Multi-class DRDoS Attack Detection Method Based on Feature Selection

Tianqi Yang*, Weilin Wang, Ying Liu, and Huachun Zhou
School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
{19120156, 20120122, yliu, hchzhou}@bjtu.edu.cn

Abstract

Distributed denial of service (DDoS) attack is one of the most serious threats to the Internet The emergence of distributed reflection denial of service (DRDoS) attacks has increased the harm of DDoS attacks. Aiming at the common DRDoS attacks such as Memcached, TFTP, NTP, SSDP, SNMP and Chargen in the network, a multi-class DRDoS attack detection method based on feature selection is proposed. Through the analysis of the behavior and characteristics of attack, combined with probability distribution of features and feature importance to obtain a feature subset of 24 features. When constructing XGBoost model, the input features are the feature subset obtained by the above feature selection, and the model outputs multi classification results. The selected features can better reflect the characteristics of DRDoS attack and improve the detection performance of the model. Experimental results show that the feature subset obtained by this method has high precision in multi classification against DRDoS attacks, and is better than the traditional methods such as support vector machine and multi-layer perceptron. Feature selection not only reduces the processing time, but also reduces the malicious traffic by 99.93%.

Keywords: DRDoS, feature selection, malicious traffic reduction rate, ensemble learning

1 Introduction

DRDoS attack is also called reflection attack or amplification attack. It uses IP spoofing to send forged requests to a large number of servers on the Internet to reflect traffic, so as to send a large number of packets to the victim to attack. The above server is also called reflector [1]. The harm of DRDoS attack is that a small number of forged requests sent by attacker will eventually lead to a large number of responses from the server. The size ratio of response to request is called amplification factor which is used to measure the effect of a DRDoS attack [2]. At present, the amplification factor of a protocol used for DRDoS attack is generally between 20 and 100.

According to the DDoS attack resource analysis report of China in the second quarter of 2021 [3] issued by the national computer network emergency technology processing coordination center, the number of three types of key reflectors is 2915043, the domestic reflectors account for 80.0%, Memcached servers account for 3.5%, and network time protocol (NTP) servers accounted for 23.7%, and simple service discovery protocol (SSDP) servers accounted for 72.8%.

With the development of machine learning technology, scholars and researchers can analyze, detect and defend DDoS attacks by extracting the features of network traffic, so as to build model at low cost in the big data environment [4]. The general apply process of machine learning in cyberspace security research mainly includes six phases: abstract security problem, data collection, data preprocessing and

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 7, Article No. 15 (November 15, 2021)
DOI:*10.22667/ReBiCTE.2021.11.15.015*

*Corresponding author: Beijing Jiaotong University No.3 Shangyuancun Haidian District Beijing 100044 P. R. China, Tel: +86-17610361702

security feature extraction, model building, model verification and model performance evaluation. In the whole process, each phase cannot exist independently, and there is a certain correlation between them [5].

Feature selection and feature extraction are two important sub contents of feature engineering. Feature extraction is a process of dimensionality reduction by which an initial set of raw data is reduced to more manageable groups for processing, and feature selection is to select valuable features from candidate features to obtain the best feature subset [6]. Feature selection can reduce over fitting and improve model performance. Therefore, feature selection is an important step in machine learning.

XGBoost [7] is an ensemble learning method based on boosting, which reduces the error by paying more attention to the samples of learning errors in the previous round during the training process of each round of weak learners. XGBoost can not only regularize terms to prevent over fitting, but also support column sampling reduction calculation. At present, it has been widely used in industry.

The emergence of DRDoS attack intensifies the harm of DDoS attack. How to detect DRDoS attacks has become an urgent security problem. Quadir et al. [8]. have proposed a method to detect attack servers from legitimate traffic. This method uses an algorithm activated by the overrun traffic in the network. The overrun traffic is determined by the rate and ratio of request and response. The algorithm extracts the IP address of server, detects which server sends more packets than the requested packets or which server is not requested, and then blocks these servers with a firewall or access control list. Kshirsagar et al. [9] uses information gain (IG) and correlation (CR) to calculate score of features for feature selection. By setting thresholds of 0.5 and 0.25, feature subsets IGFS1, IGFS2, IGFS3, CRFS1, CRFS 2 and CRFS3 are obtained respectively. Then, the feature union of IGFS 1 and CRFS1 is taken as the new feature subset NMRFS, and the feature intersection of IGFS2 and CRFS2 is taken as the new feature subset NRFS. Finally, J48 classifier is used to train and detect the features in NMRFS and NRFS. Dodia et al. [10] proposed an SDN based system for filtering garbage traffic from ISP networks. The system uses a special type of honeypot to collect information about ongoing DRDoS attacks. Firewall rules derived from these data are used to prevent incoming amplification attack requests from reaching the reflectors, so as to avoid abuse of vulnerable servers. Xu et al. [11] proposed a DRDoS detection and defense method based on deep forest model, and integrated into the defense model to filter DRDoS attack traffic. Firstly, from the statistical point of view of different stages of DRDoS attack traffic in big data environment, the host based DRDoS threat index (HDTI) is extracted from the network traffic. Then, a DRDoS detection and defense model based on deep forest is built by using the features of HDTI. Finally, the detection results of deep forest model are used to discard the traffic identified at different stages and different detection points.

Most of the detection and defense methods against DRDoS attack are for specific protocols, and the designed detection method is difficult to be extended to other protocols. Many methods are based on statistical learning of traffic, such as calculating entropy or distance between network traffic, which mainly detect whether DRDoS attacks occur without specific classification of traffic. These methods have high requirements for computing resources, relatively low detection performance and high false positive rate.

This paper proposes a multi-class DRDoS attack detection method based on feature selection. This method extracts the features of network traffic, selects the relevant features of DRDoS attack through a series of feature engineering, and inputs XGBoost model for multi-class detection. Combining the advantages of ensemble learning method XGBoost and feature selection, this method can not only improve the accuracy of detection, but also reduce the processing time, effectively detect a variety of DRDoS attacks in the network and improve network security.

