Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.051194

ARTICLE

IGED: Towards Intelligent DDoS Detection Model Using Improved Generalized Entropy and DNN

Yanhua Liu[1,2,3], Yuting Han[1,2,3], Hui Chen[1,2,3], Baokang Zhao[4,*], Xiaofeng Wang[4] and Ximeng Liu[1,2,3]

[1]College of Computer and Data Science, Fuzhou University, Fuzhou, 350108, China

[2]Engineering Research Center of Big Data Intelligence, Ministry of Education, Fuzhou, 350108, China

[3]Fujian Key Laboratory of Network Computing and Intelligent Information Processing, Fuzhou University, Fuzhou, 350108, China

[4]College of Computer, National University of Defense Technology, Changsha, 410073, China

*Corresponding Author: Baokang Zhao. Email: bkzhao@nudt.edu.cn

Received: 29 February 2024 Accepted: 11 June 2024 Published: 15 August 2024

ABSTRACT

As the scale of the networks continually expands, the detection of distributed denial of service (DDoS) attacks has become increasingly vital. We propose an intelligent detection model named IGED by using improved generalized entropy and deep neural network (DNN). The initial detection is based on improved generalized entropy to filter out as much normal traffic as possible, thereby reducing data volume. Then the fine detection is based on DNN to perform precise DDoS detection on the filtered suspicious traffic, enhancing the neural network's generalization capabilities. Experimental results show that the proposed method can efficiently distinguish normal traffic from DDoS traffic. Compared with the benchmark methods, our method reaches 99.9% on low-rate DDoS (LDDoS), flooded DDoS and CICDDoS2019 datasets in terms of both accuracy and efficiency in identifying attack flows while reducing the time by 17%, 31% and 8%.

KEYWORDS

DDoS; real-time; improved generalized entropy; DNN

1 Introduction

With the rapid advancement of network technologies [1], the landscape of DDoS attacks has has expanded dramatically in both magnitude and sophistication. These sophisticated assaults pose formidable challenges, precipitating disruptions in service delivery, exacerbating network latencies, and engendering comprehensive exhaustion of computational resources. Consequently, the imperative to promptly and accurately detect DDoS attacks has emerged as a pivotal aspect in maintaining the integrity and functionality of networked systems, which underscores the critical need for advanced detection methods. Fig. 1 shows a DDoS attack scenario where the attacker launches a DDoS attack on some important servers by manipulating multiple puppet machines [2]. These DDoS attacks come from different puppet machines, and each puppet machine may execute different types of DDoS attacks.

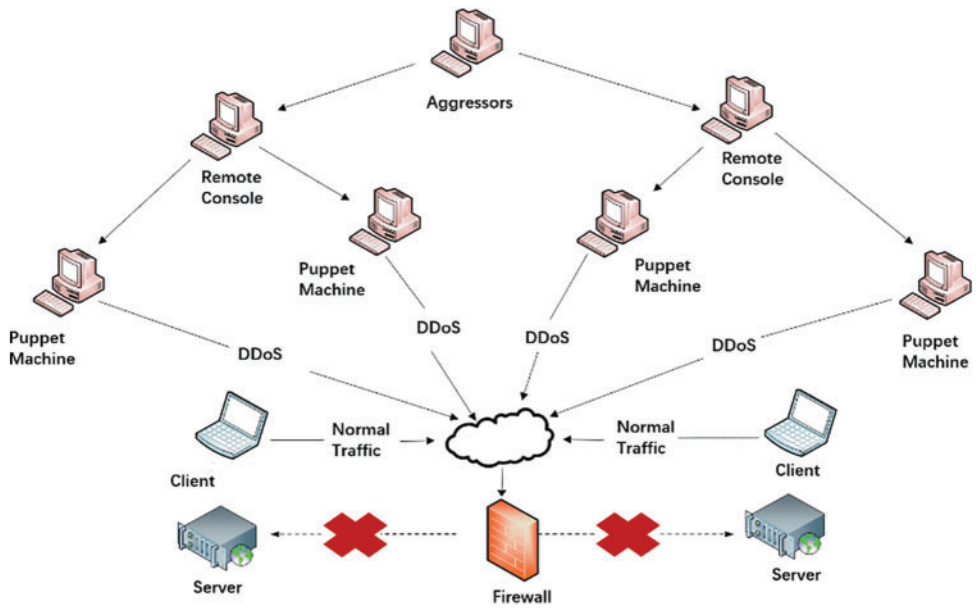


Figure 1: Example of DDoS attacks

Nowadays DDoS detection techniques can be categorized into three types: statistic-based methods [3], machine-learning-based methods [4], and deep-learning-based methods [5]. The statistic-based DDoS detection methods adjust the threshold by enhancing entropy to identify and filter DDoS attacks [6]. However, their relative simplicity in model design and paucity of extracted features contribute to a limitation in achieving high detection accuracy. Therefore, a deep learning-based approach was proposed by training a model from a compact representation of the input data and applying a random threshold method to detect DDoS [7–9]. While machine learning and deep learning methods boast superior accuracy in detection tasks, they are encumbered by a heightened degree of implementation complexity and a sluggish detection pace [10], which does not meet the real-time requirements of the network [11]. Therefore, some scholars currently detect DDoS by combining statistics and deep learning methods [12,13]. Nonetheless, a commonality above these methods lies in their reliance on the information entropy, which is insufficient in dynamically adapting the entropy value to effectively discern and counteract DDoS attacks [6,14]. With the persistent escalation in network bandwidth and transmission velocities [15,16], current DDoS detection methods often struggle to keep pace with the constantly evolving attack techniques employed by attackers, which are difficult to achieve high accuracy and real-time performance.

