Anti-Reactive Jamming Technology Based on Jamming Utilization

Xin Liu[1,2], Mingcong Zeng[1,2*], Yarong Liu[1,2], Mei Wang[2,3] , and Xiyu Song[3]
[1] Guilin University of Technology College of Information Science and Engineering Guilin, China
[2]Guangxi key Laboratory Fund of Embedded Technology and Intelligent System, Guilin University of Technology, Guilin 541007, China
[3]Provincial Ministry of Education Key Laboratory of Cognitive Radio and Signal Processing, Guilin University of Electronic Technology, Guilin 541004, China.
[e-mail: zengmingcong@glut.edu.cn]
[*]Corresponding author: Mingcong Zeng

Received June 5, 2023; revised September 1, 2023; accepted September 17, 2023; published October 31, 2023

Abstract

Since the existing anti-jamming methods, including intelligent methods, have difficulty against high-speed reactive jamming, we studied a new methodology for jamming utilization instead of avoiding jamming. Different from the existing jamming utilization techniques that harvest energy from the jamming signal as a power supply, our proposed method can take the jamming signal as a favorable factor for frequency detection. Specifically, we design an intelligent differential frequency hopping communication framework (IDFH), which contains two stages of training and communication. We first adopt supervised learning to get the jamming rule during the training stage when the synchronizing sequence is sent. And then, we utilize the jamming rule to improve the frequency detection during the communication stage when the real payload is sent. Simulation results show that the proposed method successfully combated high-speed reactive jamming with different parameters. And the communication performance increases as the power of the jamming signal increase, hence the jamming signal can help users communicate in a low signal-to-noise ratio (SNR) environment.

Keywords: Jamming Utilization, Anti-Jamming, Anti-Intelligent Jamming, Deep Learning, Spectrum Waterfall

This research work was supported by the National Natural Science Foundation of China under Grant 61961010, 62071135, the Key Laboratory Found of Cognitive Radio and Information Processing, Ministry of Education (Guilin University of Electronic Technology) under Grant No. CRKL200204, No. CRKL220204, RZ18103102, and the 'Ba Gui Scholars' program of the provincial government of Guangxi.

http://doi.org/10.3837/tiis.2023.10.016 **ISSN：1976-7277**

1. Introduction

Wireless communications are becoming more essential than ever before, as various techniques, i.e., 5G cellular, unmanned aerial vehicles (UAV), vehicle-to-everything (V2X), and so on, are gradually being used in daily life. Meanwhile, wireless communications are becoming more vulnerable as user-configurable communication devices significantly lower the cost of building smart or intelligent jamming devices. For example, a malicious adversary can detect and analyze the waveform of the legitimate user signal and then release targeted jamming by using a universal software radio peripheral (USRP) device. Therefore, how to counter intelligent jamming is a hot topic in the field of anti-jamming communication.

Traditional anti-jamming technologies, such as frequency hopping (FH) [1] and adaptive technology [2], have been widely used in wireless communications. Unfortunately, these traditional anti-jamming methods cannot adapt to the dynamic spectrum state caused by intelligent jamming due to the lack of learning ability [3]. Aiming at this problem, [4-5] has carried out some innovative work, introducing game theory to model the adversarial relationship between legitimate users and malicious jammers. However, most of these works assume that legitimate users can obtain jammers' channel state information (CSI), which is unrealistic in adversarial environments.

Considering the difficulty of obtaining the state information of the jammer, reinforcement learning (RL) [6-7] and deep reinforcement learning (DRL) [8-11] are introduced to solve the problem of anti-intelligent jamming. In [8], the authors propose a fast anti-jamming algorithm based on intra-domain knowledge reuse against dynamic unknown jamming, while in [9], a deep reinforcement learning algorithm based on Dual Action Network is proposed and verified in the field environment. Although the above research can avoid slow reactive jamming, it has certain limitations in dealing with high-speed reactive jamming. This jammer can change the channel almost synchronously with the user, but the effect of resisting high-speed reactive jamming is not apparent.

Aiming at high-speed reactive jamming, we proposed a new method to utilize the jamming instead of avoiding jamming, and some similar works have been investigated in [12-17]. In [12], the author proposed an anti-jamming scheme IA (Opportunistic IA, OIA) based on wireless energy harvesting, which can optimize the transmission rate and collect jamming energy to help users communicate. Furthermore, [14] proposed an anti-jamming scheme combining neural network structure and ambient backscatter communication technology. This scheme can reflect the transmitted data to the receiving end through the jamming signal and collect the energy of the jamming signal to support its communication. In [16], the author introduced an intelligent deception mechanism to deal with the super-reactive jammer, allowing the sender to attract the jammer and transmit the information to the receiver using the ambient backscatter tag. In addition, a signal detector based on deep learning is proposed, which can achieve the best BER performance of ML detection. However, these methods proposed in [12-15] will have relatively low jamming utilization efficiency due to the channel loss of wireless transmission, while the detector based on deep learning proposed in [16] requires certain high-quality training data. To improve the efficiency of jamming utilization, [17] proposed a method of using jamming signals to transmit user information, which regards the user signal as the excitation of the jamming signal and guides the decision of jamming signal. But this method relies on the separation of the signal source estimation, which is only applicable to scenarios where the user signal and jamming signal are uncorrelated with each other. For more general scenarios, we propose an intelligent jamming utilization method, which adopts a neural network to learn the jamming pattern and utilize the jamming signal.

Specifically, we designed an intelligent differential frequency hopping(IDFH) framework containing two stages, namely, the training stage and the communication stage. During the training stage, the transmitter sends the fixed and pre-known hopping signal to learn the changing rule of the jamming signal corresponding to the change of the user signal. And at the communication stage, the extracted jamming rule, the neural network model, can be used to utilize the jamming signal to improve the frequency detection performance. Simulation analysis shows that the IDFH can utilize jamming signals more efficiently so as to get better communication performance compared with existing utilization methods. The main contributions of this paper are summarized as follows, and in order to show the difference between our work and the existing work, we also summarize in **Table 1**.

(1) An jamming utilization method based on intelligent learning is proposed to achieve more general jamming signal utilization. This method first extracts the rule between the jamming signal and the user signal through deep learning, and then combines this correlation to assist user frequency point detection. Because we extract information based on the jamming waveform collected on-site, we do not need to set the spectrum shape and reaction time of the jamming in advance and can cope with various types of reactive jamming.

(2) An jamming utilization scheme based on DFH, namely IDFH, is proposed, and its performance improves with increased jamming power. The scheme simplifies the processing of communication signals, ensures the timeliness of user communication, can deal with more complex reactive jamming, and is suitable for more general application scenarios.

Table 1. The contribution of this paper

Related Study	Research Status	Innovation of this paper
Anti-jamming communication based on intelligent learning	It is necessary to know the jamming information in advance, such as [5]	Learning the jamming information according to the mixed signal received on-site
	Unable to resist high-speed reactive jamming, such as [10]	Actively use jamming based on the idea of jamming utilization
Anti-jamming communication based on jamming utilization	Jamming utilization efficiency is limited by wireless transmission, such as [12-15]	Directly using the rule of jamming signal rather than collecting jamming energy
	Depending on the specific type of jamming, such as [17]	Neural network is introduced into the framework to enhance generalization ability.