The main contributions of this paper are as follows:

1. Build servers in the testbed, write scripts to simulate multiple kinds of DRDoS attacks, including Memcached, simple file transfer protocol (TFTP), NTP, SSDP, simple network management

protocol (SNMP) and Chargen, and complete the collection of DRDoS attack traffic and normal traffic.

2. Through the analysis of attack principle, probability distribution of features and feature importance, the feature subset that plays a key role in DRDoS attack detection is obtained, which helps to improve the performance and efficiency of detection. Compared with many machine learning methods, XGBoost with the highest classification performance is selected as the detection model.

3. In the experimental environment, the online detection system is realized, and the performance of different schemes is compared. The detection results show that the multi-class DRDoS attack detection method based on feature selection proposed in this paper can significantly improve the detection performance and detect a variety of DRDoS attacks.

2 Proposed Methods

The system framework of multi category DRDoS attack detection based on feature selection is divided into offline and online phases, as shown in Figure 1.

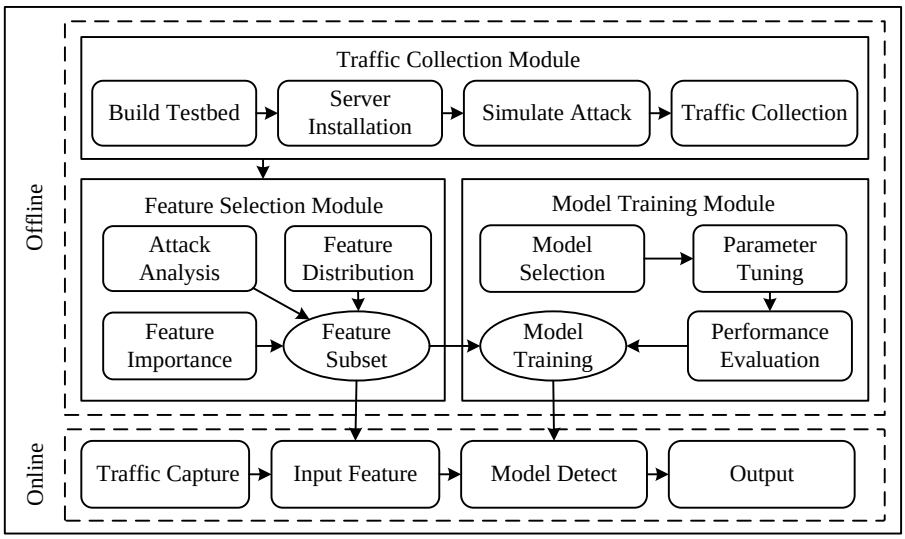


Figure 1: System framework.

1. Offline phase: the offline phase is divided into traffic collection module, feature selection module and model training module. The first is the traffic collection module, which collects traffic by simulating a variety of DRDoS attacks in the testbed, uses CICFlowMeter [12] to extract flow records of the collected traffic, obtains the CSV file with 84 bidirectional flow features, and establishes the data set of DRDoS attacks. The feature selection module performs feature selection on the offline dataset, including the principle analysis of specific DRDoS attacks, the ranking of feature importance by using machine learning method, and the analysis of probability distribution of specific features of normal traffic and DRDoS attack traffic, and finally obtains the feature subset valuable for DRDoS attack detection. Finally, the model training module uses the feature for model training. By comparing the performance of different machine learning methods, the machine learning method model with the best detection performance is selected for online detection.

2. Online phase: the process of online phase needs to be supported by offline phase. Firstly, the traffic at the network entrance is captured. CICFlowMeter is used to extract the features of the

captured traffic to obtain the flow records. The feature subset obtained by the feature selection module is used to filter the flow records, which are input into the model obtained by the model training module. The model detects and outputs the classification results.

2.1 Traffic Collection

There are many DDoS attack simulation softwares on the Internet, but because DRDoS attack use servers to attack, there is no tool to directly simulate DRDoS attacks.

From the perspective of security and convenience, the DRDoS attack traffic in the offline dataset is collected in the testbed. Install servers with different protocols in the testbed, and make necessary settings for these servers to meet the requirements of the attack, and then write a python script to send forged requests to the server. The response sent by the server is the DRDoS attack traffic to be collected. Because the traffic is obtained from the experimental environment, the data set does not have security risks, and because the traffic is obtained from the real server, the simulated attack process is the same as the real attack process, which can reflect the real characteristics of DRDoS attack.

The network topology of the experimental environment for collecting DRDoS attack traffic is shown in Figure 2. It contains six virtual machines (VM), of which R1 and R2 are routers. S1 and S2 are servers and installed with servers with different protocols, including Memcached, TFTP, Chargen, NTP, SNMP and SSDP, so as to simulate DRDoS attacks with different protocols. Running a python script on an attacker sends requests to simulate attack. The DRDoS attack traffic is collected on the victim, and TCPdump is used to capture traffic and generate PCAP files.

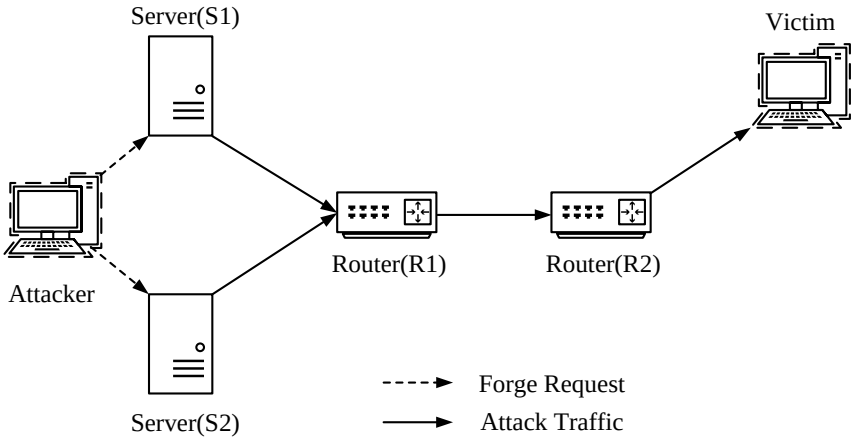


Figure 2: DRDoS attack traffic collection network topology.

