Journal of Computers Vol. 33 No. 4, August 2022, pp. 133-144
doi: 10.53106/199115992022083304011

GAN-based Technology of Generating Spoofing-jamming I/Q Signal

Rui-Ze Xu[1,2], Sheng-Bo Hu[1,2,3*], Ye Lv[2,4], Man-Qin Zhu[1,2], Xin Meng[1,2]

[1] School of Big Data and Computer Science, Guizhou Normal University, Guiyang 550001, Guizhou, China
2438672814@qq.com
[2] Institute of Intelligent Information Processing, Guizhou Normal University, Guiyang 550001, Guizhou, China
hsb@nssc.ac.cn
[3] Center for RFID and WSN Engineering, Department of Education Guizhou, Guiyang 550001, Guizhou, China
[4] School of Mathematical Sciences, Guizhou Normal University, Guiyang 550001, Guizhou, China

Received 21 September 2021; Revised 15 January 2022; Accepted 15 February 2022

Abstract. The existing wireless communication interference methods rely heavily on the characteristics of the target signals obtained in communication reconnaissance, require complex prior knowledge, and have problems in keeping up with the dynamic changes of relevant parameters. This paper proposes a GAN-based technology of generating spoofing-jamming I/Q signals. The jammer will be able to deceive and interfere with op-ponents through GAN by generating spoofing-jamming I/Q signals highly correlated to real I/Q signals without prior knowledge. This paper first introduces the principle of GAN and the GAN model to be adopted; uses a software radio system composed of LabView and NI USRP software and hardware plat-forms to simulate real communication scenarios to collect real I/Q signal data; generates spoofing-jamming I/Q signals through GAN model; uses t-SNE algorithm to perform dimensionality reduction on both the real and the spoofing-jamming I/Q signal data to visualize their distributions; finally, tests the spoofing-jamming I/Q signals on receiver's pre-trained classifier. The experimental results show that GAN provides an effective method for generating high-quality spoofing-jamming I/Q signals.

Keywords: communication interference, GAN, spoofing-jamming I/Q signal, NI USRP

1 Introduction

Being an important part in communication countermeasure, spoofing-jamming signals can effectively suppress and destroy the communication process, to eventually achieve the goal of weakening or even disabling the communication of opponents. Therefore, the research on generation of high-performance spoofing-jamming signals has always been a hotspot.

Currently, game theory [1] and nonconvex optimization [2] are widely used in spoofing-jamming signals generation. For example, S. Shafiee et al. [3] propose a method that the jammer adds linear interference to the intercepted signals through mutual information games and adjusts its transmitting power to deceive the receiver, provided that the jammer knows the channel characteristics of the opponents in advance. Xu et al. [4] propose a method to design spoofing-jamming signals via exploiting the symbol-level relationship between each original constellation point of the transmitter and the expected constellation point of the jammer, and optimize the spoofing-jamming signal design and power allocation under BPSK and QPSK modulations. However, this method requires prior knowledge on the transmitter in advance, such as fading channels, modulation modes. The spoofing-jamming using traditional methods often needs to master the relevant parameters of the target signals and require complex prior knowledge; On the other hand, in a real communication countermeasure scenario, the opponents will dynamically adjust the relevant parameters according to the change of radio frequency environment. Once the parameters change, the jammer needs to re-obtain the parameters and adjust the spoofing-jamming signals with spending a lot of resources.

In recent years, with artificial intelligence being more and more widely used, the intelligence level of the wireless communication systems is continuously improving [5-6]. Correspondingly, in order to combat the intelligent wireless communication systems, the jammer is also trying to improve its own intelligence level, and relevant research has attracted attention. For example, Hui et al. [7] uses genetic algorithm to screen interference strategies and save individuals according to decision rules, and Nasir et al. [8] propose strategies like reinforcement learning. The purpose of these methods is to replace the manual search for the optimal deception and interference

* Corresponding Author

strategy. However, to achieve the above goals, it is still necessary to obtain the relevant parameters of the target signals in advance. These methods will not work when the opponents' parameters change dynamically.

Adversarial learning is a new direction in the field of artificial intelligence. And GAN (Generative Adversarial Network) being the main subject [9], its powerful generative ability provides a new framework for data generation [10]. At present, GAN research has developed from the initial field of computer vision [11] to the fields like natural language processing [12], communication, and so on. The communication field mainly includes signal data generation [13-16], signal enhancement [17-18], RFID [19-20], and channel modeling [21], etc. For example, Zhu et al. [22] propose a method of radar signal data enhancement based on GAN. The radar signals are generated through GAN, which enhance the dataset, to improve the training effect of the neural network model and the accuracy of target recognition; Song et al. [23] propose a GAN-based HRRP (High Resolution Range Profile) data enhancement method. HRRP is scarce but more HRRP data can be generated through GAN to provide data support for the next work.

Considering that GAN has been widely used in the generation of communication signal, this paper proposes a novel method using GAN to generate spoofing-jamming I/Q signals. Compared with the traditional methods, it doesn't require obtaining relevant parameters of the target signals in advance and the spoofing-jamming signals with high authenticity can be generated directly through GAN. This reduces the process of human intervention in decision-making, and solves the dynamic changes of opponents' parameters.

