Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025810
Article

Tech Science Press

An Optimal Framework for SDN Based on Deep Neural Network

Abdallah Abdallah[1], Mohamad Khairi Ishak[2], Nor Samsiah Sani[3], Imran Khan[4], Fahad R. Albogamy[5], Hirofumi Amano[6] and Samih M. Mostafa[7,*]

[1]Department of Industrial Engineering, School of Applied Technical Sciences German Jordanian University, Amman, 35247, Jordan
[2]School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Nibong Tebal, 14300, Malaysia
[3]Center for Artificial Intelligence Technology, Faculty of Information Science and Technology, The National University of Malaysia (UKM), Bangi, 43600, Selangor, Malaysia
[4]Department of Electrical Engineering, University of Engineering and Technology, Peshawar, 814, Pakistan
[5]Turabah University College, Computer Sciences Program, Taif University, Taif, 21944, Saudi Arabia
[6]Research Institute for Information Technology, Kyushu University, Fukuoka, 819-0395, Japan
[7]Computer Science-Mathematics Department, Faculty of Science, South Valley University, Qena, 83523, Egypt
*Corresponding Author: Samih M. Mostafa. Email: samih_montser@sci.svu.edu.eg
Received: 05 December 2021; Accepted: 12 January 2022

Abstract: Software-defined networking (SDN) is a new paradigm that promises to change by breaking vertical integration, decoupling network control logic from the underlying routers and switches, promoting (logical) network control centralization, and introducing network programming. However, the controller is similarly vulnerable to a "single point of failure", an attacker can execute a distributed denial of service (DDoS) attack that invalidates the controller and compromises the network security in SDN. To address the problem of DDoS traffic detection in SDN, a novel detection approach based on information entropy and deep neural network (DNN) is proposed. This approach contains a DNN-based DDoS traffic detection module and an information-based entropy initial inspection module. The initial inspection module detects the suspicious network traffic by computing the information entropy value of the data packet's source and destination Internet Protocol (IP) addresses, and then identifies it using the DDoS detection module based on DNN. DDoS assaults were found when suspected irregular traffic was validated. Experiments reveal that the algorithm recognizes DDoS activity at a rate of more than 99%, with a much better accuracy rate. The false alarm rate (FAR) is much lower than that of the information entropy-based detection method. Simultaneously, the proposed framework can shorten the detection time and improve the resource utilization efficiency.

Keywords: Deep neural network; computer networks; data security; optimization

1 Introduction

Distributed denial of service (DDoS) has always been one of the main threats to the Internet [1–4]. The DDoS attackers scan the network to find the vulnerable hosts and use these vulnerable hosts as the puppet machine to send a large number of request packets to the target server, causing the target host to lose its service function and cause network failure. There are many types of DDoS attacks, and the more common ones are distributed reflection DoS attacks using user datagram protocol (UDP) and the use of transmission control protocol (TCP) three-way handshake process attacks such as synchronize (SYN) flood attacks, etc. [5]. Nowadays, the network mostly adopts distributed architecture. This network architecture was originally constructed to reflect its highly scalable distributed structure, but it also led to the emergence of many security vulnerabilities [6]. The software defined network (SDN), as a new network architecture, has gradually become popular and has been widely studied, and is considered as the direction of network development [7]. Therefore, regarding the prevention of DDoS attacks in SDN networks, its safety is very important [8].

SDN is an implementation of network virtualization. It separates the control and data layers of the network to achieve the purpose of "software management network". The control layer of the SDN can centrally control the information of the entire network. A programming interface is convenient for the network administrators to manage the network. The centralized control of the SDN makes the controller the main target of DDoS attackers [9]. When the attacker launches a DDoS attack on the SDN, in order to pass the network security equipment, disguising the source IP address, the switch continuously receives a large number of data packets, which are not in the original flow table. The controller continuously receives the forwarded data packets from the switch and becomes the target of attack. When the controller's resources are exhausted, the entire SDN network is paralyzed. Therefore, timely detection and termination of DDoS attack traffic in the SDN network has become a current research hotspot. But how to detect the abnormal traffic in time and accurately identify has become a difficult point in current research [10].

In order to defend against DDoS attacks, how to find the abnormal traffic in the network is the main research method. In most cases, the attackers disguise abnormal traffic as normal traffic, so it is difficult to distinguish the detection methods based on information entropy and detection based on machine learning. The method is two of many detection methods, but both of these detection methods have shortcomings. The detection algorithm based on information entropy has a fast detection speed and does not need to construct more traffic characteristics. But compared with the algorithm based on machine learning (ML), there exists the disadvantages of low accuracy and high FAR. The DDoS traffic recognition method based on ML has a high accuracy rate (AR), but it needs to manually construct more traffic characteristics during the detection process, which affects the detection speed. So how to find a method, which not only has a high detection rate (DR) of abnormal traffic, but also has the ability to respond to high-speed traffic and detection efficiency, that has become a difficult point and challenge for research.

