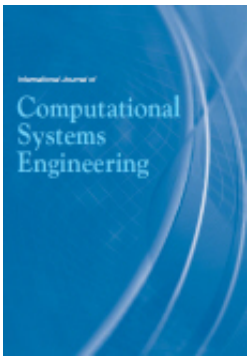


International Journal of Computational Systems Engineering

ISSN online: 2046-3405 - ISSN print: 2046-3391
https://www.inderscience.com/ijcsyse

Research on network intrusion detection model that integrates WGAN-GP algorithm and stacking learning module

Xiaoli Zhou

DOI: 10.1504/IJCSYSE.2025.10059074

Article History:

Received:	09 June 2023
Last revised:	06 July 2023
Accepted:	22 July 2023
Published online:	02 September 2024

Research on network intrusion detection model that integrates WGAN-GP algorithm and stacking learning module

Xiaoli Zhou

School of Information Engineering,
Sichuan Top IT Vocational Institute,
Chengdu, 610000, China
Email: Xiaoli_Zhou2023@outlook.com

Abstract: With the development of network technology, current network intrusion detection models have effectively detected some network intrusion methods. In order to improve the detection performance of network intrusion detection models, a new network intrusion detection model combining data augmentation technology is proposed. The model incorporates the WGAN-GP data augmentation module for data balance enhancement and a stacking learning module for model classification accuracy. In the performance comparison analysis of the WGAN-GP algorithm, it was found that the accuracy and F1 value of the WGAN-GP algorithm were 98.25% and 0.792, respectively, which were superior to the comparison algorithm. The above results indicate that the detection performance of the WGAN-GP algorithm is superior to that of the comparison algorithm. Therefore, integrating the WGAN-GP algorithm into network intrusion detection models can effectively improve its intrusion detection performance and promote the development of the field of network intrusion detection.

Keywords: stacking algorithm; WGAN-GP algorithm; network ID model; WGAN algorithm; SMOTE algorithm; ADASYN algorithm.

Reference to this paper should be made as follows: Zhou, X. (2024) 'Research on network intrusion detection model that integrates WGAN-GP algorithm and stacking learning module', *Int. J. Computational Systems Engineering*, Vol. 8, No. 6, pp.1–10.

Biographical notes: Xiaoli Zhou graduated from Chengdu College of Sichuan Normal University with a Bachelor's degree in 2011. She is currently a Lecturer and Information System Project Manager at Sichuan Top IT Vocational Institute. She is interested in computer networks and software technology.

This paper was originally accepted for a special issue on 'AI and Cognitive Computing for Next Generation Mobile Networks' guest edited by Dr. Arvind Dhaka, Dr. Amita Nandal, Dr Edmar Candeia Gurjão and Dr. Dijana Capeska Bogatinoska.

1 Introduction

Network security is one of the important issues to be solved urgently. With the rapid development of the internet, the threat of network intrusion is increasing, which brings great risks to the information systems of individuals, enterprises and countries (Mao et al., 2021). Therefore, the development of efficient and accurate network intrusion detection (ID) model becomes the key to protect network security. In recent years, the rapid development of deep learning technology has provided new solutions for network ID (Chen and Miao. 2021). Generative adversarial network (GAN), as a powerful generative model, has been widely used in various fields. However, the traditional GAN model has some challenges in network ID, such as unstable model training and pattern collapse (Qi et al., 2022). To solve these problems, the Wasserstein GAN with gradient penalty (WGAN-GP) algorithm is proposed. By introducing a gradient penalty term to replace the discriminator loss function in traditional GAN, WGAN-GP algorithm effectively improves the stability and convergence rate of the model (Feng and Dou, 2021). However, it is still difficult to obtain satisfactory results using WGAN-GP algorithm alone. The learning module of stacking is an ensemble learning method that improves the generalisation ability of the model by training a meta-classifier with the predictions of multiple basic classifiers as inputs. In network ID, the learning module can combine the predictions of multiple WGAN-GP models to more accurately determine whether network traffic has intrusion behaviours (Tsakiridis et al., 2019). Therefore, this study further combines the WGAN-GP algorithm with the stacking learning module to further improve the performance of network ID. The network ID model that integrates WGAN-GP algorithm and stacking learning module proposed in this paper makes an important contribution to solving the network ID problem. By

improving the stability and generalisation ability of the model, the model can more accurately judge whether the network traffic has intrusion behaviour, so as to improve the network security and accuracy. This paper is divided into four parts. Section 2 is to analyse the research status of data enhancement technology and network security model. Section 3 is to construct the network ID model that integrates WGAN-GP algorithm and stacking learning module. Section 4 is to compare and analyse the performance of the algorithm and the network ID model. Section 5 is the conclusions.

2 Related work

Nowadays, data enhancement technology is used more and more widely. Aiming at the problem that the arc fault diagnosis model is difficult to train, Zhang's team proposed an adaptive arc fault diagnosis model incorporating data processing technology. It turned out that the model was more robust than the traditional arc fault diagnosis model, and had a higher accuracy of arc fault diagnosis (Zhang et al., 2021a). Wang et al. proposed a power generation countermeasure network model combined with data processing technology to improve the prediction accuracy of NOx emissions from coal-fired power plants. The analysis of the simulation example of the model showed that the proposed model was more accurate than similar models (Wang et al., 2021). Gao's team also proposed a soft sensor data supplement model with the generation of a countermeasure network, which was conducive to the use of effective data supplement methods. The empirical analysis of this method showed that the prediction accuracy of this method was better (Gao et al., 2022). To make better use of the deep learning algorithm of big data to realise new AI, Zhao et al. (2021) proposed a data enhancement method with Wasserstein to generate a confrontation network and specific deep learning model and used this method to provide more accurate data to realise AI. The empirical analysis of this method showed that this method provided an idea of data enhancement for future research (Zhao et al., 2021).

