Industrial Engineering and Applications
L.-C. Tang (Ed.)

doi:10.3233/ATDE230062

Hybrid Continuous Variational Quantum Neural Networks for Network Intrusion Detection

Suya CHAO [1] , Guang YANG and Min NIE
School of Communication and Information Engineering Xi'an University of Posts and Telecommunications
ORCiD ID: Suya Chao https://orcid.org/0000-0002-2061-7468,
ORCiD ID:Guang Yang https://orcid.org/0000-0002-9726-7742,
ORCiD ID:Min Nie https://orcid.org/0000-0001-6238-4167

Abstract. In order to solve the problem of excessive parameters and slow computing speed of classical neural networks, this paper uses the powerful parallel computing power of quantum computing to improve the computing speed of classical neural network models, and proposes a hybrid continuous variational quantum neural network (HCVQNN) model that can be used for network intrusion detection. The continuous variable layer of the model is realized through Gaussian gate and non-Gaussian gate, in which Gaussian gate performs operations such as quantum state weight addition and offset term setting, and non-Gaussian gate performs nonlinear operations, thereby improving the overall expression ability of the network model. In addition, aiming at the unbalanced problem of UNSW-NB15 in the network intrusion dataset, this paper proposes to design the algorithm from the feature level and the algorithm level, using the ReliefF algorithm for feature selection at the feature level, and oversampling and undersampling processing at the algorithm level by combining the Borderline-SMOTE algorithm and GMM algorithm. The classification experimental results on the UNSW-NB15 network intrusion dataset show that compared with the other two network models, the HCVQNN network model obtains higher classification accuracy and lower loss function value in both binary classification and multi-classification tasks, and the classification accuracy for minority categories is also improved.

Keywords. classical neural networks, HCVQNN, network intrusion detection, UNSW-NB15

1. Introduction

With its powerful nonlinear information processing ability and generalization ability, classical neural network has become an important machine learning model and is commonly used in signal processing, natural language processing, image classification and other fields[1-4].Quantum computing is based on the coherent superposition and entanglement of quantum states, which can provide powerful parallel computing capabilities[5-7].How to combine quantum computing with classical neural networks and give full play to the advantages of both, so as to improve the classical neural network

[1] Corresponding Author: Suya Chao, 1920464642@qq.com.

architecture and improve network computing performance has become an important direction that people pay attention to.

Quantum neural network (QNN) model inspired by the classical neural network in the early stage, which provided a reference for research in this field[8-10]. In 2019, the quantum convolutional neural network (QCNN) proposed by Cong et al. only uses O(log(N)) variational parameters as the input size of N qubits to reduce the complexity of the network[11]; in 2020, Henderson et al. proposed the concept of quantum convolution layer, which enhanced the ability to extract features from data through random quantum circuits, but lacked nonlinear operations to enhance the generalization of the network[12]; in 2021, Niu proposed a QNN with multi-layer activation function, which enhanced the robustness of the network model[13]. For two-dimensional image data, in 2022, Houssein et al. proposed using randomized quantum circuits to construct a hybrid QNN model, which achieved a high classification accuracy in the experiment of classifying images of COVID-19[14].

However, the QNN proposed so far is the model output obtained through quantum measurement. Compared with the classical neural network, it lacks the deep data relationship brought by the nonlinear operation, thus reducing the expressive ability of the network. The continuous variation quantum circuit has been gradually applied to the field of machine learning by taking advantage of the nonlinearity brought by its non-Gaussian gate and the continuous variation characteristic brought by the Gaussian gate[15]. At the same time, a linear kernel classifier model based on continuous variable quantum circuits was proposed in[16], and finally a two-dimensional benchmark dataset was used to verify the classification effect of the model. The results showed that it had better classification performance and faster calculation speed.

