Anomaly Detection in Network Access-Using LSTM and Encoder-Enhanced Generative Adversarial Networks

Jian Hu[1*], Yingjun He[1], Wenqian Xu[2,3], Yixin Jiang[2,3], Zhihong Liang[2,3], Yiwei Yang[2,3]
[1]Yunnan Power Grid Information Center, China Southern Power Grid, Kunming 650217, China
[2]Electric Power Research Institute, China Southern Power Grid, Guangzhou 510663, China
[3]Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou 510663, China
[*]E-mail: hjian127@163.com
[*]Corresponding Author

Keywords: generative adversarial networks, anomalous access, detection algorithms, models

Received: September 29, 2024

Along with the continuous development of information technology, the database has become an important module for enterprises and individuals to apply computers, and some important data are stored in the database, which also leads to the database becoming the target of malicious intruders. The abnormal access behavior detection algorithm for data can quickly identify abnormal access situations, timely intervention and processing to ensure data security. Based on this, this paper proposes an abnormal defense behavior detection algorithm based on generative adversarial network, the new algorithm has the applicability as well as two derivative models of generative adversarial network for network abnormal access detection with high efficiency. In this paper, we experiment the classification accuracy of network anomaly detection algorithm, i.e., F1, by using three models, namely, the original Generative Adversarial Network (GAN), Generative Adversarial Network using Long and Short-Term Memory Network (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder (GAN+Encoder), and the result of this paper shows that the GAN+Encoder model is the most effective. And based on these three models of the generator and discriminator loss trends are compared, as well as through the iteration of 50 times of training results show that the GAN + Encoder model is relatively simple, and the training time is shorter and more efficient.

Povzetek: Razvita je metoda GAN+Encoder za zaznavanje anomalij v omrežnem dostopu, ki omogoča krajši čas učenja in boljšo prilagodljivost pri prepoznavanju nenavadnega dostopa.

1 Introduction

In today's digital age, network security has become a crucial issue. With the continuous development and popularization of the internet, abnormal access behavior is also increasing, bringing huge risks to individuals, businesses, and society. Traditional methods for detecting abnormal access behavior often suffer from issues such as low accuracy and poor adaptability when facing complex and ever-changing network environments. Generative Adversarial Networks (GANs), as an emerging deep learning technology, have shown great potential in the field of anomaly access behavior detection. Generative Adversarial Networks (GANs) are a type of deep learning model consisting of a generator and a discriminator. Its basic principle originates from the zero-sum game of game theory, which learns the distribution of data through the adversarial process between the generator and discriminator. Since Ian Goodfellow et al. proposed GAN in 2014, it has developed into one of the most cutting-edge technological fields in the field of deep learning [1]. With the continuous deepening of research in the field of generative adversarial networks, problems such as models being too free and uncontrollable, models not converging, and models collapsing in the original generative adversarial networks (GANs) have gradually been exposed. Researchers have continuously proposed new generative adversarial network derived models to address these issues. So far, there have been hundreds of derivative models of generative adversarial networks, and various new derivative models are still being proposed [2]. Generative adversarial networks have achieved great success in multiple fields. For example, in the field of image generation, GAN can generate realistic facial photos, animal photos, comic characters, etc; In the field of style transfer, GAN can transform one form of image into another, such as converting photos into oil paintings, three-dimensional into anime, etc. These successful applications provide rich ideas and methods for GAN in the field of anomaly detection.

Currently, some scholars have conducted research on database anomaly access detection based on log records generated by user access to databases. Due to the large number of system log files and the presence of redundant information, traditional feature engineering manually extracts features from relational entities, which is cumbersome and time-consuming, making it

very difficult to establish detection models and resulting in low efficiency in anomaly detection. Therefore, based on the network anomaly access detection algorithm of generative adversarial networks, this article proposes two derivative models of generative adversarial networks, namely the LSTM based generative adversarial model and the encoder based generative adversarial model. And through the comparative analysis of the three models, the advantages of the encoder-based generative adversarial model are highlighted, in order to be able to provide a more novel reference for the field of anomaly detection.

2 Generative adversarial network

In the process of training the generative adversarial network, the generator tries hard to "deceive" the discriminator so that it decides that the generated data is real data, and the discriminator also needs to try its best to make the correct judgment between the real sample and the generated sample, so the two form an adversarial relationship, and the ultimate goal of the GAN is to generate the generator to generate enough fake samples to match the real one. fake samples. The loss function of the original generative adversarial network is as follows:

$$\min_G \max_D V(D,G) = \mathrm{E}_{x\sim p_{data}(x)}[\log D(x)] + \mathrm{E}_{x\sim p_z(z)}[\log(1-D(G(z)))] \quad (1)$$

Where $p_z(z)$ denotes that the input z of the generator is sampled from a certain distribution, usually taking a -some simple distribution, such as Gaussian distribution, uniform distribution. $G(z;\theta_g)$ denotes a parameterized θ_g network G, whose purpose is to map a simple distribution to the data space. $D(x;\theta_d)$ denotes a parameterized θ_d network D, whose output ranges from 0 to 1 to indicate the probability of generating samples from the real probability from the data. The discriminator $D(x;0_d)$ is designed to distinguish whether its input sample x is from the generator or from the real data, defining the real data distribution as label y=1 and the data generated from the generator as label y=0 [3]. The probability that the output of the discriminator is 1 (real data) can then be defined as.

$$p(y=1|x) = D(x;\theta_d) \quad (2)$$

The probability that the output of the discriminator is 0 (generator generated data) can be defined as:

$$p(y=0|x) = 1 - D(x;\theta_d) \quad (3)$$

For the generator, its goal is to minimize the loss function of the above equation (1), that is to say, to generate samples as close as possible to the real data, and then make the discriminator produce a misjudgement, so that its output tends to.