Nowadays, more and more attention is paid to network information security, and various methods are applied to network ID models to protect network information security. Dong's team proposed an ID model with correlation analysis. The empirical analysis of this model showed that the accuracy rate of this model was 82.15%, which was superior to other models (Dong et al., 2020). To improve the efficiency of wireless sensors, Han et al. (2019) integrated game theory into the ID model. The simulation experiment showed that the test model can effectively predict attacks and reduce energy consumption (Han et al., 2019). Balamurugan's team put forward an ID model with the DNN to solve the problem of cloud computing being vulnerable to attacks. The performance evaluation of the model showed that the performance of the model can improve the security of cloud computing in all aspects (Balamurugan et al., 2022). Rahman et al. (2020) proposed a detection model incorporating joint learning to settle a dispute about insufficient security of the internet of things. The empirical analysis of the model showed that the accuracy of the model was close to that of the centralised method, which can effectively improve security performance (Rahman et al., 2020). To design an optimal intrusion model for monitoring malicious activities on the network, Gayathri's team used the naive Bayesian model and the Gaussian model to detect the anomalies of the ID system. The simulation experiment showed that the model had higher accuracy, F1 score, and accuracy value (Gayathri and Pramila, 2022).

The aforementioned research findings demonstrate the widespread use of data enhancement technology in numerous fields. Additionally, the results highlight the various methods utilised in network ID models. However, there is a scarcity of studies that combine data enhancement technology and ID. Therefore, the research applies data enhancement technology to the network ID model and optimises the network ID model using WGAN-GP and stacking algorithm, hoping to improve the accuracy of the network ID model in this way.

3 Construction of a network ID model combining data enhancement technology

3.1 Construction of an improved network ID model based on stacking algorithm

With the increase of our country's emphasis on information security, network ID technology has also developed and grown (Siddiqui and Boukerche, 2021). ID technology refers to an active defence method that collects and analyses key information such as hosts, security logs, and sent messages. Defence means to ensure the security of network information (Zhang et al., 2021b). The ID model is a network security model that uses ID technology to identify the source and intent of intrusion attacks and adopts effective strategies to ensure information security. This model can respond to malicious intrusions in a timely manner, prevent intrusions and avoid the influence of the invasion is further expanded (Alqahtani, 2022). Figure 1 is the schematic diagram.

The event generator module installs monitoring programs in multiple locations in the network, actively obtains events from various network segments, and passes the events to the detection model in the event analyser module through sensors. The main function of the event analyser module is to analyse and judge the information provided by the event generator and judge whether there is an intrusion situation at present. If there is, the response unit will be activated. If not, the result will be transmitted to the behaviour database in the event database module. The function of the response unit is to respond to different intrusion situations to a corresponding degree. The response methods are mainly divided into three types: alarm response, network interruption, and administrator warning. Among them, network interruption is a strong response

method, while alarm response and administrator warning are weak response methods. The event database module in the ID model is the basis of the whole model, which is mainly divided into the behaviour database and intrusion database. The data in the behaviour database is transmitted from the normal records in the event analyser, and the data in the intrusion database is transmitted from the abnormal records in the event analyser. At present, the traditional ID model has a poor detection effect on intrusion behaviour. To improve the detection effect of the ID model on network intrusion behaviour, the study adopts an ID model that combines improved WGAN-GP and stacking algorithms.

From Figure 2, the network ID model with WGAN-Stacking is divided into three different stages. Firstly, to balance the original unbalanced intrusion dataset, the majority and minority data are separated. Next, the symbolic features of both types of data are encoded, followed by ensuring a correlation between each numerical feature through normalisation. The second stage is to use the WGAN-GP data enhancement module to perform data enhancement on the pre-processed minority class data, generate data enhancement samples that are closest to the real samples, and mix the enhanced minority class data and majority class data to get a more balanced training data set. The final step of the model involves inputting the enhanced training dataset into the ID module using the stacking algorithm. All learners at different levels are trained and their hyperparameters are tuned to classify the intrusion data. The results are then evaluated to determine the classification effectiveness. The stacking algorithm is a common learning method, whose main principle is to classify different samples by training multi-level learners, so it is essentially a multi-level machine learning model (Cheng et al., 2021). In this study, the stacking algorithm is used to classify the enhanced data set to increase the accuracy of intrusion data detection. The common stacking algorithm is the two-layer stacking algorithm. Figure 3 is the flow chart.

In Figure 3, the stacking algorithm first uses the initial data set to train different base classifiers to obtain different secondary training sets. In the training process, if the training set obtained by the base classifier is directly used as the secondary training set, the risk of overfitting the obtained data is high. To avoid this problem, the study adopts the method of k-fold cross-validation to train the base classifier and generate a secondary training set. In the Stacking algorithm, the key to its learning performance is the selection of the base learner and the meta-learner. Through comparison, the research selects a model with a large difference as the base learner and selects the logistic regression model as the meta-learner to reduce the training cost and the risk of overfitting in the process. The study puts the enhanced data set through the WGAN-GP model into the Stacking algorithm for learning and classification, thereby improving the detection accuracy of the network ID model.

3.2 Construction of WGAN-GP model in ID model GAN model and its optimisation model

GAN model is a deep learning model that is mainly used for unsupervised learning on complex distributions (Liu et al., 2021). The model mainly consists of a generative model (GM) and a discriminative model (DM). The GAN model alternately learns real samples through the GM and the DM to generate new samples. The specific process is shown in Figure 4.