The structure of this paper is as follows:

1. A GAN model suitable for communication signal is designed based on the analysis of the basic principle of GAN and the characteristics of communication signal. The model structure is displayed in detail in the section 2.1;

2. A real communication scenario is simulated by using the software radio system composed of LabVIEW and NI USRP (National Instruments Universal Software Radio Peripheral) software and hardware platform, to collect real I/Q signal data [24]; one-dimensional convolutional neural networks (1D-CNN) is used at the receiver to pre-train a classifier [25] for the receiver having certain discrimination ability;

3. Three validations are designed to verify that the spoofing-jamming I/Q signals generated through GAN are highly correlated with the real I/Q signal:

- Compare the spoofing-jamming I/Q signal data with the real I/Q signal data in images;
- Use t-SNE (t-Distributed Stochastic Neighbor Embedding) [26] algorithm to perform dimensionality reduction on spoofing-jamming I/Q signal data and real I/Q signal data to visualize their distributions, and calculate the KL divergence value between them;
- Use the pre-trained classifier of receiver to classify the signals.

The three validations jointly verify the feasibility of the method proposed in this paper.

2 GAN Principle and GAN Model

2.1 GAN Principle

GAN consists of two antagonistic neural network models: a generator model with random noise as input that outputs fake data consistent with the real data dimension, and a discriminator model with real and fake data as input that outputs discrimination results. See Fig. 1 the basic structure of GAN.

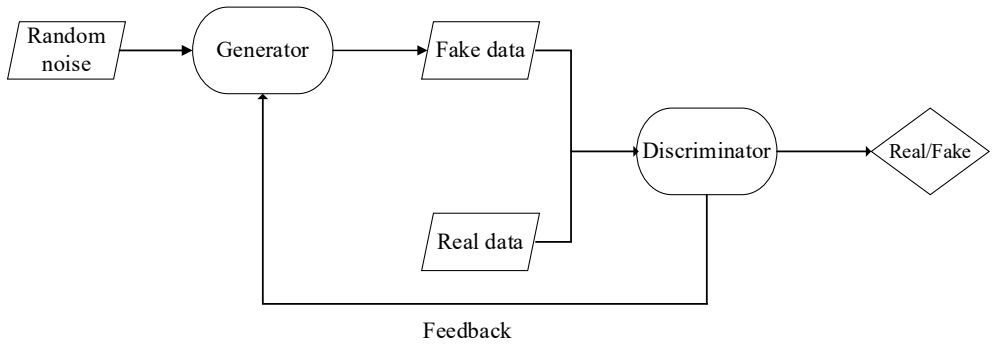


Fig. 1. Basic structure of GAN

Since GAN is composed of two neural networks, the loss function of the GAN network is also composed of two parts, see Equation 1 the function expression:

$$\left.\begin{aligned} G\_Loss &= (1-y)\log(1-D(G(z))) \\ D\_Loss &= -y\log(D(x)) - (1-y)\log(1-D(G(z))) \end{aligned}\right\}. \tag{1}$$

Where G_Loss represents the loss function of the generator; D_Loss represents the loss function of the discriminator; y represents the label of the data, where 1 is for the real data, and 0 for the fake data; z is a low-dimensional random noise vector that obeys a certain distribution; $G(z)$ represents the data generated by the generator; $D(\bullet)$ represents the probability that the data is identified to be real by the discriminator, and the value is between 0 and 1. The goal of the generator is generating fake data with the distribution as similar as possible to the real data to cause discrimination error from the discriminator, which means the fake data generated is classified as real data. The target of the discriminator is improving its classification accuracy to discriminate between the real and the fake data as accurately as possible. The generating capability of the generative network and the discriminating ability of the discriminative network are continuously improving during the mutual games. This process is also called confrontation. Therefore, the loss functions of the generator and the discriminator can be combined and written in the form of $\min\text{-}\max$ game as the objective function of GAN, as shown in Equation 2:

$$\begin{aligned} \min_G \max_D V(D,G) = {} & E_{z \sim p_z(z)}[\log(1-D(G(z)))] + \\ & E_{x \sim P_{data}(x)}[\log D(x)] \end{aligned}. \tag{2}$$

Where $p_z(z)$ represents the distribution of input noise, and $P_{data}(x)$ represents the distribution of real data. Treat the GAN training process as a minimax problem which essentially is an alternate neural network optimization. First, fix the parameters of the generator, then use the real data and fake data as input to train the discriminator to maximize the value $V(D,G)$, that is, $D(x)$ increases and $D(G(z))$ decreases, so that the discriminator can accurately verify the authenticity of the input data; after the discriminator has been trained for several times, fix the parameters of the discriminator, and optimize the generator to minimize $V(D,G)$, that is, $D(x)$ decreases and $D(G(z))$ increases, so that the fake data generated by the generator is so close to the real data that the discriminator can no longer discriminate accurately. The above process is continuously performed alternately, improving both networks. When the fake data generated by the generator can play the effect of "fake the real", and the accuracy of the discriminator is stable at about 50%, it can be considered that the generator has completed the learning of the real data distribution, and the model has converged.

2.2 GAN Model

The spoofing-jamming I/Q signals highly correlated with the real I/Q signals are generated through GAN. The designed GAN model is composed of a generator and a discriminator using Deep Neural Networks (DNN). For the model, the real data are the real I/Q signals, and the fake data are the spoofing-jamming I/Q signals. The input of the generator is random noise that obeys the standard normal distribution, and the output is the spoofing-jamming I/Q signals with dimensions consistent with the real I/Q signals. Input of the discriminator is the real I/Q signals and spoofing-jamming I/Q signals, and the output is discrimination results. Considering the time-domain waveform structure of the wireless signal simple without much complicated feature information compared with the multi-dimensional data, it is enough to achieve the generation and discrimination of signal data using DNN. The network structure of the GAN model designed in this paper is shown in Fig. 2.