The emergence of deep learning (DL) algorithms solves the limitations of ML. The process of DL is to use multiple processing layers to abstract high-level data to obtain multiple nonlinear transformation functions. Deep neural network (DNN) in the image recognition, speech recognition and other fields have achieved good results. Compared with traditional ML, the DNNs combine low-level features to form more abstract high-level representations through multi-layer non-linear transformations, so that a learning system cannot rely on artificial feature selection, and found that the distributed nature of data representation, and learn to express complex function [11]. With the continuous development of graphical processing unit (GPU) technology and a variety of deep learning

(DL) platform, making the depth of the neural network can quickly process huge amounts of data classification [12,13]. Therefore, based on the DNN to identify the abnormal DDoS traffic, there is no need to manually design too many traffic characteristics, and it has higher detection accuracy and faster detection time. However, in practical applications, the SDN medium traffic is huge, and the detection of all traffic consumes huge computing resources and affects the real-time performance of the detection.

As a result, based on prior research and learning, this article proposes an innovative DDoS detection framework based on DNN. The proposed framework includes an initial inspection module based on information entropy and a detection module based on DNN. The detection model draws on the advantages of information entropy and DNN algorithm, and the accuracy measurement is performed after the initial inspection module finds the abnormal flow. This model makes up for the shortcomings of the detection algorithm based on information entropy of low DR and high FAR. It also shortens the detection time based on DNN algorithm, reducing the resource occupancy rate, not only can improve the accuracy of detection, but also shorten the processing time of detection, and save the frequency of resource usage by the DNN algorithm.

The main contributions of this article have three aspects:

1) A model for detecting the DDoS attacks in SDN is proposed. The model includes a preliminary inspection module based on information entropy and a DNN detection module. Combining the advantages of the two methods, it improves the DR and accuracy of the model, and reduces the FAR of the model. It speeds up the DR and reduce the occupancy rate of computing resources.
2) Using OpenFlow protocol fields, manual extraction and other methods to construct a 19-dimensional feature vector, as the input of the DNN model. After training and testing, the accuracy of the proposed model to identify DDoS traffic is higher than that of traditional ML methods, and has a lower FAR.
3) Propose a lightweight initial inspection method based on information entropy, and determine the suspected abnormal traffic by calculating the information entropy of the packet unit. The determined threshold allows the proposed method to have a recognition rate of more than 99%. As an initial inspection method, high false alarms can be ignored compared with the direct use of DNN-based detection algorithms, 2/3 the detection time and the occupancy rate of computing resources are reduced.

2 Literature Review

The development of DDoS attacks has become a major security threat to the Internet today [14]. The continuous development of network technology, the emergence of various new network architectures and the popularization of smart devices have made DDoS attack methods showing a trend of frequent development [15]. With the advancement of network technology, the DDoS attackers have begun to use new network equipment or network architecture to launch attacks. In recent years, the SDN networks have become a research hotspot for researchers and network service providers, and the problem of DDoS attacks in SDN is one of the research topics [16,17].

Reference [18] proposed a method of setting up a backup controller. When the SDN network is subjected to a DDoS attack, the switch disconnects from the controller and connects to other backup controllers. This method can temporarily mitigate the DDoS attack. However, it cannot fundamentally prevent it. Once the backup controllers are also attacked, the entire SDN network will lose control. Reference [19] proposed a method to predict the attacks based on traffic thresholds. The method

constructs flow characteristics by extracting NetFlow flow data, and calculates the flow characteristics and design thresholds through detection functions. However, this method needs to process the data flow collected in advance and requires a lot of preparatory work. In addition, the success of the test is closely related to the actual experience of the researcher.

Reference [20] proposed a fast entropy calculation method to detect the DDoS attacks in traffic, and calculate the entropy value over a period of time by counting the network traffic. If the entropy value exceeds the threshold, it is determined that a DDoS attack has occurred in the network. This method successfully improved the detection speed, but failed to significantly improve the detection accuracy, and the algorithm has a high FAR. Reference [21] proposed a large-scale network detection mechanism based on flow entropy and packet sampling. This method improves the detection accuracy and reduces the FAR, but it sets a threshold based on relevant experience and increases the influence of human factors. Reference [22] proposed a statistical solution to detect the DDoS attacks in SDN. The method extracts the flow characteristics, generates a characteristic matrix, and finds the abnormal flow by calculating the joint entropy of different combinations of flow characteristics. Compared with the previous detection algorithm based on entropy, this method has a great improvement, and the detection range is accurate. The rate has been greatly improved, but this method requires a long period of preparation and statistics, the calculation is more complicated, the scalability is poor, and the real-time performance is not high. Reference [23] proposed an entropy-based SDN early detection technology for TCP SYN flooding attacks. This technology is based on traffic characteristics and measures the degree of randomness of the data packets received at the SDN controller by calculating the entropy value of the traffic characteristics in a time-based data packet window sequence and compared with the threshold (adaptive) under this example. This method can detect the early attack. However, this method assumes that there is only one target node, which is not universal, and the method is only for TCP SYN flood attacks. The above research shows that, in SDN, it is difficult for the existing DDoS detection methods based on information entropy to have both high accuracy and high DR.

