our method has nearly 100% Accuracy, 0% FPR and FNR, less than 0.01% RAE, and no more than 0.01% RRSE, which indicates that the concluded features are useful, and that this idea could perform well in discriminating between DDoS attacks and FCs.

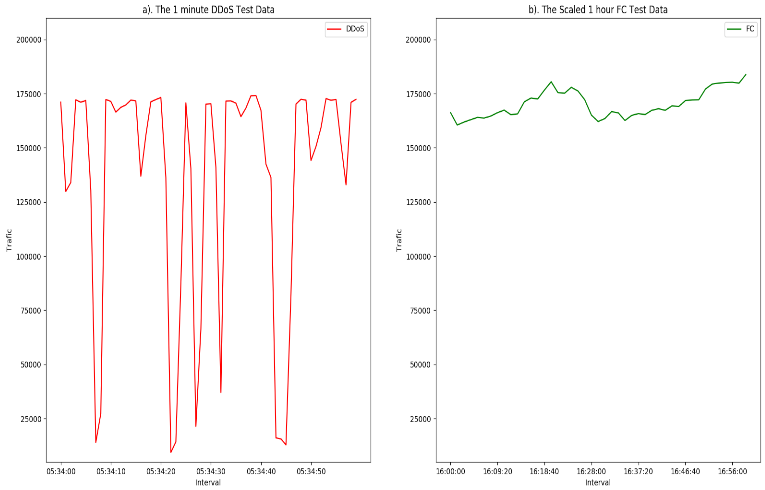

Fig. 3. a). The 1 minute DDoS Data with the interval-1s from 2007-08-05 05:34:00 to 2007-08-05 05:35:00. b). The scaled 1 hour FC Data with the intervel-80s from 1998-07-03 16:00:00 to 1998-07-03 17:00:00.

Table 4. Distinguished Results With 4 Data Mining Methods on Test Sets.

Methods		Logistic		Multilayer Perceptron		J48		PART	
Confusion Matrix		DDoS	FC	DDoS	FC	DDoS	FC	DDoS	FC
	DDoS	60	0	60	0	60	0	60	0
	FC	0	45	0	45	0	45	0	45
Relative Absolute Error (RAE)		0 %		0.007 %		0%		0 %	
Root Relative Squared Error (RRSE)		0 %		0.0075 %		0 %		0 %	
Accuracy		100%		100 %		100 %		100 %	
False Positive Rate (FPR)		0%		0 %		0%		0 %	
False Negative Rate (FNR)		0%		0%		0%		0%	

4.3. Experiments Analysis

In this section, we compare our proposed method with traditional methods. Yu et al. [41] made use of information distance, such as Sibson and Jeffrey distance measures, to discriminate between DDoS and FCs, and achieved only 65% accuracy. Bhatia et al. [5] proposed a few parameters (different from our parameters) to distinguish between DDoS and FCs and conducted experiments that did not achieve any accuracy. The methods used by Bhatia et al. [5] involved only simple statistics, and the study was totally different from our study. Saravanan et al. [30] employed a behavior-based detection method on Application Layer to distinguish between DDoS and FCs and achieved about 91% Accuracy.

To further compare our proposed method with traditional methods, such as the entropy method [35], we selected the Shannon Entropy of Source IPs (srcIPs) in each interval as a feature. The values of Shannon Entropy were calculated by the following formula:

$$Entropy = -\sum_{i=1}^{n} p_i * log_2(p_i) \tag{5}$$

where, p_i is the probability of each source IP or client in each interval.

The results are shown in Fig. 4. The red line represents the entropy of DDoS, and the green line represents the entropy of FCs, which indicates that it is not easy to discriminate DDoS and FCs using the entropy of srcIPs because their entropies are quite similar, which results in the discrimination thresholds rarely being selected.

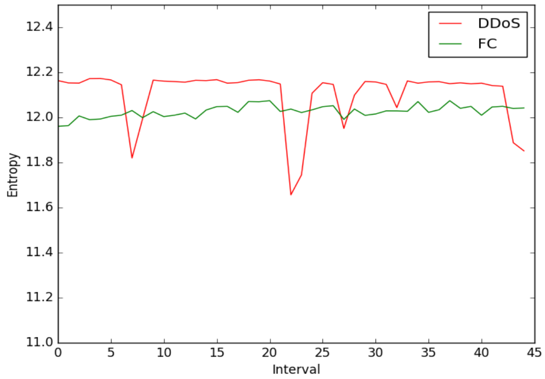

Fig. 4. Shannon Entropy of Source IPs In Each Interval.