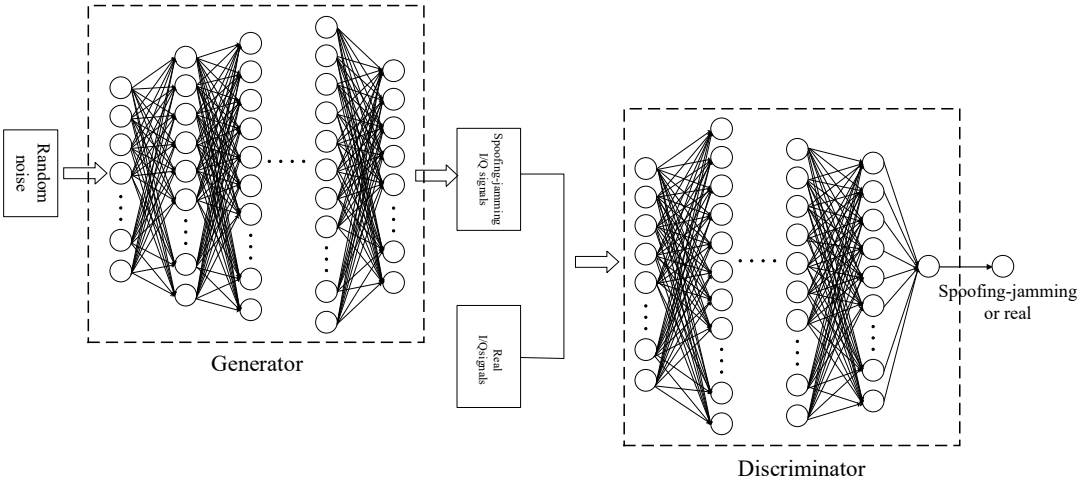


Fig. 2. GAN network structure

Adding more neural network layers to the network structure may bring the training a better generation effect, but it also means that the training difficulty increases. Therefore, is it to pursue a good generation effect or to reduce the difficulty of training is a question worth thinking about. After a lot of adjustment and testing, the generator and discriminator adopt 8-layer and 6-layer neural network design structures respectively. This structure not only ensures a better generation effect, but also balances the training difficulty of the model. The specific structures of the genera-tor and the discriminator in Fig. 2 are shown in Table 1 and Table 2.

Table 1. Generator structure

Layer Type	Output Dimension
Input	Batch Size x Latent_dim
Dense+tanh	Batch Size x 128
Batch Normalization	
Dense+tanh	Batch Size x 256
Batch Normalization	
Dense+tanh	Batch Size x 512
Batch Normalization	
Dense+tanh	Batch Size x Data_dim

Table 2. Discriminator structure

Layer Type	Output Dimension
Input	Batch Size x Data_dim
Dense+LeakyRelu	Batch Size x 512
Dense+LeakyRelu	Batch Size x 256
Dense+LeakyRelu	Batch Size x 128
Dropout	
Dense+Sigmoid	Batch Size x 1

The signals input in the model are samples. The discriminator only needs to verify whether they are real or fake, which is equivalent to a binary classification problem, where p_{real} is the probability that a sample is a real I/Q signal, and $p_{fake} = 1 - p_{real}$ is the probability that it is a spoofing-jamming I/Q signal. Therefore, the discriminator output layer uses Sigmoid as the activation function, and it only needs one output node. The BCE (binary_crossentropy) loss function is suitable for binary classification tasks and is usually used with the Sigmoid activation function. Its expression is shown in Equation 3:

$$Loss = -\frac{1}{n}\sum_{i=1}^{n} y_i \cdot \log \hat{y}_i + (1 - y_i) \cdot \log(1 - y_i) \ . \tag{3}$$

Where n represents the number of samples, y_i represents the label of the samples, and $\hat{y}_i$ represents the probability that a sample is identified as a real I/Q signal by the discriminator. The cross-entropy loss function well measures the similarity between y and $\hat{y}$, and accurately feeds back the loss values of the generator and the discriminator. Therefore, BCE is used as the loss function of the GAN model. Compared with other relevant literatures, the network structure of the GAN model designed in this paper has a faster training speed, a shorter convergence period, and a better generation effect.

The entire generation process of spoofing-jamming I/Q signals is divided into the following steps:

Step 1: GAN uses intercepted real I/Q signal data for adversarial training;

Step 2: After the training converges, extract the generator model to generate spoofing-jamming I/Q signals.

3 Experimental Data Acquisition and Classifier Pre-Training

3.1 Experimental Scenarios

The spoofing-jamming process in this paper is described as: Firstly, the jammer intercepts the real I/Q signals from the transmitter, and uses the intercepted I/Q signals as training data. Then the jammer generates spoofing-jamming I/Q signals similar to the real I/Q signals using GAN to deceive and interfere with the receiver. To carry out the spoofing-jamming in a real scenario, this paper has designed experiment scenarios shown in Fig. 3. Assuming that the physical locations of the jammer and the receiver are very close, the channel between the jammer and the transmitter is similar to the channel between the receiver and the transmitter, and then the signal intercepted by the jammer is similar to the signal received by the receiver. In this case, the signal data received by the receiver directly are input into the GAN model for adversarial training.