Reference [24] proposed a DDoS traffic detection algorithm based on extreme gradient boost (XGBoost). The method uses the XGBoost classifier to test the knowledge discovery and data mining (KDD) 99 data set. The test results show that the method has the characteristics of high detection accuracy and fast DR. But The detection effect of this method on other experimental environmental data is unknown. Reference [25] used the support vector machines (SVM) to detect the DDoS traffic in SDN. This method is also tested on the KDD 99 data set. The test results show the effectiveness of the method. This method also faces the problem of unknown actual detection effect. At the same time, the methods proposed in [24,25] requires manual construction of a large number of features, which affects the detection efficiency. Reference [26] proposed a method for detecting abnormal traffic in SDN based on DL. This method designs traffic characteristics and uses DL algorithms to detect the abnormal traffic in the SDN. Compared with the previous ML methods, the accuracy is improved. However, the detection efficiency is not high. When the traffic is huge, the detection of normal traffic will consume the resources of the DL hardware and increase the calculation time.

Through the above research, it is found that there are many problems in the detection algorithm based on information entropy: the determination of the threshold often brings about the contradiction between the DR and FAR, high computational complexity, poor scalability, low detection rate, and data statistical cycle. Detection algorithms based on ML also have problems such as low DR, high central processing unit (CPU) usage, and unused actual data verification. DL algorithms have high accuracy and low FAR. However, when the network traffic is too large, it will affect the detection time and occupy computing resources. To address the shortcomings of the preceding research methods, this

paper proposes a detection model based on information entropy and DL. This model combines the previous detection methods based on information entropy and ML. The information entropy method is used to conduct the preliminary detection of traffic, and then DNN is used to accurately detect the suspected problem traffic. Compared with the traditional methods based on information entropy and ML, this method has higher detection accuracy, lower FAR and higher detection efficiency.

3 Proposed Framework

3.1 Overall Architecture

The proposed detection model is deployed in the controller in the SDN. It includes two main parts: an abnormal initial detection module based on information entropy and a DDoS traffic detection module based on DNN, as shown in Fig. 1. In the SDN network, every time the switch receives a new data packet, the controller will update the flow table entry of the switch. When the SDN network is attacked, the controller will receive a large number of data packets from the switch, resulting in control device interrupts the service and the network is paralyzed. The abnormal initial detection module collects the *packet_in* data packets in the SDN controller, calculates the entropy value of the data characteristics in the fixed interval data packet window, and compares it with the set threshold. Once it is not within the normal range, the traffic is deemed to be suspected to be abnormal, and it is subjected to the DNN-based anomaly detection. The DDoS traffic detection module based on DNN extracts the required characteristics through the switch flow table entry, and performs further detection to confirm whether a DDoS attack occurs in the network. If an attack occurs, a warning will be issued and the network manager will be notified for further processing.

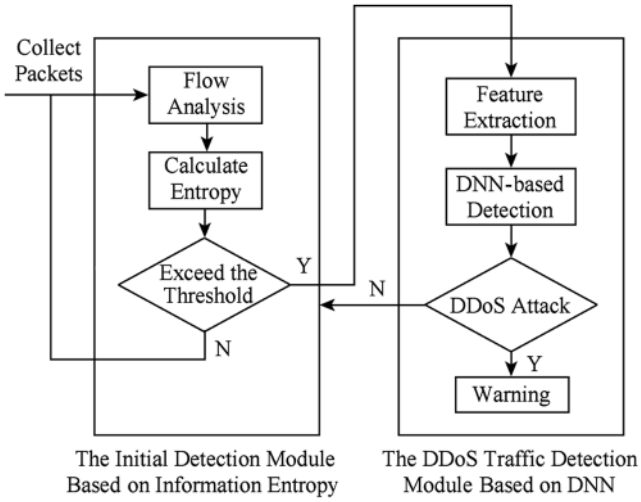

Figure 1: Proposed system model

3.2 Anomaly Initial Inspection

Information entropy reflects the degree of uncertainty in the value of random variables (RVs). When the value of the RV is more random, the value of information entropy is higher. When the value of the RV is more consistent, the information entropy has lower value [27]. We use the Shannon's

formula to calculate the sample entropy:

$$H(x) = -\sum_{i=1}^{N} \left(\frac{n_i}{S}\right) \ln \left(\frac{n_i}{S}\right) \tag{1}$$

Among them, the data sample $x = \{n_i; i = 1, 2, \ldots, N\}$ indicates that a certain sample i in the data has occurred n_i times. $S = \sum_i^N n_i$ which indicates the total number of sample values X. From Eq. (1), we can see that the size of the sample entropy changes in the interval (0; ln S). When the value distribution of the sample is the most concentrated, the entropy value is 0, then $n_1 = n_2 = \ldots = n_N$ means that all the sample values are the same. When the distribution of the sample is the most dispersed, the entropy value is the largest, and all sample values are different at this time.

Due to the self-similarity of network traffic, we consider that the sparseness and denseness of the data packet feature samples are only related to the number of samples, and the size of the entropy value is only determined by the similarities and differences of the sample data. For example, two sample sequences of the same number X and Y, where X is a sample sequence collected within 30 s, Y is a sample sequence collected within 45 s, but the entropy of the two sample sequences is the same. Then it is inferred that X and Y have the same degree of sparse distribution [28].

