EasyChair Preprint

№ 15434

Research on Ddos Attack Security Situation Assessment Model Based on Fuzzy C Clustering Algorithm

Yao Hu, Xiaolin Chen and Yuexin Zhang

November 16, 2024

Research on Ddos Attack Security Situation Assessment Model Based on Fuzzy C Clustering Algorithm

Yao Hu[a, b], Xiaolin Chen[*a, b], Yuexin Zhang[c]
[a] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China 100085
[b] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China 100049
[c] School of Public Finance and Taxation, Southwest University of Finance and Economics, Chengdu, China 611130
{huyao, chenxiaolin}@iie.ac.cn, {42204341}@smail.swufe.edu.cn

***Abstract*—As SDN (Software Defined Network) becomes more and more widely used, the risk of SDN network facing DDoS (Distributed Denial of Service, Distributed Denial of Service) attacks is also increasing. The attack traffic generated by DDoS attacks will cause serious damage to SDN. The network brings huge load pressure, which affects the normal network business. In severe cases, it may cause the entire SDN network to be paralyzed and cause property losses. Therefore, the detection of attack methods is very necessary and of great significance. This paper proposes an attack detection method based on Fuzzy C-means clustering algorithm (FCM), and designs a DDoS attack detection and defense system that includes three major functions: data collection, attack detection, and attack defense. Finally, the effectiveness of the proposed DDoS attack detection algorithm and defense strategy was verified through experiments. Experimental results show that the missed detection rate and bit error rate of the FCM fuzzy clustering algorithm are only 4.15% and 3.75%, which have obvious advantages over other commonly used detection methods.**

***Index Terms*—DDoS attack; fuzzy C-means clustering algorithm; network security; security situation prediction**

I. Introduction

The development of network intelligence has made network security a potential security risk for national information and personal information. Since its emergence, DDoS has gradually become one of the severe threats in the network [1] [2]. At present, research on machine learning algorithms is becoming increasingly mature, and classification algorithms such as K-means (K-means), Decision Tree (DT), and Naive Bayesian (NB) are widely used in low-level applications. Rate DDoS attack detection. Compared with traditional statistical methods, it shows great advantages. The training time is short and it can distinguish different types of attack behaviors. It has achieved remarkable results in the field of intrusion detection. However, attack forms are becoming increasingly diverse, and simple machine learning algorithms cannot effectively learn the characteristics of different attack types, so it is difficult to meet the accuracy requirements of attack detection [3] [4].

Currently, a large amount of research has been conducted at home and abroad on the detection and protection of DDoS attacks. Bhayo J et al. proposed a new SDN-based IoT security architecture, in which the DDoS attack detection module is used to implement rapid detection of DDoS attacks in the SD-IoT network [5]. Gaurav A analyzed various types of DDoS attacks and defense technologies in intelligent systems, and conducted a comprehensive review of the field of DDoS attack detection in intelligent systems. He also conducted a comprehensive and comprehensive review of various views, definitions and trends in this field. and organized summaries [6]. Jia B proposed a virtual reality parallel anti-Ddos chain design idea based on hybrid ensemble learning, as well as a distributed anti-Ddos chain inspection method. In his research, he discovered a more powerful generalization performance, versatility and complementarity, which can accurately identify the attack characteristics of DDoS attacks in P2P networks, and can also adopt a variety of methods to simulate protection [7]. Vinayakumar et al. used RNN to process NSL-KDD and UNSW-NB15 datasets. As an extension of artificial neural network, RNN is suitable for learning long-range temporal features. Its internal feedback loop mechanism enables the network to ultimately store time-related information and form an acyclic graph [8]. Azizjon et al. conducted research on RNN, LSTM and GRU. They benchmarked these three models on multi-class classification, using the KDD-99 data set [9]. Khan et al. conducted research using CNN and RNN. CNN and RNN are two types of time series data A combination of very different types of neural networks used. The idea is that CNNs learn spatial features by increasing the number of kernels, thereby learning coarse features at the beginning of the network and more detailed features at the later stages of the network. The RNN in the model focuses on learning temporal features from time series data. The model consists of multiple CNN layers and 2 LSTM layers after preprocessing the data set [10]. Gaurav et al. designed a cost-effective DDoS attack for small entrepreneurs in the context of the Covid-19 epidemic. Detection model. The model identifies traffic characteristics by calculating the entropy of incoming traffic and further uses machine learning algorithms to classify these entropy values to distinguish normal traffic from attack traffic. The proposed model is reactive