In response to the aforementioned challenges, we propose a dual-phase strategy, which consists of an initial detection model based on improved generalized entropy and a fine detection model based on DNN. By synergistically harnessing the rapid computational prowess of the generalized entropy methods and the heightened precision offered by DNN to filter as much normal traffic as possible in the initial detection model, followed perform precise DDoS detection in the fine detection model. The main contributions of this work are as follows:

(1) Feature extraction and extension of captured traffic. Firstly, feature extraction of traffic is performed by utilizing the importance of traffic features to reduce the dimensionality of traffic data, which can effectively reduce the time and memory overhead of neural network training.

Then, feature expansion based on one-hot coding technique with threshold is performed to solve the issue of data irregularity.

(2) The initial detection model is proposed, which adopts the generalized entropy method to fully learn the characteristic distribution law of DDoS attacks. The generalized entropy is further improved to realize the parameter self-training process by introducing the threshold value to automatically optimize the model parameters.

(3) Research on DNN precision detection model containing a discard layer. This design enables the DNN to randomly omit neurons during each training iteration with a predefined probability. By doing so, it introduces stochasticity into the learning process, effectively curtailing the likelihood of overfitting and reducing the time consumption.

2 Background

2.1 Generalized Entropy

Generalized entropy constitutes a broader extension of information entropy [17]. The formulation for calculating the generalized entropy associated with IP address $x = (x_1, x_2, \ldots, x_n)$ is given below:

$$H_\alpha(x) = -\frac{1}{1-\alpha}\log_2\left(\sum_{i=1}^{n} p_i^{\alpha}\right) \tag{1}$$

The probability of p_i being x_i, $p_i \geq 0$ and p_i satisfies $\sum_{i=1}^{n} p_i = 1$ in Eq. (1). α denotes the generalized entropy index, $\alpha \geq 0, \alpha \neq 1$. By taking the derivative of α in Eq. (1), $H_\alpha(x)$ is a non-increasing function under the condition that $\alpha \geq 0$, $\alpha \neq 1$. The maximum generalized entropy value $H_0(x) = \log_2(n)$ is obtained when $\alpha = 0$ or $p_1 = p_2 = \ldots = p_i$. At this time, the IP address x is maximally decentralized. The generalized entropy converges to the information entropy when $\alpha \to 1$, Eq. (2) can be obtained. The minimum information entropy value $H_\infty(x) = 0$ can be obtained when $\alpha \to \infty$, at which time the IP address x is maximally centralized in x_i.

$$H_1(x) = -\sum_{i=1}^{n} p_i \log_2(p_i) \tag{2}$$

The high probability events have more influence on the value of generalized entropy from Eq. (1) when $\alpha > 1$. Flooding DDoS attacks have more influence on the value of generalized entropy. The low probability events have more influence on the value of generalized entropy from Eq. (1) when $0 < \alpha < 1$. LDDoS attacks have more influence on the value of generalized entropy.

2.2 DNN

DNN comprises an input layer, multiple hidden layers, and an output layer. The ReLu function [18] and the Sigmoid function [19] activation functions in DNN, and their formulas are given below:

$$F(x) = \max(0, x) \tag{3}$$

$$S(x) = \frac{1}{1 + e^{-x}} \tag{4}$$

The dropout layer discards neurons with probability of p, the formula for the dropout rate $r^{(K)}$ of the K-th layer is given below; $r^{(K)}$ obeys the Bernoulli Distribution:

$$r^{(K)} \sim Bernoulli\left(p\right) \tag{5}$$

The formula of loss function is given:

$$L\left(\hat{y}, y\right) = -\sum_{i=1}^{m} \left(y_i \log\left(\hat{y}_i\right) + (1 - y_i) \log\left(1 - \hat{y}_i\right)\right) \tag{6}$$

3 Our Method

We propose a DDoS detection model based on improved generalized entropy and DNN, named IGED, and the model framework is shown in Fig. 2.