2. Related Work

In this section, we review the related work research in two areas: jamming utilization and differential frequency hopping.

2.1 Jamming utilization

Traditional anti-jamming methods such as FHSS (Frequency Hopping Spread Spectrum) cannot achieve an ideal anti-jamming effect in the face of fast and complex reactive jamming. In [18], the author first mentioned the concept of antifragile communications, and based on this concept, several models adapted to reactive jamming are proposed. Therefore, the research direction of jamming utilization is mainly divided into jamming information utilization, jamming energy collection, jamming assisted guidance, and jamming assisted positioning. In the jamming information utilization, Fang et al. [19] proposed a method of transmitting information by using the reaction time of jamming. This method does not assume the spectral coverage and power of the jammer, can be applied to more scenarios. Similarly, Ma et al. [20] proposed an active anti-jamming (AAJ) scheme, which re-modulates the jamming signal and transmits information using different energy levels of the jamming signal. In the jamming energy collection, Van Huynh et al. [13] based on deep reinforcement learning, proposed a jamming utilization algorithm. When the jammer attacks the channel, the transmitter modulates the jamming signal into backscatter information and sends it to the receiver, while the energy required for transmission comes from the energy collection of the jamming signal. Based on [13],[14] developed an intelligent deception strategy, which actively emits false transmissions to attract jammers for jamming and collects the energy of jamming signals to improve the efficiency of jamming utilization further. In the jamming assisted guidance, Xu et al. [21] designed an anti-jamming spectrum access algorithm based on cooperative learning (CLASA), guiding users to perform spectrum coordination using jamming signals. In the jamming assisted positioning, Di Pietro et al. [22] proposed a JAM-ME algorithm, which uses the jamming signal to locate the position of the jammer, and establishes a jamming signal aided navigation system.

2.2 Differential Frequency Hopping

The existing differential frequency hopping research work can be divided into frequency transfer function and system performance.

Recent studies on frequency transfer functions mainly combine frequency transfer functions with cryptography to enhance randomness and security. Ning et al.[23]proposed a time-varying frequency shift algorithm to improve the randomness and security of the frequency hopping sequence. Bao et al.[24]combined encryption algorithm and signal modulation method to reduce the consumption of resources and time required for receiving signals and improve the security performance of the system. Chen et al. [25] proposed the use of the GOST algorithm and RSA algorithm to construct the probability transfer function of encryption, which improves the randomness, complexity and security. Ai et al. [26] proposed a frequency transfer function based on chaotic encryption algorithm. The long-period pseudo-random sequence generated by logistic chaotic function is used to encrypt and disturb the frequency hopping sequence.

In the study of system performance, the research focused on the anti-jamming performance of the system. In order to reduce the damage of jamming signals to users, Qian et al. [27] proposed a JADE algorithm, which separates frequency hopping signals from mixed signals by using the statistical independence of differential frequency hopping signals.Zhu et al. [28] introduced convolutional error correction coding into a differential frequency hopping to further improve the anti-partial-band jamming performance of the system.Dong et al. [29] proposed a differential frequency hopping communication system with compressed spectrum, which can obtain a higher bit error rate (BER) gain under the same bandwidth condition by compressing the spectrum. Ning et al. [30] proposed a local error-correcting sequence detection algorithm, which effectively enhances the system's reliability by local pre-correction and less continuous frequency decision errors.

Although some studies have enhanced the anti-jamming performance of differential frequency hopping, there are few studies on more intelligent reactive jamming. For example, Teng et al. [31] only analyzed the performance impact of different types of reactive jamming on differential frequency hopping, but the method of dealing with reactive jamming is not pointed out. In [17], although a method to deal with reactive jamming was proposed, this method still has some limitations. Inspired by the idea of jamming utilization, this paper proposes an intelligent differential frequency hopping communication framework to effectively deal with reactive jamming through jamming utilization technology.

3. System Model and Problem Formulation

3.1 System Model

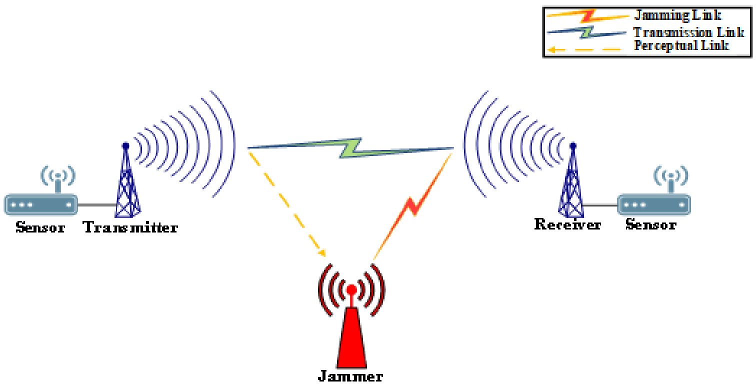

Fig. 1. System Model

The system model considered in this paper is shown in **Fig. 1**, where a user pair (a transmitter and a receiver) is pitted against an intelligent jammer, and both the receiver and jammer can sense the spectrum. Users communicate using DFH technology [32]. Different from the traditional frequency hopping communication, the DFH technology maps the bit information to be transmitted to the corresponding frequency by $G()$ (frequency transfer function) and uses adjacent frequencies to transmit the information. We assume the set of user's hopping frequencies is $F(f_0, f_1, f_2, \dots, f_M)$, where M denotes the number of available frequency points. At the time slot k, the next hop frequency decision is made by the current data symbol X_k and the current frequency decision f_k^U, as shown in (1), where f_k^U, $f_{k+1}^U \in F$.

$$f_{k+1}^U = G(f_k^U, X_k) \tag{1}$$

For the receiver, it is only necessary to detect the user communication frequency of each time slot to obtain the bit information by $G^{-1}(f_k^U, f_{k+1}^U)$, where $G^{-1}()$ is the inverse function of $G()$.