3 Detection of abnormal access behavior based on adversarial network

3.1 Network anomalous access detection model

Adversarial network-based anomalous access behavior detection is a method that uses the adversarial network technique in deep learning to detect anomalous access behavior. It detects abnormal access behavior by training an adversarial network to generate normal access behavior data and comparing it with real access behavior data. In contrast, adversarial network-based anomalous access behavior detection methods can take advantage of the powerful fitting ability of deep learning technology to achieve accurate detection of anomalous behavior [4].

The overall structure of the primitive GAN-based network anomalous access detection model is shown in Figure 1, a network anomaly detection model is mainly composed of two parts: model training as well as anomaly detection. The upper half of Figure 1 shows the training process of the generative adversarial network, the Generator uses Noise to generate "fake data", the discriminator is trained by the real sample data in the Training Data as well as the fake data generated by the Generator. The closer the result is to 1, the more the discriminator is true, otherwise it is false. The second half of Figure 1 is the anomaly detection stage, where the test data is input into the discriminator, and the trained discriminator will determine whether this data is anomalous or not.

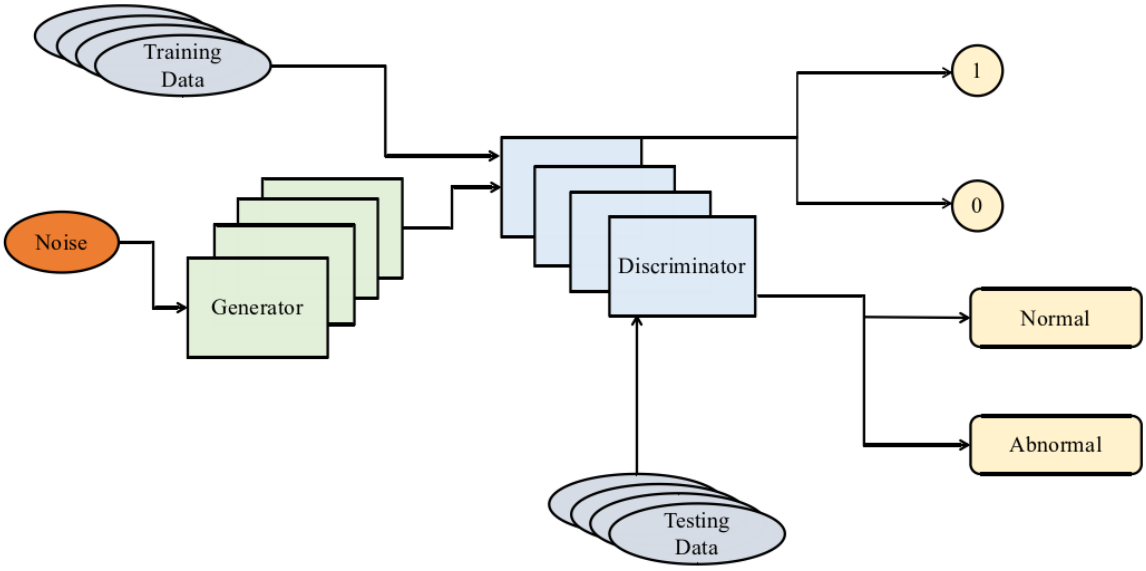


Figure 1: General framework of GAN-based network anomaly access detection

Although the original generative adversarial model can be used to complete the detection of abnormal network access data, however, due to the generative adversarial network itself has the problem that the discriminator is too strong and the generator is too weak which makes the model difficult to be trained, so the original generative adversarial model needs to be adapted and adjusted. In this paper, two GAN-based network anomalous access detection models are designed. The first method uses the advantage of LSTM in processing time series to design LSTM-based generative adversarial model, so as to achieve the optimization effect on the original model. The second method is to add an encoder (Encoder) in the generative adversarial model, and learn jointly with the generator in the generative adversarial network through the Encoder [5, 6].

3.1 Generative adversarial model based on LSTM

Figure 2 shows the model architecture of a generative adversarial model based on LSTM. The left half of the figure is a GAN framework, where the generator and discriminator are obtained through iterative adversarial training. On the right is the anomaly detection process, where the discriminator trained with GAN calculates the discrimination score, the generator calculates the reconstruction score, and then combines them.