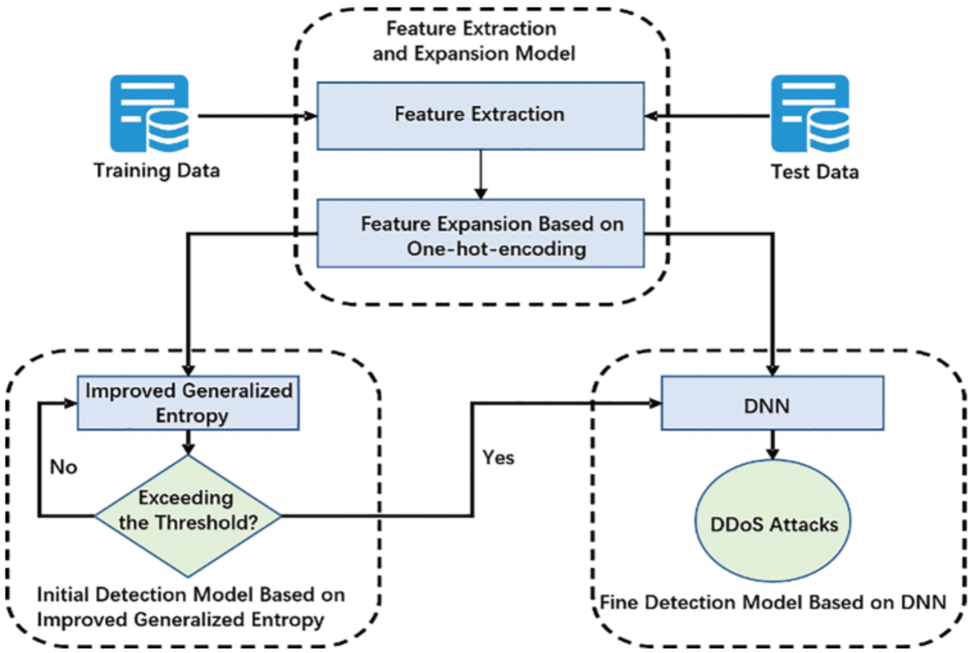


Figure 2: Framework of IGED

The IGED framework consists of a feature extraction and expansion module, an improved generalized entropy initial detection module, and a DNN fine detection module. The feature extraction and expansion module preprocesses the traffic data. The initial detection model is to pre-screen potential DDoS attack traffic and mark it as suspicious traffic, which helps to reduce the burden of the fine detection module. The fine detection model is to improve the accuracy and reliability of the detection through a more complex DNN for in-depth detection of suspicious traffic.

3.1 Feature Extraction and Expansion

Different traffic features are extracted separately for the initial and fine detection models because of their different design concepts and objectives. In addition, the traffic features need to be expanded for better detect DDoS attacks.

3.1.1 Feature Extraction

The initial detection module need to have both a high degree of detection accuracy and expedited processing speed. Therefore, only a few important features in the traffic data are taken to realize the fast calculation of generalized entropy. The features extracted for the initial detection module are shown in Table 1.

Table 1: Features of traffic analysis based on generalized entropy

Traffic feature	Detailed description
Src IP	Source IP address
Dst IP	Destination IP address

DDoS attacks are characterized by large data size and many data features, so it is necessary to reasonably screen the traffic features. Consequently, the employment of DNN within the fine detection module emerges as a choice, capitalizing on its capability to enhance accuracy. The features extracted for the fine detection module are shown in Table 2.

Table 2: Input features based on DNN detection model

Feature name	Detailed description
Src IP	Source IP address
Dst IP	Destination IP address
Src port	Source port
Dst port	Destination port
Protocol	Protocol
Flow duration	Flow duration
Tot Fwd Pkts	Number of forward packets
Tot Bwd Pkts	Number of backward packets
TotLen Fwd Pkts	Forward packet size
TotLen Bwd Pkts	Backward packet size
Flow IAT Mean	Average time between two packets sent in a flow
Fwd Pkts/s	Number of positive packets per second
Bwd Pkts/s	Number of backward packets per second
Pkt len mean	Average length of packets
SYN flag Cnt	Number of packets with SYN
PSH flag Cnt	Number of packets using PSH
ACK flag Cnt	Number of packets with ACK
URG flag Cnt	Number of packets with URG
Pkt size avg	Average packet length
Active mean	Average time stream is active before becoming idle
Idle mean	The average time stream is idle until activated
Label	Traffic labels

3.1.2 Feature Expansion

Since the traffic features contain string type fields such as "Src IP" and "Dst IP" which cannot realize the corresponding computation in neural networks, the one-hot-encoding technique is used to reconstruct the "Src IP" and "Dst IP" fields. One-hot-encoding is known as one-bit efficient encoding that encodes N different IP addresses in the dataset using N columns. Each IP address has its own independent column and only one of them is valid at any given time. Essentially, the one-hot-encoding technique transforms the dataset by expanding its original K feature columns into a new format consisting of K + N different binary columns.

Due to the large amount of data and the multitude of different IP addresses in DDoS attacks, using One-hot-encoding directly will lead to the addition of too many columns of data. Consequently, an improvement to the conventional one-hot-encoding technique has been introduced by incorporating a threshold criterion. Under this modification, only those IP addresses that occur with a frequency meeting or exceeding the predefined threshold undergo one-hot-encoding; IP addresses with occurrences falling below this threshold are directly classified as "Other IP". The results with the threshold value set to 2 can be shown in Table 3.

Table 3: Example of one-hot-encoding in a dataset

IP address	18.219.193.20	18.219.9.1	Other IP
18.219.193.20	1	0	0
172.31.69.28	0	0	1
172.31.69.25	0	0	1
18.219.9.1	0	1	0
18.219.193.20	1	0	0
18.219.9.1	0	1	0

3.2 Initial Detection Model Based on Improved Generalized Entropy

To tackle the issue of artificially set parameters in generalized entropy, we propose an initial module that incorporate a parameter self-training procedure. The framework is shown in Fig. 3.

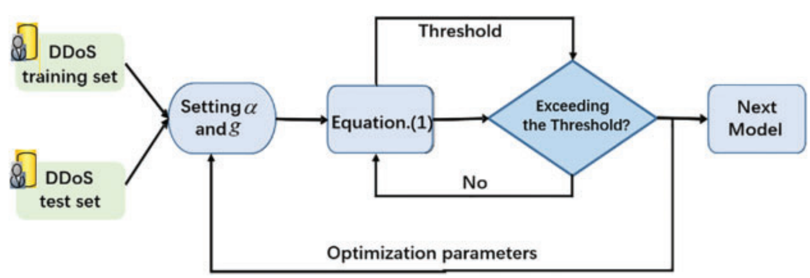


Figure 3: Framework of the initial detection model

The parameter self-training process entails dividing both the training and test datasets into g groups, subsequently computing the generalized entropy for each group's "Src IP" and "Dst IP" attributes sequentially by employing Eq. (1). The threshold is set using the smallest calculated generalized entropy value from the data groups in the training set that contain DDoS attacks.