In Figure 4, the generated data is acquired by inputting random variables into the GM. Subsequently, both the real and generated data are input into the DM. The DM discriminates between the input data and compares the generated data by providing feedback to the DM. This process is repeated until the optimal discriminant model is achieved. In this process, the GAN model has a loss value, and the expression of its loss function is shown in formula (1).

$$V(D,G) = E_{x\sim Pdata(X)}[\log D(x)] + E_{\beta\sim p\beta(Z)}[\log(1-D(G(\beta))] \tag{1}$$

In formula (1), x is the real sample, β is the random Gaussian noise, $G(\beta)$ is the generated sample of input β of the GM, $D(x)$ is the probability that the DM judges x as the real sample, and $D(G(\beta))$ is the probability that the DM judges $G(\beta)$ as the real sample. In the GAN model, the goal of the discriminant model is to accurately judge the real sample and the generated sample, and the goal of the generated model is to make the generated sample fit the real sample to a large extent. So after unifying the optimisation goals of the two models, the min-max problem is shown in formula (2).

$$\min_G \max_D V(D,G) = E_{x\sim Pdata(X)}[\log D(x)] + E_{\beta\sim p_{\beta(Z)}}[\log(1-D(G(\beta))] \tag{2}$$

The optimal DM D can be obtained through formula (2), and then the GM is trained through the DM to obtain the optimal generative model G. Through continuous optimisation iterations throughout the process, the final G samples generated by the GM are close to the data distribution of real samples, so the G data generated by the GM can be used to enhance the data of minority categories. Because the ID data set has the characteristics of mixing continuous and discrete features, the GAN model is difficult to apply in the field of network ID data (Xie et al., 2021). In addition, the GAN model still has problems such as gradient disappearance and gradient explosion in the actual application process. To solve the above problems of the GAN model, the gradient penalty item is introduced into the generative confrontation network model, and the Wasserstein distance is used instead of the JS divergence pair. The distance of the data distribution is measured. The WGAN-GP model used in the study is shown in Figure 5.

Figure 1 Working principle of ID model (see online version for colours)

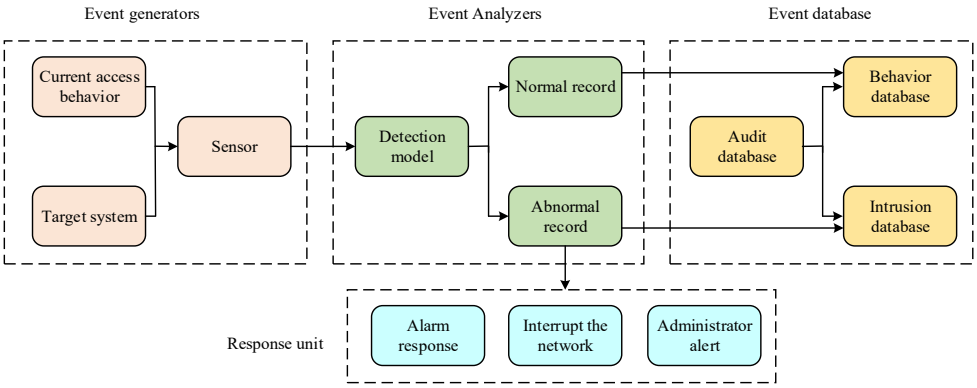


Figure 2 Network ID model with WGAN-stacking (see online version for colours)

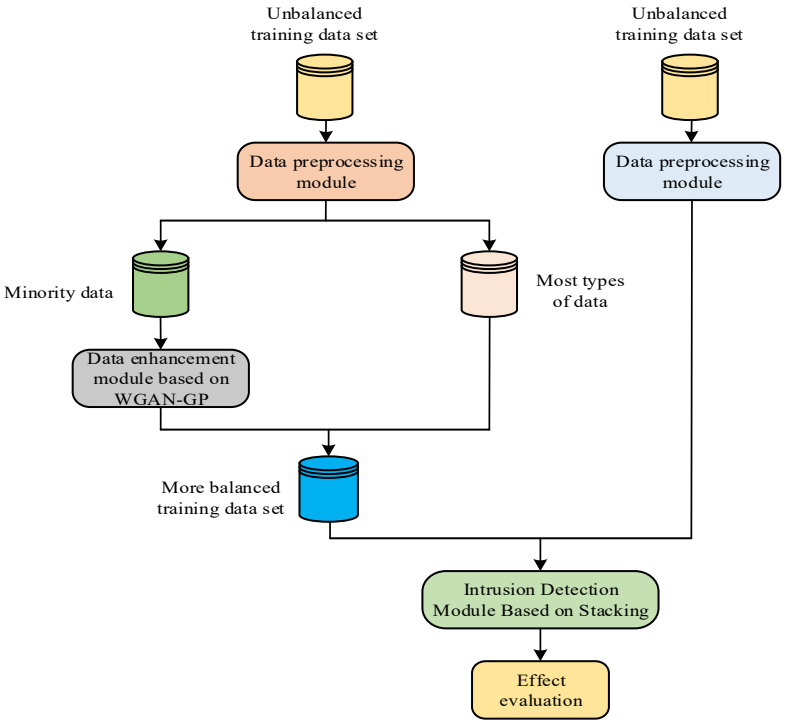


Figure 3 Stacking algorithm flow (see online version for colours)