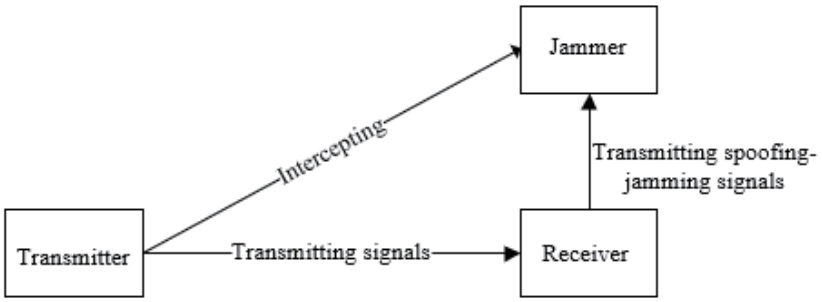


Fig. 3. Experimental scenarios

In the scenarios, two NI-USRP 2930 with Labview are used to transmit and receive signal data respectively. The distance between the two USRP devices is adjusted to 3 meters with no obstructions in the middle, and using LabView configures the NI-USRP 2930. One USRP is used as the signal transmitter to continuously transmit BPSK I/Q signals, with frequency of 915MHz, I/Q sampling rate at 500k/sec and SNR of 12dB; the other USRP is used as the signal receiver to continuously collect the signals from the transmitter. Form one I/Q signal sample with every 200 sampling points, where each sampling point is composed of In-phase/Quadrature parts. Collect a total of 5000 I/Q signal samples as the real I/Q signal dataset intercepted by the jammer. The signal transmission and reception process by USRP is shown in Fig. 4.

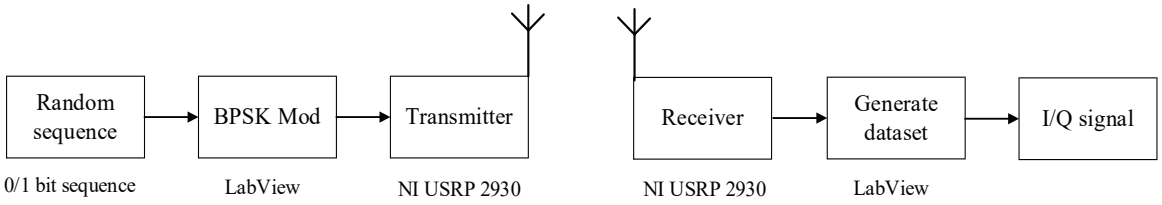


Fig. 4. Data generation and acquisition

Since the receiver itself should have certain ability to verify whether the signals received are from the target transmitter, its classifier needs to be pre-trained with I/Q signal data from the target transmitter and other trans-

mitters.

To obtain I/Q signal date from other transmitters, the parameters is modified to continuously transmit the I/Q signals. And the receiver collects the time-domain waveform of the signals. One I/Q signal sample is composed of 200 sampling points, where each sampling point includes real/image parts. Collecting a total of 500 I/Q signal samples are used as signal data from other transmitters.

3.2 Classifier Pre-Training

The structure of 1D-CNN is similar to that of two-dimensional convolutional neural networks (2D-CNN). The basic structure includes input layer, convolutional layer, pooling layer, and fully connected layer. Compared with 2D-CNN, 1D-CNN is more suitable for processing data related to time series.

The collected signals are used to pre-train the classifier. The sub-process of pre-training involves two possible classification errors, called false alarm and misdetection respectively. The false alarm is that the signals from the target transmitter are classified as coming from other transmitters and the misdetection is that signals from other transmitters are classified as from the target transmitter. The probabilities of false alarm and misdetection are represented by p_{FA} and p_{MD}, respectively. It is assumed that there are n signal samples for the pre-training. Among them, N_T signal samples are from the target transmitter, and there are n_{FA} false alarms and n_{MD} misdetections, then $p_{FA} = \frac{n_{FA}}{N_T}$, $p_{MD} = \frac{n_{MD}}{n - N_T}$. To enable the verification ability of the classifier, the network structure and parameters are adjusted during the pre-training process to minimize the $\max\{p_{FA}, p_{MD}\}$.

Fig. 5 is the 1D-CNN structure of the classifier to be pre-trained. The waveform structure of the time-domain signal is simple, and there is not much feature information. To ensure the information integrity and avoid complex statistical feature conversion, the most primitive I/Q signal data are used as the input of the model for completely retaining the characteristic information in the signals. Since every 200 sampling points form one I/Q signal sample, and each sampling point is composed of real/image parts, the input dimension of the neural network is 1×400. In this neural network, tanh is used as the activation function of the convolution layer of the feature extraction module, Fil represents the window size of the convolution calculation for the local input data, Ker represents the length of the time domain windows of the convolution kernel, Relu is used as the activation function of the dense layer of the classifier module, and Softmax is used as the activation function of the output layer.

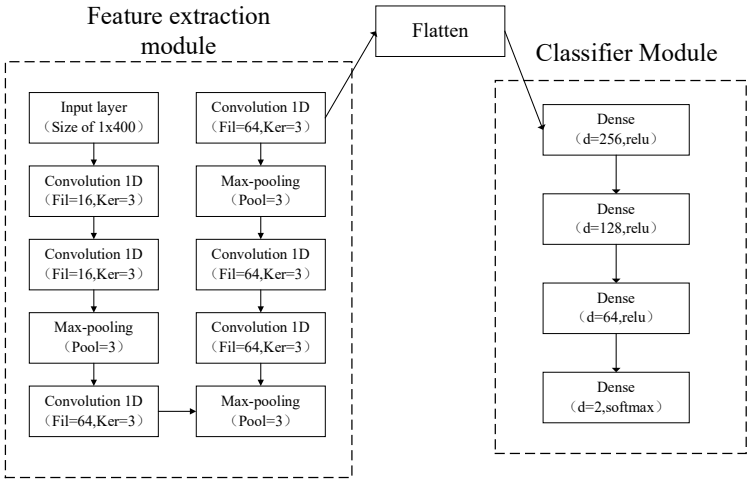


Fig. 5. 1D-CNN network structure

As described in the section 3.2, 500 signals are collected from other transmitters, and 500 signals from real I/Q signal dataset from target transmitter are collected respectively. The signal data from the target transmitter are labeled as 0 and signal data from other transmitters as 1, and the training – test ratio is set to 7:3. The specific parameters corresponding to Fig. 5 are shown in Table 3.