The collection of normal traffic should not only consider the authenticity, but also consider the complexity of traffic in the real network. The normal traffic in this offline dataset comes from the real traffic collected on the personal computer, including different types of traffic such as browsing web pages, sending and receiving emails, downloading files, chatting online and so on.

Finally, the PCAP files of the collected traffic are extracted by CICFlowMeter tool to generate CSV files, and the offline dataset is obtained.

2.2 Feature Selection

In this paper, through the analysis of DRDoS attack principle, the probability distribution of features and feature importance of normal traffic and DRDoS attack traffic are analyzed for feature selection.

2.2.1 Attack principle analysis and feature distribution

Firstly, the principle of specific DRDoS attack is analyzed. Based on the analysis results, the related features are selected. DRDoS attack reflect and amplify traffic through the reflector, but different DRDoS attacks have different specific principles for traffic amplification. The following will introduce different DRDoS attack principles and analyze the features that can reflect their principles, so as to find the common important features for detecting DRDoS attacks.

TFTP amplification attack uses TFTP protocol. The goal of TFTP protocol is to establish a transmission protocol similar to file transfer protocol (FTP) but only supports file upload and download functions on UDP. It is a simplified version of FTP based on UDP. The attacker abused it to carry out DRDoS attack [13]. The principle of TFTP attack is shown in Figure 3.

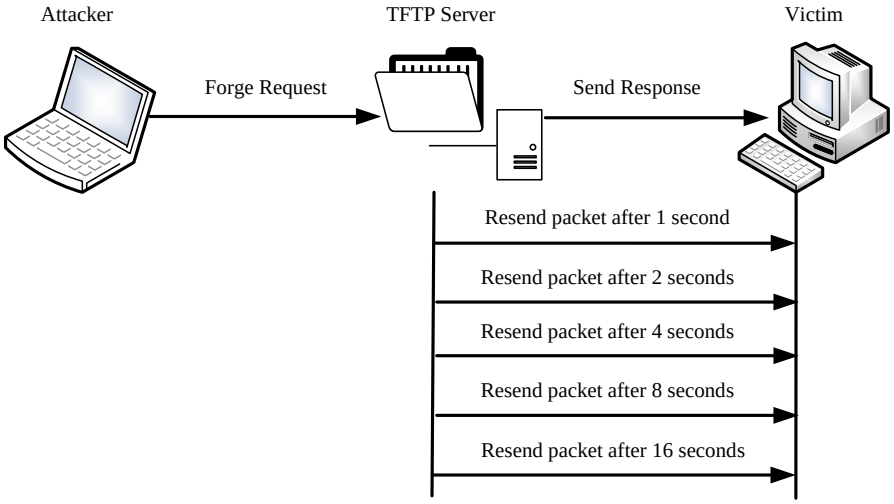


Figure 3: TFTP attack principle.

TFTP amplification attack uses the retransmission mechanism of TFTP protocol to amplify traffic. The attacker sends forged requests to the TFTP server to obtain files. After receiving the requests, the server sends responses of data block to the victim. Because the victim does not send requests to the server, the responses cannot be acknowledged, and the server will retransmit. The retransmission time of TFTP increases exponentially. As shown in Figure 3, TFTP will retransmit after 1, 2, 4, 8 and 16 seconds. The total retransmission time is 31 seconds and the total number of packets is six. So related features will be helpful for TFTP amplification attack detection.

Among the 84 features extracted by CICFlowMeter, many features related to time are included. For example, "Flow Duration" is the feature used to describe the duration of a traffic flow, and the size of this feature of TFTP corresponds to the total retransmission time of TFTP of 31 seconds. The probability distribution of "Flow Duration" is shown in Figure 4. Benign represents normal traffic. It can be seen that the probability distribution of normal traffic is concentrated in a lower range, while the duration of TFTP is fixed at $3.1 * 10^7$ microseconds.

In addition, the payload size of the response packet sent by TFTP is 516 bytes, and many features are related to the packet size, such as "Fwd Packet Length Max", "Fwd Packet Length Min" and "Fwd Packet Length Mean", these features are used to describe the maximum, minimum and average packet load of the forward flow, and their sizes are fixed at 516. The probability distribution of "Fwd Packet Length Mean" is shown in Figure 5. The normal traffic is widely distributed, and the size is mainly below 500, while the size of TFTP is fixed at 516.

A complete TFTP attack sends a total of six packets, corresponding to the size of "Total Fwd Packet"

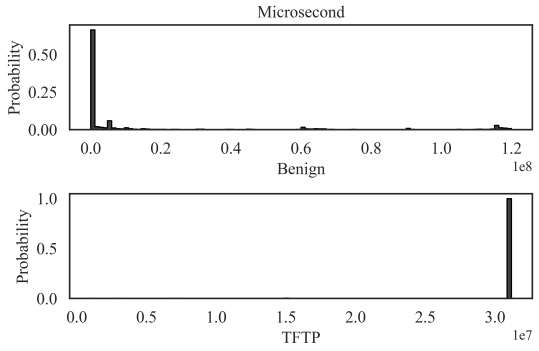


Figure 4: Probability distribution of "Flow Duration".