More and more neural networks are used for intrusion detection.[17-18]Therefore, in view of the nonlinearity of the quantum neural network, this paper proposes a continuous variational quantum neural network (HCVQNN) to be applied to network intrusion detection to achieve the purpose of improving the expressive ability of the network model under the premise of reducing computational overhead. On the other hand, in view of the unbalanced characteristics of the network intrusion dataset UNSW-NB15, this paper adopts a processing method combining feature level and algorithm level. At the feature level, the Relief F algorithm is used for feature screening, redundant features are removed, and data complexity is reduced. At the algorithm level, a combination of the Borderline-SMOTE algorithm and the GMM (Gaussian Mixture Model) algorithm is used to perform a separate analysis on the minority category samples. Oversampling and clustering undersampling are performed on samples of most categories to improve the overall detection performance of the network model. Finally, simulation experiments on the UNSW-NB15 network intrusion dataset show that the algorithm proposed in this paper has higher classification accuracy in binary classification and multi-classification than other network models. At the same time, the classification accuracy is also significantly improved for minority class samples. Thus further verifying the effectiveness of the unbalanced algorithm and HCVQNN network model proposed in this paper for network intrusion detection, which has certain positive significance for the future application and development of QNN.

2. Unbalanced dataset

2.1. Unbalanced Dataset Definition

In the intrusion detection dataset UNSW-NB15 used in this paper, the four major attack categories of Analysis, Backdoors, Shellcode, and Worms account for a relatively small proportion of the total number of samples, so there is an imbalance in the data distribution. This section mainly reduces the impact of data imbalance on network performance from the level of feature processing and algorithm design.

2.2. Research at the feature level

From the feature level, the unbalanced distribution of data features is the main reason for the imbalance of data categories, because when the features of some minority categories are ignored, the classification results of the network model will be more biased towards the majority category, resulting in data imbalance. Therefore, it is very important to select the important features that can best distinguish the majority category and the minority category by removing redundant features through certain feature selection.

This paper mainly uses the ReliefF algorithm to reduce the dimensionality of the UNSW-NB15 dataset. The principle is to select important features by assigning larger weights to the features that contribute greatly to the classification results. The algorithm is not only simple in design, but also has no specific data type restrictions. The selected most important feature subset is input into the network model for training, thereby improving the performance of the network model and improving the classification accuracy.

The main process of the Relief F algorithm is as follows: 1) There are several different types of sample data, and each type of sample is called x_n. Among all sample data, a sample a is randomly selected. 2) In the sample group of the same category as a, take the k nearest neighbor samples. 3) In all sample groups that are not of the same category as a, also take k nearest neighbor samples. 4) Calculate the weight of each feature. The weight for each feature can be calculated as:.

$$W(A) = W(A) - \sum_{j=1}^{K} diff(A, R_i, H_j) / (m * k) + \sum_{C \neq class(R)} [\frac{p(C)}{1 - p(class(R))} \sum_{j=1}^{k} diff(A, R_i, M_j(C))] / (m * k) \quad .(1)$$

$$diff(A, R_1, R_2) = \begin{cases} \dfrac{R_1[A] - R_2[A]}{\max(A) - \min(A)}, & if \text{ A is continous} \\ 0, \quad if \text{ A is discrete and } R_1[A] = R_2[A] \\ 1, \quad if \text{ A is discrete and } R_1[A] \neq R_2[A] \end{cases} \quad .(2)$$

In the formula, m is the number of samples, $M_j(C)$ is the jth nearest neighbor sample in a different category C than the sample, and P(C) represents the proportion of the target sample number of class C to the total number of samples; class(R_i) indicates the class of sample R_i; diff(A,R_1,R_2) is used to calculate the distance between samples R_1 and R_2 with respect to feature A.

The average weight of each feature can be obtained by repeating the above process m times. The criterion for feature selection is to see the size of the average weight of each feature obtained in the end. Because the higher the weight, the higher the classification contribution of the feature to the network model, and vice versa, the lower the classification contribution to the network model.

After processing by Relief F algorithm, the intrusion dataset can effectively eliminate the noise feature items, thereby reducing feature redundancy and obtaining a low-dimensional excellent feature subset. This algorithm can effectively reduce the problem of complex network structure caused by the large amount of intrusion data, and also obtain better classification results through the filtered feature subset.

2.3. Research from the Algorithmic Level

From an algorithm perspective, in the UNSW-NB15 network intrusion data set, the number of samples of different categories is unevenly distributed, which will cause the network model to classify most types of network traffic data samples when performing multi-classification of attack categories. The classification accuracy rate is high, but the classification accuracy rate for samples containing a few types of network traffic data is low. Therefore, it is necessary to use algorithms to deal with the problem of unbalanced distribution of network traffic data categories. In this paper, the Borderline-SMOTE algorithm is used to oversample a few types of network traffic data, and the GMM (Gaussian Mixture Model) algorithm is used to cluster and undersample most types of network intrusion data. The two methods are combined to balance the number of samples in each category, thereby improving the overall detection performance of the network model.