Compared with the traditional methods-Entropy in Fig. 4, and review the results of our idea in Tab. 3 and Tab. 4. We find that our idea has a better accuracy to distinguish DDoS and FC with the new feature set on Train Set and Test Set than that of the traditional Entropy method.

Why could our idea achieve a better accuracy? On the basis of an extensive analysis of DDoS and FCs (see Fig. 5), we believe that this feature set plays a vital role in our proposed method, achieving better accuracy. In Fig. 5, the red color represents FCs, and the blue color represents DDoS. This figure shows the distribution of the class for each feature dimension. In Fig. 5, we found that each concluded feature had a slightly better distinguished effect. In addition, traditional methods are primarily threshold-based and usually required crafted thresholds, which are difficult to obtain in reality. Through Data Mining, our proposed method was able to detect DDoS and FCs with fewer human interruptions and better accuracy. Our method is based on the analysis of end-victim. As a result, it is easier to deploy without modifying the existing network protocols, just to deploy at the front of end-victim.

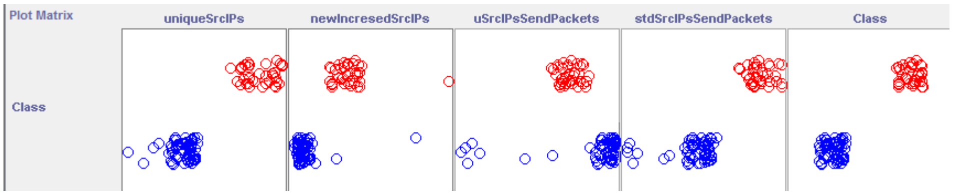

Fig. 5. The Correlation Between Each Feature And The Class. The Red Color Represents FC, While The Blue Color Represents DDoS

4.4. Issues and Limitations

The experiments demonstrated that our method could differentiate between DDoS and FCs well; however, this method does have some insufficiencies. Because this method is based on a few assumptions, the following corresponding issues existed.

1) We assumed that compromised machines do not use spoofing IPs. Although many methods can be used to handle spoofing (such as Ingress and Egress filtering [10], [9], HCF [16], Packet Marking [38], [43]), it is still a useful and potential technique for sophisticated users. According to the MIT Spoofer Project, which provides an aggregate view of ingress and egress filtering and IP spoofing on the Internet, 23% of autonomous systems and 16.8% of IP addresses are able to spoof, which means that an estimated 560 million out of 3.32 billion IP addresses still can be spoofed [28].

2) We also assumed that the number of Bots that can simultaneously launch attacks is limited, so for a Flooding attack, Bots have to send as many packets as possible [33], [8]]. Today, many other types of DDoS attacks occur. For example, low-rate DDoS (LDDoS), which our method cannot distinguish. And Botnets are becoming increasingly larger and more complex [14] with new techniques (such as Cloud Computing [31], Internet of Things [6], [26], SDN [39]) that have brought new challenges.

3) We also had a few other issues. In this paper, our proposed method relied mainly on time intervals, not individuals. As a result, our method could detect abnormalities but not identify attackers, which omitted the vulnerabilities for those mimicking attacks [40], [3].

For these reasons, we should not be overly optimistic. The battle to protect the Internet in a relatively secure environment is ongoing and much more research is required to solve these dilemmas.

5. Conclusion

To discriminate between DDoS attacks and FCs, we first categorized existing methods to clarify the issue. We conducted an extensive analysis of DDoS and FCs and identified a few features to profile DDoS attacks and FCs. Using these features, we translated the discrimination issue into a method to classify points in Euclidean n-spaces. As a result of this analysis, we proposed a method to employ Data Mining to discriminate between DDoS attacks and FCs. We evaluated the results of our experiments and found that the idea employed Data Mining techniques based on identified features can achieve high accuracy and reduced FPR and FNR. We further compared this method to a traditional method (i.e., entropy method), and the results indicated that our proposed method could have a better distinguished effect than that of the entropy method. At last, we discussed some shortcomings in this paper; for example, our method cannot detect LDDoS, and although it could detect abnormalities, it could not identify attackers.