Firstly, this article constructs the generator and discriminator of GAN as two Long Short-Term Memory (LSTM) neural networks, as shown in the left half of Figure 3-2. According to the original GAN framework, the generator takes a sequence from a random latent space as its input to generate fake access data, and passes the generated sequence samples to the discriminator, which attempts to distinguish the generated (i.e., "fake") data sequence from the actual (i.e., "true") normal training data sequence. This model does not handle each data stream separately, but considers the entire dataset simultaneously in order to capture potential interactions between variables in the model.

In order to utilize the advantages of LSTM in processing time series in this method, both the generator and discriminator of GAN are long short-term memory neural networks (LSTM). After sufficient rounds of training iterations, the trained discriminator and generator can be used to detect anomalies in the data. The advantage of using GAN is that it can train both a discriminator and a generator simultaneously. This article uses discriminators and generators to jointly train and identify network anomalies.

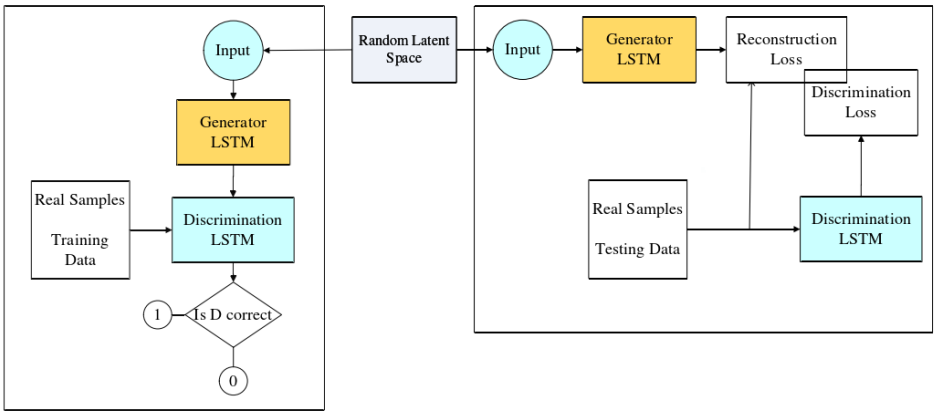


Figure 2: Generative adversarial model based on LSTM

3.2 Encoder based generative adversarial model

A GAN trained to adapt to a normal sample distribution should be able to reconstruct a normal sample from some potential representation. However, since GANs can only implicitly model data distributions, using them for anomaly detection requires a complex optimization process to recover the potential representation of a given input example, which is a very time-consuming approach for large datasets or real-time applications. Therefore, this article designs a GAN model based on an encoder for anomaly detection, with the aim of learning the encoder while training the GAN to achieve better anomaly detection performance.

This model is based on the GAN method and simultaneously learns an encoder E that maps the input sample X to a latent representation Z, a generator G, and a discriminator D during training, which can avoid the problem of high computational complexity in recovering latent representations during testing. Unlike the discriminator in conventional GANs that only considers real or generated samples, in this case, discriminator D also considers potential representations (generator input or encoder). The structure of the encoder based generative adversarial model is shown in Figure 3.

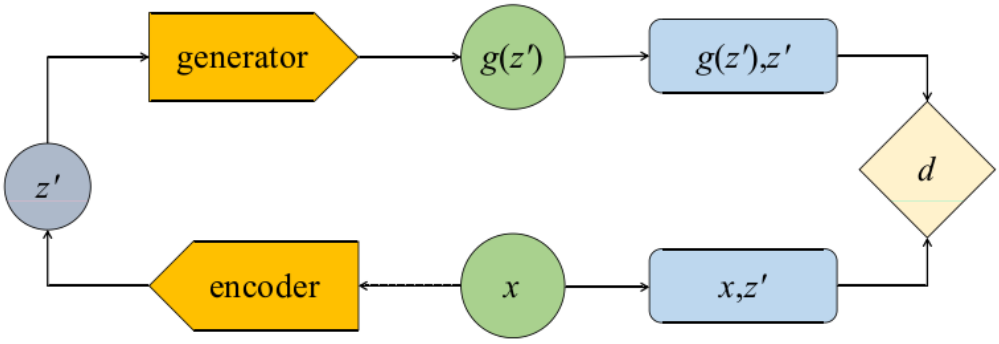


Figure 3: Encoder+GAN model structure

There are different strategies for training encoders, where G and E are jointly learned. In order to optimize the training process of the original GAN, this paper defines V (D, E, G) as equation (4):

$$V(D,E,G)=E_{X-PX}\left[E_{Z-PE(\cdot|X)}\left[\log D(x,z)\right]\right]+\left[E_{X-PG(\cdot|z)}\left[1-\log D(x,z)\right]\right] \quad (4)$$

Here PX (X) is the distribution of the data, Pz (z) is the distribution on the latent representation, PE (z | x) and PG (x | z) are the distributions of the encoder and generator, respectively. After training the model on normal data to generate G, D, and E, this paper defines a score function A $_{(x)}$, which is a combination of reconstruction loss L_G and discriminator-based loss L_D. The specific form of detecting whether example x is abnormal is:

$$A(x)=aL_G(x)+(1-a)L_D(x) \quad (5)$$

Where a represents the weight of the reconstruction loss in the overall loss of the model, and 1-a represents

the weight of the discriminator loss. Among them,

$$L_G(x) = \| xG(E(x)) \|_1 , \text{L}_\text{D}\ (\text{x})$$

are defined in two ways. Firstly, taking the cross-entropy loss of x's discriminator as an example: it captures the discriminator's confidence in the distribution of samples from real data. The second method of defining L_D has a "feature matching loss", were

$$L_D(x) = \| f_D(X, E(x)) - f_D(G(E(x), E(x))) \|_1$$

evaluates whether the reconstructed data has features similar to the real sample in the discriminator, and samples with larger $A_{(x)}$ values are considered more likely to be abnormal.