The Boderline-Smote algorithm is mainly used to solve the problem of feature distribution of minority network traffic data samples. It mainly performs synthetic sampling on the boundaries of minority samples so that there is no redundancy in the newly synthesized samples, which greatly improves the feature distribution interval of the sample and the classification performance of the network model. In addition, Borderline-Smote sampling divides the minority class samples into three parts: noise samples, dangerous samples and safe samples. The specific process is as follows: 1) For each sample x in the minority category set A, consider the set A as a training set, and calculate the Euclidean distance from all points in A to the sample point. And thus select k nearest neighbor points, and then record all majority class sample sets in its neighbor points as k1. 2) Comparing the total sample size of k and k1, when the total sample size of k1 exceeds half of the total sample size of k, the selected samples are classified as dangerous samples and put into the dangerous sample set DangerSet; if the total sample size of k1 is equal to If the total number of k samples is the same, the selected samples are classified as noise samples; if none of the above conditions are met, they are classified as safe samples, and neither the noise samples nor the safe samples will be operated subsequently. 3) For the dangerous samples put into the DangerSet set, it is necessary to find out the corresponding k adjacent sample points. 4) Finally, perform sample synthesis for each point in the DangerSet set.

The GMM algorithm is an algorithm described by a parameterized probability distribution frame model, which is represented by a linear combination of several Gaussian normal distribution functions. If all network traffic sample data come from

multiple Gaussian normal distribution functions with different parameters, the samples belonging to the same distribution function are classified into the same cluster, and GMM can return sample traffic data x belonging to different clusters according to the following formula class probability.

$$P(x \mid \theta) = \sum_{k=1}^{K} \alpha_k \phi(x \mid \theta_k) \cdot \tag{3}$$

In the formula, α_k is the probability that the k*th* subframe model is selected in the network traffic set, $\alpha_k \geq 0$, $\sum_{k=1}^{K} \alpha_k$ =1, $\theta_k = (\mu_k, \delta_k^2)$, $\phi(x, \theta_k)$ is the Gaussian normal distribution density of the kth subframe model, as shown in the following formula:

$$\phi(x \mid \theta_k) = \frac{1}{\sqrt{2\pi}\delta_k} \exp(\frac{x - \mu_k}{2\delta_k^2}) \cdot \tag{4}$$

3. HCVQNN Structure Design

This paper proposes a new hybrid continuous variational quantum neural network model. By combining the classic CNN and continuous variational quantum neural network (CVQNN) to construct a hybrid network model, the spatial characteristics of the data can be preserved through CNN, and the non-Gaussian gate of the CVQNN realizes nonlinear functions, achieving the effect of high-speed parallel processing of data while retaining the complex characteristics of mining data. Among them, CVQNN is mainly composed of multiple basic layers, and one basic layer includes linear operations performed by Gaussian gates and nonlinear operations performed by non-Gaussian gates.

3.1. CVQNN Basic Layer Structure

The basic layer structure of CVQNN is shown in Fig 1. The first four parts $U_1(\theta,\phi)$、$S(r)$、$U_2(\theta,\phi)$、$D(\alpha)$ are linear operations performed by Gaussian gates, and the last part $\mu(\lambda)$ is nonlinear operations performed by non-Gaussian gates.

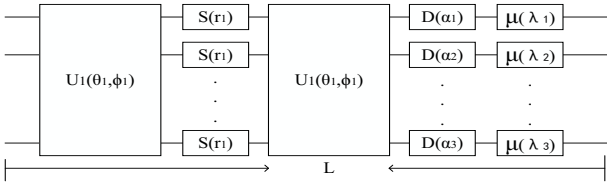

Figure 1. CVQNN basic layer structure.