Proceeding to the test set, each group's generalized entropy measurement is compared against this established threshold. If the generalized entropy exceeds the predetermined threshold, the data group is devoid of DDoS assaults, indicative of a more decentralized distribution of IP addresses. Conversely, should the generalized entropy fall below the threshold, it raises a flag suggesting the potential presence of a DDoS attack within that data group, indicating to a concerning centralization of IP addresses. Setting group g and the parameter α in Eq. (1) repeatedly and calculating the precision rate of the data groups larger than the threshold. Recording the parameter α and group g when the maximum value of the precision occurs for the last time that ensures that there is a maximum recall under the maximization of the precision.

The DDoS initial detection algorithm based on improved generalized entropy is shown in Algorithm 1.

Algorithm 1: DDoS initial detection

Input: DDoS training set G and DDoS test set D after feature extraction and expansion; Divide G and D into groups g, $g \leq n$; Parameter α in Eq. (1), $\alpha \leq m$; The optimal value of parameters (α, g, T) is denoted as Ans; Threshold T; The i-th group of generalized entropy value t_i in G, $i = 1, 2, \ldots, g$; The i-th group of generalized entropy value d_i in D, $i = 1, 2, \ldots, g$; Precision P;

Output: Suspicious DDoS dataset S

```
for g ← 1 to n do
  if Ans unchanged then
    break
  end if
  for α ← 0 to m do
    for i ← 1 to g do
      use Eq. (1) to calculate t_i for G
    end for
    T = max(t_1, ..., t_g)
    for i ← 1 to g do
      use Eq. (1) to calculate d_i for D
      if d_i > T then
        d_i is normal traffic
      else
        d_i is suspicious
      end if
    end for
    calculate P
    if P = 1 then
      Ans = (α, g, T)
    else
      utilize Ans = (α, g, T) to filter D
      output S
    end if
  end for
end for
```

3.3 Fine Detection Model Based on DNN

Considering the real-time demands of network attack detection, this paper designs a five-layer structure of DNN. The model commences with an input layer accommodating a dimensionality of K + N. Two dropout layers are introduced and each configured to randomly deactivate neurons with a probability of $p = 0.2$. One hidden layer containing 40 neurons. These intermediate layers use the ReLu as their activation function. Culminating in one-dimensional output layer employing the Sigmoid activation function. In the constructed DNN, the learning rate is 0.01 and the loss function used is binary cross entropy. The framework of the fine detection model is shown in Fig. 4.

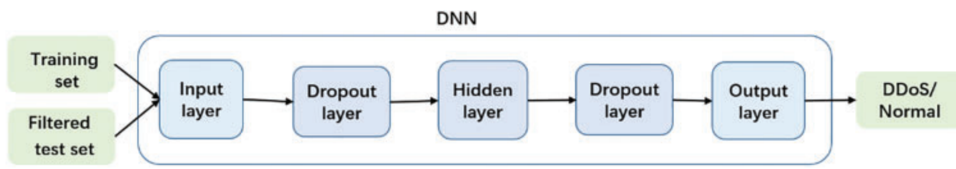


Figure 4: Framework the fine detection model

As a result, the DDoS fine detection algorithm based on DNN can be obtained as shown in Algorithm 2.

Algorithm 2: DDoS fine detection

Input: DDoS training set G and test set S; DNN B with dropout layers; Number of iterations E; Loss function L; The number of S is n; The j-th data detection result in S is $flag_j, j = 1, 2, \ldots, n$;
Output: Detection results W for DDoS test set S, $W = (w_1, w_2, \ldots, w_n)$;

for $i \leftarrow 1$ to E do
  DNN $B \leftarrow$ training set G
  calculate L by using Eq. (10)
  if L is the current minimum value
    save B
  end if
end for
for $j \leftarrow 1$ to n do
  $flag_j \leftarrow B \leftarrow j$
  if $flag_j$ then
    j is a DDoS attack
  else
    j is normal traffic
  end if
end for
return W

Firstly, the DNN is trained using the training set, and then input the suspicious dataset filtered by the initial detection model into the trained DNN to realize the accurate judgment of DDoS attacks. From Algorithm 1, we can get that the main computational cost of improving the generalized entropy is in the feature and iterative computation, so the computational complexity is o(G), where G is the size of the training set data. The size of the dataset filtered by Algorithm 1 is of size n. From Algorithm 2, we know that the main computational cost of the deep neural network model depends on the size of the data samples, so the computational complexity of the deep neural network model is o(n). So the computational complexity of the deep neural network model is based on the improved generalized entropy and is o(G).

4 Experiments and Results

All experiments are done by using TensorFlow framework, and the Linux system used for experiments is Intel(R) Core(TM) i7-4720HQ CPU @ 2.60 GHz, GPU is NVIDIA GeForce GTX 950 M with 16 GB RAM.

4.1 Datasets

To evaluate the efficiency of the model for DDoS attack detection, three datasets are used for the experiments. The information about three datasets are shown in Table 4.