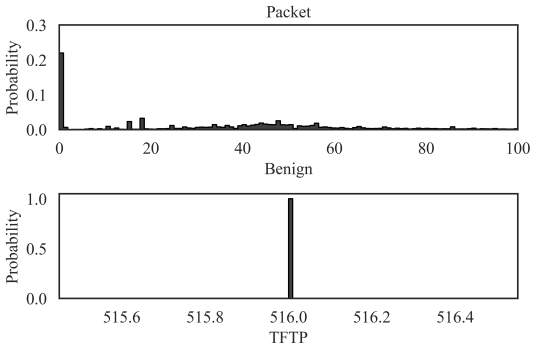


Figure 5: Probability distribution of "Fwd Packet Length Mean".

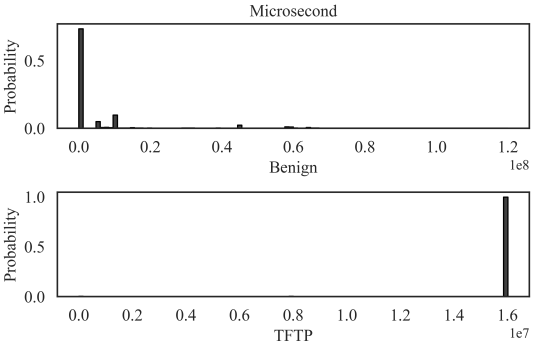


Figure 6: Probability distribution of "Idle Max".

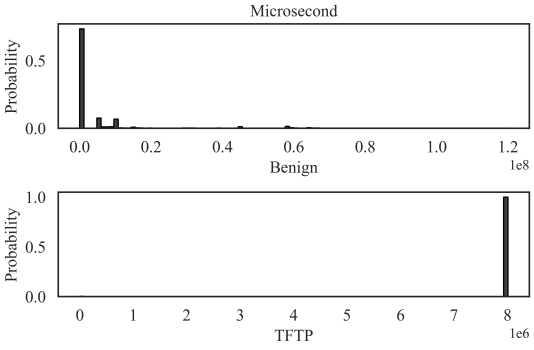


Figure 7: Probability distribution of "Idle Min".

feature is 6. Through these features, the characteristics of TFTP attack can be clearly distinguished from normal traffic, and it can be easily distinguished by machine learning method.

In addition, due to the special retransmission mechanism of TFTP, the time interval between two TFTP packets may reach 8 seconds or 16 seconds after receiving no ack, exceeding the active time threshold of 5 seconds set in CICFlowMeter, which is judged as idle by CICFlowMeter. However, due to the absence of TFTP retransmission mechanism, normal UDP will hardly be idle.

As shown in Figure 6 and Figure 7, the probability distribution of normal traffic are distributed near the lower value, while the feature "Idle Max" of TFTP is mainly distributed around 16 seconds and feature "Idle Min" are mainly distributed around 8 seconds. TFTP and normal traffic are obviously distinguished in the features related to idle time.

In the Memcached amplification attack, the characteristic of Memcached is used to provide memory cache services to carry out amplification attacks. The attacker first uses the "set key value" request to set a large value in the server, the size of which can reach 1 MB. And then obtains the value through command of "get key", the request has only 20 bytes, but it can return 1 MB data, which can achieve tens of thousands of times the amplification effect. The response of Memcached amplification attack is divided into multiple packets with a payload size of 1400 bytes. The number of packets in a single response can reach hundreds and the amplification factor can reach tens of thousands. Therefore, the features of Memcached attack are related to the size and number of packets. The response to the attack can reach hundreds of packets, which corresponds to the "Total Fwd Packet" feature.

The NTP amplification attack utilizes its special "monlist" command, which is used to monitor the NTP server [14]. The attacker sends a forged "monlist" command request. After the NTP server responds to the "monlist" command, it will return the IP addresses of the last 600 clients with which it has synchronized. The response packets are divided according to every six IP addresses. The "monlist"

command request of a single NTP can return 100 packets. The payload size of these response packets is 440 bytes, which can achieve high traffic amplification effect. Because the new version of NTP server fixes this vulnerability and discards the "monlist" command, if a stream containing a large number of NTP packets is found, it can basically be judged as NTP amplification attack. Its characteristics are also related to "Total Fwd Packet" feature.

From the probability distribution of "Total Fwd Packet" feature in Figure 8, it can be seen that the distribution of packets with normal traffic is low, while the number of packets in Memcached is often more than that of normal traffic due to the features of attack. NTP is similar.

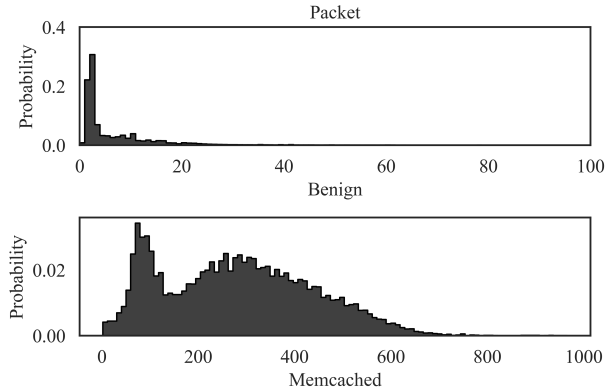


Figure 8: Probability distribution of "Total Fwd Packet".

In addition, Chargen server returns any character for amplification after receiving the request. SSDP is a service discovery protocol, which returns multiple packets carrying network device information after receiving the request. SNMP server returns a large amount of management information after receiving the request from "GetBulkRequest" command. Therefore, Chargen, SSDP, and SNMP attacks are strongly related to packet size and number of packets. In short, DRDoS attacks has a strong correlation with the characteristics of packet size and number of packets due to its amplification characteristic. These features can well reflect the characteristics of DRDoS attacks and help to detect DRDoS attacks..

2.2.2 Feature Importance

Feature importance can help in feature selection. By analyzing the features with high feature importance, it can help to judge the stability and rationality of the model. This paper integrates the feature importance ranking obtained by two methods. One is the feature importance ranking of XGBoost based on tree model, and the other is the permutation importance [15]. Permutation importance method judges the importance by removing the impact of a single feature on the overall prediction effect. The importance ranking of the two features is shown in Table 1.On the left is the importance ranking of XGBoost method and on the right is the importance ranking obtained by permutation importance method. Ten features with the greatest importance are selected and sorted in descending order, ignoring the remaining features with minimal importance.