In the experiment, the *packet_in* data packet of the SDN controller is regarded as the unit data packet. We define a fixed packet number interval as a packet unit data packet (packetbin). That is, the continuous data packet is divided into a packet unit according to a specific number of packets (bin). We use some feature sequence values in packetbin as sample data, and calculate the entropy value of the feature sequence sample data. We have selected two most important features that can reflect the current network status: source and destination IP addresses. The choice of the number of packets W in each packetbin controls the change of sample characteristics in a short period of time. If the value of W is too large, the entropy value will not change significantly, which will reduce the accuracy of detection. In the SDN network of this experimental environment, according to the number of hosts and traffic conditions, after measurement and analysis, it is found that $W = 100$ is a good compromise for the deployed data. When calculating the entropy, it is $S = W = 100$ in Eq. (1), we calculate the information entropy of the source and destination IP addresses in the first consecutive W packets, and then move to the next adjacent W packets to calculate the corresponding entropy. We get an abnormal traffic analysis index based on the information entropy, as shown in Tab. 1.

Table 1: Index variables of flow with abnormalities

Description	Index	Entropy
Source IP	SIP	$H(SIP)$
Destination IP	DIP	$H(DIP)$

We set the experimental threshold T. If the information entropy in the indicator is not within the threshold range, it is observed that some abnormality has occurred in the SDN, issue a warning, and start the DDoS traffic detection module based on DL at this moment. The traffic in the SDN is detected, DDoS attacks are found and the warnings are issued. Unlike other entropy-based methods, this study does not set a confidence interval because it does not use a criterion for judging whether the DDoS occurs in the network, but only use it as the initial inspection method. Because the pure entropy-based detection method has limitations, for example, how to determine the threshold will affect the accuracy of the entire algorithm, and this method often results in a higher FAR. In our

initial inspection model, the threshold is set to a wider range. This method has a higher detection and recognition rates, but it has a higher FAR. As a preliminary inspection method, it only requires a higher recognition rate.

The abnormal initial inspection module based on information entropy observe the network traffic, and inputs the generated suspected abnormal traffic to the DL module for further processing. It not only completes the detection of abnormal traffic, but also slows down the DL module pressure of the required resources.

3.3 Feature Extraction and Construction

In traditional ML algorithms, how to select the features will affect the success of the entire algorithm. Choosing good features can improve the accuracy of the algorithm. But too many feature designs will increase the complexity, and the process of manually selecting features will affect the detection speed. The DNN model can automatically extract the features layer by layer, and assign weights to the extracted features to achieve the best results.

In the experimental DNN model, we directly extracted some of the fields in the OpenFlow flow table as the feature input of the first layer. In addition to the features that can be directly extracted in the flow table, we manually designed two features, which are also used as the input of the DL network. The input characteristics are shown in Tab. 2.

Table 2: Input characteristics

Characteristic	Description
table_id	Table of id
cockie	Cockie
Duration	Flow duration
n_packets	Number of packets
n_Bytes	Number of bytes
protocol	Protocol of IP
ip_src	Source IP
ip_dst	Destination IP
tcp_src	Source port number of TCP
actions	Switch action
mac_dst	Destination address of MAC
mac_src	Source address of MAC
idle_timeout	Time-out duration
tcp_dst	Destination port number of TCP
n_packets_ave	Average number of packets
n_bytes_ave	Average number of bytes

(Continued)

Table 2: Continued

Characteristic	Description
udp_src	Source port number of UDP
udp_dst	Destination port number of UDP

The two features manually extracted are the average number of data packets and the number of data packets. Among them, the average number of data packets *n_packets_ave* is the number of packets (*n_packets*) divided by the flow duration (duration), which is the number of data packets per second:

$$n\_packets\_ave = \frac{n\_packets}{duration} \tag{2}$$

The average number of data packets (*n_bytes_ave*) is the number of packets (*n_bytes*) divided by the stream duration (*duration*), that is, the number of data packets per second:

$$n\_bytes\_ave = \frac{n\_bytes}{duration} \tag{3}$$

In summary, this paper constructed the 19-dimensional feature input of the DL detection model based on the flow table information. These features can be directly read in the flow table entry, and the manually constructed features are also easier to obtain. This 19 dimensional feature vector is used as the input of the DL detection model to identify the abnormal DDoS traffic.

3.4 Detection Model

DNN is a fully connected network that includes an input layer, multiple hidden layers, and an output layer [29]. Fig. 2 depicts a 5-dimensional vector input, 7-dimensional vector output and DNN network model with $L-1$ hidden layers.

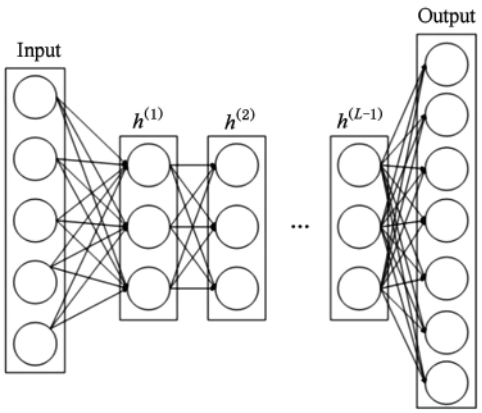

Figure 2: Proposed DNN model

In the DNN network, each layer contains the weight vector W and the offset vector $\boldsymbol{b}$. We calculate the output l^h of the h-th layer:

$$l^h = \tanh(\boldsymbol{b}^h + \boldsymbol{w}^h l^{h-1}) \tag{4}$$

Among them, $\boldsymbol{b}^h$ is the offset vector, $\boldsymbol{w}^h$ is the weight matrix, and the nonlinear function is the tanh. The top-level output l^μ and the supervised target output y are combined to form the loss function $\omega(l^\mu, y)$. The output layer linear regression function is

$$l_i^\mu = \frac{e^{b_i^\mu + w_i^\mu l^{\mu-1}}}{\sum_j e^{b_j^\mu + w_j^\mu l^{\mu-1}}} \tag{5}$$