Table 4: DDoS datasets information

Dataset	Training set		Test set		Total
	Benign	DDoS	Benign	DDoS	
Mixed-type DDoS	5057362	1035845	1264340	258962	7616509
LDDoS	221021	45252	55239	11329	332841
CICDDoS2019	46091	8443	10772	2329	68510

The mixed-type DDoS dataset is derived from the Kaggle competition platform which consists of various types of DDoS attacks and normal traffic from the public datasets CSE-CIC-IDS2018-AWS, CICIDS2017, and CIC DoS dataset (2016).

The LDDoS dataset is derived from data that is tagged with LDDoS label within the CSE-CIC-IDS2018-AWS dataset.

CICDDoS2019 is a dataset containing various DDoS attacks. Since the number of DDoS attacks in this dataset far exceeds the number of normal traffic, to make it have the same division ratio as the other two datasets, we choose to use all the normal traffic data and take some DDoS attack traffic from the CICDDoS2019 dataset according to the corresponding ratio to build the dataset we need.

The three datasets are labeled as "DDoS" and "Benign", incorporating a total of 84 features. The LDDoS dataset comprises 332,841 pieces of traffic data, the mixed-type DDoS dataset contains a total of 76,165,090 pieces of traffic data, while the CICDDoS2019 holds 68,510 pieces of traffic data. 17% of the traffic data across these datasets are flagged as "DDoS" and 83% of the traffic data are flagged as "Benign". The experiments were conducted by dividing the three datasets into a training set and a test set in the ratio of 8:2, respectively.

4.2 Evaluation Metrics

We choose four metrics to evaluate the performance of the proposed DDoS attack detection model: accuracy (ACC), precision (P), recall (R), and F_1-Score (F_1). The relevant formulas are as follows:

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{7}$$

$$P = \frac{TP}{TP + FP} \tag{8}$$

$$R = \frac{TP}{TP + FN} \tag{9}$$

$$F_1 = 2\frac{R * P}{P + R} \tag{10}$$

TP, *FN* are defined as actual normal traffic is classified as normal traffic, DDoS attack; *TN*, *FP* are defined as actual DDoS traffic are classified as DDoS attack, normal traffic.

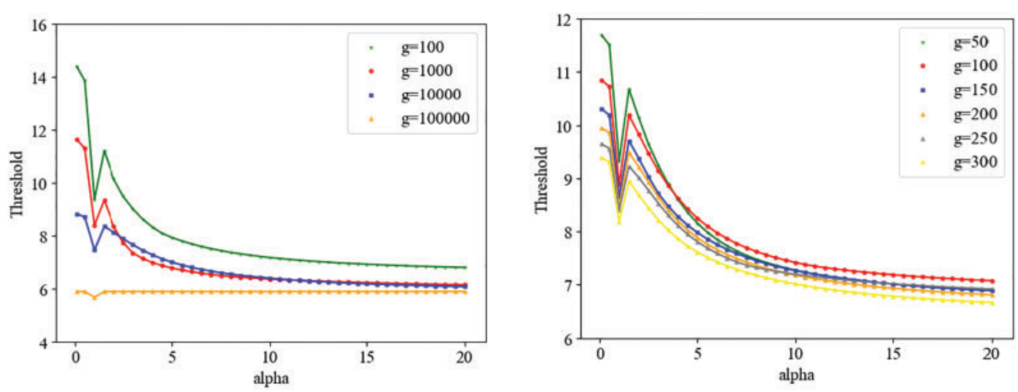
4.3 Initial Detection Model Experiment

Due to the processed CICDDoS2019 dataset in this paper is small and belongs to the same type as the mixed-type dataset, both of which contain a variety of DDoS attacks, we only use the mixed-type dataset and the LDDoS dataset for our experiments in the initial and fine detection modules, and use all three datasets in the control experiments.

Since the directional nature of traffic transmission, where "Src IP" and "Dst IP" are correspondent, "Src IP" and "Dst IP" in each traffic data is viewed as a tuple. The generalized entropy is then computed for all tuples within the defined window size and the specific steps are shown in Algorithm 1. The effect of the group numbers g and α in Eq. (1) on the precision of detection is further researched to obtain the best model parameters. The thresholds of the model are first calculated and then the validity of the model is examined.

4.3.1 Calculate the Optimal Model Thresholds

Fig. 5 illustrates the impact of partitioning the training set into g groups and α as per the formulation in Eq. (1) in both mixed-type DDoS and LDDoS datasets. In particular, it is noted that the thresholds decrease more at $\alpha = 1$ in Fig. 5 when the generalized entropy degrades to information entropy. When $0 \leq \alpha < 1$ or $\alpha > 1$, α and the threshold are negatively correlated from Fig. 5. In addition, compared to the LDDoS attack dataset, the DDoS attack thresholds on the mixed-type DDoS dataset have a larger range of values, which indicates that the mixed-type DDoS dataset has a higher complexity of DDoS attacks.