3.2 Problem Formulation

As shown in the system model, the receiver needs to detect the communication frequency of the user signal at each time slot, and this is equivalent to determining the presence of user signals at each channel $f \in F$. Therefore, we set the user-selected frequency f_k^U to transmit the signal at the time slot k. The power of the signal is expressed as $P_U = \int_{-b_{u/2}}^{b_{u/2}} S(f)df$,where $S(f)$ represents the power spectral density (PSD) of lowpass equivalent of a bandpass signal of the user, b_U expressed the bandwidth of the user's baseband signal. After sensing the user's frequency decisions at the time slot k ,the jammer selects the frequency f_k^J and power P_J to jamming user. In order to ensure its jamming performance, the jammer will definitely launch a jamming signal to the target frequency with a higher transmitting power. With the above settings, we can express the instantaneous environmental state of the time slot k as $\mathbf{s}_k = \left\{s_k^1, s_k^2, \ldots, s_k^m\right\}$, s_k^m denotes the received power of the signal with frequency m at the time slot k. The (2) is the specific forms.

$$s_k^m = P_U g_U \delta(m = f_k^U) + P_J g_J \delta(m = f_k^J) + n(f) \tag{2}$$

The g_U represents the transfer function of signals from the transmitter to the receiver, g_J represents the transfer function of signals from the jammer to the receiver. Where the $\delta(x)$ is the indicator function, the value of $\delta(x)$ gets one when x is true and gets zero when x is false, $n(f)$ is the PSD function of noise. Considering that the environment is dynamic and unknown, there are many unknown quantities, such as g_U and g_J, so it is not practical to obtain the communication frequency directly based on $\mathbf{s}_k$. In this regard, [17] proposes a matched filter approach. Specifically, this method separates the jamming waveform from the mixed signal by a blind source separation technique and also designs multiple jamming waveforms matching filters on each channel. Since the jamming signal is correlated with the user signal, as long as a jamming waveform is matched on a channel, it is assumed that there is a jamming signal on that channel, and there is a high probability that there is a user signal. Although the communication frequency can be determined by this method, this method relies on the separation estimation of the jamming signals, and the system performance will be dramatically degraded in more complex jamming environments.

To achieve jamming utilization in complex jamming environments, inspired by [10], although the process of obtaining the jamming decision becomes difficult, for intelligent jamming, the decision may be related to the user communication frequency. Thus, we define the environment state as $\mathbf{S}_k = \left\{\mathbf{s}_k, \mathbf{s}_{k-1}, \ldots, \mathbf{s}_{k-L+1}\right\}$, where L is the length of the backtracking time. $\mathbf{S}_k$ is a two-dimensional matrix of size $L \times M$, its thermodynamic diagram is called a spectrum waterfall, and the waterfall contains both frequency and time domain information. From the spectrum waterfall diagram, we can also see that the frequency decision of jamming has a certain regularity with the user communication frequency.

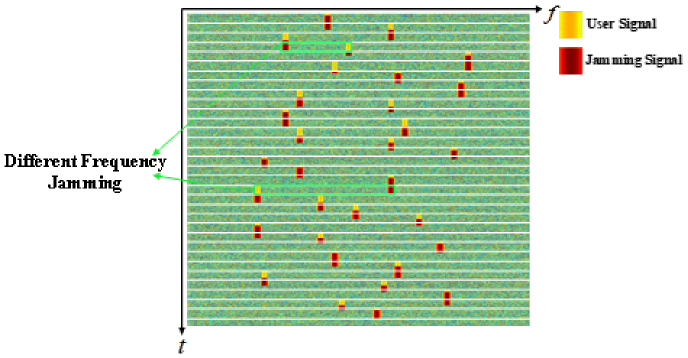

Fig. 2. Spectrum waterfall of the user and the reactive jamming signal

Fig. 2 shows the spectrum waterfall diagram of a complete communication flow in a reactive jamming environment, where the interval between each white line is one hop communication time. As shown in **Fig. 2**, we can see that in each time slot, the jamming signal completes the jamming action by sensing the current communication channel of the user. For differential frequency hopping, If the jamming signal is synchronized with the user signal, it can be considered as the same frequency jamming at each hop. In this case, the performance of frequency detection based on energy detection is improved because the jamming increases the signal power of every hop. However, the channel state in the real environment always changes dynamically, and all the jamming signals do not overlap with the user signals every time. We can also see from **Fig. 2** that the same frequency jamming at the previous time will become the different frequency jamming at the next time, resulting in frequency detection error. Because the jamming signal is dynamic and unknown, it is necessary to learn the rule of dynamic jamming. In this regard, we design an IDFH framework to learn the jamming rule on the spectrum waterfall through neural networks, then improve the frequency detection performance according to the rule.

The IDFH communication framework designed in this paper is shown in **Fig. 3**, and its structure is similar to the DFH framework proposed in [32]. In the transmitter part, we map the required transmitted bit information to a differential frequency hopping sequence through the frequency transfer function $G()$. The frequency hopping sequence controls the frequency synthesizer to synthesize the transmitting carrier frequency and generates a differential frequency hopping signal through the radio frequency part. In the receiver part, we replace the frequency sequence detection receiver proposed in [32] with a frequency detecting network, which have intelligent learning ability and frequency detection ability. Finally, we integrate the identified communication frequency points into a frequency sequence and input the frequency sequence to demodulate all bit information.

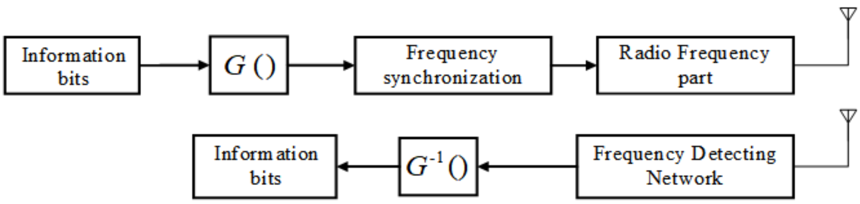

Fig. 3. IDFH Communication Framework

4. The Jamming Utilization Method Based on IDFH

In Section 3.2, we mention that the realization of jamming utilization needs to learning jamming rules and implement them through neural networks. Therefore, we designed the IDFH communication framework based on this requirement. Correspondingly, we also divide the communication process into the communication stage and the training stage. In this part, we will introduce the receiving process and specific details of the frequency detecting network.

4.1 IDFH Receiver Framework

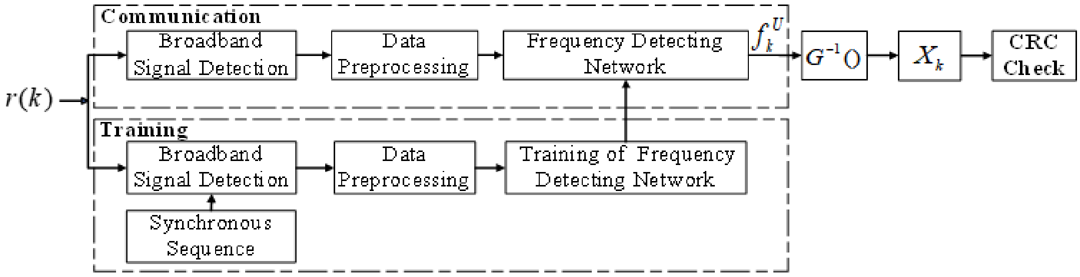

Fig. 4. IDFH Receiver Framework

The specific receiving process of IDFH is shown in **Fig. 4**. Due to the dynamic change of jamming signal, we add a training stage to learn the change rule, so the received user signal has two stages: training stage and communication stage. Since these two stages are in the same communication process, the way to generate differential frequency hopping signals is the same. Similarly, the user signal is also divided into synchronous signal and communication signal. We set that the synchronous signal is pre-known, so it will be used as a training sample of the network. The details of the two stages are as follows:

(1) **Training stage:** In the training stage, we preprocess the synchronous signal so that the synchronous signal is input into the network in the form of a spectrum waterfall. Then, the network uses supervised learning to learn the rule of the jamming in the spectrum waterfall. Specifically, when in the training stage, the user 's frequency point at each moment is clear, but the received signal may contain a composite signal in which the user signal and the jamming signal coexist. The neural network is mainly used to extract the correlation between the characteristics of the composite signal and the frequency of the user signal. These correlations include the reaction time required for jamming and the spectrum pattern of jamming. When the training converges, in the communication stage, the user 's communication frequency can be determined according to the correlation extracted in the training stage and the currently received composite signal, thereby achieving jamming utilization. Finally, we load the trained network into the communication stage.