The conversion performed by the common Gaussian gates $U(\theta,\phi)$ (generally represented by $\hat{B}S(\theta)$), $S(r)$、$D(\alpha)$、$R(\phi)$, and non-Gaussian gates $\mu(\lambda)$ can be represented by the following formula:.

$$\hat{R}(\phi):\begin{bmatrix}x_1\\x_2\end{bmatrix}\mapsto\begin{bmatrix}\cos\phi & \sin\phi\\-\sin\phi & \cos\phi\end{bmatrix}\begin{bmatrix}x_1\\x_2\end{bmatrix}. \tag{5}$$

$$\hat{D}(\alpha):\begin{bmatrix}x_1\\x_2\end{bmatrix}\mapsto\begin{bmatrix}x_1+\sqrt{2}\,\mathrm{Re}(\alpha)\\x_2+\sqrt{2}\,\mathrm{Im}(\alpha)\end{bmatrix}. \tag{6}$$

$$\hat{S}(r):\begin{bmatrix}x_1\\x_2\end{bmatrix}\mapsto\begin{bmatrix}e^{-r} & 0\\0 & e^{r}\end{bmatrix}\begin{bmatrix}x_1\\x_2\end{bmatrix}. \tag{7}$$

$$\hat{BS}(\theta):\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}\mapsto\begin{bmatrix}\cos\theta & -\sin\theta & 0 & 0\\\sin\theta & \cos\theta & 0 & 0\\0 & 0 & \cos\theta & -\sin\theta\\0 & 0 & \sin\theta & \cos\theta\end{bmatrix}\begin{bmatrix}x_1\\x_2\\x_3\\x_4\end{bmatrix}. \tag{8}$$

$$\mu(\lambda)=\exp(i\frac{\lambda}{3}\hat{x}^3)\cdot \tag{9}$$

3.2. HCVQNN Multilayer Structure

Fig 2 is a multi-layer structure model of the HCVQNN network, in which the input between the output of a certain layer and the input of a certain layer can be achieved by measuring or applying a non-Gaussian gate to reduce the effect of qubits, thereby reducing the complexity of the quantum network. Among them, the input of the network can be classical data or quantum data. In this paper, the network is used to intrude the classical data, and the Gaussian gate is used to realize the conversion from classical data to quantum data.

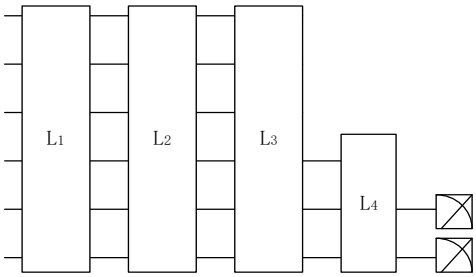

Figure 2. HCVQNN multilayer structure

3.3. HCVQNN Overall Structure

The overall structure of HCVQNN is shown in Fig 3. It consists of two parts, the classic CNN layer and CVQNN. After the classic data is trained by the classic CNN layer, it is input to each Gaussian gate and non-Gaussian gate of CVQNN to complete the training of the entire model. When performing binary classification, only the non-Gaussian gate can be used to get the final classification results ,When performing multi-classification, adding a fully connected layer behind the quantum network can achieve multi-classification tasks.

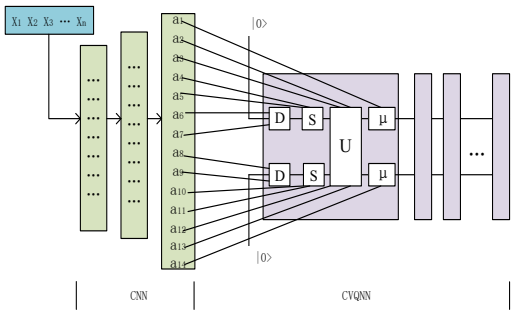

Figure 3. The overall structure of HCVQNN

The network training steps of CVQNN are as following:.

- Gaussian phaseless U-gate is used to act on the double quantum state to add the quantum state weight.

$$\begin{aligned}\hat{U}_1\left|\bar{x}\right\rangle &= \hat{U}_1\left[\bigotimes_{i=1}^{N}\left|x_i\right\rangle\right] \\ &= \bigotimes_{i=1}^{N}\left|\sum_{j=1}^{N} C_{ij}x_{ij}\right\rangle, \\ &= \left|C\bar{x}\right\rangle\end{aligned} \tag{10}$$

where C is the orthogonal matrix. Therefore, the Gaussian phaseless U-gate implementation multiplies the qubit by an orthogonal matrix to realize the setting of the weight parameter.