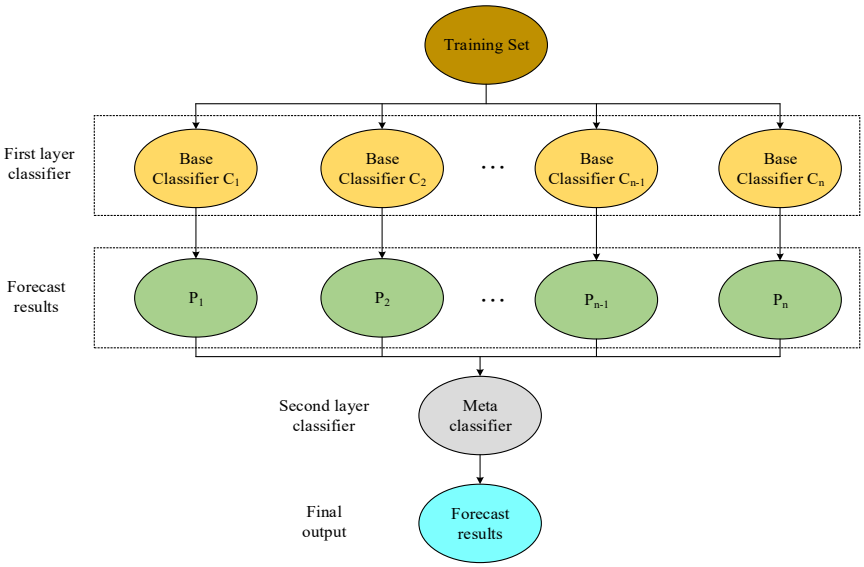


Figure 4 GAN network framework (see online version for colours)

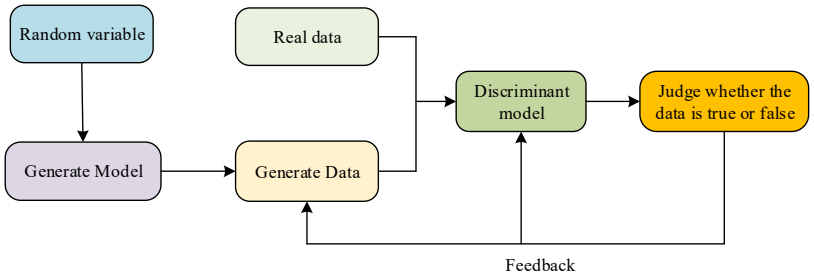


Figure 5 WGAN-GP model structure (see online version for colours)

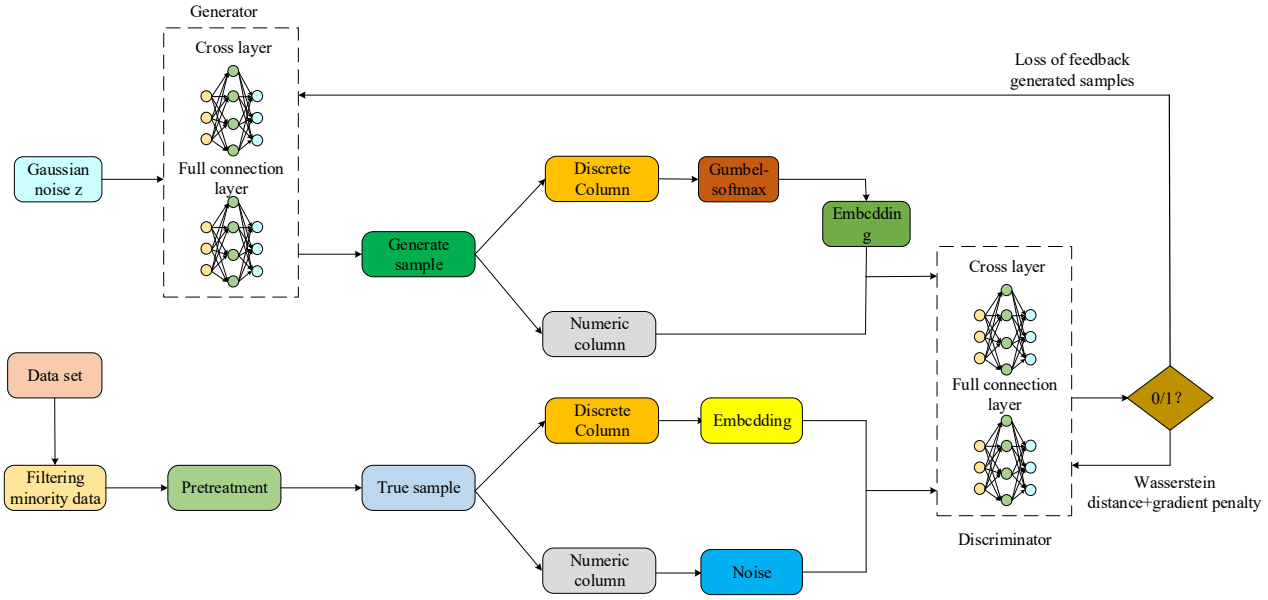
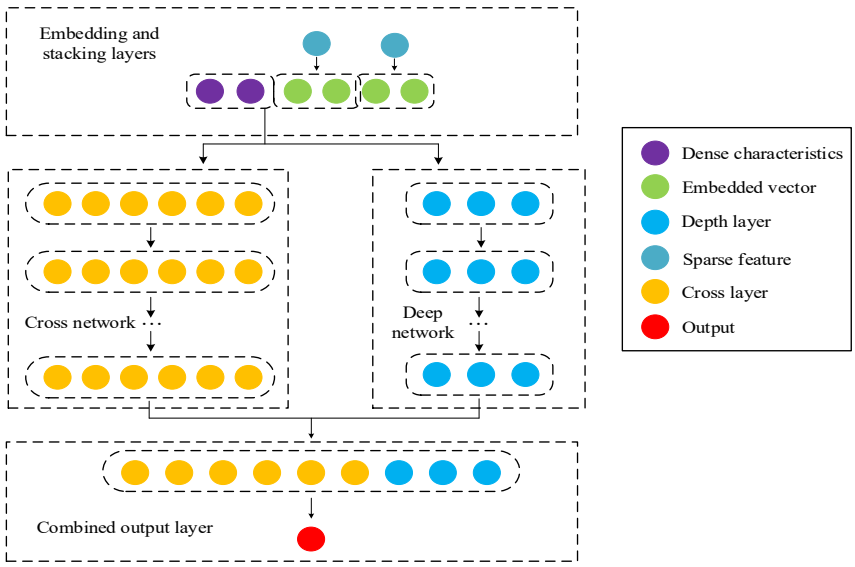


Figure 6 DCN model structure (see online version for colours)



In Figure 5, the biggest improvement of the model is the introduction of Wasserstein distance and gradient penalty term. Among them, the GM and the DM borrow the deep cross network (DCN) model that can automatically learn feature interaction for sparse and dense inputs. The model starts with embedding and stacking layers, and then connects the parallel cross network and deep network, and finally combines output through the combined output layer. Figure 6 shows its structure.