4 Experimental results and analysis

4.1 Experimental data

To verify the effectiveness of the proposed method, this paper uses the publicly available dataset KDDCUP1999Data1 as experimental data and analyzes the experimental results using the two model evaluation metrics mentioned earlier. The experimental environment is as follows: using the industry's mainstream deep learning framework Tensor Below to implement data loading and model training, and conducting experiments using PyCharm software.

The samples in the KDDCUP1999 dataset are network connections, each network connection is labeled as normal and abnormal, and the abnormal types are mainly categorized into the following four types:

(1) Denial-of-service attack (DOS, denial-of-service);

(2) The remote computer is not authorized to access the local computer (R2L, the remote computer is not authorized to access the local computer);

(3) super user has unauthorized access (U2R, super user has unauthorized access);

(4) port monitoring or scanning (surveillance and probing) [7].

In this paper, K-fold cross validation method is used for the training set and test set. The dataset is randomly divided into mutually exclusive subsets, and the k subsets are randomly divided into two groups, one with k-1 subsets and the other with one subset. In each kind of grouping result, the group with k-1 subsets is treated as a training set and the other as a test set, generating predictions, which are averaged. In this paper k is chosen as 12 during the processing of the dataset [8, 9].

4.2 Network transmission data anomaly identification method

4.2.1 Preprocessing of network transmission data

Before data anomaly identification, certain preprocessing of network transmission data is required. This study applies the normalization method to control the network transmission data between 0 and 1, with the expression:

$$Y = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \quad (6)$$

Due to the large volume of network transmission data, coupled with the fact that the subsequent construction of the model requires a training set and a test set, a Gaussian mixture model is applied in this section to partition the network transmission data set. Gaussian mixture model can effectively partition the network transmission data set into 2 sets, respectively, the training set (dark circle) and the test set (light circle), which are recorded as sets Y1 and Y2, laying a solid foundation for the realization of the subsequent network transmission data anomaly identification.

4.2.2 Network transmission data anomaly identification model construction

Based on the preprocessed network transmission data collection, LSTM, a deep learning technique, is introduced to construct a network transmission data anomaly identification model, which provides support for the realization of the research objectives.

The Encoder+GAN based network transmission data anomaly identification model is specifically shown in Fig. 4.

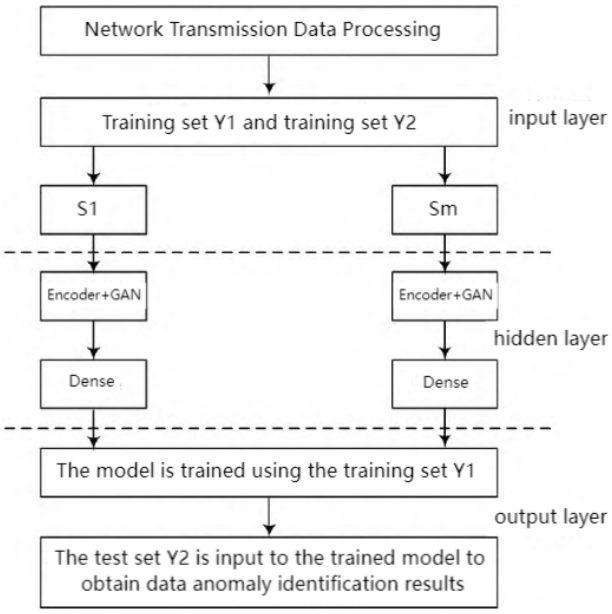


Figure 4: Schematic diagram of network transmission data anomaly identification model

Due to the network transmission data in the time dimension there is a back and forth relationship, with time series characteristics, coupled with the data

transmission is a more complex process, but also subject to a variety of factors directly or indirectly, resulting in the existence of anomalous data with a certain degree of uncertainty, and LSTM has a better convergence of the time series data processing, so this is the basis for the construction of the network transmission data anomaly identification model.

4.2.3 Network transmission data input remodeling

Because the LSTM neural network contains long-term and short-term memory unit states in the above model, it has certain requirements on the input data form, therefore, it is necessary to reshape the network transmission data to make it meet the requirements of the model input, and maximize the recognition accuracy of the anomalous data.

Setting the network transmission data as

$$Y = \{y_1, y_2, ..., y_m\},$$

LSTM neural network long-term and short-term memory unit association length is LC and LD respectively, then the expression of input data after reshaping is:

$$z_i = \frac{y_i}{\alpha_c \cdot L_c} + \frac{y_i}{\alpha_D \cdot L_D} \quad (7)$$

The entire network transmission data is reshaped and processed using Eq. (7) to obtain the set of input data $S = \{s_1, s_2, ..., s_m\}$

for constructing the model, in preparation for the implementation of network transmission data anomaly identification.