Table 3. Classifier parameters

Parameter name	Setting
Optimizer	Adam
Loss	Categorical_cross-entropy
Batch Size	32
Epoch	40

The final testing result shows that 5 signals from the target transmitter are classified as from other transmitters, and 15 signals from other transmitters are classified as from the target transmitter, which means $p_{FA} = \frac{5}{500} = 1\%$, $p_{MD} = \frac{15}{500} = 3\%$, and the $\max\{p_{MD}, p_{FA}\}$ = 3%. It is proved that this model has a high classification accuracy rate and the pre-trained neural network model can be used as the receiver's classifier.

4 Experimental Validation and Analysis

After obtaining the real I/Q signal dataset and a pre-trained classifier, the generation effect of the GAN model can be tested.

4.1 Signal Comparison in Images

The GAN model composed of DNN is not only fast training, but also has a better generation effect. It also has disadvantages like unstable training process, etc. Therefore, performing multiple trainings on the GAN model, the best training results are selected for experimental analysis.

Each signal sample in the real I/Q signal dataset is composed of 200 sample points, and each sample point is composed of In-phase/Quadrature parts. The number of neurons in the output layer of the generator and the input layer of the discriminator are set to be 400. And the other training parameters are shown in Table 4.

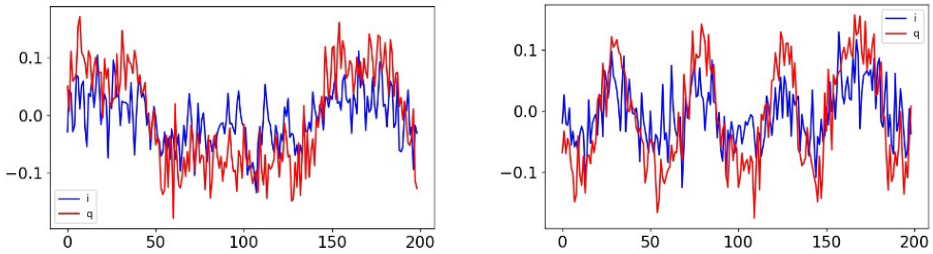
Table 4. Training parameters

Parameter Name	Setting
Latent_dim	100
Data_dim	400
Batch Size	512
Eopch	35000
Optimizer	Adam
Learning Rate	0.001

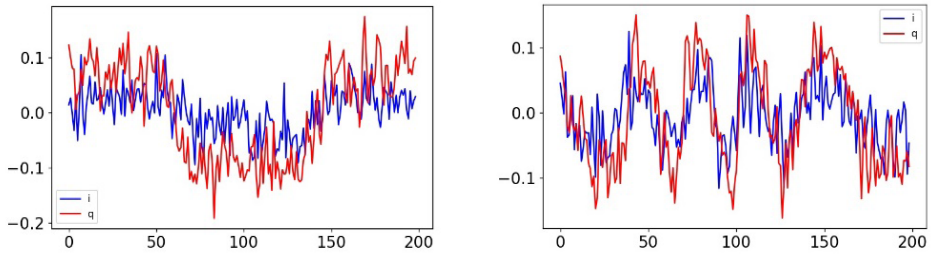
The real I/Q signal dataset contains 5000 signal samples. The batch size is set to be 512, which improves the training speed. After continuous training adjustment, the learning rate is finally determined to be 0.001, and the training result is the best under this parameter.

During the training, extracting a batch of generated spoofing-jamming I/Q signals every 500 training epochs is analyzed to investigate the improvement process of the generator. When the loss of the generator and the discriminator tends to be stable during a long training epoch, the GAN model is considered to be converged and the training can be stopped.

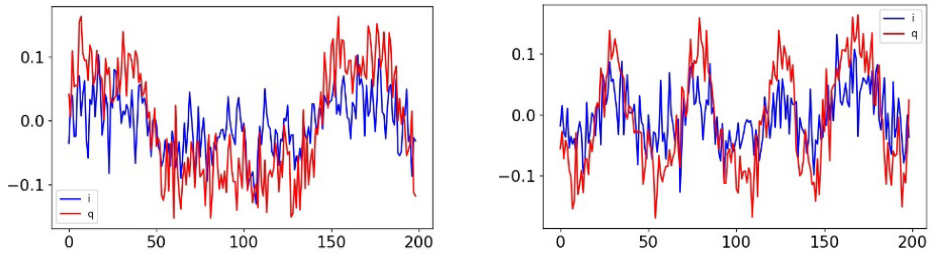
Fig. 6 shows the time-domain waveform of the real I/Q signals and the spoofing-jamming I/Q signals generated through GAN at different training epochs.