and can provide faster response time and higher detection accuracy, thereby effectively dealing with DDoS attack threats [11]. Batchu et al. proposed a new automatic detection technology and conducted experiments on CICDDoS2019. In this model, after data preprocessing, feature selection is done with the help of filters and embedding methods. In the hyperparameter search process, a grid search algorithm is used to implement it. Each hyperparameter combination is trained, and the optimal hyperparameter is finally determined through the selection of verification scores. The obtained features and hyperparameters are assigned to various classification techniques. The best results are achieved through gradient boosting learning [12]. Yungaicela et al. applied multiple machine learning and deep learning algorithms to detect application and transport layer DDoS attacks. The algorithm was tested on two data sets, CICDoS2017 and CICDDoS2019 data sets. The authors deployed a simulated environment with an open network operating system SDN controller using the Mininet simulator. In the simulation environment, the LSTM model showed high results in the detection rate of application layer attacks and transport layer attacks [13]. Cil et al. proposed a deep learning model aimed at improving optimal classification accuracy. The best results are achieved on the CICDDoS2019 dataset. The deep neural network (DNN) model integrates supervised learning and unsupervised learning methods in the process of achieving high accuracy. This model can also be applied to SDN-related fields in intrusion detection [14]. Doriguzzi et al. proposed a lightweight DDoS attack detection model that uses a CNN model to achieve low processing overhead and less attack detection time. The authors use three datasets (ISCX2012, CIC2017 and CSECIC2018) to conduct experimental analysis of feature importance in classification. The CNN model for online DDoS attack detection uses a unique traffic preprocessing method that can identify how data flows across network devices and allows network traffic to be fed to the CNN model [15]. Haider et al. proposed an Ensemble-CNN model to detect DDoS attacks. The method consists of integrating LSTM, RNN, CNN and hybrid RL and combining two models M1 and M2 into another model M3. The outputs of M1 and M2 serve as the input of the M3 model, which ultimately classifies benign traffic and attack traffic. Experimental results show that the Ensemble-CNN model has better anomaly detection results on the CICIDS-2017 data set [16]. Dong et al. detect DDoS attacks based on the number of DDoS attacks. The degree of DDoS attack is calculated based on the four characteristics of traffic length, traffic duration, traffic size, traffic proportion and its average NGain value. The author uses hping3 to generate traffic data including UDP, TCP and ICMP. This solution improves the accuracy of DDoS attack detection [17].

Although the research of the above-mentioned scholars has played a certain positive role in the detection of DDoS attacks, the effect is still not ideal and needs further improvement.Therefore, this paper proposes a DDoS attack security situation assessment model under the fuzzy C-means clustering algorithm to achieve accurate identification of DDoS attacks.

The rest of this paper is organized as follows: Section II reviews the related work on SDN, DDoS and FCM. The details of our method is given in Section III. The experiments results and system output performance is shown in Section IV. Section V is conclusions and future work.

II. RELATED WORK

A. Software-defined Networking

The Open Networking Foundation (ONF) elaborated on the SDN architecture in the SDN white paper released in 2012, which mainly includes three major planes and two major interfaces. The three major planes are divided into application planes from top to bottom. (Application Plane), Control Plane (Control Plane), Data Plane (Data Plane), the two major interfaces are Northbound Interface (NBI) and Southbound Interface (Southbound Interface, SBI). The control plane serves as the hub and connects to the application plane through the northbound interface to realize flexible control and policy distribution of upper-layer applications; it connects to the data plane through the southbound interface to realize command issuance and status monitoring of the underlying network equipment. The SDN architecture is shown in Figure 1. This architectural design enables SDN to achieve centralized control, flexible programming and efficient management of the network.