4.2.4 Network transmission data anomaly identification

The gradient descent method is applied to formulate the training procedure for constructing the model, determine the abnormal data discrimination rules, input the test set into the trained recognition model, and its output is the abnormal data recognition result.

The training process of network transmission data anomaly identification model based on gradient descent method is shown below:

1) Initialize the parameters of the recognition model, set the initial step size to 0.001 and the initial decay rate to 0.9.

2) Collect a random sample data q in the training set Y_1, which is noted as $\{y_1, y_2, ..., y_q\}$, and its corresponding model output target is R_j.

3) Calculate the gradient values g and update the biased first-order moment estimate H and biased second-order moment estimate K.

4) Correct the biased first-order moments and second-order moments to obtain new estimates, denoted as H vs K.

5) Calculate the updated parameters.

6) Repeat steps 2) to 5) until the maximum number of iterations is satisfied, and output the parameters of the final recognition model. The anomalous data discrimination parameter is calculated as:

$$\Gamma = \sqrt{\frac{1}{n-1}\sum_{t-1}^{n}[y(t) - \hat{y}(t)]^2} \quad (8)$$

Where: Γ denotes the anomalous data discriminating parameter; $y(t)$ and $\hat{y}(t)$ denote the model fitting value and the actual value, respectively.

Based on the calculation results of Eq. (8), the rules of abnormal data discrimination are formulated: when Γ is greater than or equal to 0.43, it is recognized that the data transmitted by the network are abnormal data; when Γ is less than 0.43, it is recognized that the data transmitted by the network are normal data. Substituting the relevant parameter values and abnormal data discrimination rules obtained from the above training into the network transmission data abnormality identification model, the training and improvement of the identification model can be completed. The test set is used as the input of the identification model, and the output of the model is the result of abnormal data identification, thus realizing the accurate identification of network transmission data abnormality, providing a more effective guarantee for the security of network transmission data, and facilitating the querying of demand data to a certain extent.

4.3 Anomaly detection results and analysis based on classification accuracy

In order to verify the performance of the network anomaly access detection method based on generative adversarial network proposed in this paper, this paper uses One-ClassSVM, Isolation Forest Algorithm, Local Anomaly Factor Algorithm and Covariance Estimation Algorithm for comparison experiments [10].

Before analyzing the experimental results, this paper selects the same number of network anomaly access data from the preprocessed data and uses a variety of traditional algorithms as a comparison experiment. The experimental results are shown in Table 1:

Table 1: Classification accuracy of traditional machine learning methods

Model	Precision	Recall	F1
Isolation Forest	0.4415	0.3260	0.3750
One-Class-SVM	0.7457	0.8523	0.7954
Local Outlier Factor	0.7913	0.8045	0.7743
Covariance estimation	0.7879	0.7736	0.7851

From the experimental results, it can be seen that among all the machine learning methods, the use of Isolation Forest for anomaly detection has the worst effect, and the accuracy rate of detecting network anomalies is even less than half, while the accuracy rate of using One-Class SVM, Local Anomaly Factor Algorithm, and Covariance Estimation Algorithm is relatively similar, and among them, the Local Anomaly Factor Algorithm has the best experimental results. Among all the machine learning methods, the highest accuracy was achieved using the Local Outlier Factor method. Although the experimental results show that the results are not bad when using traditional machine learning algorithms for network anomalous access detection, however, for the Internet as a whole, every time one more network attack goes undetected, its potential damage increases exponentially [11]. In this paper, we propose a network anomaly detection algorithm based on generative adversarial networks, and the accuracy rates under different models and parameters are shown in Table 2:

Table 2: Classification accuracy of the network abnormality detection algorithm based on GAN

Model	Parameter	Precision	Recall	F1
GAN(Feature Matching)	w=0.1	0.7382	0.7500	0.7741
GAN(Cross-E)	w= 0.1	0.7859	0.7984	0.7921
GAN(Feature Matching)	w=0.3	0.7292	0.7408	0.7349
GAN(Cross-E)	w=0.3	0.7858	0.7984	0.7920
GAN + LSTM(Cross-E)	w =0.1	0.7983	0.8650	0.8303
GAN + LSTM(Feature Matching)	w= 0.1	0.7719	0.8467	0.8134
GAN + LSTM(Cross-E)	w =0.3	0.7959	0.8646	0.8300
GAN + LSTM(Feature Matching)	w=0.3	0.7597	0.8250	0.7954
GAN + Encoder(Cross-E)	w=0.1	0.9508	0.9659	0.9583
GAN + Encoder(Feature Matching)	w= 0.1	0.9492	0.9643	0.9567
GAN + Encoder(Cross-E)	w=0.3	0.9507	0.9658	0.9582
GAN + Encoder(Feature Matching)	w=0.3	0.9104	0.9249	0.9176