(a) Mixed-type DDoS (b) LDDoS

Figure 5: Validity of the initial detection model

4.3.2 Validity of the Initial Detection Model

In order to validate the efficacy of the improved generalized entropy method on the test set, the experimental procedure commences with computing the generalized entropy value for each data group within the test set and then compares it with the thresholds of the corresponding parameter calculated in Fig. 5. The test set's traffic is classified accordingly through this process and the precision and recall of the test results are obtained. Calculations reveal that with model parameters set at $g = 100, \alpha = 3$, the outcome yields an precision of $P = 1$ and a recall of $R = 0.3235$ by employing Algorithm 1. At this point, the validity is performed in the mixed-type DDoS dataset that successfully filters out 409,646 pieces of normal traffic data from the test set while the information entropy method ($\alpha = 1$) only exclude 74,347 pieces of normal traffic data. Consistently, an analogous experiment was conducted on the LDDoS dataset, following the identical method, leading to a congruent conclusion. With the generalized entropy optimal parameters $g = 50, \alpha = 6$, it effectively filters out 11,958 pieces of normal traffic data from the test set while information entropy approach exclude merely 49 pieces of normal data. Compared to the information entropy method ($\alpha = 1$) and other generalized entropy methods with values of g and α, the model has better results which are shown in Tables 5 and 6 in filtering more normal traffic when the model takes the optimal parameters on both DDoS datasets.

Table 5: Generalized entropy parameters in the mixed-type DDoS dataset

g	α	P	R	Filtered data
100	1	1	0.0588	74373
100	3	1	0.3235	**409646**
1000	1	1	0.0028	3522
1000	2	1	0.0710	89806
10000	1	0	0	0
10000	20	1	0.0001	173

Table 6: Generalized entropy parameters in the LDDoS dataset

g	α	P	R	Filtered data
50	1	1	0.0009	49
50	6	1	0.2727	**11958**
100	1	0	0	0
100	20	1	0.1143	6313
150	1	0	0	0
150	20	1	0.0755	4169

Drawing from the analysis and findings above, it can be inferred that the P of the initial detection model reaches optimum value of 1, which can greatly optimize the parameters automatically and then reflect the distribution of DDoS attacks to achieve the filtering of traffic. However, its R is low, that stills shows a large amount of normal traffic in the traffic detected as DDoS attacks. So it's necessary to use the fine detection model to accurately detect the suspicious DDoS attack traffic.

4.4 Fine Detection Model Experiment

The test set comprises potentially containing DDoS attacks, having undergone initial screening by our detection algorithm. The related information is shown in Table 7. In addition, the early stopping method [20] is added to the training process of each model to stop the training when ACC on the validation set does not increase compared to the first 10 rounds of training.

Table 7: Suspicious DDoS dataset information

Dataset	Training set		Test set		Total
	Benign	DDoS	Benign	DDoS	
Mixed-type DDoS	5057362	1035845	854694	258962	7206863
LDDoS	221021	45252	43281	11329	320883

This section undertakes a series of comparative experiments aimed at validating the efficacy of the model's feature expansion method based on the One-hot-encoding technique. Leveraging the dataset of suspected DDoS attack traffic, these experiments employ Algorithm 2, varying the One-hot-encoding thresholds to scrutinize its impact on DDoS detection capabilities. The results are shown in Tables 8 and 9. The experiment regards the dataset when the threshold is 0 as the original dataset without feature processing in Section 3.1, which contains all the features. In addition, the smaller the threshold of the feature extraction and expansion model is taken, the more features are expanded. An excessive count of features will impede detection speed; whereas a limited features will easily cause the model ignoring the features related to the IP address so that reducing the accuracy. Therefore, the thresholds are appropriately selected for comparison One-hot-encoding according to the size of the dataset.

Table 8: Comparison of different thresholds on results in the mixed-type DDoS dataset

Threshold	Time/s	ACC	P	R	F_1
0	842.7	0.9864	0.9343	0.9711	0.9522
7500	1064.9	0.9981	**0.9972**	0.9893	0.9932
10000	559.4	**0.9991**	0.9951	**0.9988**	**0.9969**
15000	480.9	0.9982	0.9958	0.9915	0.9937
20000	**419.6**	0.9985	0.9952	0.9940	0.9946

Table 9: Comparison of different thresholds in the LDDoS dataset

Threshold	Time/s	ACC	P	R	F_1
0	200.9	0.9797	0.8895	0.9735	0.9296
50	255.9	0.9980	0.9987	0.9893	0.9940
100	40.1	**0.9998**	0.9991	**0.9997**	**0.9994**
150	30.5	0.9975	0.9944	0.9915	0.9907
200	**25.9**	0.9978	**0.9996**	0.9844	0.9920

In summary, based on the performance metrics corresponding to each threshold, a threshold of 10,000 is selected for the mixed-type DDoS attack dataset while a threshold of 100 is selected for the LDDoS dataset. The model are compared with the K-nearest neighbor method (KNN) [21], decision tree (DT) [22], random forest (RF) [22], extreme gradient boosting(XGBoost) [23], and long short-term memory network (LSTM) [24]. The results are shown in Tables 10 and 11.

Table 10: Comparison of different fine detection models in the mixed-type DDoS dataset

Model	Time/s	ACC	P	R	F_1
KNN	20136.5	0.9930	0.9691	0.9820	0.9755
DT	**97.9**	0.9724	0.9323	0.8660	0.8979
RF	224.5	0.9868	0.9577	0.9480	0.9528
XGBoost	332.2	0.9910	0.9649	0.9712	0.9680
LSTM	36300.8	0.9861	0.9701	0.9478	0.9587
This paper	559.4	**0.9991**	**0.9951**	**0.9988**	**0.9969**

Table 11: Comparison of different fine detection models in the LDDoS dataset

Model	Time/s	ACC	P	R	F_1
KNN	110.7	0.9788	0.9190	0.9278	0.9233
RF	5.0	0.9936	0.9767	0.9773	0.9771
XGBoost	19.2	0.9913	0.9771	0.9592	0.9680
LSTM	1078.1	0.9952	0.9899	0.9751	0.9824
This paper	40.1	**0.9998**	**0.9991**	**0.9997**	**0.9994**

The designed DNN model is better than other models in terms of ACC, P, R and F_1, which all reach more than 99.9% in Tables 10 and 11. It is only lower than DT, RF, and XGBoost models in terms of time metric. In summary, the DNN model has excellent practical usability.

