Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7941367, 14 pages
https://doi.org/10.1155/2022/7941367

Research Article

A Novel Approach of Protocol Behavior Identification for TDMA-Based Frequency Hopping Communication

Junyi Zhang,[1] **Mengtian Tan**,[2] **Fei Shi**,[1] **Yong Yang**,[1] **and Zhutian Yang**[3]

[1]*The 54th Research Institute of CETC, Shijiazhuang 050081, China*
[2]*School of Electronics and Information Engineering, Harbin Institute of Technology, Shenzhen 518055, China*
[3]*School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China*

Correspondence should be addressed to Yong Yang; yangyong5454@126.com

Received 14 February 2022; Revised 10 March 2022; Accepted 12 March 2022; Published 30 March 2022

Academic Editor: Mingqian Liu

Frequency hopping (FH) communication technology is adopted widely in military and civil fields, due to its excellent communication characteristics such as antisearch and anti-interference. Efficient reconnaissance methods of FH communication are becoming a research hotspot. In this paper, a novel reconnaissance approach for FH communication emitters is proposed, by using the TMDA protocol behavior identification. Based on the signalling used in the TDMA protocol, the protocol behavior for FH communication can be specified. These behaviors are usually used for the process controlling of FH communication and network maintenance. Therefore, recognition of FH communication protocol behaviors can be used for emitter intention reasoning indirectly. Simulation results show that the proposed approach is effective and potential for application.

1. Introduction

Frequency hopping (FH) communication is an important application of spread spectrum communication, which was widely used in both military and civil affairs [1–5]. Due to its excellent anti-interference ability, as well as its capability to increase the security of wireless services, FH has been implemented diffusely, e.g., in Bluetooth [6], advanced extremely high-frequency (AEHF) communication satellites [7], Military Strategic and Tactical Relay (MILSTAR) communication satellites [8], and emerging dynamic communication systems [9]. FH communication proves practical in various radiofrequency systems, and it is developing toward faster hopping speed and higher hopping-frequency bandwidth, which will strengthen the original advantages of FH communication in both military and civil applications.

Meanwhile, due to a wide application in military fields, the activities of FH communication emitters gradually become an important source of information in electronic reconnaissance. However, advanced FH technology has brought great challenges to electronic countermeasures. Wider bandwidths, more complex frequency variations, along with many other factors further complicate the electromagnetic spectrum, increasing the difficulty of extracting effective information. Therefore, many researchers have devoted efforts to spectrum cognition in complex electromagnetic environments [10–14]. The cognition process, which is an integral section for the awareness of complex situations, connects the perception of signals with decision making process [15–19].

Electromagnetic countermeasures in a complex electromagnetic environment necessitate not only the analysis of the signal but also the cognition of communication emitter behaviors, such as broadcast, relay, and link establishment. Specifically, various parameters of FH signals and control signalling used in protocols manifest the behavior of communication emitters. Therefore, the identification of protocol behaviors can be a novel approach information retrieval for electronic countermeasures. If the mapping relation between signals and the behavior of the FH communication emitter can be successfully established, it would provide a tremendous positive impact on future communication countermeasures. However, to our best knowledge, the research on frequency hopping communication signals mainly lies in the reconnaissance of frequency hopping communication signals, including signal detection, interception, sorting, and parameter estimation [20–23], few on the cognition of radiation source target.

Against this background, this paper proposes a new scheme for electromagnetic countermeasures based on FH communication signals, that is, through signal processing technology, according to the electromagnetic signal law formed by the radiation source target performing specific functions, the behavior and related task information of the radiation source target can be recognized. The proposed method solves two main problems, i.e., the positioning of the signalling signal and the identification of the signalling signal, by using noncooperative signal blind demodulation and machine learning.

The rest of this paper is organized as follows. Section 2 presents the system model. Section 3 introduces the positioning of the signalling signal. Section 4 presents the recognition of the radiation source target behavior, followed by performance evaluation in Section 5. Finally, Section 6 concludes this paper.

2. System Model

In this research, we propose a new scheme for communication emitter reconnaissance. We consider a frequency hopping communication system in the VHF band. There are two important models to be built in the system. One is the time frame sequence model of FH communication. The other is the radiation source target model of FH communication.