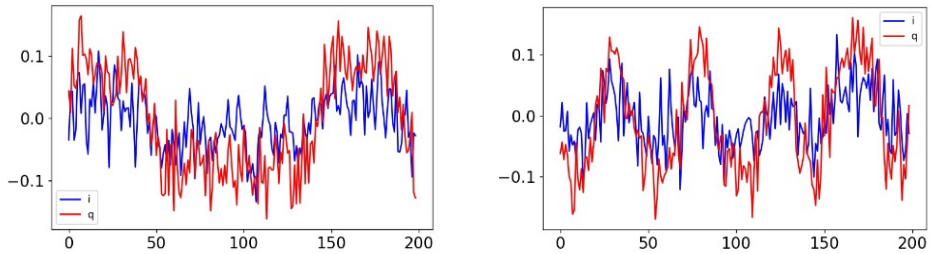
(a) Real I/Q signals



(b) 15,000th Epoch



(c) 25,000th Epoch



(d) 35,000th Epoch

Fig. 6. Real I/Q signals and Spoofing-jamming I/Q signals generated through GAN at different training epochs

Through comparative analysis, it can be clearly observed that:

- When reaching to the 15,000th training epoch, the spoofing-jamming I/Q signals generated through GAN have initially learned the waveform characteristics of the real I/Q signals, but differences can still be visually observed. At this point, the generator of the GAN model is considered to have certain generation ability;
- After reaching to the 25,000th training epoch, the spoofing-jamming I/Q signals generated through GAN has fully learned the waveform characteristics of the real I/Q signals, and the time-domain waveform of the spoofing-jamming I/Q signals is basically no different from the real I/Q signals.

The training results show that, if only considering the time-domain waveform of the generated signals, the GAN model has completed the learning process of the real I/Q signals and has great generation ability.

4.2 Comparison After Dimensionality Reduction by t-SNE

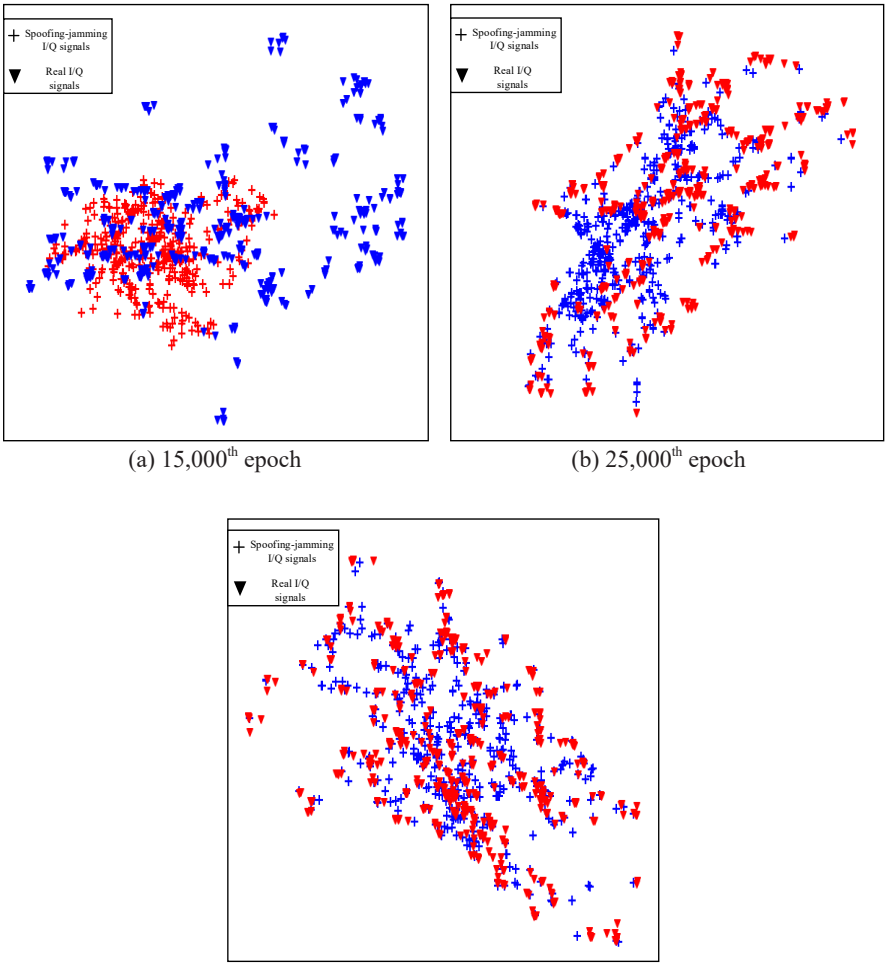
t-SNE is a non-linear dimensionality reduction algorithm used to express the high-dimensional dataset in a two or three-dimensional space to visualize its distribution.

Reducing the dimensionality of the spoofing-jamming I/Q signal data and the real I/Q signal data with the t-SNE algorithm, their distributions can be displayed in a two-dimensional space. And the difference of the distribution can be calculated using KL divergence to analyze the learning results of the generator. The calculation of KL divergence is shown in Equation 4:

$$D_{KL}(p \,||\, q) = \sum_{i=1}^{n} p(x_i) \log\left(\frac{p(x_i)}{q(x_i)}\right) \quad . \tag{4}$$

where $p(x)$ represents the probability distribution of the real I/Q signal data and $q(x)$ represents the probability distribution of the spoofing-jamming I/Q signal data. The smaller the KL divergence value is, the closer the two probability distributions are.

The 3 batches of spoofing-jamming I/Q signal data previously are extracted at the 15,000th, 25,000th, and 35,000th training epoch in the section 4.1, and a batch of the same number of signals randomly are selected from the real I/Q signal dataset. Using the t-SNE algorithm to reduce their dimensionality to visualize their distributions is shown in Fig. 7. The Fig. 7 shows the distributions of the real I/Q signal data and the signal data generated at the 3 different training epochs.



(a) 15,000th epoch (b) 25,000th epoch

(c) 35,000th epoch

Fig. 7. The distributions of real I/Q signal data and spoofing-jamming signal data at different training epochs

Due to the uncertainty of the t-SNE algorithm, the distribution results shown in Fig. 7 are random, but this does not affect the analysis on the generation effect of the GAN model.