It can be seen from Table 1 that the importance of features obtained by the two methods is relatively consistent, but the order of some features changes. According to the feature importance ranking of both methods, the three most important features are "Protocol", "Packet Length Min" and "Fwd Packet Length Max". Since the protocols used by DRDoS attacks are basically based on UDP, the "Protocol" feature is very important. The other two features are related to the packet size, which is in line with the amplification features of DRDoS attack.

Based on the above, the feature subset finally used to detect DRDoS attacks is obtained, as shown

Table 1: Feature importance ranking

No.	XGBoost	Permutation Importance
1	Packet Length Min	Protocol
2	Protocol	Packet Length Min
3	Fwd Packet Length Max	Fwd Packet Length Max
4	Fwd Packet Length Min	Total Length of Fwd Packet
5	Average Packet Size	Idle Mean
6	Bwd Bytes/Bulk Avg	Fwd Seg Size Min
7	Fwd Packet Length Mean	Packet Length Mean
8	Packet Length Mean	Fwd IAT Min
9	Flow IAT Min	Flow IAT Min
10	Fwd IAT Min	Average Packet Size

in Table 2, including 24 features. These features jointly reflect the general characteristics of DRDoS attacks. For example, DRDoS attacks is basically based on UDP, so the "Protocol" feature is very important. Secondly, DRDoS attacks have the characteristics of amplification, which shows that the number and size of response packets are significantly larger than normal traffic, so the feature subset contains many features related to packet size and number of packet. In addition, some DRDoS attacks are amplified by retransmission mechanism, which are strongly related to idle and active time.

Table 2: Feature subset

No.	Feature	No.	Feature
1	Protocol	13	Packet Length Max
2	Flow Duration	14	Packet Length Mean
3	Total Length of Fwd Packet	15	Packet Length Std
4	Total Length of Bwd Packet	16	Fwd Act Data Pkts
5	Fwd Packet Length Max	17	Idle Mean
6	Fwd Packet Length Min	18	Idle Std
7	Fwd Packet Length Mean	19	Idle Max
8	Fwd Packet Length Std	20	Idle Min
9	Bwd Packet Length Max	21	Active Mean
10	Bwd Packet Length Std	22	Active Std
11	Fwd Header Length	23	Active Max
12	Packet Length Min	24	Active Min

2.3 XGBoost

XGBoost is a ensemble learning method based on the principle of boosting. It can prevent over fitting, and support column sampling to reduce calculation. It has great advantages in performance and time.

As shown in Figure 9, XGBoost adopts a binary tree model. At the beginning, all samples are on one leaf node. Then the leaf nodes gradually generate a tree by splitting. The basic idea of splitting is to pre sort all features according to the value of the feature, then find the best segmentation point on the feature when traversing the segmentation point, and then split the data into left and right child nodes. As shown in the example in Figure 9, take 100 as the segmentation point of feature 1, then split, and then further split through feature 2 and feature 3 to complete the final classification. XGBoost classifies data through the splitting of multiple features, which is similar to the idea mentioned in this paper that finding normal and attack traffic through the distribution of features has multiple features that can clearly

distinguish and finally determine the classfication. XGBoost can automatically deal with missing values, abnormal values, data imbalance by default. Compared with other machine learning methods that need to normalize the data values in the databset, XGBoost can directly use the original values of the features in the dataset for training, and can better learn the real characteristics of attacks and normal traffic.

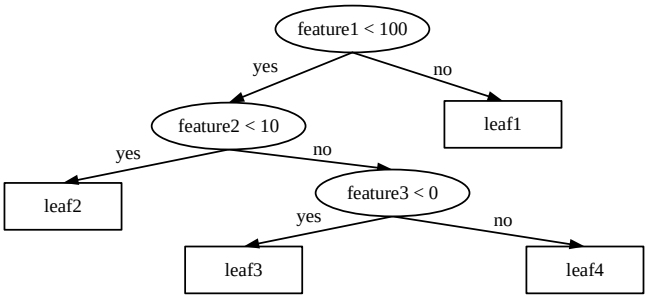


Figure 9: XGBoost tree model.

3 Experiments

3.1 Testbed

This experiment builds an experimental environment based on VMware. One physical server was used in the experiment. The virtual machine operating system was Ubuntu 18.04. The number of virtual cores was 1 and memory was 8GB.

This paper selects six amplification attacks: Memcached, NTP, Chargen, TFTP, SNMP and SSDP. The server of these protocols is installed on the virtual machine as the reflector, and the attack host uses Python to write a script to send forged requests. According to the specific principles of different DRDoS attacks, the settings of the server in the experimental environment and the server open on the Internet are consistent, and the attack process in the experimental environment is the same as the real attack process, which can reflect the authenticity characteristics.

After collecting attack traffic in the experimental environment, CICFlowMeter is used for feature extraction together with normal traffic to establish the dataset. Distinguish different types of traffic according to IP address and port to add labels. The number and proportion of different traffic types are shown in Table 3. The total number of flow records in the dataset is 194919.

Table 3: The number and proportion of flow records of different types in the dataset

Type	**Number**	**Proportion**
Benign	43720	22.42%
TFTP	42059	21.57%
SSDP	22035	11.30%
NTP	9430	4.8%
Memcached	39021	20%
Chargen	23077	11.84%
SNMP	15577	8%

The experiment evaluates the performance of the model through five metrics: accuracy, precision, recall, F1 score and confusion matrix. The left side of the confusion matrix is the real label and the lower

side is the predicted label. In addition, this paper proposes the malicious traffic reduction rate to reflect the proportion of malicious traffic reduction after model detection. Its definition is shown as Eq (1).

$$rate = \sum_{i=0}^{n} T_i / \sum_{i=0}^{n} A_i \tag{1}$$

Where n is the number of attack types, A_i is the real number of flow records of each attack type, T_i is the number of flow records of corresponding attack types correctly judged by the model, and the proportion of malicious traffic reduced after attack detection is calculated by the number of correct types of attacks and the number of true types of attacks.