The time frame sequence model of FH communication is built based on the TDMA communication protocol, which is complete, representative, and widely used in many kinds of frequency hopping communication equipment, such as frequency hopping radio. Besides, the method proposed in this paper is generalizable to recognition under other protocols. Therefore, it is assumed that a TDMA protocol is adopted in the FH communication system, where there exist N nodes in the network. In a super time frame (STF), each node has a time frame (TF) for transmitting, and each time frame contains 14 time slots (TS). In this protocol, the frequency hopping rate of the radio communication is 64000/105 hops/sec, namely, 64000 frequency hops within 105 seconds. The time for 40 frequency hops is defined as a time slot, and 140 bytes are transmitted within the duration of a time slot.

A time slot is divided into three parts: synchronization sequence, data, and control sequence. From the 0th to 7th hops, the Walsh synchronization sequence is transmitted, which is used for time slot synchronization. From the 8th to 37th hops, the information data sequence is transmitted for radio communication, which includes signalling sequence and voice data sequence. Within the last 2 hops, the control sequence is transmitted, which is used for transmit-receive switching, information proofreading and protection.

The time slot types in a time frame are generally divided into three types: fixed time slot type (fixed slot (FS)), static time slot type (static slot (SS)), and dynamic time slot type (dynamic slot (DS)). The fixed time slot type refers to the time slot that is permanently occupied by a certain node. Generally, the first time slot of a frame is the fixed time slot fixedly occupied by the central node. The static time slots refer to the time slots that are fixedly allocated to certain nodes in a time frame. The allocation of the static time slots in different time frames is different. The dynamic time slots refer to the time slots that can be reserved and occupied by any node, that is, the occupancy of time slots is dynamically allocated. The allocation formula for static and dynamic time slots in each time frame is as follows:

Static time slots (SS):

$$P_{\mathrm{id}} = (5F_{\mathrm{id}} + \mathrm{SS}_{\mathrm{id}})\%N. \tag{1}$$

Dynamic time slots (DS):

$$P_{\mathrm{id}} = \left[N\frac{(7-5D_{\mathrm{id}})\%8}{8} + F_{\mathrm{id}}\right]\%N, \tag{2}$$

where P_{id} denotes the time slot number; F_{id} denotes the time frame number in a superframe, and the value is $0, 1, 2..N-1$; SS_{id} denotes the static time slot number in a time frame, and the value is $0, 1 \ldots 4$; N denotes the number of nodes in the network; and D_{id} denotes the dynamic time slot number in a time frame, and the value is $0, 1 \ldots 7$.

We assume that the protocol in this research is conflict free, where only the node with the time slot occupancy can send data in the time slot, while other nodes cannot send and can only be in the receiving state.

In order to match the encoding rate of the voice encoder in the frequency hopping radio communication system, one-way unidirectional voice data transmission needs to occupy two time slots in a time frame. Two time slots form a group, and 8 dynamic time slots are divided into 4 groups. The 4 groups are called reserved time slots, which are used to transmit voice data.

Signalling is used in the communication protocol to establish and remove communication links and transmit voice data. According to the different functions, signalling can be divided into three types: time slots reservation control signalling (AC), reservation links control signalling (RC), and voice data transmission signalling (RD). The three types of signalling include 11 specific signalling types, and each signalling has a length of 19 bits, including 8-bit long feature codes and 11-bit long signalling content. The voice transmission types in the protocol are generally divided into three types: unicast direct voice transmission, relay voice transmission, and broadcast voice transmission. Among them, unicast direct voice transmission can be divided into unicast one-way voice transmission and unicast bilateral voice transmission; relay voice transmission can be divided into relay one-way voice transmission and relay bilateral voice transmission. Each transmission type corresponds to a different signalling transfer process, which is also the theoretical basis for us to realize the target behavior recognition of the radiation source based on the signalling signal.

So far, we can achieve time-frame sequence modeling, the schematic diagram of the time-frame sequence model is shown in Figure 1.

The target modeling of the frequency hopping communication radiation source is realized based on the composition and working principle of the frequency hopping communication system. The composition and working principle of the frequency hopping communication system are shown in Figures 2 and 3.