Our future work will focus mainly on how to identify individuals. To do this work, more refined features that may better profile the traffic behavior of clients should be identified. Other researches are to find new datasets or real-world applications to further evaluate.

References

1. AYAHs: website:ayahs. `http://areyouahuman.com`
2. Behal, S., Kumar, K.: Trends in validation of ddos research. Procedia Computer Science 85, 7–15 (2016)
3. Behal, S., Kumar, K.: Detection of ddos attacks and flash events using novel information theory metrics. Computer Networks 116, 96–110 (2017)
4. Bhatia, S.: Detecting distributed denial-of-service attacks and flash events (2013)
5. Bhatia, S., Mohay, G., Tickle, A., Ahmed, E.: Parametric differences between a real-world distributed denial-of-service attack and a flash event. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. pp. 210–217. IEEE (2011)
6. Borgohain, T., Kumar, U., Sanyal, S.: Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211 (2015)
7. DDoS: Caida ddos attack 2007 dataset. `http://www.caida.org/data/passive/ddos-20070804_dataset.xml` (2007)
8. Feily, M., Shahrestani, A., Ramadass, S.: A survey of botnet and botnet detection. In: Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on. pp. 268–273. IEEE (2009)
9. Ferguson, P.: Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing (2000)
10. Ferguson, P., Senie, D.: Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing. Tech. rep. (1997)
11. FlashCrowds: World cup 1998 dataset. `http://ita.ee.lbl.gov/html/contrib/WorldCup.html` (1998)
12. Gupta, P., Bansal, P.: A survey of attacks and countermeasures for denial of services (dos) in wireless ad hoc networks. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. p. 25. ACM (2016)
13. Han, J., Kamber, M., Pei, J.: Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 3rd edn. (2011)
14. Hoque, N., Bhattacharyya, D.K., Kalita, J.K.: Botnet in ddos attacks: trends and challenges. IEEE Communications Surveys & Tutorials 17(4), 2242–2270 (2015)
15. Ismail, Z., Jantan, A.: A review of machine learning application in botnet detection system. Sindh University Research Journal-SURJ (Science Series) 48(4D) (2016)
16. Jin, C., Wang, H., Shin, K.G.: Hop-count filtering: an effective defense against spoofed ddos traffic. In: Proceedings of the 10th ACM conference on Computer and communications security. pp. 30–41. ACM (2003)
17. Jung, J., Krishnamurthy, B., Rabinovich, M.: 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. ACM (2002)

18. Kandula, S., Katabi, D., Jacob, M., Berger, A.W.: Botz-4-sale: Surviving organized ddos attacks that mimic flash crowds (awarded best student paper). In: NSDI. USENIX (2005)
19. Latif, R., Abbas, H., Assar, S., Latif, S.: Analyzing Feasibility for Deploying Very Fast Decision Tree for DDoS Attack Detection in Cloud-Assisted WBAN. Springer International Publishing (2014)
20. Li, K., Zhou, W., Li, P., Hai, J., Liu, J.: Distinguishing ddos attacks from flash crowds using probability metrics. In: NSS. pp. 9–17. IEEE Computer Society (2009)
21. Mansfield-Devine, S.: The growth and evolution of ddos. Network Security 2015(10), 13–20 (2015)
22. Marcus, G., Rossi, F., Veloso, M.: Beyond the turing test. Ai Magazine (2016)
23. Networks, A.: Worldwide infrastructure security report (2016)
24. Ngo, T.: Data mining: Practical machine learning tools and technique, third edition by ian h. witten, eibe frank, mark a. hell. SIGSOFT Softw. Eng. Notes 36(5), 51–52 (Sep 2011), `http://doi.acm.org/10.1145/2020976.2021004`
25. Oikonomou, G., Mirkovic, J.: Modeling human behavior for defense against flash-crowd attacks. In: 2009 IEEE International Conference on Communications. pp. 1–6. IEEE (2009)
26. Patel, K., Thoke, A.: A details survey on black-hole and denial of service attack over manet environment (2016)
27. Prasad, K.M., Reddy, A.R.M., Rao, K.V.: Discriminating ddos attack traffic from flash crowds on internet threat monitors (itm) using entropy variations. African Journal of Computing & ICT 6(3) (2013)
28. Project, M.S.: `http://spoofer.cmand.org/summary.php`
29. Sachdeva, M., Kumar, K., Singh, G.: A comprehensive approach to discriminate ddos attacks from flash events. J. Inf. Sec. Appl. 26, 8–22 (2016)
30. Saravanan, R., Shanmuganathan, S., Palanichamy, Y.: Behavior-based detection of application layer distributed denial of service attacks during flash events. Turkish Journal of Electrical Engineering & Computer Sciences 24(2), 510–523 (2016)
31. Somani, G., Gaur, M.S., Sanghi, D., Conti, M., Buyya, R.: Ddos attacks in cloud computing: Issues, taxonomy, and future directions. arXiv preprint arXiv:1512.08187 (2015)
32. Somani, G., Gaur, M.S., Sanghi, D., Conti, M., Buyya, R.: Ddos attacks in cloud computing: issues, taxonomy, and future directions. Computer Communications (2017)
33. Thakar, B., Parekh, C.: Advance persistent threat: Botnet. In: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. p. 143. ACM (2016)
34. Thapngam, T., Yu, S., Zhou, W., Beliakov, G.: Discriminating ddos attack traffic from flash crowd through packet arrival patterns. In: Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. pp. 952–957. IEEE (2011)
35. Thomas M. Cover, J.A.T.: IEEE (1991)
36. Von Ahn, L., Blum, M., Langford, J.: Telling humans and computers apart automatically. Communications of the ACM 47(2), 56–60 (2004)