As shown in Figure 6, the DCN model is mainly composed of four parts: embedding and stacking layer, cross network, deep network and combined output layer.

The operation process of the model is shown as follows. The DCN model first converts the discrete features of the input into low-dimensional dense vector representation through the embedding layer in the embedding layer to capture the correlation between the features. Then, these embedding vectors are stacked by stacking layers to form a high-dimensional feature vector. Secondly, multi-layer cross-operation is carried out in the cross-network part to learn the higher-order interaction between features, and then generate new feature vectors. Then, in the deep network part, linear transformations and activation function operations are performed on the input feature vectors to learn more complex feature representations. Finally, the output of cross network and deep network is combined in the combined output layer to get the final prediction result. In the embedding and stacking layer, the one-hot encoding method is usually used for feature classification. This method will lead to high-dimensional sparse features. To solve the problem, the embedding process is added in this process, and the encoding of sparse features is converted into an embedding vector. The expression of this process is shown in formula (3).

$$x_{embed,i} = W_{embed,i} \tag{3}$$

Embedding vector $W_{embed,i}$ in formula (3) represents the corresponding embedding matrix $x_{embed,i}$. After optimisation, the embedding vector and the dense vector x_{dense} will be superimposed to form a new vector. The expression of the new vector is shown in formula (4).

$$x_0 = \left[x_{embed,1}^T, x_{embed,2}^T, \cdots, x_{embed,k}^T, x_{dense}^T \right] \tag{4}$$

In the cross-network layer of the DCN model, the cross network performs feature crossing in a specific way, and the output value expression of each cross layer is shown in formula (5).

$$x_{l+1} = x_0 x_l^T w_l + b_l + x_l = f\left(x_l, w_l, b_l\right) \tag{5}$$

In formula (5), x_l and x_{l+1} are column vector, x_l is the cross layer output of layer l, x_{l+1} is the cross layer output of layer $l + 1$, w_l is the weight of layer l, and b_l is the offset value of layer l. In the cross-network layer, the characteristic high-order cross can be obtained through the unique structure of the cross network. The deep network layer of the DCN model is mainly to make up for the insufficient number of cross network parameters and to better replenish high-order nonlinear cross features through the deep network layer. The output expression of each deep network layer is shown in formula (6).

$$h_{l+1} = f\left(w_l h_l + b_l\right) \tag{6}$$

In formula (6), h_l is the hidden layer of the l^{th} layer, h_{l+1} is the hidden layer of the $l + 1^{\text{th}}$ layer, w_l and b_l is the weight and bias value of the l^{th} deep network layer. The final output result is obtained by combining the output of the cross-network layer and the deep network layer, and then outputting to the combined output layer. Both the GM and the DM use the DCN model to improve the performance of the model. In the traditional GAN model, the DM is optimised according to the loss function shown in formula (2), and the expression shown in formula (7) is obtained.

$$V(D, G) = \int \left[p_r(x) \log(D(x) + p_g(x) \log(1 - D(x)\right] dx \tag{7}$$

The expression of the optimal discriminator can be obtained from formula (7) as shown in formula (8).

$$D^*(x) = \frac{P_r}{P_r(x) + P_g(x)} \tag{8}$$

Substituting the optimal discriminator into formula (7) simplifies to get formula (9).

$$\max_D V(D, G) = 2JS\left(p_r(x) \| p_g(x)\right) - 2\log 2 \tag{9}$$

From formula (9), it can be obtained that if the generator is to be optimal, the JS divergence needs to be the smallest, but in the traditional GAN model, the JS divergence is fixed at log2. To obtain a better GM, the study uses the Wasserstein distance instead of the JS divergence to obtain the WGAN model. The expression of Wasserstein distance is shown in formula (10).

$$W\left(p_r, p_g\right) = \inf_{\tau - \Pi\left(p_r, p_g\right)} E_{(x,y)}\left[\|x - y\|\right] \tag{10}$$

In formula (10), $\Pi(p_r, p_g)$ represents the set of joint distribution of p_r and p_g. τ represents any joint distribution. x is the real sample and y represents the generated sample. Therefore, the loss function expression of the WGAN model can be obtained as shown in formula (11).

$$\min_G \max_D V(G, D) = E_{x \sim pr}[D(x)] + E_{x \sim p_g}[D(x)] \tag{11}$$

In the actual training process, the WGAN model is still prone to gradient disappearance or explosion. To solve the problem, the WGAN-GP model is obtained by introducing a gradient penalty term into the WGAN model. The study discriminates the relationship between the discriminator gradient and K by adding a loss function. The loss function of the WGAN-GP model is shown in formula (12).

$$\begin{aligned} L = {} & E_{x \sim p_g}[D(x)] - E_{x \sim pr}[D(x)] \\ & + \lambda E_{x \sim P_{penalty}}\left[\left(\|\nabla_x D(x)\| - 1\right)^2\right] \end{aligned} \tag{12}$$