- The Gaussian S-gate is used to act on a single quantum state to realize the expansion and scaling of the amplitude of the quantum state.

$$\hat{S}(r_i)\left|x_i\right\rangle = \sqrt{c_i}\left|c_i x_i\right\rangle, \tag{11}$$

where $c_i = e^{-r_i}$, when $c_i \le 1$, Corresponds to quantum state amplitude compression, when $c_i > 1$, Corresponds to the amplitude expansion of quantum states. The general form of its S-gate for element scaling can be expressed as:

$$\hat{S}(\bar{r})\left|\bar{x}\right\rangle = e^{-\frac{1}{2}\sum_i r_i}\left|\sum \bar{x}\right\rangle. \tag{12}$$

In the formula, $\sum := diag(\{c_i\}) > 0$.

- Gaussian D-gate is used to act on a single quantum state to realize the setting of the offset term of the coding vector.

$$\hat{D}(\alpha_i)\left|x_i\right\rangle = \left|x_i + \sqrt{2}\alpha_i\right\rangle. \tag{13}$$

For $\alpha_i \in R$, the above equation can be uniformly written as:

$$\hat{D}(\bar{\alpha})\left|\bar{x}\right\rangle = \left|\bar{x} + \sqrt{2}\bar{\alpha}\right\rangle. \tag{14}$$

Therefore, the setting of the offset term $\bar{\alpha}$ can be realized, so as to better fit the data and achieve the role of enhancing the generalization of the network.

- Nonlinear operations are performed using non-Gaussian gates.

$$\mu(\lambda)\left|\bar{x}\right\rangle = \left|\varphi(\bar{x})\right\rangle. \tag{15}$$

Through the above Gaussian gate, the conversion operation of a layer of CVQNN can be completed.

4. Experimental Results and Performance Analysis

By comparing the binary classification performance and multi-classification performance of HCVQNN、CNN and CVQNN network models, the simulation experiment verifies the effectiveness and feasibility of the algorithm for processing unbalanced datasets and the HCVQNN model.

4.1. Experimental Model Parameters

Table I shows the HCVQNN model structure. The HCVQNN model uses two layers of one-dimensional convolutional layers, two layers of maximum pooling, one Flatten layer, two layers of fully connected layers, two layers of CVQNN layers, and finally uses the softmax layer as the classifier for multi-classification. All parameters of the HCVQNN model are the best parameters obtained after many experimental debugging.

TABLE I. HCVQNN NETWORK MODEL PARAMETERS

Operations	Filter	Stride	Padding
1D Conv+Relu	128	1	same
Max pooling	10	2	same
1D Conv+Relu	64	1	same
Max pooling	5	2	same
Flatten	--	--	none
Dropout	0.6	--	none
Dense+Elu	28	--	none
Dense+Elu	14	--	none
CVQNN	2	--	none
CVQNN	2	--	none
Dense+Softmax(multi-classification)	10	--	none

4.2. Comparative Analysis of HCVQNN Binary Classification Results

The binary classification accuracy curves of CNN network model, CVQNN network model and HCVQNN network model on the UNSW-NB15 network intrusion dataset are shown in Fig 4.

It can be seen from Fig 4 that in the iterative process of the network model, compared with the other two models, the HCVQNN network model proposed in this paper has always had a high binary classification accuracy, up to 94.27%, and can make the model reach a stable state at the fastest speed.