(2) **Communication stage:** In the communication stage, we input the received communication signal in the form of spectrum waterfall into the trained network for frequency detecting. In the detecting process, because the rule of jamming has been learned in previous training, the jamming signal can be used to improve frequency detecting performance. Finally, the frequency point information is input to $G^{-1}()$ to obtain the bit information.

4.2 Data Preprocessing

It is worth noting that since the signal is input into the network in the form of a spectrum waterfall, we also need to preprocess the signal. The process is shown in (3), (4) and (5). In practice, we obtain s_k^m by discrete Fourier transform (DFT), which is shown in (3), where $m_{index} = \frac{m \cdot N}{f_s}$ is the index of the DFT result with frequency m, N is the number of sampling points and f_s is the sampling frequency. Then we can get the spectrum waterfall by superimposing and combining the DFT results of multiple continuous time points, which are shown in (4) and (5). After the data preprocessing process, we input $\mathbf{S}_k$ into the network in the form of the thermodynamic diagram for training.

$$s_k^m = x[m_{index}] = \sum_{n=0}^{N-1} x[n] \cdot e^{-j\frac{2\pi}{N} m_{index} n} \tag{3}$$

$$\mathbf{s}_k = (s_k^1, s_k^2, s_k^3, \ldots, s_k^m) \tag{4}$$

$$\mathbf{S}_k = \begin{bmatrix} \mathbf{s}_{k-1} \\ \mathbf{s}_{k-2} \\ \vdots \\ \mathbf{s}_{k-L} \end{bmatrix} = \begin{bmatrix} s_{k-1}^1 & s_{k-1}^2 & \cdots & s_{k-1}^m \\ s_{k-2}^1 & s_{k-2}^2 & \cdots & s_{k-2}^m \\ \vdots & \vdots & \vdots & \vdots \\ s_{k-L}^1 & s_{k-L}^2 & \cdots & s_{k-L}^m \end{bmatrix} \tag{5}$$

4.3 Frequency Detecting Network

With the development of computer and artificial intelligence technology, pattern recognition is applied more and more widely. In this paper, the spectrum waterfall contains the time-frequency information of the environment, so we input the spectrum waterfall into the network for frequency detection. In this regard, the frequency-detecting problem can be transformed into a supervised classification problem in pattern recognition. Specifically, because the synchronization signal and its frequency are pre-known in the training stage, we use the spectrum waterfall map corresponding to different frequencies as a category and use the supervised learning method for classification training. After completing the training, in the communication stage, the current communication frequency can be determined by classifying the current spectrum waterfall of the communication signal. In summary, by changing the problem, we can use the neural network to complete the frequency detection work and effectively use the learned jamming information.

4.3.1 Network Structure Design and Parameter Update Method

Table 2. Network Structure

Layer	Parameter
Input	Input Size:150×150×3
Conv2D	8filters(activation: ReLU), Kernel Size:3×3(stride:1)
Pooling	Max Pooling, Kernel Size:2×2(stride:2)

FC	128(activation: ReLU)
Dropout	Probability:0.2
FC	64(activation: ReLU)
Dropout	Probability:0.2
Output	32

The model structure is shown in **Table 2**. Since the input information needs to be processed in real time in actual communication, we refer to and improve the structure proposed in [33] to further reduce the number of network parameters. The network structure is similar to the Le-Net5 model. Since we mentioned that the frequency detection problem is transformed into a multi-classification problem in pattern recognition. Therefore, the loss function used in this paper is Cross-Entropy loss function, and its expression is shown in (6)

$$Loss(\hat{y}, y) = -\sum_{i=1}^{M} y_i \log(\hat{y}_i) \tag{6}$$

In (6), M is the total number of categories of spectrum waterfalls. $\hat{y}$ is the frequency point prediction value of the input spectrum waterfall $\mathbf{S}_k$ and y is the true frequency point label value. y_i represents the probability of the category corresponding i to the true label and $\hat{y}_i$ represents the probability of predicting the corresponding category i .According to the [34], the optimization goal of this paper is (7).

$$Min(Loss(\hat{y}, y)) = -Min\sum_{i=1}^{M} y_i \log(\hat{y}_i) \tag{7}$$

Based on the above settings, the weight update used in this paper is shown in (8), where η is the learning rate and w is the model parameter.

$$\mathrm{w}_{t+1} = \mathrm{w}_t - \eta \frac{\partial(Loss)}{\partial(\mathrm{w}_t)} \tag{8}$$

4.3.2 Training and Communication Process

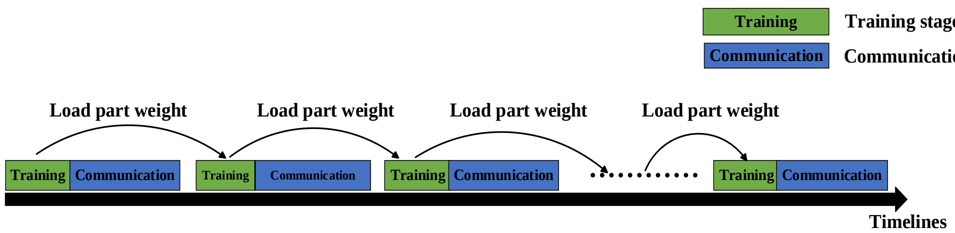

Fig. 5. Learning Strategy

Due to the dynamic change in the communication environment, in order to learn the rule of jamming more effectively, we adopt the learning strategy of online learning, that is, the network is trained at each communication cycle. At the same time, based on our analysis, the weights of the convolution layer are relatively stable as it only extracts the basic time-frequency characteristics of jamming and user signals. Therefore, we refer to the transfer learning method in [35] and only update the weights of the full connection layer, which can not only deal with the dynamic characteristics of jamming, but also reduce the operational complexity of all parameter updates.The FLOPs of the model proposed in this paper is 1.08×10^{7}, and the total FLOPs required for the model to iterate 50 epochs is 6.91×10^{11}.The GPU used in the experimental environment is NVIDIA GeForce RTX 3060 Ti, and its floating-point computing performance per second is 16.2×10^{12}, so it can meet the real-time requirements of online learning in the communication process.