In the transmitter, the baseband signal is digitally modulated to generate the corresponding modulation signal $m(t)$, and the frequency synthesizer is controlled by the FH sequence generator to synthesize the local oscillator signal of the corresponding frequency. The local oscillator signal $p(t)$ can be expressed as

$$p(t) = \cos\left[(\omega_0 + n\omega_\Delta)t + \varphi_n\right], \tag{3}$$

where ω_0 denotes the center frequency of transmitter and ω_Δ denotes the FH interval of the frequency synthesizer.

The modulated signal $m(t)$ is then mixed with the local oscillator signal $p(t)$ to obtain the transmitted signal $S_t(t)$ whose frequency hops with time:

$$s_t(t) = m(t)\cos\left[(\omega_0 + n\omega_\Delta)t + \varphi_n\right]. \tag{4}$$

During transmission, there are other frequency interferences $J(t)$ and noise $n(t)$ in the channel at this time, and the FH signals transmitted by other network stations in the FH communication system $s_j(t)$. Therefore, the mixed signal $s_r(t)$ that reaches the receiver part is

$$s_r(t) = s_t(t) + \sum_{j=1}^{k} s_j(t) + n(t) + J(t). \tag{5}$$

In the case of FH synchronization at the receiver part, the local oscillator frequency synthesized by the frequency synthesizer has the same hopping rule as the transmitter part and there is always an intermediate frequency difference ω_I between the local oscillator frequency at the transmitter part and the receiver part. The local oscillator frequency synchronously generated by the frequency synthesizer at the receiver part is $\omega_r + n(t)\omega_\Delta$, where ω_r is the center frequency, $\omega_I = \omega_r - \omega_0$, $n(t)$ is an integer that changes over time, and ω_Δ is the FH interval of the frequency synthesizer.

Mixing the received signal $s_r(t)$ with the local oscillator signal of the receiver $p_r(t)$ can get

$$s_p(t) = s_r(t)p_r(t) = \left[s_t(t) + \sum_{j=1}^{k} s_j(t) + n(t) + J(t)\right] \cdot \cos\left[(\omega_r(t) + n\omega_\Delta)t + \varphi_r\right]. \tag{6}$$

If the transmitting and receiving parts maintain a high degree of synchronization, the transmitted signal $s_t(t)$ is substituted into the above formula to obtain

$$\begin{aligned} s_p(t) = {} & \frac{1}{2}m(t)\left\{\cos\left(\omega_I t + \varphi_I\right) + \cos\left[(\omega_r + \omega_0 + 2n\omega_\Delta)t + \varphi_r + \varphi_n\right]\right\} \\ & + \left[\sum_{j=1}^{k} s_j(t) + n(t) + J(t)\right]\cos\left[(\omega_r(t) + n\omega_\Delta)t + \varphi_r\right]. \end{aligned} \tag{7}$$

In order to extract the intermediate frequency signal $m(t)\cos(\omega_I t + \varphi_I)$ carrying the relevant information of the modulation signal $m(t)$ in the above formula, we can use the intermediate frequency filtering method to extract the intermediate frequency signal and filter out other interference signals. Therefore, the useful signal component $s_d(t)$ obtained by intermediate frequency filtering is

$$s_d(t) = m(t)\cos\left(\omega_I t + \varphi_I\right). \tag{8}$$

Then, the intermediate frequency signal $s_d(t)$ is sent to the intermediate frequency mixer to obtain the information modulated signal $m(t)$. The modulated signal is demodulated and decoded to obtain the source information it carries.

3. Signalling Signal Location

In order to identify the behavior of the FH communication emitter, the signalling information should be extracted. Because signalling is usually used for link control, such as establishment, supervision, and teardown, the technical route of the entire implementation method is shown in Figure 4.

According to the TDMA communication protocol mentioned, the signallings are at the beginning of the time slot sequence. Therefore, in order to recognize the kind of signalling through signalling signal accurately, signalling signal location is necessary. Otherwise, the length of signal input to CNN is too long, and the recognition accuracy cannot be guaranteed. Therefore, to extract the signalling information, the signalling should be located first. Signalling location can be realized in two steps: frame length estimation and frame structure analysis. The frame structure analysis is to determine the location of signalling according to the frame length estimation result. After the location of signalling is determined, the signalling signal location is realized combining the relevant parameters of the intermediate frequency signal.