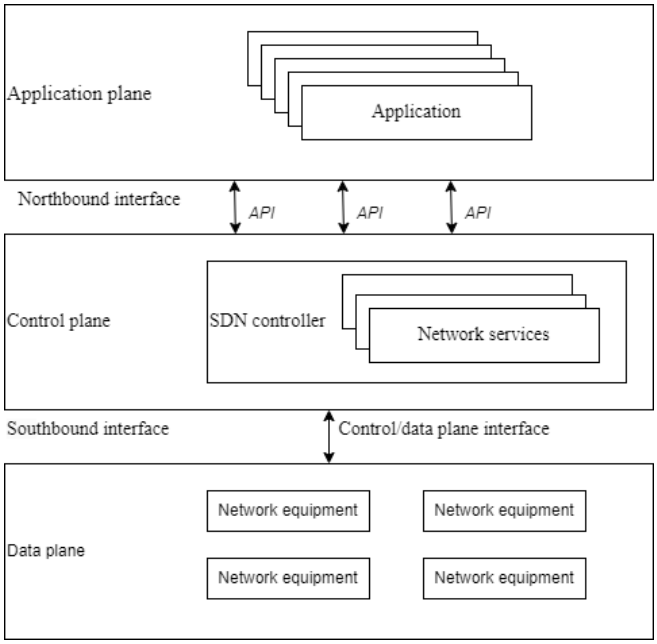

Fig. 1. SDN System Architecture

B. DDoS

1) Basic principles of DDoS attacks: A relatively complete DDoS attack system usually consists of four parts: attackers (Attacker), controllers (Masters), attackers (demons, also known as Slaves) and victims (Victim). The first part:

The Attacker issues control instructions, which is the controller of the DDoS attack [18] [19]. The second part: the control of the puppet computer by Masters, and the Attacker will execute DDoS on the puppet computer. Main program. The main program passes the attack instructions to Slaves. The third part is the attack. Masters send instructions to Slaves. After receiving the instructions, Slaves will attack the target machine. The fourth part: Slaves, the target of the DDoS attack. It may be a host, or it may be a switch, router, etc. The DDoS attack system is shown in Figure 2.

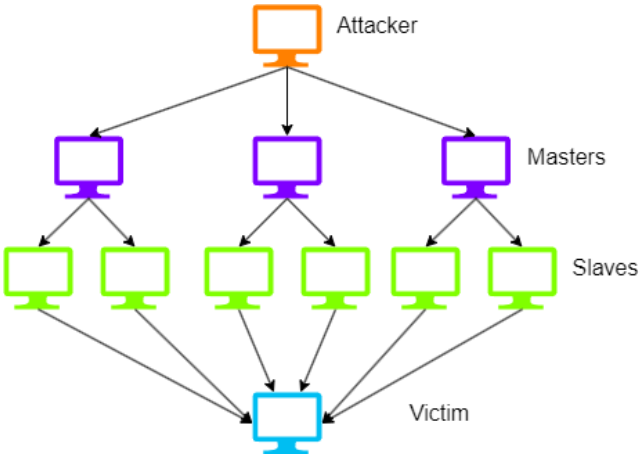

Fig. 2. DDoS attack architecture diagram

2) DDoS attack classification: DDoS attacks can be defined as manual, semi-automatic and automatic attacks. This standard is classified according to the degree of automation of the attack process; according to the standard of attack rate, it can be divided into fixed-rate attacks and variable-rate attacks; according to the data rate of the attack , Traffic in the network is divided into high-rate DDoS attacks and low-rate DDoS attacks, among which high-rate attacks are divided into system resource consumption type and network bandwidth consumption type [20].