4.5 Comparison Experiment

To evaluate the effectiveness of the model based on improved generalized entropy and DNN, as well as to show the superiority of the improved generalized entropy method, we added the CICDDoS2019 dataset for comparison experiments that contain the proposed model, the detection model based on DNN, and the detection model [13] based on information entropy and DNN. The results of the experiments are shown in Tables 12–14. To accurately compare the evaluation metrics, all models perform metrics evaluation based on the original dataset.

The ACC, P, R and F_1 of IGED reach 99.9% while the time overhead on three datasets are reduced by 31%, 17% and 8% compared with other models from Tables 12–14 which are all better than the other models. The improved generalized entropy is better than other methods for filtering the initial traffic, which can filter more normal traffic and reduce the data size of the fine detection module and the use of DNN is more accurate than other fine detection methods. Therefore, the superiority of the DDoS attack detection method with improved generalized entropy and DNN is proved by the results of the comparison experiments.

Table 12: Comparison of different detection models in the mixed-type DDoS dataset

Model	Time/s	ACC	P	R	F_1
DNN	1220.3	0.9899	0.9562	0.9860	09708
Entropy and DNN	813.3	0.9984	0.9976	0.9907	0.9941
IGED	**559.4**	**0.9995**	**0.9999**	**0.9993**	**0.9996**

Table 13: Comparison of different detection models in the LDDoS dataset

Model	Time/s	ACC	P	R	F_1
DNN	48.4	0.9990	0.9992	0.9950	0.9971
Entropy and DNN	49.7	0.9991	0.9990	0.9958	0.9974
IGED	**40.1**	**0.9998**	**0.9993**	**0.9998**	**0.9996**

Table 14: Comparison of different detection models in the CICDDoS2019 dataset

Model	Time/s	ACC	P	R	F_1
DNN	69.8	0.9994	0.9985	0.9993	0.9972
Entropy and DNN	22.8	0.9986	0.9968	0.9940	0.9995
IGED	**20.9**	**0.9998**	**0.9996**	**0.9996**	**0.9996**

5 Conclusion

In this paper, we propose an intelligent DDoS detection method IGED based on improved generalized entropy and DNN. Firstly, we propose an improved generalized entropy method to initial screening traffic in order to reduce data size. Then we propose a DNN-based method for further precise detection of suspicious traffic. Experimental results show that the proposed method can filter more normal traffic, which provides both improved accuracy and enhanced timeliness for swift response and mitigation of attacks.

Although the detection method proposed in this paper successfully identifies DDoS attack behavior, its discriminative capability is currently limited to generalized attack detection, falling short of precisely categorizing different types of DDoS attacks. Therefore, in future work, we should focus on devising an innovative detection model that, while maintaining efficient real-time responsiveness, can conduct deeply granular multi-classification of DDoS attacks. By employing more advanced algorithms and deep learning methodologies, the objective should be twofold: not just to augment the accuracy in identifying established attack patterns, but also to bolster the model's adaptability and predictive efficacy against emerging attack tactics and their variants, thereby securing its long-term viability.

Acknowledgement: The authors would like to express appreciation to the National Natural Science Foundation of China, the Natural Science Foundation of Fujian Province, and the Major Science and Technology project of Fuzhou for their financial support. The authors would like to thank the editor-in-chief, editor, and reviewers for their valuable comments and suggestions.

Funding Statement: This work is supported by the National Natural Science Foundation of China (Grant Nos. U22B2005, 62072109), the Natural Science Foundation of Fujian Province (Grant No. 2021J01625), and the Major Science and Technology Project of Fuzhou (Grant No. 2023 -ZD-003).

Author Contributions: Study conception and design: Yanhua Liu, Baokang Zhao; data collection: Xiaofeng Wang; analysis and interpretation of results: Xiaofeng Wang, Yuting Han; draft manuscript preparation: Ximeng Liu, Hui Chen. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data openly available in a public repository. The data that support the findings of this study are openly available at https://www.kaggle.com/devendra416/ddos-datasets (accessed on 19/04/2024).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Liu, Z. Liu, X. Liu, and W. Guo, "A web back-end database leakage incident reconstruction framework over unlabeled logs," *IEEE Trans. Emerg. Top. Comput.*, vol. 11, no. 1, pp. 237–252, 2022. doi: 10.1109/TETC.2022.3198080.

[2] D. Tang, Y. Yan, C. Gao, W. Liang, and W. Jin, "LtRFT: Mitigate the low-rate data plane DDoS attack with learning-to-rank enabled flow tables," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 3143–3157, 2023. doi: 10.1109/TIFS.2023.3275768.

[3] R. Fuladi, T. Baykas, and E. Anarim, "The use of statistical features for low-rate denial-of-service attack detection," *Ann. Telecommun.*, vol. 132, no. 1, pp. 1–13, 2024. doi: 10.1007/s12243-024-01027-3.