In formula (12), $x \sim P_{penalty}$ represents the random interpolation of the sum line between p_g and p_r, $\nabla_x D(x)$ is the normal form of $D(x)$. $\lambda E_{x \sim P_{penalty}}\left[\left(\|\nabla_x D(x)\| - 1\right)^2\right]$ represents the gradient penalty term. Through the data enhancement of the WGAN-GP model, it can ensure that the generator can generate generated sample data that approximates the real sample distribution, thereby increasing the accuracy of network ID. To test the performance of the network ID model proposed in the research, the research selects accuracy rate, recall rate, precision rate and F1 value as indicators, and the accuracy rate expression is shown in formula (13).

$$Acc = \frac{TP + FN}{TP + FP + TN + FN} \tag{13}$$

The precision rate expression is shown in formula (14).

$$P = \frac{TP}{TP + FP} \tag{14}$$

Recall rate is shown in formula (15).

$$R = \frac{TP}{TP + FN} \tag{15}$$

F1 value expression is shown in formula (16).

$$F1 = \frac{2 * TP}{2 * TP + FP + FN} \tag{16}$$

4 Performance analysis and comparative experiment of WGAN-GP model

To verify the effectiveness of the network ID system with the WGAN-GP Stacking model, the NSL-KDD data set was selected as the data set of this experiment. The research analysed the effectiveness of samples generated by the WGAN-GP-Stacking model and the actual performance of the WGAN-GP algorithm in the model and the classic SMOTE algorithm, ADASYN algorithm, and WGAN algorithm in the oversampling technology.

To verify the effectiveness of the generated samples, the study compared the scatter plots of the mean and standard deviation of the features generated by the WGAN-GP-Stacking model and the real samples and calculated the Pearson correlation coefficient of the mean and standard deviation. A scatterplot of the mean and standard deviation of the generated and real samples is shown in Figure 7.

Figure 7 draws a scatter diagram of the mean and standard deviation of the WGAN-GP-Stacking model-generated samples and real samples. In Figure 7(a), the real samples and generated samples are very close to each other, and the Pearson correlation coefficient of the mean value is 0.9931, which shows that the mean value of the generated sample is highly similar to the real sample. In Figure 7(b), the scatter points of the real sample and the generated sample are also very close, and the mean value of the Pearson correlation coefficient is 0.9928, which shows that the standard deviation of the generated samples is also highly similar to the real samples. In summary, the generated samples of the WGAN-GP-Stacking model followed the data distribution of the original samples. During the performance comparison experiment of the WGAN-GP model, the test set in the NSL-KDD dataset was used for testing, and the three indicators of accuracy, precision-recall, and F1 value were selected as evaluation indicators. The study repeated 12 comparison experiments and recorded all data in the 12 comparison experiments. Two representative comparative experiments were selected to analyse the precision-recall (PR) curves of the four algorithms. The PR curve represents the relationship between accuracy and recall. Generally, recall is set to the horizontal axis and precision is set to the vertical axis. The PR curves of the two representative comparative experiments are shown in Figure 8.

Figure 7 Scatter of mean and standard deviation of generated samples and real samples, (a) mean scatter chart, (b) scatter plot of standard deviation (see online version for colours)

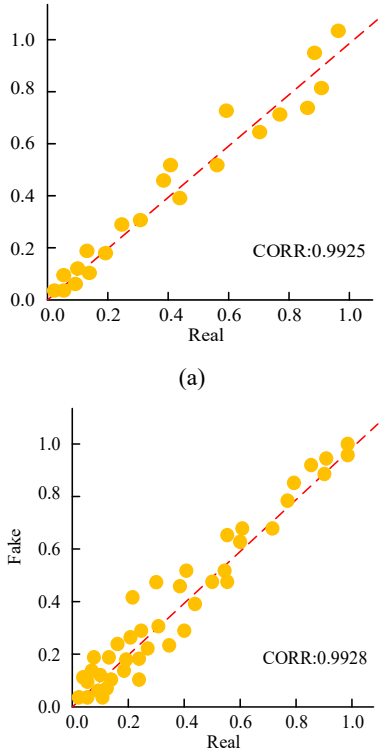


Figure 8(a) shows the PR curves of the four algorithms in one of the representative comparative experiments. The area under the curve of the WGAN-GP algorithm is larger than that of the WGAN algorithm, and the area under the curve of the WGAN algorithm Greater than the SMOTE algorithm. The ADASYN algorithm has the smallest area under the curve. Figure 8(b) shows the PR curves of the four algorithms in another representative comparison experiment. The area under the curve of WGAN-GP algorithm is still larger than that of WGAN algorithm, and the area under the curve of WGAN algorithm is larger than that of SMOTE algorithm, while the area under the curve of ADASYN algorithm is the smallest. To sum up, from the PR curves, WGAN-GP algorithm has the best performance. In addition, the accuracy curves of the four algorithms in 12 comparative experiments are shown in Figure 9. The accuracy curve in Figure 9 is intended to show the variation of the accuracy rate between different experimental times. The smaller the fluctuation ranges of the curve and the higher the overall position, the better the accuracy performance of the algorithm.

Figure 8 Accuracy recall curve of four algorithms, (a) the first comparative experiment, (b) the second contrast experiment (see online version for colours)