3.2 Offline Training

In this section, four machine learning methods based on different principles are selected for comparative experiments, and the performance of offline training is compared between XGBoost and traditional machine learning methods, such as multi-layer perception (MLP), support vector machines (SVM) and k-nearest neighbor (KNN), The feature used is the feature subset obtained by feature selection. The experimental results are shown in Table 4. From the accuracy obtained from offline training, XGBoost has the highest accuracy, reaching 99.97%, and SVM has the lowest accuracy, only 76.68%. The performance of MLP and KNN is also excellent, and the accuracy can reach about 99%. In terms of training time, XGBoost has the shortest time and KNN has the longest time. It can be seen that XGBoost has obvious advantages in training time.

Table 4: The number and proportion of different types of flows in the offline dataset

Method	**Accuracy**	**Time/Second**
XGBoost	99.97%	11.77
SVM	76.68%	156.83
KNN	99.24%	499.34
MLP	99.23%	47.15

The precision and recall of different classifiers in multi classification are shown in Figure 10 and Figure 11 respectively. As can be seen from Figure 10 and Figure 11, XGBoost has the highest precision and recall, and all categories are close to 1. The other three classifiers have a large gap with XGBoost, and the detection precision and recall of Chargen and SNMP amplification attacks are very low. The precision and recall of SVM against Chargen attack even reach 0, while XGBoost still has high precision and recall. Based on the above analysis, XGBoost has excellent performance in accuracy, precision and recall of multi classification.

3.3 Online Detection

In the online detection experiment part, the normal traffic is replayed in the experimental environment, and the DRDoS attack is carried out to generate the traffic required for online detection. The network topology of the online detection domain is shown in Figure 12. A total of seven virtual machines are used, of which VM3 and VM4 are routers. VM2 is attacker, which is used to send forged requests to VM5 and VM6 as servers to generate DRDoS attack traffic, and VM7 uses TCPreplay to replay normal traffic, The victim receives attack and normal mixed traffic. Online detection is performed at the victim's network entry router1, which can receive mixed traffic generated by normal traffic and attack traffic.

In the phase of online detection, the performance of the three schemes is compared to prove excellent performance of the proposed method. Scheme 1 is the method proposed in this paper, using the feature

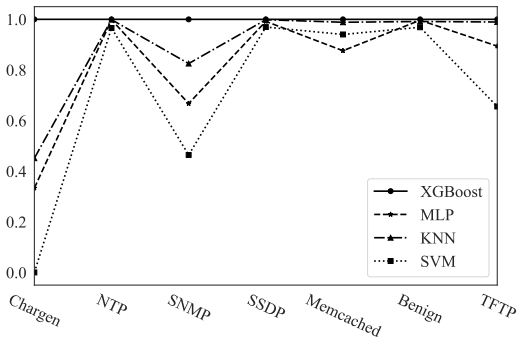


Figure 10: Precision of different classifiers.

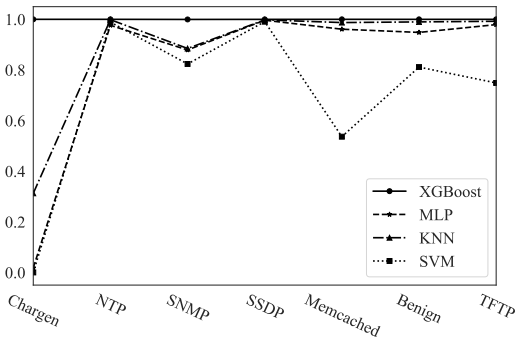


Figure 11: Recall of different classifiers.

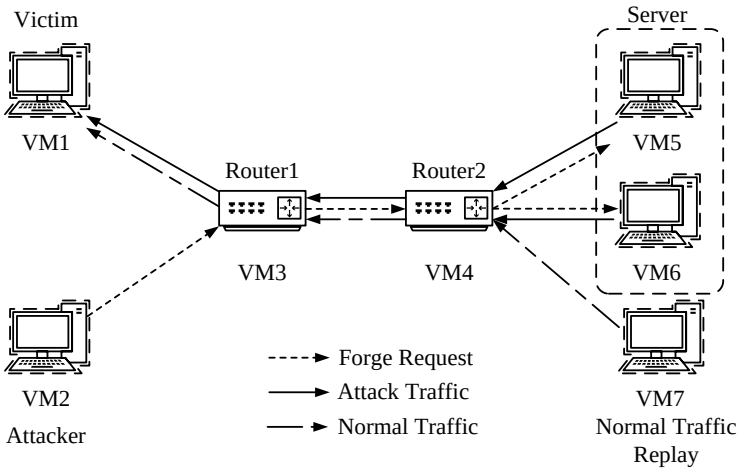


Figure 12: Network topology of online detection.

subset selected as the input and XGBoost as the classifier. Scheme 2 uses 77 features as input and XGBoost as classifier, where 77 is the number of all features that can be used for model training and detection after removing the seven features including “Flow ID”, “Src IP”, “Src Port”, “Dst IP”, “Dst Port”, “Timestamp” and “Label”. Scheme 3 uses the method in [9] to perform the feature selection through IG and CR, obtains the feature subsets NMRFS and NRFS as the input, and uses J48 as the classifier. The online detection performance of the three schemes is shown in Table 5.