DDoS attacks at each level of SDN can be divided into three categories: plane DDoS attacks, control plane DDoS attacks, and data plane DDoS attacks. DDoS attacks that may occur on different planes are shown in Table 1.

TABLE I
POSSIBLE DDOS ATTACKS ON SDNS

Location	possible attacks
Application plane	Northbound API exhaustion, application layer DDoS attacks (HTTP flooding, Slowloris, etc.)
Control plane	Controller resource exhaustion, OpenFlow bandwidth exhaustion, amplification attacks
Data plane	Switch DDoS, TCAM exhaustion, other traditional DDoS (ICMP flood, TCP flood, SYN flood, etc.)

3) DDoS attack detection technology:

a) Anomaly detection: The operation of a computer can be divided into two categories: normal and abnormal. As long as an abnormality occurs, abnormal detection needs to be carried out. Anomaly detection needs to start from multiple characteristic indicators, the main ones of which are: attack traffic rate size, packet size and port distribution, packet arrival time distribution, concurrent traffic number, advanced protocol characteristics, and inbound and outbound rates. The main attack detection methods include statistical analysis, rule reasoning and neural network methods.

b) Feature detection: It is assumed that attacker activities can be represented by a pattern, giving a deterministic description of known attacks or attack methods, and forming corresponding event patterns. System detection is carried out for this type of event pattern. This method can detect traditional DDOS attacks, but it is powerless against variants of DDoS attacks.

In addition to the above-mentioned anomaly detection and feature detection, DDoS attack detection methods also include many detection technologies, such as network protocol analysis and fuzzy clustering methods. The clustering algorithm first discovers abnormal network behavior patterns and detects corresponding DDoS attacks by mining statistics based on the distribution patterns of distributed denial-of-service attack characteristics. This method has more advantages than commonly used detection techniques. Therefore, this paper proposes a fuzzy C-means clustering algorithm to detect and research DDoS attacks, which will greatly improve the performance of DDoS attack detection.

C. Analysis of fuzzy C-means clustering algorithm

1) Fuzzy clustering: The fuzzy clustering algorithm simplifies the clustering analysis into a constrained nonlinear programming problem, and uses the optimization solution method to obtain the optimal fuzzy division and clustering results of the data set [21]. This algorithm has the advantages of simple operation and easy implementation, and during the solving process, many problems can be converted into optimal problems and then solved by nonlinear programming in mathematics. In view of the fact that DDoS attacks usually have similarities with ordinary attacks without obvious taxonomic characteristics, using fuzzy clustering analysis to detect DDoS attacks will have a positive impact.

2) Fuzzy clustering analysis process:

a) Feature extraction: The steps for feature extraction are as follows: Suppose the domain of discussion $m = \{m_1, m_2, \ldots, m_i\}$ is the object to be classified, and each object is represented by n features: $m_e = \{m_{e1}, m_{e2}, \ldots, m_{en}\}$, $e = 1, 2, \ldots, i$. Therefore, the original data matrix is obtained:

$$\begin{pmatrix} m_{11} & \cdots & m_{1n} \\ \vdots & \ddots & \vdots \\ m_{i1} & \cdots & m_{ni} \end{pmatrix} \quad (1)$$

In the above matrix, m_{ni} represents the original data of the n-th indicator of the i-th classification object.

b) Data standardization: In the process of data processing, the data dimensions are often different, which leads to a problem. To process the data, data conversion is required. The conversion process is: translation standard deviation transformation → translation range transformation → logarithmic transformation.

c) Calibration: Assume the domain of discussion $A = \{m_1, m_2, \ldots, m_i\}$, $m_e = \{m_{e1}, m_{e2}, \ldots, m_{en}\}$. By using clustering, the similar system ratio and the degree of similarity between m_e and k_e can be determined. For $r_{ij} = R(m_i, m_j)$, the corresponding fuzzy similarity matrix can be generated. Determining r_{ij} can be achieved by relying on traditional clustering methods, such as similarity coefficient method, distance method, etc. [22] [23].