From the Fig. 7, it can be observed that when reaching to the 15,000th epoch, the distribution of generated data is mainly concentrated in a certain part of the distribution of the real I/Q signal data. It indicates that the data generated by the GAN model has a certain degree of authenticity but still lacks diversity.

When reaching to the 25,000th epoch, the data generated by the model already has a better diversity compared with the 15,000th epoch, but its distribution is not completely consistent with the real I/Q signal data.

When reaching to the 35,000th epoch, it can be clearly observed that, the distribution of the spoofing-jamming I/Q signal data generated through GAN fits well with the distribution of the real I/Q signal data. The generated data has both high authenticity and diversity.

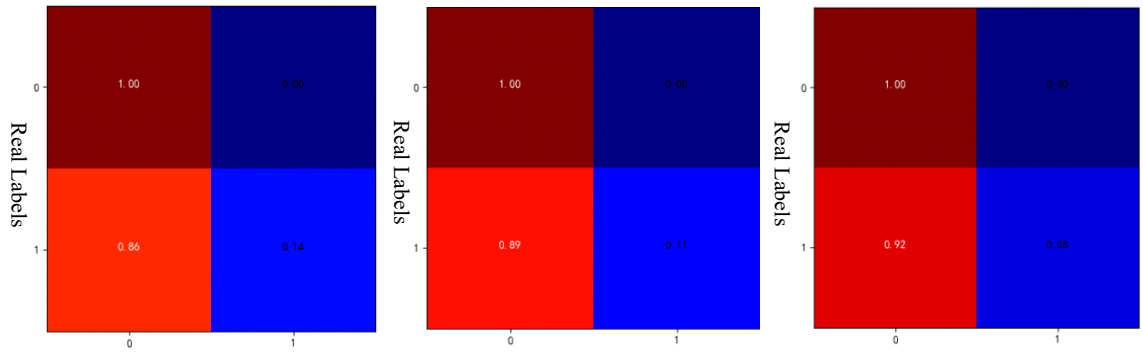
In addition to visualizing the distributions, the KL divergence value is also calculated to numerically analyze the difference between the two distributions at different epochs. According to the Table 5, as the GAN training epoch increases, the KL divergence value between the two distributions decreases. This also proves that the spoofing-jamming I/Q signals generated through GAN are highly similar to the real I/Q signals.

Table 5. KL divergence values at different epochs

Epoch	KL divergence value
15,000	0.248
25,000	0.142
35,000	0.122

4.3 Classification by Pre-Trained Classifier

Like in section 4.2, the 3 batches of spoofing-jamming I/Q signal data previously are extracted at the 15,000th, 25,000th, and 35,000th training epoch in the section 4.1, and are labeled as 1; then the extracted 500 signals from the real I/Q signal dataset are labeled as 0. The 1,000 signals are put into the pre-trained classifier for classification test, and the classification results at the three different epochs are shown in Fig. 8.



(a) 15,000th Epoch (b) 25,000th Epoch (c) 35,000th Epoch

Fig. 8. Confusion matrix of classification results of the classifier at different epochs

It can be observed from Fig. 8 that:

- When reaching to the 15,000th training epoch, the probability that the spoofing-jamming I/Q signals with label 1 are classified as real I/Q signals with label 0, which is also called successful deception rate, is $p_{sd} = 86\%$; this shows that the generated spoofing-jamming I/Q signals already have quite high authenticity;

- When reaching to the 25,000th training epoch, the $p_{sd} = 89\%$. The authenticity of the generated signal has improved compared with the 15,000th training epoch;

- When reaching to the 35,000th training epoch, the $p_{sd} = 92\%$. It proves that the generator is already capable of generating spoofing-jamming I/Q signals highly similar to the real I/Q signals which causes great classification errors from the classifier;

- At the same time, it can be observed that all the real I/Q signals labeled as 0 are completely and correctly classified, which means the false alarm rate $p_{FA} = 0\%$. This proves that the pre-trained classifier itself has certain discrimination ability.

The experimental results show that as the GAN training epoch increases, the authenticity of the generated spoofing-jamming I/Q signals continuously improves. This is consistent with the conclusion in the section 4.2 that the distribution of the spoofing-jamming I/Q signal data becomes more and more similar to the real I/Q signal data with the increase of training epoch.

To sum up, as the spoofing-jamming I/Q signal data generated through GAN has caused great classification errors from the classifier of the receiver, the jammer has achieved the goal of deceiving opponents.

5 Conclusions and Prospects

This paper proposes a GAN-based spoofing-jamming I/Q signal generation technology. As GAN has the ability of learning independently the potential distribution of target data, the jammer trains the GAN with the intercepted real I/Q signals to obtain spoofing-jamming I/Q signals with time-domain waveform characteristics highly similar to the real I/Q signals.

Compared with the traditional methods, the GAN-based method proposed in this paper does not require obtaining parameters of the target data in advance or need complex prior knowledge. As GAN has the ability of extracting independently the characteristics of the target signal data to generate spoofing signal data, it reduces human intervention in decision-making, and can better keep up with the dynamic change of the relevant parameters which is more practical. Meanwhile, the spoofing-jamming I/Q signals generated have high authenticity that can cause high classification errors from the pre-trained classifier of the receiver, and achieve certain deception purposes.