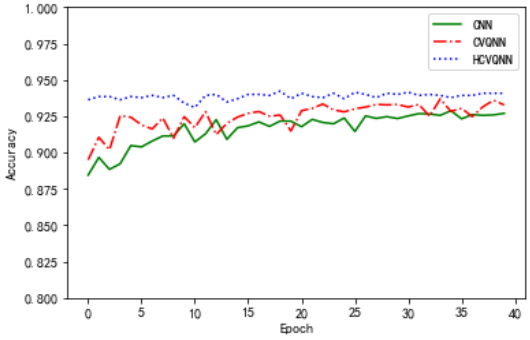

Figure 4. CNN, CVQNN and HCVQNN binary classification accuracy comparison

The classification accuracy of the CVQNN network model is higher than that of the CNN network model. Therefore, the HCVQNN network model proposed in this paper not only solves the problem of data imbalance, but also increases the classification accuracy of the model for intrusion data due to its non-Gaussian gate nonlinearity. At the same time, the comparison curve of the loss function values of these three network models with the number of iterations is shown in Fig 5. It can be seen from Fig 5 that the HCVQNN network model has the fastest speed to make the loss function value reach a steady state close to 0, followed by the CVQNN network model and the CNN network model, respectively. Based on Fig 4 and Fig 5, it can be seen that in terms of the convergence speed of the model, the performance is reduced by the HCVQNN network model, CVQNN network model and CNN network model, which also reflects that the HCVQNN network model has a faster convergence speed than the other two models.

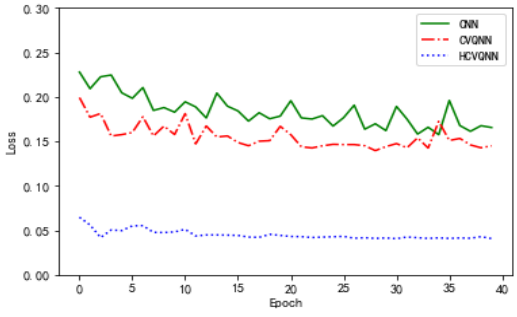

Figure 5. CNN, CVQNN and HCVQNN binary classification loss functions

Table II compares the performance indicators of Accuracy, Precision, Recall and F1-sorce on the UNSW-NB15 dataset of CNN network model, CVQNN network model and HCVQNN network model.

It can be seen from Table II that the classification accuracy Accuracy, Precision Precision, Recall and F1 values of the HCVQNN network model proposed in this paper all achieve high score compared with the other three network models. It can be seen that the HCVQNN network model has a strong overall intrusion detection effect.

TABLE II. CNN, CVQNN AND HCVQNN BINARY CLASSIFICATION PERFORMANCE INDICATORS

Model	Accuracy%	Precision%	Recall%	F1-Score%
CNN	92.70	97.39	90.50	93.82
CVQNN	93.58	97.38	92.08	94.65
HCVQNN	94.27	98.36	98.62	95.68

The classification accuracy of the HCVQNN network model for normal data and intrusion data is statistically obtained, and the final classification accuracy is shown in Fig 6.

It can be seen from Fig 6 that the HCVQNN network model proposed in this paper can achieve high classification accuracy for normal data types and intrusion data types, which proves that the HCVQNN network model achieves better classification performance for network intrusion datasets than CNN and CVQNN by taking advantage of its continuous variational and increasing nonlinear processing.

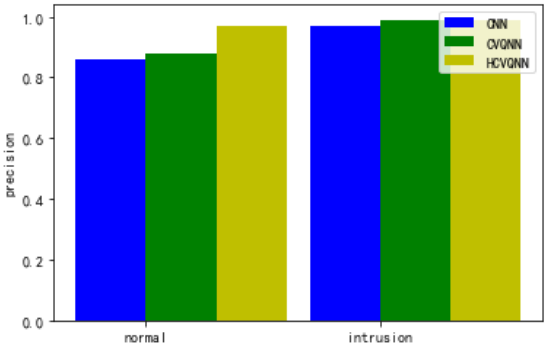

Figure 6. Classification category precision

4.3. Comparative Analysis of HCVQNN Multi-classification Results

The multi-classification accuracy curves of CNN network model, CVQNN network model and HCVQNN network model on the UNSW-NB15 network intrusion dataset are shown in Fig 7.

It can be seen from Fig 7 that in the iterative process of the network model, compared with the other two models, the HCVQNN network model proposed in this paper has always had a high multi-classification accuracy, up to 87.66%, and can make the model reach a stable state at the fastest speed.

The classification accuracy of the CVQNN network model is higher than that of the CNN network model. Therefore, the HCVQNN network model proposed in this paper not only solves the problem of data imbalance, but also increases the classification accuracy of the model for intrusion data due to its non-Gaussian gate nonlinearity. At the same time, the loss function value comparison curve of these three network models with the number of iterations is shown in Fig 8.