Among them, w_i^μ is the i-th row of w^μ. In this case, we use the conditional log-likelihood function as the loss function with $l_i^\mu > 0$ and $\sum_i l_i^\mu = 1$

$$\eta(l^\mu, y) = -\log P(Y = y\ x) = -\log(l_y^\mu) \tag{6}$$

The expected value on the (x, y) pair is minimized. During training, back propagation (BP) and gradient descent (GD) algorithms are used to adjust the weight value and bias according to the output error value of each neuron. The amount of shift is adjusted. When the output of the cost function is the smallest, the best result is achieved.

The output selects the softmax function and defines the cross entropy error as follows

$$F(w) = \sum_{i=1}^{N} \log\{1 + e^{-y^n w^{\mathrm{T}} x^n}\} \tag{7}$$

Wherein, N is the number of units by the w obtained with respect to each weight w_k cost function $F(w)$, which is defined as

$$\theta_h = \frac{\partial}{\partial(w_k)} F(w) \tag{8}$$

where

$$w_{h+1} = w_h - \tau_h \theta_h \tag{9}$$

Among them, τ_h is called the learning efficiency [30]. Finally, according to Eqs. (7)–(9), the corresponding stochastic gradient descent algorithm is used to minimize the cost function, and finally we will get the best weight value. The experiment uses a DNN structure including an input layer, an output layer and 10 hidden layers. In the hidden layer, the hyperbolic tanh function is used for nonlinear processing, and the current activation is performed in the output layer. After multiple batches of GD training, the final detection model is determined.

4 Experimental Results

4.1 Configuration

This article uses Mininet to build an SDN, where the controller uses the JAVA-based open source controller Floodlight, and the operating system is Ubuntu 16.04. The DL module is developed based on the Tensorflow framework. The developed hardware environment is a 48-core CPU server. Before the experiment, we used the scapy tool to inject the traffic into the mininet virtual network (VN) to imitate the DDoS attack. The network topology created by Mininet is shown in Fig. 3. The SDN

consists of ten switches, each switch connects ten hosts, select two of them as the source of DDoS attacks, and launch an attack on the SDN network.

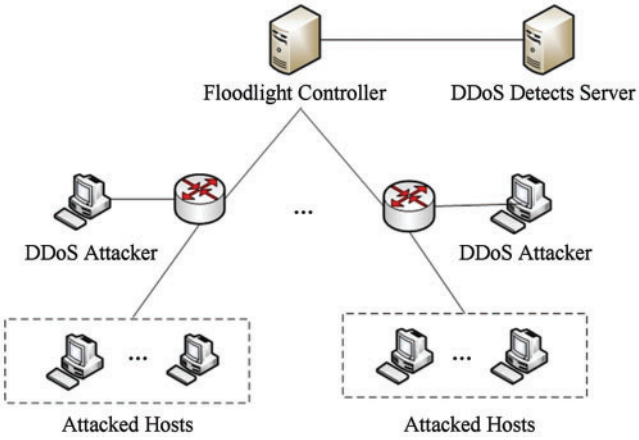

Figure 3: Proposed network configuration

The experiment uses three indicators: *DR*, accuracy (*ACC*), and *FAR* as the criteria for evaluating the model. The DR is the ratio of the correctly identified to all DDoS attack traffic in the sample which is expressed as

$$DR = \frac{TP}{TP + FN} \tag{10}$$

The ACC is the ratio of correctly identifying normal and abnormal flows in the total data set

$$ACC = \frac{TP + TN}{TP + TN + FP + FN} \tag{11}$$

The FAR refers to the ratio of normal traffic that is misidentified as DDoS attack traffic by the model to all normal traffic in the test set. The lower the FAR, the better the classification effect of the model

$$FAR = \frac{FP}{FP + TN} \tag{12}$$

Among them, the true positive (TP) rate refers to the rate at which the abnormal DDoS traffic is identified by the model, and the false positive (FP) rate refers to the rate at which normal traffic is incorrectly identified as DDoS traffic. The true negative (TN) rate refers to the rate at which the normal traffic is correctly identified. False negative (FN) rate refers to the rate at which the DDoS traffic is incorrectly identified as normal traffic [31].

4.2 Results Analysis Based on Information Entropy

In the abnormal initial detection module based on information entropy, we propose an abnormal traffic analysis indicator, by calculating the entropy value of each feature vector in several windows, and judging whether the network has occurred according to whether the entropy value exceeds the threshold collect the *packet-in* of normal network traffic in the switch, read the source and destination IP addresses in the data packet, and then calculate the characteristic entropy value in each window, namely 100 data packets. The SDN network is subject to DDoS during the attack, 100,000 pieces of

data traffic are collected, the source and destination IP addresses are analyzed, and the information entropy value is calculated. The comparison is shown in Figs. 4 and 5.