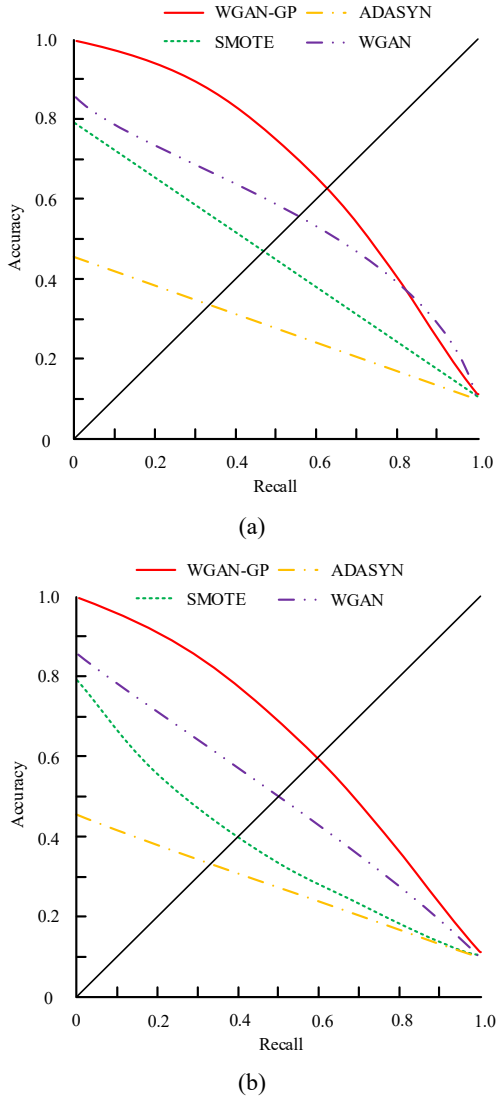


Figure 9(a) shows the accuracy comparison curves of the four algorithms in the first six comparison experiments. From it, in the first six comparison experiments, WGAN-GP algorithm has the highest accuracy. And its average accuracy rate is 98.25%. The accuracy rate is second only to the WGAN-GP algorithm. The WGAN algorithm has an average accuracy rate of 95.38%. Among the four algorithms, the algorithm with the lowest accuracy rate is the ADASYN algorithm. 89.13%. Figure 9(b) shows the accuracy comparison curves of the four algorithms in the last six comparison experiments. From it, in the last six comparison experiments, WGAN-GP algorithm has the highest accuracy. The average accuracy of WGAN-GP algorithm, WGAN algorithm, SMOTE algorithm, and ADASYN algorithm is 98.59%, 95.89%, 91.24%, and 87.56% respectively. From the above results, it can be concluded that from the perspective of model accuracy, the performance of the WGAN-GP algorithm is better than the other three algorithms. Figure 10 is a scatter comparison diagram of the F1 values of the four algorithms in 12 comparison experiments.

Figure 9 Accuracy curve off our algorithms, (a) accuracy of four algorithms in the first six comparative experiments, (b) accuracy of four algorithms in the last six comparative experiments (see online version for colours)

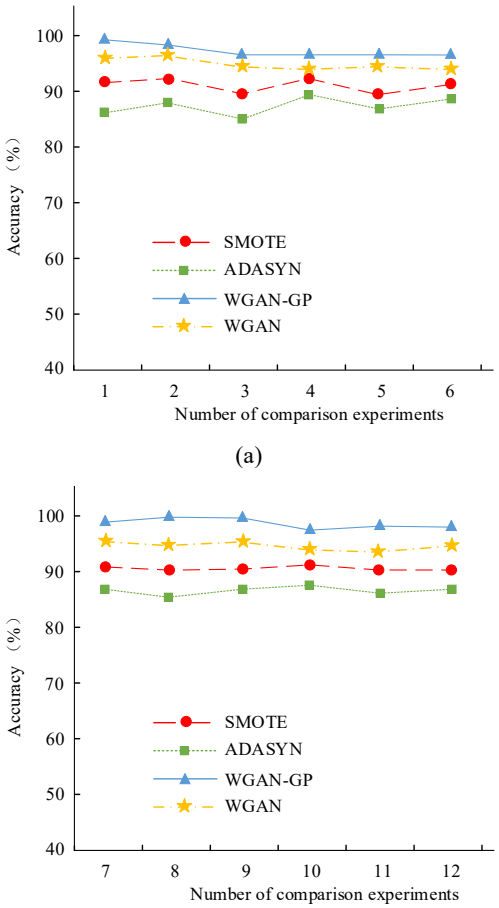


Figure 10 F1 value scatter diagram of four algorithms in comparison experiment (see online version for colours)

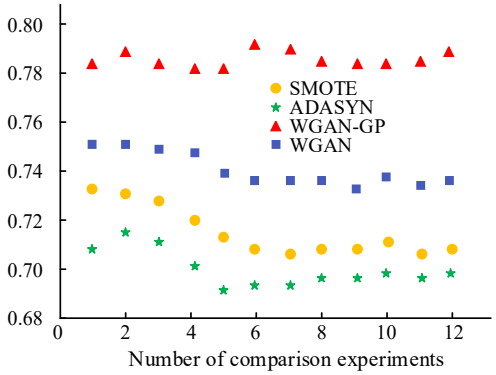


Figure 10 is a scatter diagram of F1 values of WGAN-GP algorithm, SMOTE algorithm, ADASYN algorithm, and WGAN algorithm in 12 comparison experiments. From Figure 10, the F1 of the WGAN-GP algorithm is higher than that of the other three algorithms, and in 12 comparison

experiments, the maximum F1 of the WGAN-GP algorithm is 0.798, and the minimum F1 value is 0.0783, the average F1 is 0.792; among the four algorithms, the F1 value of the SMOTE algorithm is only higher than that of the ADASYN algorithm. Its average F1 value is 0.724, while the ADASYN algorithm has the lowest F1 with an average of 0.698. From the F1 value dimension, the WGAN-GP algorithm is the best. According to the comparison results of the above dimensions, the WGAN-GP algorithm has better performance than the SMOTE algorithm, ADASYN algorithm, and WGAN-GP algorithm, and it has a better data enhancement effect on ID data.