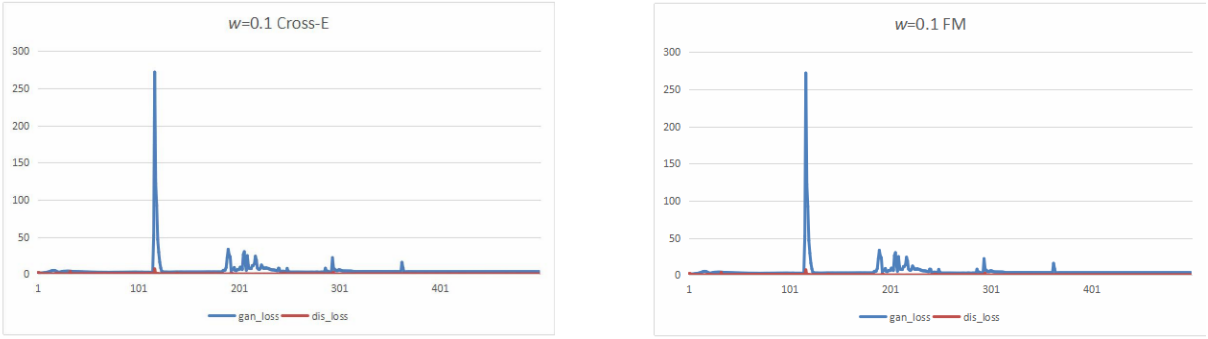
In this case, the accuracy rate is the percentage of data points that are correctly detected as anomalous. A higher accuracy rate means that the model can accurately find out the abnormal data with better results. Among the three models, the accuracy rate of GAN + Encoder is higher than the other two models, which is around 0.9. Recall is the ratio between data points that are correctly detected as anomalous and all anomalous data points. The higher the recall, the more comprehensively the model is able to identify anomalous data. Among the three models, the GAN + Encoder model has the highest value, which indicates better results. F1 value is a combined assessment of accuracy and recall, which is used to measure the overall performance of the model. Higher F1 values represent better anomaly detection ability of the model. Among the three models, GAN + Encoder has a relatively high F1, which shows the advantage of its detection ability.

In Table 2, w is the weight, which indicates the proportion of the generator's loss to the overall loss of the generative adversarial model, and the corresponding loss weight of the discriminator is 1-w. Through the experimental results, it is not difficult to see that the experimental results are the best when w is taken to be 0.1, and the classification accuracy rate is in a decreasing trend with the increasing w. On the other hand, this paper uses two kinds of loss functions, cross-entropy and feature matching, and experiments are conducted with different loss functions under each parameter, and the results show that in the process of using generative adversarial network for network anomalous access detection, cross-entropy as a loss function is more effective for classification compared to feature matching. When the original generative adversarial network is used, the anomaly detection

effect that can be achieved is similar to the result of using local anomaly detection methods, and when the discriminator and generator in the GAN use LSTM, it can produce a certain enhancement to the accuracy of classification. Finally, when the GAN+Encoder method is used, for anomalous access detection Data Table 2 GAN-based Network Anomaly Detection Algorithm achieves the best accuracy in terms of classification accuracy, which is best compared to other classification models [12].

4.4 Anomaly detection results and analysis based on generator discriminator loss

In this paper, a total of three different generative adversarial network models are used for anomaly detection, which are the original Generative Adversarial Network (GAN), Generative Adversarial Network using Long and Short-Term Memory Networks (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder (GAN+Encoder). The strengths and weaknesses of the models can be observed through the loss variations of the generators and discriminators of these three models.



(a) (b)

Figure 3: Trend of GAN loss change. (a)Loss variation of GAN with loss function Cross-E (b) Loss variation of GAN with loss function as FM

As shown in Figure 3, Figure 3a shows the loss variation of GAN using Cross-Entropy as the loss function, and Figure 3b shows the loss variation of GAN using Feature Matching as the loss function. When using the same parameters to train the original GAN, it can be found that the generator loss will first become larger and larger, this is due to the initial period of training the model discriminator is stronger, the generator is weaker, at this time the discriminator can easily distinguish between the real data and the fake data generated by the generator, so at this time, the loss of the discriminator is very small, and the generator's loss is larger, and continues to show an upward trend. However, in the process of continuous adversarial training, the generator gradually learns how to generate more "realistic" fake data, and then the generator loss begins to decline, and eventually converge to a smaller value, until the generator and discriminator losses converge [13].