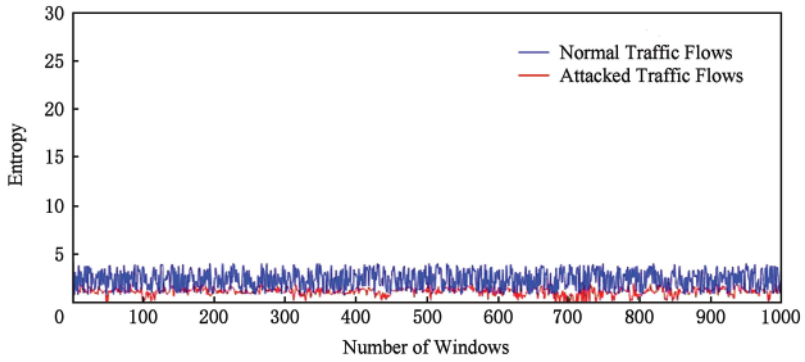

Figure 4: Entropy evaluation *vs.* number of windows of source-IP

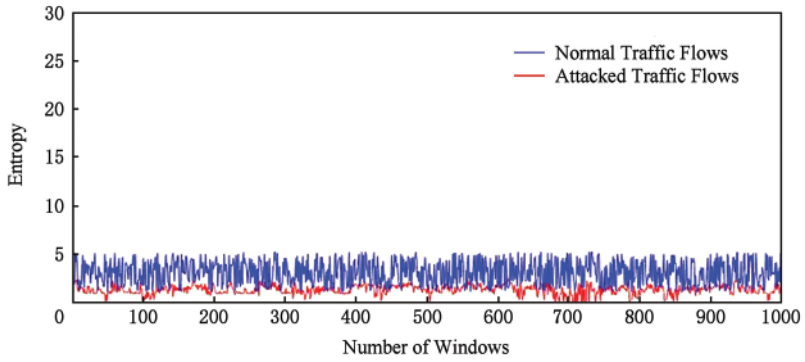

Figure 5: Entropy evaluation *vs.* number of windows of destination IP

It can be seen from Figs. 4 and 5 that when a DDoS attack occurs in SDN, the characteristic information entropy value has changed significantly, and the characteristic vector value has dropped rapidly, and the range of change is small. The initial inspection module based on information entropy is to be able to identify the abnormal traffic in the network, so it must have a high DR, but because it is only a preliminary inspection module, it is not required to have a very low FAR. According to the above principles, to analyze the experimental data, the threshold of the feature entropy value is shown in Tab. 3.

Table 3: IP values analysis

Parameter	Source IP	Destination IP
Threshold value	2.5192	2.5557

According to the analysis of experimental data, when the source IP address information entropy threshold is set to 2.5192, the DR of abnormal traffic identification is 100%, and the FAR is 42.769%. When the destination IP address information entropy threshold is set to 2.5557, the DR of abnormal traffic is 100%, and the FAR is 39.231%. When one of the two feature entropy values exceeds the specified threshold, it is concluded that an abnormality has occurred in the network.

In order to prove the effectiveness of the threshold, this study simulate the DDoS attacks and collect data, mark them to distinguish between normal and abnormal traffic, mix normal traffic with abnormal traffic, and perform anomaly detection based on information entropy. If the information entropy of a certain characteristic value is lower than the threshold, it is marked as abnormal traffic. Finally, the marking result is compared with the initial label to calculate the DR and FAR of the algorithm. The experimental results are shown in Tab. 4.

Table 4: DR and FAR evaluation

Parameter	Number of flows (million)		
	5	8	10
DR	99.8995	99.9871	99.8635
FAR	43.781	37.364	48.654

From the experimental results, it can be seen that the proposed method has a very high DR, which proves that it can effectively identify DDoS attack traffic. Although it has a high FAR, it does not affect its use as an initial check for the effectiveness.

4.3 Results Analysis Based on DNN

The experimental data set is the real traffic in the SDN. A total of 120,000 traffic data, including 70,000 normal traffic and 50,000 DDoS attack traffic is collected. Among them, 79,970 data sets are used as training sets and 40030 pieces of data are used as the test set, as shown in Tab. 5.

Table 5: Dataset values

Parameter	Dataset	
	Test set	Training set
Number of normal flows	23250	46750
Number of DDoS flows	16780	33220

The choice of the number of hidden layers of the DNN model will affect the accuracy of the model's recognition of DDoS traffic. It is very important to choose how many layers of DNN as the detection model. Therefore, we have constructed the number of hidden layers as 5 and 10 respectively. In the experiment, we use the same data set to perform 1,000 iterations of these five DNN models, and evaluate each DNN model through accuracy rate. Tab. 6 shows the comparison of the results of five DNN models with different structures after being trained for 1,000 rounds under the same training and test sets.

It can be seen from the results in Tab. 6 that the DNN model does not have more layers and has better training results. It is because too many hidden layers will even cause the accuracy of the recognition results to decline. Therefore, the experimental model chooses a 10-layer DNN model.

Table 6: Hidden layers ACC evaluation

Parameter	Number of hidden layers				
	5	10	20	50	100
Accuracy (%)	86.43	97.87	96.12	94.72	81.48

The actual data traffic set is deployed to compare the experiments with the XGBoost [24] and SVM models [25]. At the same time, the proposed model is compared with the traditional ML based K-nearest neighbor (KNN) model. The results are shown in Tab. 7. It can be seen from Tab. 7 that the proposed DNN model is better than the traditional methods in terms of DR, ACC and FAR. The ACC rate of the proposed model is 97.87%, and the FAR has dropped significantly. From the experimental results, it can be seen that the proposed model is better than traditional ML models.