5 Conclusions

Traditional network protection methods cannot effectively protect network security. To solve the problem of insufficient network protection means, a new network ID model combining the WGAN-GP algorithm and stacking algorithm is proposed. In this model, these two data augmentation techniques can improve the accuracy of generated data and the accuracy of classification to improve the accuracy of ID. Performance comparison experiments were carried out with SMOTE algorithm, ADASYN algorithm, and WGAN algorithm. The research compared the performance of the WGAN-GP algorithm with the SMOTE algorithm, ADASYN algorithm, and WGAN algorithm. The average accuracy rate of the WGAN-GP algorithm was 89.25%, higher than 81.24% of the SMOTE algorithm, 79.13% of the ADASYN algorithm and WGAN algorithm. The average F1 value of WGAN-GP algorithm was 0.692, higher than 0.624 of the SMOTE algorithms, 0.624 of the ADASYN algorithms, and 0.643 of the WGAN algorithm. In addition, in the validity experiment of the generated samples of the WGAN-Stacking model, it was found that the samples generated by the model were highly similar to the real samples. The above results showed that the new network ID model integrated with data enhancement technology had a high ID accuracy. Although the model has good ID performance, deficiencies still need to be improved. During this experiment, the WGAN-GP algorithm can enhance the data of minority samples.

References

Alqahtani, A.S. (2022) 'FSO-LSTM IDS: hybrid optimized and ensembled deep-learning network-based ID system for smart networks', *The Journal of Supercomputing*, Vol. 78, No. 7, pp.9438–9455.

Balamurugan, E., Mehbodniya, A., Kariri, E., Yadav, K., Kumar, A. and Haq, M.A. (2022) 'Network optimization using defender system in cloud computing security-based ID system with game theory deep neural network (IDSGT-DNN)', *Pattern Recognition Letters*, April, Vol. 156, No. 9, pp.142–151.

Chen, J. and Miao, Y. (2021) 'Research on security evaluation system of network information system with rough set theory', *International Journal of Internet Protocol Technology*, Vol. 14, No. 3, pp.155–161.

Cheng, F., Xia, J., Zhang, K., Zhou, C. and Ajo, J. (2021) 'Phase-weighted slant-stacking for surface wave dispersion measurement', *Geophysical Journal International*, Vol. 226, No. 1, pp.256–269.

Dong, R.H., Li, X.Y., Zhang, Q.Y. and Yuan, H. (2020) 'Network ID model with multivariate correlation analysis – long short-time memory network', *IET Information Security*, Vol. 14, No. 2, pp.166–174.

Feng, T. and Dou, M. (2021) 'A weighted ID model of dynamic selection', *Applied Intelligence*, Vol. 51, No. 7, pp.4860–4873.

Gao, S., Qiu, S., Ma, Z., Tian, R. and Liu, Y. (2022) 'SVAE-WGAN-based soft sensor data supplement method for process industry', *IEEE Sensors Journal*, Vol. 22, No. 1, pp.601–610.

Gayathri, M. and Pramila, P.V. (2022) 'Analysis of accuracy in anomaly detection of ID system using naive Bayes algorithm compared over Gaussian model', *ECS transactions*, Vol. 107, No. 1, pp.13977–13991.

Han, L., Zhou, M., Jia, W., Dalil, Z. and Xu, X. (2019) 'ID model of wireless sensor networks with game theory and an autoregressive model', *Information Sciences*, Vol. 476, No. 8, pp.491–504, ScienceDirect.

Liu, Y., Fan, H., Ni, F. and Xiang, J. (2021) 'ClsGAN: selective attribute editing model with classification adversarial network', *Neural Networks*, Vol. 133, No. 11, pp.220–228.

Mao, J., Liu, J., Zhang, J., Han, Z. and Shi, S. (2021) 'A method for detecting image information leakage risk from electromagnetic emission of computer monitors', *Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology*, Vol. 40, No. 2, pp.2981–2991.

Qi, J., Chen, H. and Chen, F. (2022) 'Extraction of landslide features in UAV remote sensing images with machine vision and image enhancement technology', *Neural Computing & Applications*, Vol. 34, No. 15, pp.12283–12297.

Rahman, S.A., Tout, H., Talhi, C. and Mourad, A. (2020) 'Internet of things ID: centralized, on-device, or federated learning?', *IEEE Network*, Vol. 34, No. 6, pp.310–317.

Siddiqui, A.J. and Boukerche, A. (2021) 'Adaptive ensembles of autoencoders for unsupervised IoT network ID', *Computing*, Vol. 103, No. 6, pp.1209–1232.

Tsakiridis, N.L., Tziolas, N.V., Theocharis, J.B. and Zalidis, G.C. (2019) 'A genetic algorithm-based stacking algorithm for predicting soil organic matter from vis – NIR spectral data', *European Journal of Soil Science*, Vol. 70, No. 3, pp.578–590.

Wang, P., Si, F., Fan, W., Shao, Z. and Ren, S. (2021) 'Data enhancement for data-driven modeling in power plants with a conditional variational-adversarial generative network', *Industrial & Engineering Chemistry Research*, Vol. 60, No. 24, pp.8829–8843.

Xie, G., Yang, L.T., Yang, Y., Luo, Y., Li, R. and Alazab, M. (2021) 'Threat analysis for automotive CAN networks: a GAN model-based ID technique', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 7, pp.4467–4477.

Zhang, T., Zhang, R., Wang, H., Tu, R. and Yang, K. (2021a) 'Series AC arc fault diagnosis with data enhancement and adaptive asymmetric convolutional neural network', *IEEE Sensors Journal*, Vol. 21, No. 18, pp.20665–20673.

Zhang, Z., Cao, Y., Cui, Z., Zhang, W. and Chen, J.A. (2021b) 'Many-objective optimization based intelligent ID algorithm for enhancing security of vehicular networks in 6G', *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 6, pp.5234–5243.

Zhao, Y., Tian, S., Yu, L. and Xing, Y. (2021) 'Combining the WGAN and ResNeXt Networks to achieve data augmentation and classification of the FT-IR spectra of strawberries', *Spectroscopy*, Vol. 36, No. 4, p.28, pp.30–32, pp.34–40.