As described in the communication framework, we first generate information bits and corresponding frequency hopping signals. Since the training signal is known in advance, we can know the training hops and receive the training signal. Then, the signal is formatted into a spectrum waterfall through data preprocessing, and the spectrum waterfall is divided into training set and test set to train the network. After training, the change rule of jamming can be learned. Because the training time is known, the time of receiving the communication signal can also be determined. Similarly, we use the trained network to classify the spectral waterfall of the communication signal, i.e., frequency detection, and obtain the bit information based on the frequency information. Finally, to further understand the jamming pattern, the bit information is checked with Cyclic redundancy check (CRC). If the CRC check is passed, the frequency detection result can be used as a training sample for the next communication. The details of the proposed algorithm are summarized in **Algorithm 1**.

Algorithm 1: Intelligent differential frequency hopping (IDFH)

Notation:

S_T : Training signal matrix

S_C : Communication signal matrix

H_T : The hops number of training

H_C : The hops number of communication

Start Communication
    Generate differential frequency hopping signal
    Start training stage
      IF hops $\leq$ H_T
          S_T = Receiving signal S_t
      END
      Spectrum Waterfall (**SW**) = Preprocess S_T
      Start network training
      End network training
    End training stage
    Start communication stage
      IF hop $\leq$ H_C
          S_C =Receiving signal S_c

14: **END**
15: Spectrum Waterfall (**SW**) = Preprocess S_C
16: Frequency Sequence = Network Classify(**SW**)
17: Communication bit $= G^{-1}$(Frequency Sequence)
18: End communication stage
19: **CRC** checks the communication bits.
20: **IF CRC** check is pass
21: The classified results are added to the training set for the next communication.
22: **END**
23: **End Communication**

5. Simulation Results and Analysis

5.1 Simulation Environment and Parameter Configuration

In the simulation part, we verify the anti-jamming performance of the IDFH system and compare the bit error rate(BER) performance of the IDFH, DFH proposed in [32], EDFH proposed in [17], Conv-DFH proposed in [28], CS-DFH proposed in [29] and LEC-DFH proposed in [30] under the same environment. The user and the jammer compete in a 20 MHz frequency band in our simulation scenario. There are $M = 32$ available hopping frequencies, and the user's signal bandwidth at each hopping frequency is set to 0.6 MHz. The modulation factor is 4 (2 bits per hop), and the hopping rate is 5000 hops/s. There are 5120 bits of training data and 20480 bits of communication data, so the hopping frequency numbers during training and communication procedures are 2560 and 10240, respectively. The mode of jamming is set to reactive jamming. As mentioned earlier, EDFH requires a certain precondition that the user signal and the jamming signal are uncorrelated, we also design the corresponding simulation to verify the improvement of IDFH in this aspect.

5.2 Network Training Parameters

Table 3. Model Training Parameters

Parameter name	Parameter value	Parameter name	Parameter value
Image Size	150×150×3	Optimizer	Stochastic Gradient Descent
Total Number of Samples	2560	Learning Rate	0.03
Training Sample Number	1280	Loss Function	Categorical
Test Sample Number	1280	Batch Number	32

The model training parameters set in this paper are shown in **Table 3**. In order to illustrate that the frequency point recognition network can meet the use in the communication environment, we set the signal-to-noise ratio (SNR) to 0 and the jamming-to-signal ratio (JSR) to 0. The training process is shown in **Fig. 6**. The training results show that the recognition accuracy of the network can meet the communication requirements in the case of small sample training.

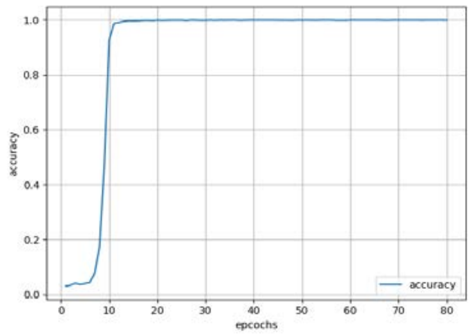

Fig. 6. Training accuracy function curve

5.3 Analysis of Simulation Results

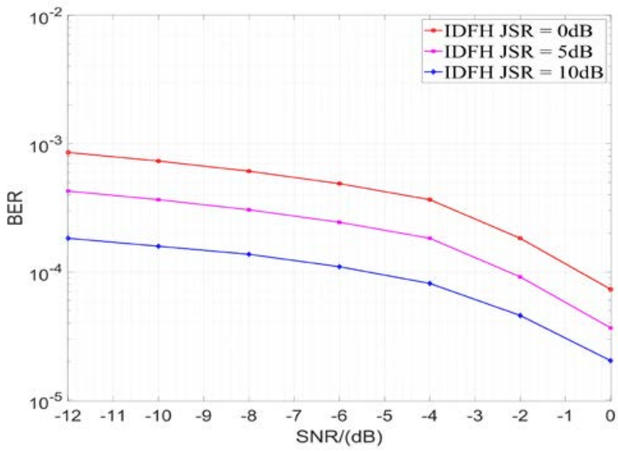

Fig. 7. The BER performance of the IDFH under different SNR

Due to the decrease in SNR, the information that the network can learn from the spectrum waterfall will decrease. In this paper, the BER performance of IDFH is analyzed by setting three kinds of JSR in the case of decreasing SNR. In the simulation, we analyze the performance of $\text{SNR} = \{-12,-10,-8,-6,-4,-2,0\}$ under different $\text{JSR} = \{0,5,10\}$. The simulation results are shown in **Fig. 7**. It can be seen from **Fig. 7** that under the same JSR, the BER performance of the system will decrease with the decrease of SNR. This is because with the decrease of SNR, it is more difficult for IDFH to learn the jamming information from the spectrum waterfall, which affects the efficiency of jamming utilization. From the **Fig. 7**, we can also see that in the same JSR case, for every 2 dB increase in SNR, the BER performance can be improved by about 1.5 dB.

In addition, we can also see from **Fig. 7** that in the case of low SNR, when the jamming power increases, it is more conducive to IDFH communication. This paper also designs the corresponding simulation analysis to illustrate. In the simulation, we analyze the performance of $\text{SNR}=\{0,-5,-10\}$ under different $\text{JSR}=\{11,9,7,5,3,1,-1,-3,-5\}$. The simulation results are shown in **Fig. 8**.

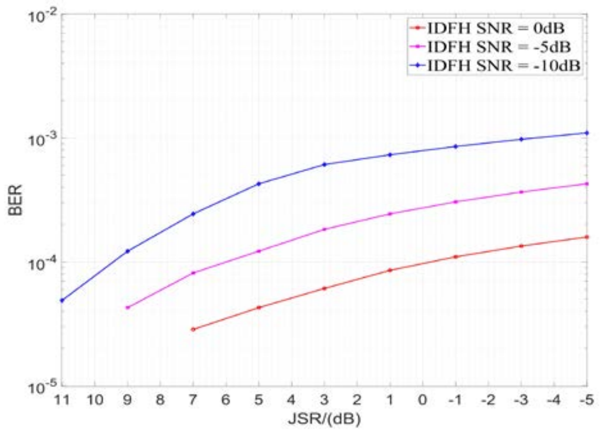

Fig. 8. The BER performance of the IDFH under different JSR

It can be seen from **Fig. 8** that under the same SNR, the BER performance of the system will increase with the increase of JSR. This is because with the increase of JSR, the characteristics of jamming information in the spectrum waterfall diagram are more obvious, which can help users learn more jamming information under the same SNR and improve the efficiency of jamming utilization. Similarly, this improvement is more obvious in the case of low SNR. We can see that when $SNR=0$, every 2 dB increase in JSR will increase the BER performance by 1.7 dB, and when $SNR=-10$, every 2 dB increase in JSR will increase the BER performance by nearly 2.3 dB.