3.1. Frame Length Estimation. Frame structure analysis refers to the following: For noncooperative communication systems, through intercepted communication signals, to obtain the greatest understanding of the time frame encapsulation structure used by the communication system to transmit information. To achieve frame structure analysis of noncooperative signals, the first thing to achieve is to accurately estimate the length of the time frame.

Since most of the frame header sequences in communication systems are sequences with good autocorrelation or cross-correlation characteristics, the sequence length between two frame headers can be regarded as the length of a frame. Thereby, the autocorrelation search algorithm can be used to find the frame header sequence, and then, the length of frame can be estimated.

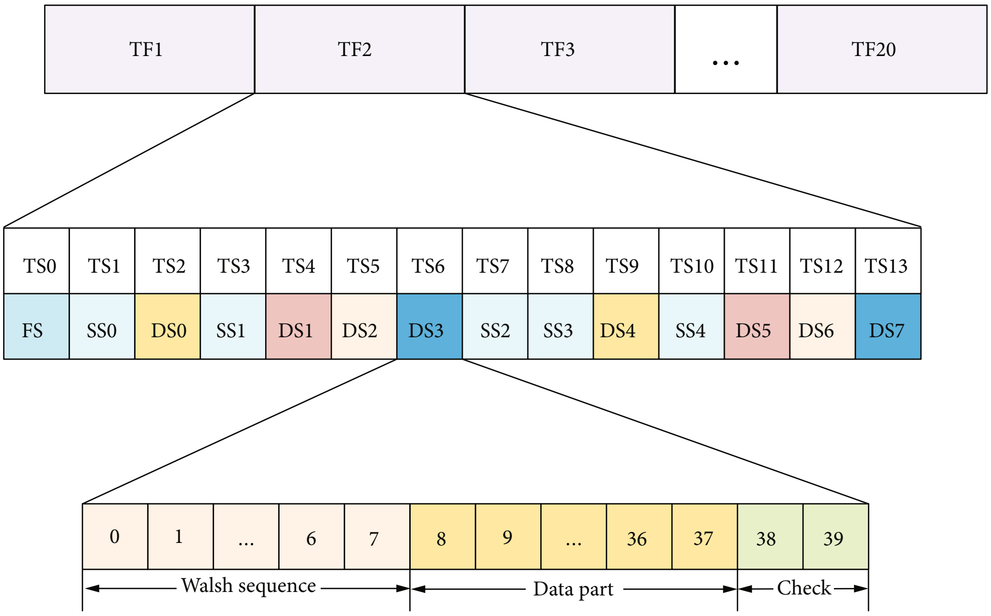

Figure 1: Schematic diagram of time frame sequence modeling.

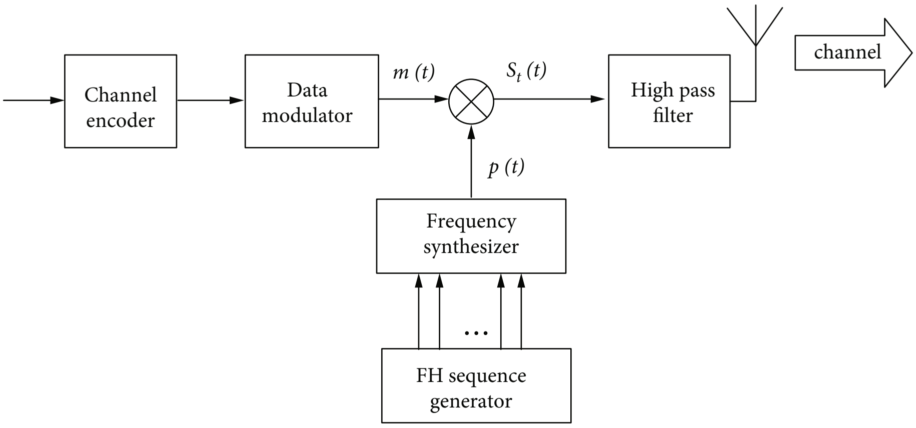

Figure 2: Transmitter part of frequency hopping communication system.