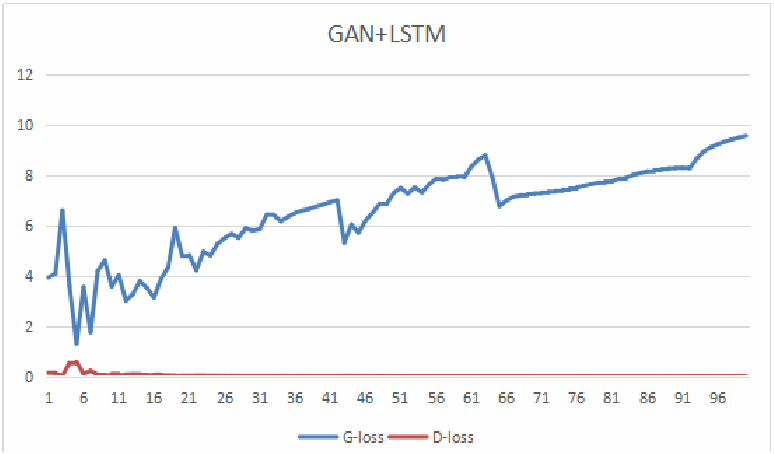
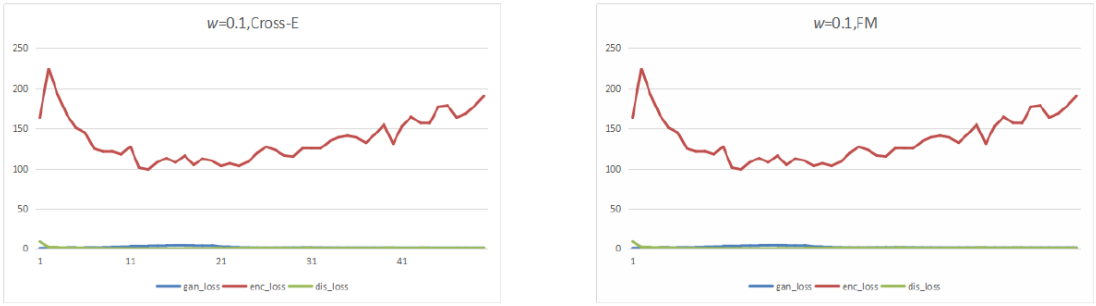


Figure 4: Loss variation of GAN+LSTM

Figure 4 shows the training loss variation of the generative adversarial network model based on Long Short-Term Memory Network (LSTM), unlike the original GAN, the generator and the discriminator of this model are all using LSTM. Through many experiments, it is found that the model's performance is the best at this time when the number of times of training is set to about 100 times. Meanwhile, compared with the original GAN, the loss of the generator and the discriminator tends to converge faster after using the GAN+LSTM model, which means that the model's classification effect is better after adding the LSTM. However, due to the increased complexity of the model, each iteration of training takes longer [14].

Figure 5 shows the loss variation of the generative adversarial network model with the addition of the Encoder. From Figure 5, it is not difficult to see that although the loss of the encoder is very large and constantly showing an upward trend, but the loss of the generator converges very quickly, at this time, only need to train about 50 times to make the model has a very good detection effect.



(a) (b)

Figure 5: Loss variation trend of Encoder+GAN. (a) The loss function is the loss variation (b) Encoder+GAN loss variation of Encoder+GAN of Cross-E with loss function as FM

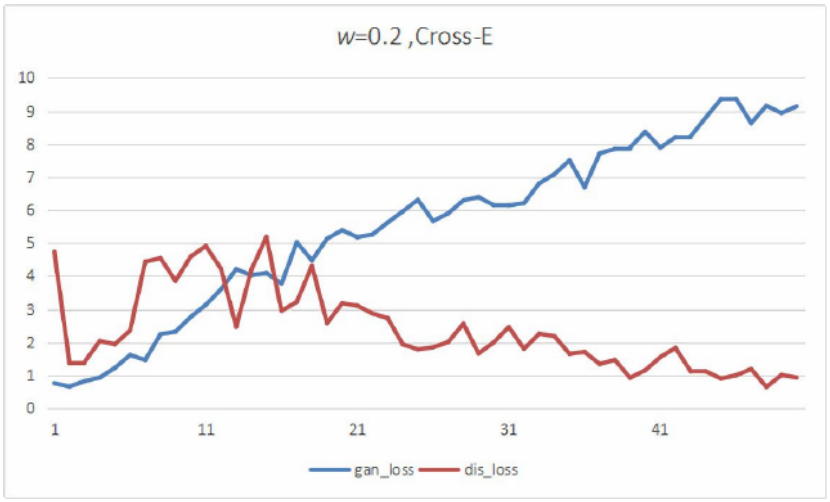


Figure 6: Training results of GAN after 50 iterations

As shown in Figure 6, in order to compare the model enhancement effect, when using the original GAN for 50 times of training, at this time it is not difficult to find that the loss of the generator is extremely large and rising, while using the GAN + Encoder at this time, the loss of the generator and discriminator has converged. At the same time compared to the GAN + LSTM model, the use of GAN + Encoder model is relatively simple, and the training time is shorter, more efficient.

5 Discussion

The research on network anomaly access detection technology is crucial in the field of intrusion detection. However, currently this technology is facing issues such as high false alarm rates, insufficient detection coverage, and inadequate detection accuracy and efficiency, which urgently require in-depth research. This article proposes a novel detection mechanism based on generative adversarial networks to address the challenge of dealing with network intrusion datasets with rich types of anomalies but limited sample sizes encountered by

traditional methods. By training the GAN model, the generator generates data through continuous adversarial training, thereby enhancing the discriminative ability of the discriminator.

This article also explores the problem of mismatched generator and discriminator capabilities during GAN training, and proposes two variant models of GAN that help the generator loss function converge faster, significantly reducing training time and improving training quality. However, due to the large number of network connection features contained in the processed data samples, the computational complexity of the GAN model is high, making it difficult to quickly achieve result output in a single machine environment. Therefore, this study suggests adopting a distributed server cluster architecture to improve program running efficiency.