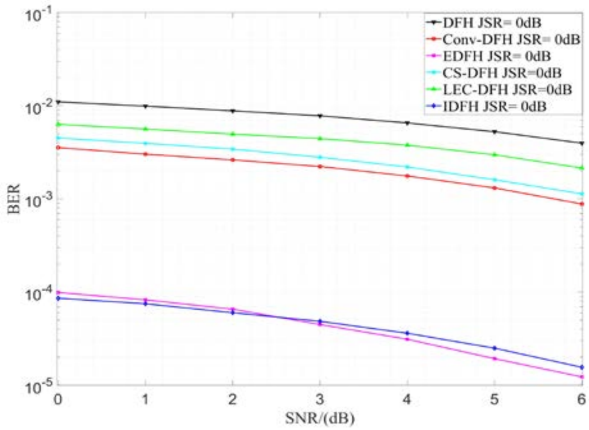

Fig. 9. Signals are uncorrelated under different SNR

As mentioned previously, EDFH requires certain preconditions, that is, the jamming signal is uncorrelated with the jamming signal. To illustrate the improvement of IDFH in this respect, we simulate and analyze the performance of all DFH systems when the two signals are uncorrelated. We test in an environment with $JSR=0$ and $SNR=\{0,1,2,3,4,5,6\}$, the simulation results are shown in **Fig. 9**.

As can be seen from **Fig. 9**, in this environment, the traditional DFH cannot effectively combat the jamming. For LEC-DFH and Conv-DFH, although some frequency decision errors can be corrected by error correction algorithm, when there are many continuous multi-hop frequency decision errors, their error correction ability still cannot meet the demand, and the BER performance of the system decreases. For CS-DFH, although the BER performance of the system is improved by increasing the coding efficiency, the presence of jamming signals will also seriously affect the system's performance. Unlike the above four DFH systems based on the idea of anti-jamming, IDFH and EDFH, based on the idea of jamming utilization, can effectively realize jamming utilization in this environment. Therefore, both of them have good performance and close performance. From **Fig. 9**, we can also see that in the same JSR case, when $\mathrm{SNR}=0$, IDFH and EDFH have BER gains close to 20 dB, 17 dB, 16 dB and 15 dB compared with traditional DFH, LEC-DFH, CS-DFH and Conv-DFH, respectively. When $\mathrm{SNR}=6$, they have BER gains of 24 dB, 21 dB, 18 dB and 17 dB, respectively.

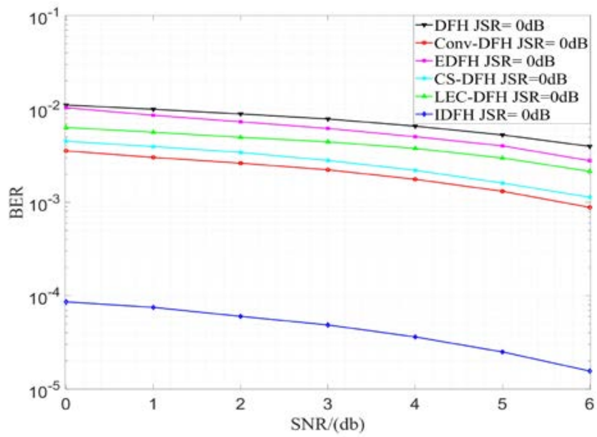

Fig. 10. Signals are correlated under different SNR

It is worth noticing that when the jamming signal is correlated to the user signal, the system of EDFH will be affected, as shown in **Fig. 10**. As can be seen from **Fig. 10**, because EDFH is challenging to separate these two signals, it is difficult to achieve jamming utilization, resulting in system performance degradation and similar to traditional DFH. Although it is also based on the idea of jamming utilization, the jamming utilization method of IDFH is not limited to the jamming waveform. It can still maintain good performance in this case. The results of **Fig. 9** and **Fig. 10** also show that under the same JSR, the BER performance of all DFH systems increases with the increase of SNR, because the noise in the environment will affect the quality of the received signal.

Then, we set all DFH systems to perform performance analysis under the same SNR and different JSR. We test in an environment with $\mathrm{SNR}=0$ under $\mathrm{JSR}=\{0,1,2,3,4,5,6\}$, The simulation results are shown in **Fig. 11** and **Fig. 12**.