[4] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, "FMDADM: A multi-layer DDoS attack detection and mitigation framework using machine learning for stateful SDN-based IoT networks," *IEEE Access*, vol. 11, pp. 28934–28954, 2023. doi: 10.1109/ACCESS.2023.3260256.

[5] D. Kumar, R. Pateriya, R. K. Gupta, V. Dehalwar, and A. Sharma, "DDoS detection using deep learning," *Proc. Comput. Sci.*, vol. 218, no. 1, pp. 2420–2429, 2023. doi: 10.1016/j.procs.2023.01.217.

[6] M. J. Santos-Neto, J. L. Bordim, E. A. Alchieri, and E. Ishikawa, "DDoS attack detection in SDN: Enhancing entropy-based detection with machine learning," *Concurr. Comput.*, vol. 36, no. 11, pp. e8021, 2024. doi: 10.1002/cpe.8021.

[7] S. Aktar and A. Y. Nur, "Towards DDoS attack detection using deep learning approach," *Comput. Secur.*, vol. 129, no. 9, pp. 103251, 2023. doi: 10.1016/j.cose.2023.103251.

[8] M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij and F. Malik, "Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method," *Symmetry*, vol. 14, no. 6, pp. 1095, 2022. doi: 10.3390/sym14061095.

[9] J. Pei, Y. Chen, and W. Ji, "A DDoS attack detection method based on machine learning," *J. Phys.: Conf. Ser.*, vol. 1237, no. 3, pp. 032040, 2019.

[10] M. Zhang, W. Zhang, and K. Fan, "Application layer DDoS detection model based on data flow aggregation and evaluation," *Commun. Inf. Process.: Int. Conf.*, vol. 289, pp. 37–45, 2012. doi: 10.1007/978-3-642-31968-6.

[11] N. Aslam, S. Srivastava, and M. Gore, "A comprehensive analysis of machine learning-and deep learning-based solutions for DDoS attack detection in SDN," *Arab. J. Sci. Eng.*, vol. 49, no. 3, pp. 3533–3573, 2024. doi: 10.1007/s13369-023-08075-2.

[12] Z. Liu, C. Hu, and C. Shan, "Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method," *Comput. Secur.*, vol. 109, no. 10, pp. 102392, 2021. doi: 10.1016/j.cose.2021.102392.

[13] L. Zhang and J. Wang, "DDoS attack detection model based on information entropy and dnn in sdn," *J. Comput. Res. Dev.*, vol. 56, no. 5, pp. 909–918, 2019.

[14] A. Alfatemi, M. Rahouti, R. Amin, S. ALJamal, K. Xiong and Y. Xin, "Advancing DDoS attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling," arXiv preprint arXiv:2401.03116, 2024.

[15] K. Jiang, Y.D. Qiu, and H. C. Zheng, "ICMPv6 DDoS attack detection method based on information entropy and LSTM," *J. Comput. Eng. Appl.*, vol. 57, no. 21, pp. 148–154, 2021.

[16] Q. Liu, P. F. Li, and Z. J. Fu, "Secure controlling method for scalable botnets," *Chin. J. Netw. Inf. Secur.*, vol. 9, no. 1, pp. 42–45, 2023.

[17] D. Tang, Y. Yan, S. Zhang, J. Chen, and Z. Qin, "Performance and features: Mitigating the low-rate TCP-targeted DoS attack via SDN," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 1, pp. 428–444, 2021. doi: 10.1109/JSAC.2021.3126053.

[18] D. Tang, S. Wang, B. Liu, W. Jin, and J. Zhang, "GASF-IPP: Detection and mitigation of LDoS attack in SDN," *IEEE Trans. Serv. Comput.*, vol. 16, no. 5, pp. 3373–3384, 2023. doi: 10.1109/TSC.2023.3266757.

[19] E. Koo and H. Kim, "Empirical strategy for stretching probability distribution in neural-network-based regression," *Neural Netw.*, vol. 140, no. 1990, pp. 113–120, 2021. doi: 10.1016/j.neunet.2021.02.030.

[20] K. Bian and R. Priyadarshi, "Machine learning optimization techniques: A survey, classification, challenges, and future research issues," *Arch. Comput. Methods Eng.*, pp. 1–25, 2024. doi: 10.1007/s11831-024-10110-w.

[21] G. G. Priya, S. H. Shriram, S. Jeeva, G. S. Priya, and K. Balasubadra, "Detection of distributed denial of service (DDOS) attack using logistic regression and K nearest neighbor algorithms," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 16s, pp. 503–508, 2024.

[22] M. S. I. Alsumaidaie, K. M. A. Alheeti, and A. K. Alaloosy, "An assessment of ensemble voting approaches, random forest, and decision tree techniques in detecting distributed denial of service (DDoS) attacks," *Iraqi J Electri. Electroni Eng*, vol. 20, no. 1, pp. 16–24, 2023.

[23] N. F. Rozam and M. Riasetiawan, "XGBoost classifier for DDOS attack detection in software defined network using sFlow protocol," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 13, no. 2, pp. 718, 2023. doi: 10.18517/ijaseit.13.2.17810.

[24] A. Thangasamy, B. Sundan, and L. Govindaraj, "A novel framework for DDoS attacks detection using hybrid LSTM techniques," *Comput. Syst. Sci. Eng.*, vol. 45, no. 3, pp. 2553–2567, 2023. doi: 10.32604/csse.2023.032078.