3) Fuzzy C-means cluster analysis: The fuzzy C-means clustering algorithm is an iterative optimization algorithm for finding extreme values, which can describe the minimization of exponential functions [24] [25] FCM is defined as follows:

For the data set $M = \{m_1, m_2, \ldots, m_i\}$, which contains i samples, the data set is divided into $a(1 \leq a \leq i)$ categories. At this time, fuzzy clustering The objective value function can be expressed as follows:

$$F(S,T) = \sum_{k=1}^{i}\sum_{n=1}^{a}(s_{nk})^e(d_{nk})^2 (2)$$

$$(d_{nk})^2 = \|m_k - t_n\| = (m_k - t_n)^P A(m_k - t_n) (3)$$

Among them, S $=[s_{nk}], s_{nk} \in [0,1]$ refers to the membership matrix, T $= [t_n], n = 1, 2, ..., a$, t_n represent the matrix composed of all cluster centers, e is the weight index or fuzzy index, generally $e = 2$, $F(S,T)$ describes the sum of the distances from all samples to all cluster centers; matrix A For a symmetric matrix, $A = I$ is generally selected, and d_{nk} is the Euclidean distance.

The main process of the algorithm can be found in Algorithm 1.

Algorithm 1 Fuzzy C-Means Clustering

Require: Data set $X = \{x_1, x_2, \ldots, x_N\}$, where N is the number of data points; Number of clusters c; Fuzziness parameter $m > 1$ (controls the degree of fuzziness in clustering); Convergence threshold ϵ; Maximum iterations max_iter.

Ensure: Cluster centers $\{v_1, v_2, \ldots, v_c\}$; Membership matrix $U = [u_{ij}]$, where u_{ij} represents the degree of membership of data point x_i in cluster j.

Initialize membership matrix U with random values such that $\sum_{j=1}^{c} u_{ij} = 1$ for all $i = 1, \ldots, N$.
repeat
  for each cluster $j = 1, 2, \ldots, c$ **do**
    Update cluster center v_j as:

$$v_j = \frac{\sum_{i=1}^{N}(u_{ij})^m x_i}{\sum_{i=1}^{N}(u_{ij})^m}$$

  end for
  for each data point x_i and each cluster $j = 1, 2, \ldots, c$ **do**
    Update membership value u_{ij} as:

$$u_{ij} = \frac{1}{\sum_{k=1}^{c}\left(\frac{\|x_i - v_j\|}{\|x_i - v_k\|}\right)^{\frac{2}{m-1}}}$$

  end for
  Check for convergence: if $\|U^{(t+1)} - U^{(t)}\| < \epsilon$, then stop.
until Convergence or reaching maximum iterations.
return the final cluster centers $\{v_1, v_2, \ldots, v_c\}$ and membership matrix U.

III. Design of DDoS detection system based on FCM algorithm

A. Overall system design

In the system design of attack detection based on FCM algorithm, the system first completes the data collection work through four functional modules of data sampling, data analysis, data transmission and data reception, and obtains the relevant data required for attack detection; then feature processing and FCM algorithm The detection module completes the attack detection of data packets; finally, the attack defense module is responsible for locating the source of the attack and taking corresponding blocking measures to block DDoS attacks.

B. System module design

1) Data acquisition module: Data collection mainly includes four functional modules: data sampling, data analysis, data transmission and data reception. Data collection is the first step in DDoS detection. It aims to obtain network data packets in SDN and parse out the standardized data in the data packets as the source data that needs to be clustered. This is then processed through fuzzy clustering. Class data is formed into multiple clusters and clustering matrices, and then the information is processed and then passed to the database module for storage.