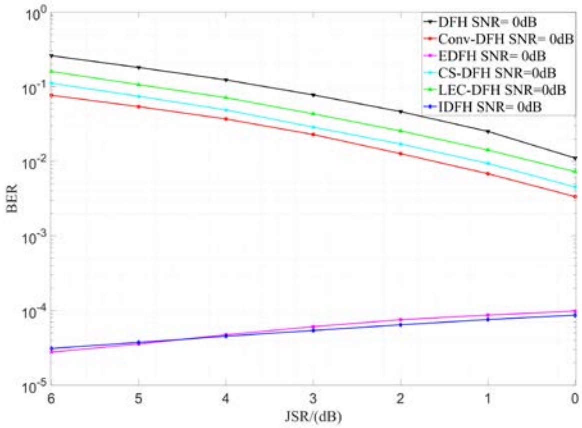

Fig. 11. Signals are uncorrelated under different JSR

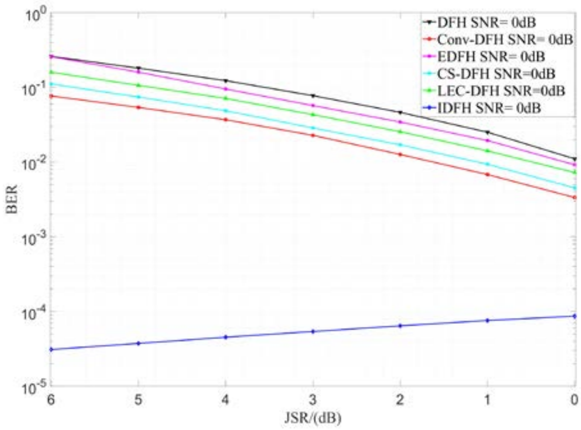

Fig. 12. Signals are correlated under different JSR

Fig. 11 is the system performance analysis that the jamming signal is uncorrelated to the user signal. In this environment, IDFH and EDFH can achieve anti-jamming communication through jamming utilization, and their performance is still relatively close. Under the same SNR, the BER performance of the system will increase with JSR every 1 dB, there will be an increase of nearly 0.85 dB. For traditional DFH, LEC-DFH, CS-DFH and Conv-DFH, although the decrease of jamming power benefits anti-jamming, it is still seriously affected by the jamming signal. The BER performance will decrease by 1.85 dB, 1.92 dB, 1.95 dB and 1.98 dB with each 1 dB increase of JSR. In addition, the BER improvement of IDFH and EDFH systems compared with the other four DFH systems will be more obvious with the improvement of JSR. When $JSR = 0$, IDFH and EDFH have 20 dB, 17 dB, 16 dB and 15 dB BER gains compared with traditional DFH, LEC-DFH, CS-DFH and Conv-DFH, respectively. When $JSR = 6$, they are 38 dB, 37 dB, 35 dB and 34dB, respectively. **Fig. 12** shows the system performance analysis that correlates the jamming signal to the user signal. In this environment, IDFH can still maintain performance. Because the jamming signal is difficult to separate from the user signal, the performance of EDFH is degraded, and the overall performance is similar to the DFH. The results of **Fig. 11** and **Fig. 12** show that under the same SNR, although the performance of DFH, CS-DFH, Conv-DFH, and LEC-DFH increases with the decrease of JSR, it will still be affected by the jammer, and the difference in BER performance with EDFH and IDFH will become more obvious with the increase of JSR. The performance of EDFH and IDFH will increase with the increase of JSR, indicating that the greater the jamming power, the more favorable it is for communication.

Analyzing the above simulation results, the performance of all DFH systems is affected by the SNR.For IDFH and EDFH, because the jamming utilization, the greater the received jamming signal power, the better the system performance, but EDFH requires certain conditions. For DFH, CS-DFH, LEC-DFH and Conv-DFH, they are all based on the idea of anti-jamming, any power jamming signal is an unfavorable factor and will affect the performance of the communication system. In addition, by comparing the simulation results of changing the JSR and the SNR, it can be seen that the influence of the jamming signal on the system is more obvious than the noise. Consequently, IDFH is a better choice for more complex reactive jamming.

6. Conclusion

This paper proposes a jamming utilization method combined with deep learning and designs an intelligent differential frequency hopping (IDFH) framework based on this method. Different from the existing jamming utilization methods, in the training stage, the framework learns the rule of jamming in the spectrum waterfall through the training signal, and in the communication stage, the learned rule can be used to improve the frequency detection performance, thereby achieving jamming utilization. Finally, the performance of IDFH under different parameter jamming environments is simulated and compared with other improved DFH frameworks. The simulation results show that the performance of IDFH increases with the increase of jamming power, and IDFH has the best performance compared with other improved DFH frameworks. In addition, IDFH does not require certain preconditions, which simplifies the processing of communication signals and ensures the communication quality in low SNR environment.

References

[1] H. Xu, Y. Cheng and P. Wang, “Jamming Detection in Broadband Frequency Hopping Systems Based on Multi-Segment Signals Spectrum Clustering,” *IEEE Access*, vol. 9, pp. 29980-29992, February 2021. Article (CrossRef Link)

[2] V. Poirot and O. Landsiedel, “eAFH: Informed Exploration for Adaptive Frequency Hopping in Bluetooth Low Energy,” in *Proc. of 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 1-8, September 2022. Article (CrossRef Link)

[3] X. Wang, J. Wang, Y. Xu, J. Chen, L. Jia, X. Liu and Y. Yang, “Dynamic Spectrum Anti-Jamming Communications: Challenges and Opportunities,” *IEEE Communications Magazine*, vol. 58, no. 2, pp. 79-85, February 2020. Article (CrossRef Link)

[4] Y. Xu, G. Ren, J. Chen, Y. Luo, L. Jia, X. Liu and Y. Yang, “A One-Leader Multi-Follower Bayesian-Stackelberg Game for Anti-Jamming Transmission in UAV Communication Networks,” *IEEE Access*, vol. 6, pp. 21697-21709, April 2018. Article (CrossRef Link)

[5] Y. Zhang, Y. Xu, Y. Xu, Y. Yang, Y. Luo, Q. Wu and X. Liu, “A Multi-Leader One-Follower Stackelberg Game Approach for Cooperative Anti-Jamming: No Pains, No Gains,” *IEEE Communications Letters*, vol. 22, no. 8, pp. 1680-1683, August 2018. Article (CrossRef Link)

[6] F. Yao and L. Jia, “A Collaborative Multi-Agent Reinforcement Learning Anti-Jamming Algorithm in Wireless Networks,” *IEEE Wireless Communications Letters*, vol. 8, no. 4, pp. 1024-1027, August 2019. Article (CrossRef Link)

[7] J. Geng, B. Jiu, K. Li, Y. Zhao and H. Liu, "Reinforcement Learning Based Radar Anti-Jamming Strategy Design against a Non-Stationary Jammer," in *Proc. of 2022 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*, pp. 1-5, December 2022. Article (CrossRef Link)
[8] Q. Zhou, Y. Niu, P. Xiang and Y. Li, "Intra-Domain Knowledge Reuse Assisted Reinforcement Learning for Fast Anti-Jamming Communication," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 4707-4720, June 2023. Article (CrossRef Link)
[9] X. Li, J. Chen, X. Ling and T. Wu, "Deep Reinforcement Learning-Based Anti-Jamming Algorithm Using Dual Action Network," *IEEE Transactions on Wireless Communications*, vol. 22, no. 7, pp. 4625-4637, July 2023. Article (CrossRef Link)
[10] X. Liu, Y. Xu, L. Jia, Q. Wu and Alagan Anpalagan, "Anti-Jamming Communications Using Spectrum Waterfall: A Deep Reinforcement Learning Approach," *IEEE Communications Letters*, vol. 22, no. 5, pp. 998-1001, May 2018. Article (CrossRef Link)
[11] W. Li, Y. Qin, Z. Feng, H. Han, J. Chen and Y. Xu, ""Advancing Secretly by an Unknown Path": A Reinforcement Learning-Based Hidden Strategy for Combating Intelligent Reactive Jammer," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1320-1324, July 2022. Article (CrossRef Link)
[12] J. Guo, N. Zhao, F. R. Yu, X. Liu and V. C. M. Leung, "Exploiting Adversarial Jamming Signals for Energy Harvesting in Interference Networks," *IEEE Transactions on Wireless Communications*, vol. 16, no. 2, pp. 1267-1280, February 2017. Article (CrossRef Link)
[13] N. Van Huynh, D. N. Nguyen, D. T. Hoang and Eryk Dutkiewicz, ""Jam Me If You Can": Defeating Jammer With Deep Dueling Neural Network Architecture and Ambient Backscattering Augmented Communications," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 11, pp. 2603-2620, Nov 2019. Article (CrossRef Link)
[14] D. T. Hoang, D.T. Nguyen, M.A. Alsheikh, S. Gong, Eryk Dutkiewicz, Dusit Niyato and Z. Han, ""Borrowing Arrows with Thatched Boats": The Art of Defeating Reactive Jammers in IoT Networks," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 79-87, June 2020. Article (CrossRef Link)
[15] N. Van Huynh, D. N. Nguyen, D. Thai Hoang, E. Dutkiewicz and M. Mueck, "Ambient Backscatter: A Novel Method to Defend Jamming Attacks for Wireless Networks," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 175-178, February 2020. Article (CrossRef Link)
[16] N. Van Huynh, D. N. Nguyen, D. T. Hoang, T. X. Vu, E. Dutkiewicz and S. Chatzinotas, "Defeating Super-Reactive Jammers With Deception Strategy: Modeling, Signal Detection, and Performance Analysis," *IEEE Transactions on Wireless Communications*, vol. 21, no. 9, pp. 7374-7390, September 2022. Article (CrossRef Link)
[17] X. Liu, L. Chen, C. Yao, M. Wang and X. Song, "Novel anti-jamming system for enhanced differential frequency hopping," *Application Research of Computers*, vol. 39, no. 6, pp. 1820-1824, June 2022. Article (CrossRef Link)
[18] M. Lichtman, M. T. Vondal, T. C. Clancy and J. H. Reed, "Antifragile Communications," *IEEE Systems Journal*, vol. 12, no. 1, pp. 659-670, March 2018. Article (CrossRef Link)
[19] S. Fang, Y. Liu and P. Ning, "Wireless Communications under Broadband Reactive Jamming Attacks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 394-408, 1 May-June 2016. Article (CrossRef Link)
[20] J. Ma, Q. Li, Z. Liu, L. Du, H. Chen and N. Ansari, "Jamming Modulation: An Active Anti-Jamming Scheme," *IEEE Transactions on Wireless Communications*, vol. 22, no. 4, pp. 2730-2743, April 2023. Article (CrossRef Link)
[21] Y. Xu, Y. Xu, X. Dong, G. Ren, J. Chen, X. Wang, L. Jia and L. Ruan, "Convert Harm Into Benefit: A Coordination-Learning Based Dynamic Spectrum Anti-Jamming Approach," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 13018-13032, November 2020. Article (CrossRef Link)
[22] R. Di Pietro, G. Oligeri and P. Tedeschi, "JAM-ME: Exploiting Jamming to Accomplish Drone Mission," in *Proc. of 2019 IEEE Conference on Communications and Network Security (CNS)*, pp. 1-9, June 2019. Article (CrossRef Link)