Table 7: Comparison of the proposed and existing algorithms

Parameter	Model			
	XGBoost	SVM	KNN	Proposed
DR	94.36	93.12	93.78	95.42
ACC	95.91	95.19	95.08	97.87
FAR	4.74	6.21	7.15	3.16

At the same time, we conducted two sets of comparative experiments using the experimental data set and using the DNN model to detect the DDoS traffic. The first group of experiments directly used the 17 feature fields extracted directly from the OpenFlow as inputs. The second group of experiments is in addition to directly extracting the 17 feature fields. Two features "Average data grouping number" and "Average data grouping bit number" are manually constructed in real time, and these 19 features are used as model inputs. At the same time, the accuracy of abnormal traffic under two different traffic feature inputs are calculated. The results are shown in Tab. 8.

Table 8: ACC and time cost evaluation of the proposed algorithm

Parameter	Input feature	
	Directly and hand-build	Directly extracted
ACC (%)	97.87	97.12
Time cost (s)	67.57	67.54

It can be seen from Tab. 8 that after adding two manually constructed features, the accuracy recognition increased by 0.75%, while the time only increased by 0.03 s. This proves the effectiveness of manually constructed features.

In addition, we also conducted two comparison experiments. The first experiment used only the detection module based on DL to detect the flow, while the second experiment used the preliminary inspection module based on information entropy for the initial inspection and the detection module based on deep learning. The results are shown in Tab. 9.

Table 9: Performance comparison of the proposed method

Parameter	Method	
	DNN	Entropy and DNN
ACC (%)	97.87	97.89
CPU utility (%)	53	22
Time cost (s)	67	24

It can be seen from the detection accuracy that the two methods have high accuracy for the identification of abnormal traffic, both reaching more than 97%, and both have a good recognition effect. However, the detection method based on information entropy and deep learning saves CPU usage rate and reduce the processing time. The initial inspection method based on information entropy is a lightweight calculation, its occupancy rate of computing resources is not high, and has a faster processing speed.

By adjusting the number of DNN layers and manually designing input features, the optimal DNN detection model suitable for the experimental environment is obtained. At the same time, a comparative test was carried out with previous research methods, and the results showed that, the proposed model has a high accuracy rate for identifying the DDoS traffic in the traffic, occupies less computing resources and faster processing speed.

5 Conclusion

This paper proposes a DDoS attack detection framework based on information entropy and DNN, as well as an abnormal traffic analysis index for calculating information entropy with a 19-dimensional flow table feature vector. The initial inspection model based on information entropy can effectively identify the abnormal traffic, and the DNN detection module confirms it. The proposed model not only solves the problem of low accuracy of detection methods based on information entropy, but also alleviates the long detection time of DL methods and occupation of computing resources. Experiments show that, the proposed method can effectively identify the abnormal DDoS traffic, provide effective information for network administrators, and provide effective guarantee for SDN network security.

Acknowledgement: The authors would like to acknowledge the support from Taif University Researchers Supporting Project Number (TURSP-2020/331), Taif University, Taif, Saudi Arabia.

Funding Statement: This publication was supported by the Ministry of Education, Malaysia (Grant code: FRGS/1/2018/ICT02/UKM/02/6).

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

References

[1] M. Tareq, E. A. Sundarajan, M. Mohd and N. S. Sani, "Online clustering of evolving data streams using a density grid-based method," *IEEE Access*, vol. 8, pp. 166472–166490, 2020.

[2] A. Nasif, Z. A. Othman and N. S. Sani, "The deep learning solutions on lossless compression methods for alleviating data load on iot nodes in smart cities," *Sensors Journal*, vol. 21, no. 12, pp. 1–23, 2021.

[3] A. S. Abdulameer, S. Tiun, N. S. Sani, M. Ayob and A. Taha, "Enhanced clustering models with wiki-based k-neared neighbors-based representation for web search result clustering," *Journal of King Saud University*, vol. 8, no. 3, pp. 878–891, 2020.

[4] W. Fook, A. Rahman, N. S. Sani and A. Adam, "Resource optimization using multithreading in support vector machine," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, pp. 356–359, 2020.

[5] G. M. Alathamneh, S. Abdullah and N. S. Sani, "Genetic algorithm selection strategies based rough set for attribute reduction," *International Journal of Computer Science and Network Security*, vol. 19, no. 9, pp. 187–194, 2019.

[6] S. Bashir, M. H. Alsharif, I. Khan, M. A. Albreem, A. Sali *et al.,* "MIMO-terahertz in 6G nano-communications: Channel modeling and analysis," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 263–274, 2020.

[7] Q. Alsafasfeh, O. A. Saraereh, A. Ali, L. A. Tarawneh, I. Khan *et al.,* "Efficient power control framework for small-cell heterogeneous networks," *Sensors*, vol. 20, no. 5, pp. 1–14, 2020.

[8] K. M. Awan, M. Nadeem, A. S. Sadiq, A. Alghushami, I. Khan *et al.,* "Smart handoff technique for internet of vehicles communication using dynamic edge-backup node," *Electronics*, vol. 9, no. 3, pp. 1–17, 2020.