2) DDoS attack detection: The main functions of the detection module are: 1. After the network data packets in SDN are divided by FCM fuzzy clustering, the corresponding clustering results are marked one by one, and normal clusters and abnormal clusters are marked for further differentiation. 2 pairs of divided data are compared with the characteristic information in the database to complete the detection of DDoS attacks. In this way, not only can existing DDoS intrusion types be found in the clusters, but also the information of abnormal clusters can be stored, thereby discovering unknown DDoS attack information to facilitate further research. The test results are stored in the database. If during detection, unknown intrusion reaches a certain level, a secondary detection is required.

3) DDoS attack defense: The defense module is the action taken by the system after the detection module detects the attack behavior. The first is to issue early warning

prompts and give corresponding warning prompts to the target host or server. At the same time, according to the level of intrusion behavior, it is divided into three types: S, A, and B. S is the highest level, A is the second, and B is the lowest. Once an A-level warning occurs, corresponding measures must be taken immediately, including temporarily cutting off the network and performing link protection in a timely manner, otherwise the server will be paralyzed and terminated.The overall process is shown in Figure 3.

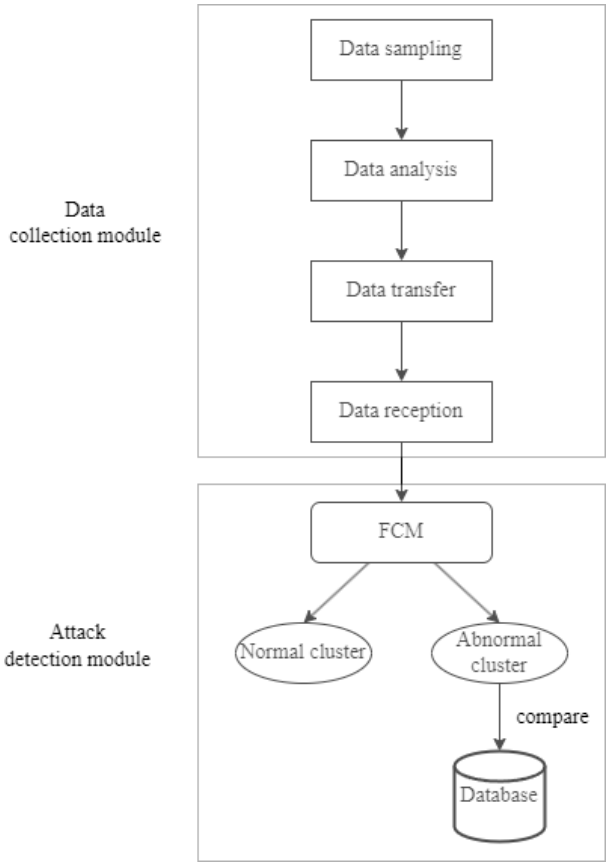

Fig. 3. System flow chart

IV. Experimental testing

A. Performance evaluation metrics

In order to analyze the detection performance of the DDoS attack detection model, this paper makes statistics and analysis of the incorrect interception and missed detection of DDoS attacks when implementing FCM algorithm detection based on the two evaluation indicators of missed detection rate and bit error rate. Set the total data packet as x, the missed DDoS attack data packet as y, the DDoS attack data packet as z, the detected DDoS attack data packet as q, and the incorrectly intercepted normal data packet as w.

$$falsenegativerate = \frac{y}{z} * 100\%(4)$$

$$probabilityoferror = \frac{w}{x - z} * 100\%(5)$$

B. Experimental test results

By conducting experiments every 40 times, and among the 4000 data packets sent, there were 2000 attack data packets, and the results in Table 1 and Figure 2 are obtained: From the data in Table 2 and Figure 4, we can know that

TABLE II
COMPARISON OF PARAMETERS OF THE THREE ALGORITHMS

Algorithm Type	x	y	z	q	w
k-means	4000	118	2000	1892	113
DTSOM	4000	102	2000	1910	94
FCM	4000	83	2000	1989	75