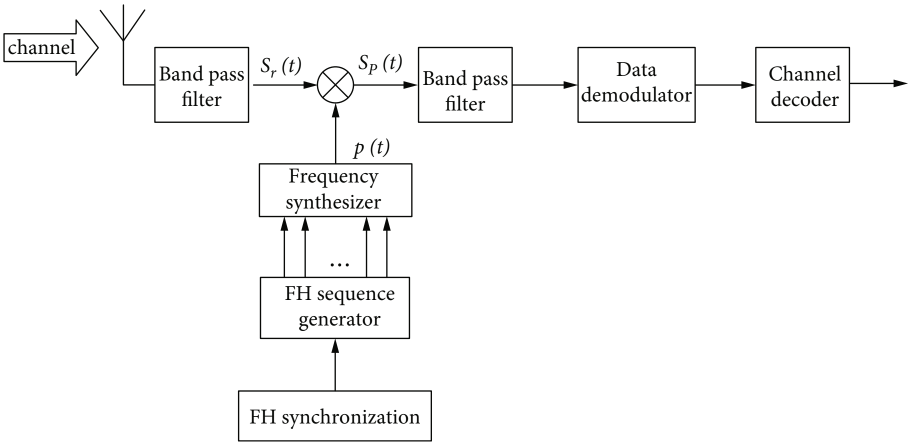

Figure 3: Receiver part of frequency hopping communication system.

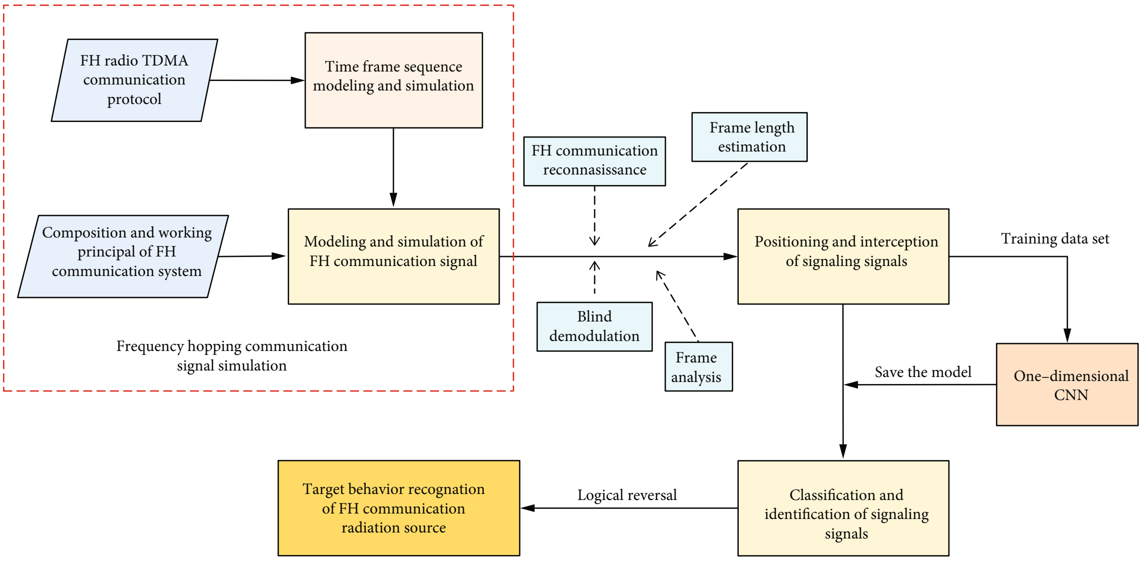
FH radio TDMA communication protocol
Time frame sequence modeling and simulation
Composition and working principal of FH communication system
Modeling and simulation of FH communication signal
Frequency hopping communication signal simulation
FH communication reconnaissance
Frame length estimation
Blind demodulation
Frame analysis
Positioning and interception of signaling signals
Training data set
One–dimensional CNN
Save the model
Classification and identification of signaling signals
Logical reversal
Target behavior recognition of FH communication radiation source

Figure 4: The technical route of the entire implementation method.

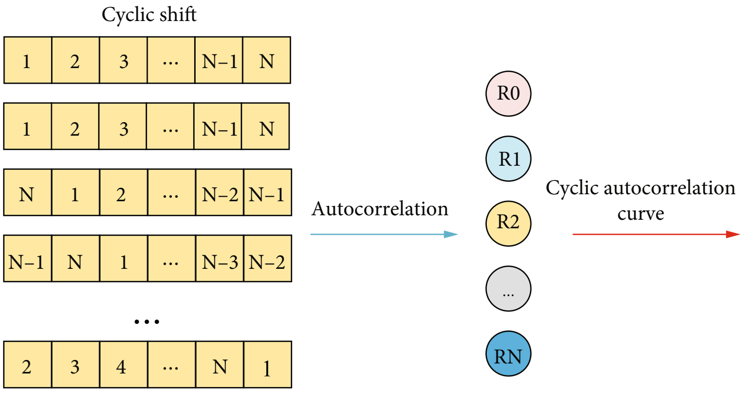

Figure 5: Schematic diagram of the frame length estimation algorithm.