This method also has certain limitations. Take the GAN model designed in this paper as an example, it is usually only applicable to one or several types of signals, but the real communication countermeasure scenario is normally composed of multiple kinds of signals. All the experiments in this paper are carried out under the condition that the transmitter and the receiver are static, without considering the position change of the devices while in a real scenario the devices often change dynamically. These limitations will be improved in future re-search.

In the future research, the author will focus on optimizing the proposed GAN model to ensure its high per-formance and enhance the generalization of the model. In order to be more in line with the real communication countermeasure scenario, the author considers conducting experiments in a designed scenario where the devices' position will change dynamically.

References

[1] L. Yu, Q. Wu, Y. Xu, Power control games for multi-user anti-jamming communication, Wireless Networks 25(5)(2019) 2365-2374.

[2] T.-T. Tran, H. Thi, P.-D. Tao, DC programming and DCA for enhancing physical layer security via cooperative jamming, Computers & Operations Research 87(11)(2016) 235-244.

[3] S. Shafiee, S. Ulukus, Mutual information games in multi-user channels with correlated jamming, IEEE Transactions on Information Theory 55(10)(2009) 4598-4607.

[4] J. Xu, L. Duan, R. Zhang, Transmit Optimization for Symbol-Level Spoofing, IEEE Transactions on Wireless Communications 17(1)(2018) 41-55.

[5] X. You, C. Zhang, X. Tan, AI for 5G: research directions and paradigms, Scientia Sinica: Informations 62(2)(2019) 13.

[6] H. Ye, G.-Y. Li, B.-H. Juang, Power of Deep Learning for Channel Estimation and Signal Detection in OFDM Systems, IEEE Wireless Communications Letters 7(1)(2018) 114-117.

[7] J. Hui, X. Song, W. Miao, A Fast Anti-jamming Decision Method Based on the Rule-Reduced Genetic Algorithm, Ksii Transactions on Internet & Information Systems 10(9)(2016) 4549-4567.

[8] Y.-S. Nasir, D. Guo, Multi-Agent Deep Reinforcement Learning for Dynamic Power Allocation in Wireless Networks, IEEE Journal on Selected Areas in Communications 37(10)(2019) 2239-2250.

[9] L. Goodfellow, J. Pouget-Abadie, M. Mirza, Generative adversarial networks, Communications of the ACM 63(11)(2020) 139-144.

[10]N. Park, M. Mohammadi, K. Gorde, S. Jajodia, H. Park, Y. Kim, Data Synthesis based on Generative Adversarial Networks, in: Proc. of VLDB, 2018.

[11]F.-J. Chen, F. Zhu, Q.-X. Wu, Y.-M. Hao, E.-D. Wang, Y.-G. Cui, A review of research on generative adversarial networks and their applications in image generation, Journal of Computer Science 44(2)(2021) 347-369.

[12]G.H.D. Rosa, J.P. Papa, A Survey on Text Generation using Generative Adversarial Networks, Pattern Recognition 119(2021) 108098.
[13]H. Yang, L. Chen, J. Zhang, Research on digital signal generation techniques based on generative adversarial networks, Electronic Measurement Technology 43(20)(2020) 127-132.
[14]F. Zhao, H. Jin, GAN-based waveform generation technique for communication interference, Systems Engineering and Electronics Technology 43(4)(2021) 1080-1088.
[15]T. Truong, S. Yanushkevich, Generative Adversarial Network for Radar Signal Generation, 2020.
[16]W. Fan, F. Zhou, Z. Zhang, Deceptive jamming template synthesis for SAR based on generative adversarial nets, Signal processing 172(7)(2020) 107528.1-107528.15.
[17]P.-Y. Cao, C.-C. Yang, L.-M. Shi, H.-C. Wu, LPI radar signal enhancement based on DAE-GAN network, Systems Engineering and Electronics Technology 43(9)(2021) 2493-2500.
[18]X. Zhou, Z. Sun, H. Wu, Wireless Signal Enhancement Based on Generative Adversarial Networks, Ad Hoc Networks 2020(103)(2020) 102151.
[19]D. Roy, T. Mukherjee, M. Chatterjee, RFAL: Adversarial Learning for RF Transmitter Identification and Classification, IEEE Transactions on Cognitive Communications and Networking 6(2)(2020) 783-801.
[20]Z. Chen, L. Peng, A. Hu, Generative adversarial network-based rogue device identification using differential constellation trace figure, EURASIP Journal on Wireless Communications and Networking 2021(1)(2021) 1-27.
[21]W. Xia, S. Rangan, M. Mezzavilla, A. Lozano, G. Geraci, V. Semkin, G. Loianno, Millimeter Wave Channel Modeling via Generative Neural Networks, in: Proc. IEEE Globecom Workshops, 2020.
[22]K.-F. Zhu, J.-G. Wang, Y.-J. Liu, Radar target recognition algorithm based on data enhancement and WACGAN under small sample conditions, Journal of Electronics 48(6)(2020) 1124-1131.
[23]Y. Song, Y. Li, Y. Wang, Data Augmentation for Imbalanced HRRP Recognition Using Deep Convolutional Generative Adversarial Network, IEEE Access 8(2020) 201686-201695.
[24]T. Izydorczyk, F. Tavares, G. Berardinelli, P. Mogensen, A USRP-Based Multi-Antenna Testbed for Reception of Multi-Site Cellular Signals, IEEE Access 7(2019) 162723-162734.
[25]J.-D. Chen, Research and Application of Radar Signal Recognition with Deep Learning Methods, [dissertation] Chengdu: University of Electronic Science and Technology, 2019.
[26]L. van der Maathen, G. Hinton, Visualizing data using t-SNE, Journal of Machine Learning Research 9(2008) 2579-2605.