Table 5: Metrics of different schemes

Scheme	Number of Features	Accuracy	Malicious Traffic Reduction Rate	Time/Second
1	24	99.96%	99.93%	1.63
2	77	97.64%	89.7%	2.43
3	35	99.28%	88.44%	1.78

As can be seen from Table 5, the scheme 1 has the highest accuracy of 99.96%, the accuracy of scheme 2 is 97.64%, which is two percentage points lower than scheme 1, and the accuracy of scheme 3 is slightly lower than scheme 1. However, the malicious traffic reduction rate of scheme 1 is much higher than the other two schemes, reaching 99.93%. In addition, the reduction of features greatly reduces the detection time.

Table 6 shows the multi classification precision, recall and F1 score of different schemes during

online detection. In terms of precision, the precision of SSDP in scheme 2 is 67.45%, and the precision of NTP in scheme 3 is 92.61%. The multi classification precision of the three is relatively consistent and basically maintained at the same level. In terms of recall, the recall of TFTP in scheme 2 is 28.57%, which is far lower than scheme 1, and the recall of NTP in scheme 3 is 20.4%, which is also far lower than scheme 1. Scheme 1 maintained a high level in precision, recall and F1 score of each category.

Table 6: Metrics of different schemes

Scheme	Metric	Benign	Chargen	Memcached	NTP	SNMP	SSDP	TFTP
1	Precision	99.99%	98.83%	100%	98.4%	99.94%	99.94%	99.87%
	Recall	99.97%	100%	100%	100%	99.66%	99.9%	100%
	F1 score	99.98%	99.41%	100%	99.19%	99.8%	99.92%	99.94%
2	Precision	99.99%	100%	100%	98.39%	99.94%	67.45%	100%
	Recall	99.94%	100%	100%	99.81%	99.66%	99.92%	28.57%
	F1 score	99.96%	100%	100%	99.1%	99.80%	80.54%	44.45%
3	Precision	99.23%	100%	100%	92.61%	99.52%	99.9%	99.9%
	Recall	100%	100%	100%	20.4%	99.6%	99.11%	100%
	F1 score	99.61%	100%	100%	33.43%	99.56%	99.5%	99.9%

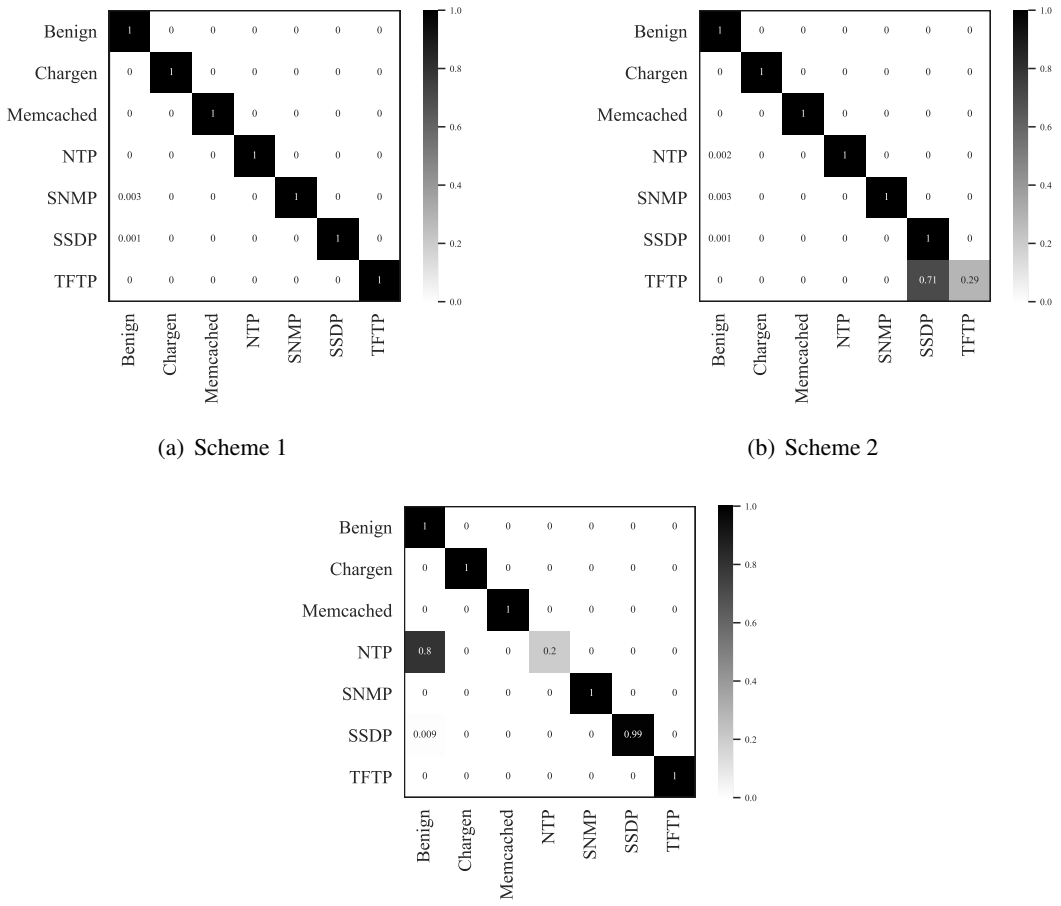
In order to understand the specific classification prediction of the scheme and analyze the specific misjudgment of the scheme, the multi classification normalized confusion matrix diagrams of the three schemes are compared, as shown in Figure 13.

The confusion matrix of scheme 1 shows excellent performance, and there are only few misjudgments in the case of multiple classification. In the confusion matrix of scheme 2, although other types of judgment are accurate, due to over fitting using too many features, a large number of TFTP traffic is misjudged as SSDP traffic. Scheme 3 has a serious misjudgment in the classification of NTP attack, and most NTP attack are classified as benign. It can be seen that the feature subset obtained by feature selection in this method can fully reflect the characteristics of DRDoS attack, so as to help improve the performance of DRDoS attack detection.