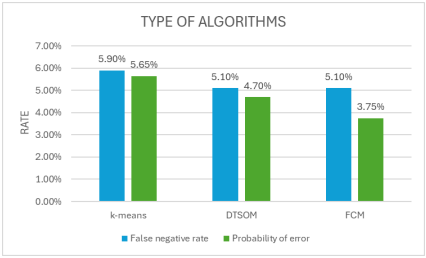

Fig. 4. False positive rates of the three algorithms

the missed detection rate and bit error rate of the FCM fuzzy clustering algorithm are significantly lower than the K-means algorithm and the DTSOM algorithm. Among them, the missed detection rate and bit error rate of the FCM fuzzy clustering algorithm are only 4.15% and 3.75%; while the missed detection rate and bit error rate of the K-means algorithm are 5.9% and 5.65%; the missed detection rate and bit error rate of the DTSOM algorithm are The rate is 5.1%, 4.7%. Therefore, the FCM fuzzy clustering algorithm has obvious advantages.

V. Conclusions and Future Work

DDoS is a very popular attack method in recent years, and it eliminates even more attacks than other attacks. The detection and protection of DDoS is extremely important, and the importance of prediction and prevention is also urgently highlighted. Scholars' progress in DDoS attack detection in SDN. Secondly, the concepts of SDN, DDoS and FCM are introduced. Then, a model using fuzzy C-means algorithm for DDoS attack detection is proposed. Then, the experiments were simulated in the established virtual network. Finally, the specific implementation plan of the test is given, and the test results are given.

Despite significant progress, DDoS attack detection in SDN still faces several key issues: the current lack of unified detection standards and frameworks in DDoS attack detection in SDN, the special threat of LR-DDoS attacks to the SDN environment, and the complexity of DDoS attacks Characteristics of sexiness and diversity, existing detection methods are not real-time enough to respond effectively in a short time, and how to reduce resource consumption while ensuring detection results, etc.

In future research, the following points can be studied: 1. Create a standard SDN data set for detecting DDoS attacks. 2. Strengthen research on LR-DDoS attacks in SDN. 3. Strengthen the distinction between DDoS attacks and FE. 4. Strengthen the detection and research of new DDoS attacks in SDN. 5. Strengthen the security protection of the SDN application plane. 6. Alleviate the problem of excessive overhead faced by SDN controllers and OpenFlow switches due to processing large amounts of traffic. 7. Research on DDoS attack detection in different SDN application scenarios.

SDN simplifies network management by decoupling the network into three layers, bringing new opportunities to the field of network security, but it also brings a series of security issues. With the development of Internet technology, network attacks are increasing year by year, and DDoS attacks have become a major hidden danger threatening network security. With the continuous emergence and application of emerging technologies, more detection methods and exploration space are provided for the research on DDoS attack detection in SDN. Relevant researchers can use the research directions described in this article as research ideas to propose more innovative solutions. Protect SDN to mitigate the potential harm caused by DDoS attacks to legitimate users.

REFERENCES

[1] K V R, Premchand P. Accurate and reliable detection of DDoS attacks based on ARIMA-SWGARCH model[J]. International Journal of Information and Computer Security, 2021, 14(2): 118-135.

[2] Gaur V, Kumar R. Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices[J]. Arabian Journal for Science and Engineering, 2022, 47(2): 1353-1374.

[3] Polat H, Turkoglu M, Polat O. Deep network approach with stacked sparse autoencoders in detection of DDoS attacks on SDN-based VANET[J]. IET Communications, 2020, 14(22): 4089-4100.

[4] Marvi M, Arfeen A, Uddin R. A generalized machine learning-based model for the detection of DDoS attacks[J]. International Journal of Network Management, 2021, 31(6): e2152.

[5] Bhayo J, Jafaq R, Ahmed A, et al. A time-efficient approach toward DDoS attack detection in IoT network using SDN[J]. IEEE Internet of Things Journal, 2021, 9(5): 3612-3630.

[6] Gaurav A, Gupta B B, Alhalabi W, et al. A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques[J]. International Journal of Intelligent Systems, 2022, 37(12): 11407-11431.