In this study, the classification accuracy and F1 results of the three models, the original Generative Adversarial Network (GAN), Generative Adversarial Network using Long Short-Term Memory Network (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder (GAN+Encoder), were analyzed experimentally in comparison to the original Generative Adversarial Network (GAN), and the Generative Adversarial Network using Long Short-Term Memory Network (GAN+LSTM), and Generative Adversarial Network with the addition of an encoder, and the F1 results show that GAN+Encoder model is the best. This is due to the fact that this model is based on stemming approach while learning an encoder E mapping input samples X to potential representations Z, a generator G, and a discriminator D during the training period, which avoids high computational complexity problems in recovering potential representations during testing. Experiments on the loss trends of the generator and discriminator based on these three models, as well as the results of training through 50 iterations show that the GAN+Encoder model is relatively simple, and has a shorter and more efficient training time. However, there are still some challenges and limitations of the method, such as the comprehensiveness of data collection, the effectiveness of feature extraction, and the robustness of the network. Future research can further explore these issues to achieve more efficient and reliable anomalous access behavior detection.

Funding

This work was sponsored in part by China Southern Power Grid Corporation technology project (059300KC2212000).

Conflict of interest

The authors declare that they have no competing interests.

Data availability statement

The data used to support the findings of this study are all in the manuscript.

References

[1] Xu XY, Fan WW, Wang SY, Zhou F. (2024). WBIM-GAN: A generative adversarial network based wideband interference mitigation model for synthetic aperture radar. *Remote Sensing*, 16(5), 910. https://doi.org/10.3390/rs16050910

[2] Vijaykumar R, Mueer Ahmad M, Ismail MA, Ahmad I, Neelum N. (2024). Deep learning-driven virtual furniture replacement using GANs and spatial transformer networks. *Mathematics*, 12(22), 3513. https://doi.org/10.3390/math12223513

[3] Zhang YL, Wang TK, Du K, Chen P, Wang HX, Sun HH. (2024). General network framework for mixture raman spectrum identification based on deep learning. *Applied Sciences*, 14(22), 10245. https://doi.org/10.3390/app142210245

[4] Zhu W, Guo QS, Yang N, Tong Y, Zheng CB. (2024). An improved generative adversarial network for generating multi-scale electronic map tiles considering cartographic requirements. *ISPRS International Journal of Geo-Information*, 13(11), 398. https://doi.org/10.3390/ijgi13110398

[5] Riaz M, Dilpazir H, Naseer S, Mahmood H, Anwar A, Khan J, Benitez IB, Ahmad T. (2024). Secure and fast image encryption algorithm based on modified logistic map. *Information*, 15(3), 172. https://doi.org/10.3390/info15030172

[6] Khemaissia R, Derdour M, Ferrag MA, Bouhamed MM. (2023). PrSChain: A blockchain based privacy preserving approach for data service composition. *Informatica*, 47(9). https://doi.org/10.31449/inf.v47i9.5081

[7] Zhu YH, Li Y, Wei TY. (2024). Classification and identification of frequency-hopping signals based on jacobi salient map for adversarial sample attack approach. *Sensors*, 24(21), 7070. https://doi.org/10.3390/s24217070

[8] AlKhonaini A, Sheltami T, Mahmoud A, Imam M. (2024). UAV detection using reinforcement learning. Sensors, 24(6), 1870. https://doi.org/10.3390/s24061870

[9] Xie Q, Huang JJ. (2024). Improvement of a conditional privacy-preserving and desynchronization-resistant authentication protocol for IoV. *Applied Sciences*, 14(6), 2451. https://doi.org/10.3390/app14062451

[10] Taurshia A, Kathrine JW, Andrew J, Eunice RJ. (2024). Securing internet of things applications using software-defined network-aided group key management with a modified one-way function tree. *Applied Sciences*, 14(6), 2405. https://doi.org/10.3390/app14062405

[11] Sun L, Chen P, Xiang W, Chen P, Gao WY, Zhang KJ. (2019). SmartPaint: a co-creative drawing

system based on generative adversarial networks. *Frontiers of Information Technology & Electronic Engineering*, 20 (12): 1644-1657. https://doi.org/10.1631/FITEE.1900386

[12] Xia LM, Wang H, Guo WT. (2019). Gait recognition based on generative adversarial image complementation network (English). *Journal of Central South University*, 26 (10): 2759-2770. https://www.cnki.com.cn/Article/CJFDTotal-ZNGY201910013.htm

[13] Hu YD, Sun L, Mao XQ, Zhang S. (2024). EEG data augmentation method for identity recognition based on spatial-temporal generating adversarial network. *Electronics*, 13(21), 4310. https://doi.org/10.3390/electronics13214310

[14] Xiao YJ, Xu WY, Jia ZH, Ma ZR, Qi DL. (2017). A non-intrusive power consumption-based anomaly detection scheme for programmable logic controllers (in English). *Frontiers of Information Technology & Electronic Engineering*, 18 (04): 519-535. https://doi.org/10.1631/FITEE.1601540