[9] W. Shahjehan, S. Bashir, S. L. Mohammed, A. B. Fakhri, A. A. Isaiah *et al.,* "Efficient modulation scheme for intermediate relay-aided IoT networks," *Applied Sciences*, vol. 10, no. 6, pp. 1–12, 2020.

[10] B. M. Lee, M. Patil, P. Hunt and I. Khan, "An easy network onboarding scheme for internet of things network," *IEEE Access*, vol. 7, pp. 8763–8772, 2018.

[11] O. A. Saraereh, A. Alsaraira, I. Khan and B. J. Choi, "A hybrid energy harvesting design for on-body internet-of-things (IoT) networks," *Sensors*, vol. 20, no. 2, pp. 1–14, 2020.

[12] A. A. Nimrat, M. Smadi, O. A. Saraereh and I. Khan, "An efficient channel estimation scheme for mmWave massive MIMO systems," in *IEEE Int. Conf. on Communications, Networks and Satellite (Comnetsat)*, Makassar, Indonesia, pp. 1–8, 2019.

[13] Q. Sun, G. Cheng, X. Wang, J. Xu, L. Wang *et al.,* "Energy-efficient routing algorithm based on small-world characteristics," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 2749–2759, 2021.

[14] Q. Yan, F. Yu and Q. Gong, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communication Surveys & Tutorials*, vol. 18, no. 1, pp. 602–622, 2016.

[15] X. An, J. Su and X. Lu, "Hypergraph clustering model-based association analysis of ddos attacks in fog computing intrusion detection system," *EURASIP Journal on Wireless Communications and Networking*, vol. 8, no. 4, pp. 1–15, 2018.

[16] A. Ibrahim, K. Tarik and S. Konstantinos, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2429–2453, 2018.

[17] B. Yi, X. Wang and K. Li, "A comprehensive survey of network function virtualization," *Computer Networks*, vol. 133, no. 5, pp. 212–262, 2018.

[18] P. Fonseca, R. Bennesby and E. Mota, "A replication component for resilient openflow-based networking," in *IEEE Symp. on Network Operations and Management*, Washington DC, USA, pp. 933–939, 2012.

[19] S. Kim, H. Kang and S. Hong, "A flow-based method for abnormal network traffic detection," in *IEEE Symp. on Network Operations and Management*, , Washington DC, USA, pp. 599–612, 2004.

[20] N. Giseop and R. Ilkyeun, "Adaptive ddos detector design using fast entropy computation method," in *IEEE 5th Int. Conf. on Innovative Mobile and Internet Services in Ubiquitous Computing*, Seoul, South Korea, pp. 86–93, 2011.

[21] J. Jun, C. Ahn and S. Kim, "DDoS attack detection by using packet sampling and flow features," in *IEEE 29th Annual ACM Symp. on Applied Computing*, New York, USA, pp. 711–712, 2014.
[22] K. Kalkan, L. Altay and G. Gur, "JESS: Joint entropy based ddos defense scheme in sdn," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 10, pp. 2358–2372, 2018.
[23] P. Kumar, M. Tripathi and A. Nehra, "SAFETY: Early detection and mitigation of tcp syn flood utilizing entropy in sdn," *IEEE Transactions on Network and Service Management*, vol. 15, no. 4, pp. 1545–1559, 2018.
[24] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu *et al.,* "XGBoost classifier for ddos attack detection and analysis in sdn-based cloud," in *IEEE Int. Conf. on Big Data and Smart Computing*, Shanghai, China, pp. 251–256, 2018.
[25] L. Yang and H. Zhao, "DDoS attack identification and defense using sdn based on machine learning method," in *IEEE 15th Int. Symp. on Pervasive Systems, Algorithms and Networks (I-SPAN)*, Yichang, China, pp. 174–178, 2018.
[26] A. Tang, L. Mhamdi, D. Mclernon, S. Zaidi and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in *IEEE Int. Conf. on Wireless Networks and Mobile Communications*, Fez, Morocco, pp. 258–263, 2016.
[27] L. Chen and V. Singh, "Entropy-based derivation of generalized distributions for hydrometeorological frequency analysis," *Journal of Hydrology*, vol. 557, no. 1, pp. 699–712, 2018.
[28] N. Lutsiv, T. Maksymyuk, M. Beshley, O. Lavriv, V. Andrushchak *et al.,* "Deep semisupervised learning-based network anomaly detection in heterogeneous information systems," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 413–431, 2022.
[29] S. Kim, M. Kojima and K. Toh, "A lagrangian-dnn relaxation: A fast method for computing tight lower bounds for a class of quadratic optimization problems," *Mathematical Programming*, vol. 156, no. 1, pp. 161–187, 2016.
[30] Y. Fan, Y. Qian and F. Soong, "Multi-speaker modeling and speaker adaptation for dnn-based tts synthesis," in *IEEE Int. Conf. on Acoustics, Speech and Signal Processing*, South Brisbane, Australia, pp. 4475–4479, 2015.
[31] T. Tang, L. Mhamdi, D. McLernon, S. Zaidi, M. Ghogho *et al.,* "DeepIDS: Deep learning approach for intrusion detection in software defined networking," *Electronics Journal*, vol. 9, no. 9, pp. 1–18, 2020.