37. Xie, Y., Yu, S.Z.: A large-scale hidden semi-markov model for anomaly detection on user browsing behaviors. IEEE/ACM Transactions on Networking (TON) 17(1), 54–65 (2009)
38. Yaar, A., Perrig, A., Song, D.: Stackpi: New packet marking and filtering mechanisms for ddos and ip spoofing defense. IEEE Journal on Selected Areas in Communications 24(10), 1853–1863 (2006)
39. Yan, Q., Yu, F.R., Gong, Q., Li, J.: Software-defined networking (sdn) and distributed denial of service (ddos) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials 18(1), 602–622 (2016)
40. Yu, S., Guo, S., Stojmenovic, I.: Fool me if you can: mimicking attacks and anti-attacks in cyberspace. IEEE Transactions on Computers 64(1), 139–151 (2015)
41. Yu, S., Thapngam, T., Liu, J., Wei, S., Zhou, W.: Discriminating ddos flows from flash crowds using information distance. In: NSS 2009: Proceedings of the third International Conference on Network and System Security. pp. 351–356. IEEE (2009)
42. Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y., Tang, F.: Discriminating ddos attacks from flash crowds using flow correlation coefficient. IEEE Trans. Parallel Distrib. Syst. 23(6), 1073–1080 (2012)
43. Zhang, J., Liu, P., He, J., Zhang, Y.: A hadoop based analysis and detection model for ip spoofing typed ddos attack. In: Trustcom/BigDataSE/I? SPA, 2016 IEEE. pp. 1976–1983. IEEE (2016)

Bin Kong is currently a Ph.D student of Beijing Jiaotong University. He is currently the deputy director of National Secrecy Science and Technology Evaluation Center and Senior Engineer. His research interests include information security, risk assessment system, anomaly detection analysis, etc.

Kun Yang is currently a Ph.D student and study in Institute of Information Engineering, Chinese Academy of Science in Beijing from 2012 to the present. His research interests focus on DDoS attack detection, network traffic analysis and Machine Learning.

Degang Sun received his master degree from Beijing Jiaotong University. He has long engaged in Information Security Technology Research. His main research interests include electromagnetic leakage emission protection, wireless communication security and so on. He has published more than 40 academic papers, 6 books and more than 10 patents.

Meimei Li received her master degree from Peking University in 2007. She is currently a senior engineer of Institute of Information Engineering, Chinese Academy of Science, Beijing and an associate professor of University of Chinese Academy of Sciences. Her research interests include high security level system security, integration analysis, abnormal behavior detection and so on.

Shi Zhixin received the PhD degree in pattern recognition & intelligent systems from

Institute of Automation, Chinese Academy of Science, Beijing in 2014. He is currently a senior assistant professor at Institute of Information Engineering, Chinese Academy of Science. His research interests include the areas of DDoS attack detection, network monitoring, massive dataset mining. He is a member of the CCF.

Received: December 30, 2016; Accepted: May 10, 2017.