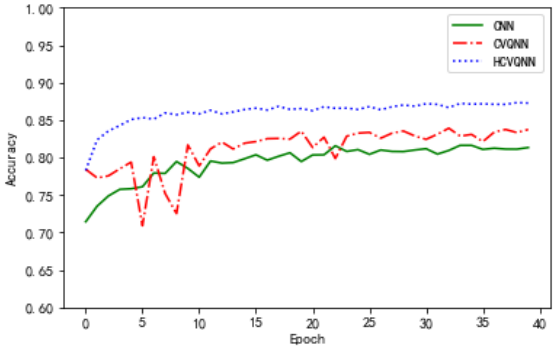

Figure 7. CNN, CVQNN and HCVQNN multi-classification accuracy comparison

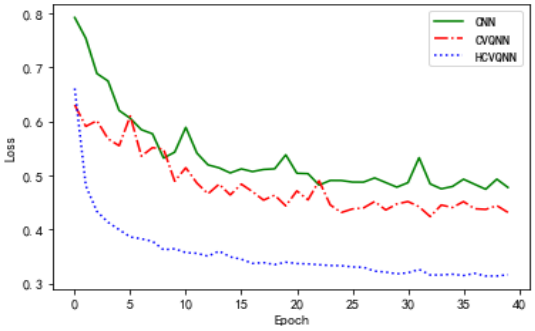

Figure 8. CNN, CVQNN and HCVQNN multi-classification loss functions

It can be seen from Fig 8 that the HCVQNN network model has the fastest speed to make the loss function value reach a steady state close to 0, followed by the CVQNN network model and the FRQCNN network model, respectively.

Based on Fig 7 and Fig 8, it can be seen that in terms of the convergence speed of the model, the performance increases in order for the CNN network model, CVQNN network model and HCVQNN network model, which also reflects that the HCVQNN network model has a faster convergence speed than the other two models.

Table III shows the performance indicators of Accuracy, Precision, Recall and F1-sorce for multi-classification of CNN network model, CVQNN network model and HCVQNN network model on UNSW-NB15 dataset.

TABLE III. CNN, CVQNN AND HCVQNN MULTI-CLASSIFICATION PERFORMANCE INDICATORS

Model	Accuracy%	Precision%	Recall%	F1-Score%
CNN	81.34	78.99	81.34	79.18
CVQNN	83.75	84.67	83.75	82.59
HCVQNN	87.66	88.76	87.66	86.29

It can be seen from Table III that the classification accuracy Accuracy, precision precision, Recall and F1 values of the HCVQNN network model proposed in this paper

achieve high scores compared with the other two network models. It can be seen that the HQLSTM network model has achieved good performance in all multi-classification evaluation indicators.

Calculate the accuracy results of normal data types and attack data types, and finally obtain the classification accuracy of each category as shown in Fig 9.

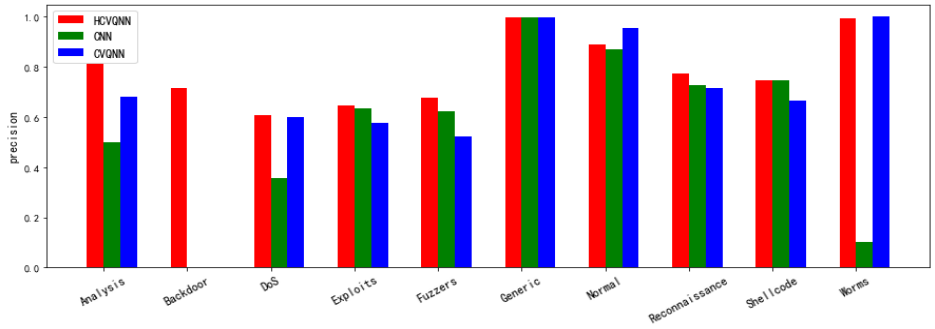

Figure 9. Classification category precision

It can be seen from Fig 9 that the unbalanced processing algorithm and HCVQNN network model proposed in this paper have improved the overall detection rate of intrusion data, and compared with the CNN and CVQNN network models, the detection rate of rare attacks has been significantly improved, and there is no situation where the detection rate of a certain type of attack is 0. It further shows that the algorithm and model adopted in this paper have significantly improved the performance of network intrusion detection.