[7] Jia B, Liang Y. Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain[J]. China Communications, 2020, 17(9): 11-24.

[8] Vinayakumar R, Soman K P, Poornachandran P. Evaluation of recurrent neural network and its variants for intrusion detection system (IDS)[J]. Deep Learning and Neural Networks: Concepts, Methodologies, Tools, and Applications, 2020: 295-316.

[9] Azizjon M, Jumabek A, Kim W. 1D CNN based network intrusion detection with normalization on imbalanced data[C]//2020 international conference on artificial intelligence in information and communication (ICAIIC). IEEE, 2020: 218-224.

[10] Khan R U, Zhang X, Alazab M, et al. An improved convolutional neural network model for intrusion detection in networks[C]//2019 Cybersecurity and cyberforensics conference (CCC). IEEE, 2019: 74-77.

[11] Gaurav A, Gupta B B, Panigrahi P K. A novel approach for DDoS attacks detection in COVID-19 scenario for small entrepreneurs[J]. Technological Forecasting and Social Change, 2022, 177: 121554.

[12] Batchu R K, Seetha H. A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning[J]. Computer Networks, 2021, 200: 108498.

[13] Yungaicela-Naula N M, Vargas-Rosales C, Perez-Diaz J A. SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning[J]. IEEE Access, 2021, 9: 108495-108512.

[14] Cil A E, Yildiz K, Buldu A. Detection of DDoS attacks with feed forward based deep neural network model[J]. Expert Systems with Applications, 2021, 169: 114520.

[15] Doriguzzi-Corin R, Millar S, Scott-Hayward S, et al. LUCID: A practical, lightweight deep learning solution for DDoS attack detection[J]. IEEE Transactions on Network and Service Management, 2020, 17(2): 876-889.

[16] Haider S, Akhunzada A, Mustafa I, et al. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks[J]. Ieee Access, 2020, 8: 53972-53983.

[17] Dong S, Sarem M. DDoS attack detection method based on improved KNN with the degree of DDoS attack in software-defined networks[J]. IEEE Access, 2019, 8: 5039-5048.

[18] Dasari K B, Devarakonda N. Detection of TCP-based DDoS attacks with SVM classification with different kernel functions using common uncorrelated feature subsets[J]. International Journal of Safety and Security Engineering, 2022, 12(2): 239-249.

[19] Singh K J, Haokip J, Chanu U S. A Novel Approach to Develop and Deploy Preventive Measures for Different Types of DDoS Attacks[J]. International Journal of Information Security and Privacy (IJISP), 2020, 14(2): 1-19.

[20] Behal S, Kumar K, Sachdeva M. D-FAC: A novel ϕ-Divergence based distributed DDoS defense system[J]. Journal of King Saud University-Computer and Information Sciences, 2021, 33(3): 291-303.

[21] Mehdi K, Mohammad S, Mahmoud F A S. Statistical analysis and fuzzy clustering model to predict limestone rock mass quality (Q srm) and degree of karstification (DK) using geophysical parameters (case study of some areas in western Iran)[J]. Modeling Earth Systems and Environment, 2022, 8(1): 245-258.

[22] Liu J, Cai Y, Zhang Q, et al. Thermal error analysis of tauren EDM machine tool based on FCM fuzzy clustering and RBF neural network[J]. Journal of Intelligent & Fuzzy Systems, 2021, 41(6): 6003-6014.

[23] Kulkarni O, Jena S, Ravi Sankar V. MapReduce framework based big data clustering using fractional integrated sparse fuzzy C means algorithm[J]. IET Image Processing, 2020, 14(12): 2719-2727.

[24] Pimentel B A, de Amorim Silva R, Costa J C S. Fuzzy C-means clustering algorithms with weighted membership and distance[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2022, 30(04): 567-594.

[25] Huang D, Wang J, Wen Z. Parallel FCM clustering algorithm of fuzzy number based on cut set[J]. Journal of Computational Methods in Sciences and Engineering, 2021, 21(4): 989-997.