4 Conclusion

This paper proposes a multi class DRDoS attack detection method based on feature selection, and builds its own data set. In order to improve the detection performance of the model, this method carries out feature selection based on the principle of DRDoS attack, and obtains the valuable feature subset for DRDoS attack detection combined with probability distribution of features and feature importance. At the same time, comparing the performance of different machine learning methods, XGBoost with the best performance is selected as the online detection model. Compared with other schemes, the accuracy of the proposed method can reach about 99%, which verifies the effectiveness of this method in detecting multi category DRDoS attacks in real-time network environment.

Compared with the traditional machine learning methods such as SVM, KNN and MLP, the multi classification detection method based on XGBoost proposed in this paper has higher precision and recall. At the same time, the feature selection of the features in the data set reduces the over fitting, which not only greatly improves the malicious traffic reduction rate to 99.93%, but also reduces time and resources, and makes up for the shortcomings of the existing DRDoS attack detection methods. The next step is to compare with more research methods for DRDoS attack detection, reflecting the advantages of this method in performance and time. At the same time, we try to carry out online detection experiments in more complex network environment to improve the applicability of this method in real network



(a) Scheme 1

(b) Scheme 2

(c) Scheme 3

Figure 13: Normalized confusion matrix of different schemes.

environment.

Acknowledgments

This paper is supported by National Key R&D Program of China under Grant No. 2018YFA0701604. Tianqi Yang is the corresponding author of this paper.

References

[1] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi. Distributed reflection denial of service attack: A critical review. *International Journal of Electrical & Computer Engineering*, 11(6), 2021.

[2] C. Rossow. Amplification hell: Revisiting network protocols for DDoS abuse. In *Proc. of the 2014 Network and Distributed System Security Symposium (NDSS'14), San Diego, California, USA*, February 2014.

[3] CNCERT. Analysis report on DDOS attack resources in China, August 2021.

[4] X. Jing, Z. Yan, and W. Pedrycz. Security data collection and data analytics in the internet: A survey. *IEEE Communications Surveys & Tutorials*, 21(1):586–618, 2018.

[5] L. Zhang, Y. Cui, J. Liu, Y. Jiang, and J. Wu. Application of machine learning in cyberspace security research. *Chinese Journal of Computers*, 41(9):1943–1975, 2018.

[6] M. Wang, Y. Lu, and J. Qin. A dynamic MLP-based DDoS attack detection method using feature selection and feedback. *Computers & Security*, 88:101645, 2020.

[7] T. Chen and C. Guestrin. Xgboost: A scalable tree boosting system. In *Proc. of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'16), San Francisco, California, USA*, pages 785–794. ACM, August 2016.

[8] A. Quadir, J. Christy Jackson, J. Prassanna, K. Sathyarajasekaran, K. Kumar, H. Sabireen, and V. Vijaya Kumar. An efficient algorithm to detect ddos amplification attacks. *Journal of Intelligent & Fuzzy Systems*, (Preprint):1–8, 2020.

[9] D. Kshirsagar and S. Kumar. A feature reduction based reflected and exploited ddos attacks detection system. *Journal of Ambient Intelligence and Humanized Computing*, Online Published, 2021. https://doi.org/10.1007/s12652-021-02907-5.

[10] P. Dodia and Y. Zhauniarovich. Poster: SDN-based system to filter out DRDoS amplification traffic in ISP networks. In *Proc. of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS'19), London, United Kingdom*, pages 2645–2647. ACM, November 2019.

[11] R. Xu, J. Cheng, F. Wang, X. Tang, and J. Xu. A DRDoS detection and defense method based on deep forest in the big data environment. *Symmetry*, 11(1):78, 2019.

[12] A. H. Lashkari, G. Draper-Gil, M. S. I. Mamun, and A. A. Ghorbani. Characterization of tor traffic using time based features. In *Proc. of the 3rd International Conference on Information Systems Security & Privacy (ICISSP'17), Porto, Portugal*, pages 253–262. Scitepress, February 2017.

[13] B. Sieklik, R. Macfarlane, and W. J. Buchanan. Evaluation of tftp ddos amplification attack. *computers & security*, 57:67–92, 2016.

[14] J. J. C. Gondim, R. de Oliveira Albuquerque, and A. L. S. Orozco. Mirror saturation in amplified reflection distributed denial of service: A case of study using snmp, ssdp, ntp and dns protocols. *Future Generation Computer Systems*, 108:68–81, 2020.

[15] A. Altmann, L. Toloşi, O. Sander, and T. Lengauer. Permutation importance: a corrected feature importance measure. *Bioinformatics*, 26(10):1340–1347, 2010.

Author Biography

Tianqi Yang received the B.S. degree in telecommunications engineering from Beijing Jiaotong University (BJTU), China, in 2019, and he is currently a graduate student at Beijing Jiaotong University. He joined the National Engineering Lab for Next Generation Internet Interconnection Devices, BJTU. His research interest includes network security, and machine learning.

Weilin Wang received the B.S. degree in telecommunications engineering from Beijing Jiaotong University (BJTU), China, in 2020, and she is currently studying for the Ph.D. degree in information and telecommunications engineering. She joined the National Engineering Lab for Next Generation Internet Interconnection Devices, BJTU. Her research interest includes the architecture of next generation internet, network security, and machine learning.

Ying Liu received the B.S. degree from Beijing Jiaotong University (BJTU), China, in 2000. She received the M.S. and Ph.D. degrees in communication and information system from Beijing Jiaotong University in 2003 and 2011, respectively. Now, she is a professor in National Engineering Lab for Next Generation Internet Interconnection Devices at BJTU. Her main research interests are in the area of communication engineering, network security and routing protocols.

Huachun Zhou received the B.S. degree from the People's Police Officer University of China in 1986. He received the M.S. in telecommunication automation and Ph.D. degrees in telecommunications and information system from Beijing Jiaotong University in 1989 and 2008, respectively. Now, he is a professor in National Engineering Lab for Next Generation Internet Interconnection Devices at BJTU. His main research interests are in the area of mobility management, mobile and secure computing, routing protocols, network management and satellite network.