5. Conslusion

In this paper, a method combining Borderline-SMOTE algorithm and GMM algorithm is proposed to process UNSW_NB15 unbalanced dataset, thereby reducing the data dimension and reducing the complexity of the network model. At the same time, in order to solve the nonlinear problem of quantum neural network, this paper proposes a quantum neural network model of HCVQNN, in which Gaussian gates are introduced to perform linear operations and non-Gaussian gates are introduced to perform nonlinear operations, so as to further improve the characteristics of the network to process complex data. Experimental results show that compared with CNN and CVQNN network models, the algorithm and model proposed in this paper have higher classification accuracy and faster convergence speed in the field of network intrusion. Moreover, through the classification accuracy of the three models for a few categories, it can be seen that the algorithm and model proposed in this paper have better classification performance.

Acknowledgement

Project supported by the National Natural Science Foundation of China (Grant Nos. 61971348, 61201194) and Natural Science Basic Research Program of Shaanxi, China (Grant No. 2021JM-464).

References

[1] Kiranyaz S, Ince T, Abdeljaber O, Avci O, Gabbouj M. 1-D convolutional neural networks for signal proc essing applications[C]//ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Sig nal Processing (ICASSP). IEEE, 2019: 8360-8364.
[2] Goldberg, Yoav. "Neural network methods for natural language processing." Synthesis lectures on human language technologies 10.1 (2017): 1-309.
[3] Liu, Yang, and Meng Zhang. "Neural network methods for natural language processing." (2018): 193-195.
[4] Yadav, Samir S., and Shivajirao M. Jadhav. "Deep convolutional neural network based medical image classification for disease diagnosis." Journal of Big Data 6.1 (2019): 1-18.
[5] Gyongyosi, Laszlo, and Sandor Imre. "A survey on quantum computing technology." Computer Science Review 31 (2019): 51-71.
[6] Wu, Yulin, et al. "Strong quantum computational advantage using a superconducting quantum processor." Physical review letters 127.18 (2021): 180501.
[7] von Burg, Vera, et al. "Quantum computing enhanced computational catalysis." Physical Review Research 3.3 (2021): 033055.
[8] Ricks B, Ventura D. Training a quantum neural network[J]. Advances in neural information processing systems, 2003, 16.
[9] Schuld M, Sinayskiy I, Petruccione F. The quest for a quantum neural network[J]. Quantum Information Processing, 2014, 13(11): 2567-2586.
[10] Farhi E, Neven H. Classification with quantum neural networks on near term processors[J]. arXiv preprint arXiv:1802.06002, 2018.
[11] Cong I, Choi S, Lukin M D. Quantum convolutional neural networks[J]. Nature Physics, 2019, 15(12): 1273-1278.
[12] Henderson M, Shakya S, Pradhan S, Cook T. Quanvolutional neural networks: powering image recognition with quantum circuits[J]. Quantum Machine Intelligence, 2020, 2(1): 1-9.
[13] Niu X F, Ma W P. A novel quantum neural network based on multi-level activation function[J]. Laser Physics Letters, 2021, 18(2): 025201.
[14] Houssein E H, Abohashima Z, Elhoseny M, Mohamed W M. Hybrid quantum-classical convolutional neural network model for COVID-19 prediction using chest X-ray images[J]. Journal of Computational Design and Engineering, 2022, 9(2): 343-363.
[15] Lau H K, Pooser R, Siopsis G, Weedbrook C. Quantum machine learning over infinite dimensions[J]. Physical review letters, 2017, 118(8): 080501.
[16] Schuld M, Killoran N. Quantum machine learning in feature Hilbert spaces[J]. Physical review letters, 2019, 122(4): 040504.
[17] Murad Abdo Rassam and Mohd. Aizaini Maarof, "Artificial Immune Network Clustering approach for Anomaly Intrusion Detection," Journal of Advances in Information Technology, Vol. 3, No. 3, pp. 147-154, August, 2012.doi:10.4304/jait.3.3.147-154
[18] Siphesihle P. Sithungu and Elizabeth M. Ehlers, "GAAINet: A Generative Adversarial Artificial Immune Network Model for Intrusion Detection in Industrial IoT Systems," Journal of Advances in Information Technology, Vol. 13, No. 5, pp. 456-461, October 2022.