[23] X. Ning, P. Jing, Z. Wang and G. Sun, "G-Function construction method based on iterative decomposition in differential frequency hopping system," *Journal of Harbin Engineering University*, vol. 44, no. 5, pp. 876-883, March 2023. Article (CrossRef Link)
[24] Q. Bao, B. Wang and F. Gao, "A New Differential Frequency Hopping Scheme based on Encryption Algorithm," *Study on Optical Communications*, vol. 4, no. 4, pp. 74-78, August 2017. Article (CrossRef Link)
[25] R. Chen, J. Shi, L. Yang, Z. Li and L. Guan, "High-Security Sequence Design for Differential Frequency Hopping Systems," *IEEE Systems Journal*, vol.15, no.4, pp. 4895-4906, December 2021. Article (CrossRef Link)
[26] Y. Ai and Y. Li, "A New Differential Frequency Hopping Scheme based on Chaotic Encryption Algorithm," *Study on Optical Communications*, no. 4, pp. 69-72, February 2022. Article (CrossRef Link)
[27] B. Qian, L. Zhang, Y. Feng and S. Sun, "Research on the method of separating differential frequency hopping signal based on JADE," in *Proc. of 2014 IEEE 5th International Conference on Software Engineering and Service Science*, pp. 736-739, June 2014. Article (CrossRef Link)
[28] Y. Zhu, L. Gan and J. Guo, "Performance of convolutionally coded differential frequency hopping systems in partial-band jamming," *Journal on Communications*, vol. 30, no. 12, pp. 85-92, December 2009. Article (CrossRef Link)
[29] B. Dong, P. Tang et al, "Performance of a Compressed Spectrum Differential Frequency Hopping Signal over Rician Fading Channel," *Journal of Electronics & Information Technology*, vol. 37, no. 4, pp. 836-840, April 2015. Article (CrossRef Link)
[30] X. Ning, P. Jin and Z. Sun, "Sequence Detection Algorithm Based on Local Error Correction in Differential Frequency Hopping System," in *Proc. of 2021 IEEE 4th International Conference on Electronics and Communication Engineering (ICECE)*, pp. 266-270, December 2021. Article (CrossRef Link)
[31] Y. Teng, Y. Feng, "An Efficiency Analysis of Differential Frequency Hopping Communication Anti-jamming," *Fire Control & Command Control*, vol. 37, no. 1, pp. 11-15, January 2012. Article (CrossRef Link)
[32] S. Xie and B. Qian, "Performance analysis of Differential Frequency Hopping Communication system over Rician channel," in *Proc. of 2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)*, pp. 1015-1019, December 2018. Article (CrossRef Link)
[33] Y. Cai, K. Shi, F. Song, Y. Xu, X. Wang and H. Luan, "Jamming Pattern Recognition Using Spectrum Waterfall: A Deep Learning Method," in *Proc. of 2019 IEEE 5th International Conference on Computer and Communications (ICCC)*, pp. 2113-2117, December 2019. Article (CrossRef Link)
[34] Zhang. X, "Structural Risk Minimization," in *Encyclopedia of Machine Learning and Data Mining Boston*, MA, USA: Springer, 2017, pp. 1200–1201. Article (CrossRef Link)
[35] J. Zhu, A. Wang, W. Wu, Z. Zhao, Y. Xu, R. Lei, K. Yue, "Deep-Learning-Based Recovery of Frequency-Hopping Sequences for Anti-Jamming Applications," *Electronics*, vol.12, no.3, pp. 496, January 2023. Article (CrossRef Link)

Xin Liu received his B.S. degree in Communications Engineering, M.S. degree in Communications and Information Systems, and Ph.D. degree from PLA University of Science and Technology, in 2004, 2008 and 2011 respectively. He has been with College of Information Science and Engineering, Guilin University of Technology since 2017, and currently as an Associate Professor. His research interests focus on anti-jamming communication, deep reinforcement learning and game theory.

Mingcong Zeng received the B.S degree in Communication Engineering from Guilin University of Technology, in 2021. He is currently a master's student in Computer Technology at Guilin University of Technology. His current research interests include jamming utilization, deep learning and anti-jamming communication.

Yarong Liu is currently the Director of the Department of Communication Engineering, School of Information Science and Engineering, Guilin University of Technology. He presided over or completed more than 10 scientific research projects at the provincial and ministerial levels with the main participants, published more than 20 papers with the first author, and authorized 9 invention patents with the first inventor.

Mei Wang received the B.S., M.S., and Ph.D. degree from Xidian University, Xi'an, China, in 1984, 1989, and 2003 respectively. She is currently a Ph.D. Tutor with Xidian University and the Guilin University of Electronic Technology. She has published more than 50 research articles in correlative journals and conferences. Her research interests include localization awareness and co-location, sensor networks, energy efficiency optimization and more.

Xiyu Song received her Bachelor's degree in electronic and communication engineering, Master's degree in physical and electronics, and Ph.D. degree in information and communication engineering from Guilin University of Electronic Technology, Guangxi, China, in 2007, 2011 and 2020, respectively. Her research interests are on robot audition, array signal processing and acoustic scene analysis.