In this paper, a simple and convenient estimation approach is adopted for frame length based on cyclic autocorrelation. The algorithm realization schematic diagram is shown as in Figure 5.

The input of this algorithm is the 0-1 bit stream data obtained after the noncooperative signal is demodulated, and the output is the curve corresponding to the cyclic autocorrelation result. Cyclic autocorrelation is to perform autocorrelation processing after the sequence is cyclically shifted. Because the beginning of the time frame is generally a synchronous sequence, which has good autocorrelation and cross-correlation characteristics. So, periodic spikes will appear in the cyclic autocorrelation results. The peak appearance period corresponds to the length of the time frame. So the average correlation peak distance can be calculated according to the position of correlation peak, and then, the estimation of the frame length can be realized. The corresponding formula of the frame length estimation algorithm for cyclic autocorrelation is

$$R_m(k) = x(k) \cdot x_m(k), \tag{9}$$

where $x(k)$ is the sequence of the frame length to be estimated, $x_m(k)$ is the result of m point cyclic shift of $x(k)$, $R_m(k)$ is the autocorrelation result of the sequence $x(k)$ and $x_m(k)$, and the values of m and k are $m = 0, 1, \cdots N - 1$; $k = 0, 1, \cdots N - 1$, where N is the length of the sequence.

3.2. Frame Structure Analysis.

After the frame length estimation is realized, the next step is to analyze the frame structure according to the frame length estimation result. The algorithm used is a frame structure analysis algorithm based on cumulative filtering. The basic principle of this algorithm is based on the similarity of the frame structure in each frame and the similar content of the frame header. The symbol stream data recovered by demodulation is accumulated in the unit of frame length, so as to realize the analysis of the frame structure. The schematic diagram of the algorithm principle is shown in Figure 6.

Based on the above processing steps, the length of a time frame, the number of time slots in a time frame, the length of a time slot, the position of the time slot in a time frame, and the beginning sequence length of the time slot are determined through the above processing. Based on this information

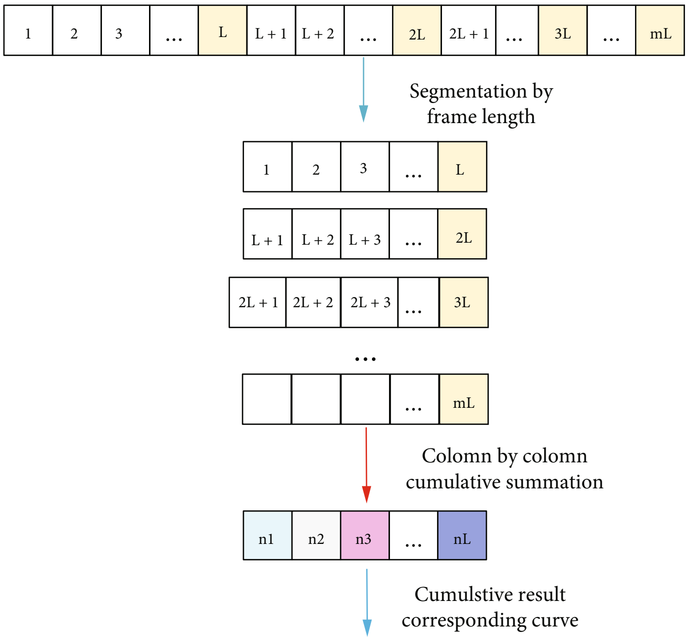
1
2
3
...
L
L + 1
L + 2
2L
2L + 1
3L
mL
Segmentation by frame length
L + 3
2L + 2
2L + 3
Colomn by colomn cumulative summation
n1
n2
n3
nL
Cumulstive result corresponding curve

Figure 6: Schematic diagram of the frame structure analysis algorithm principle.

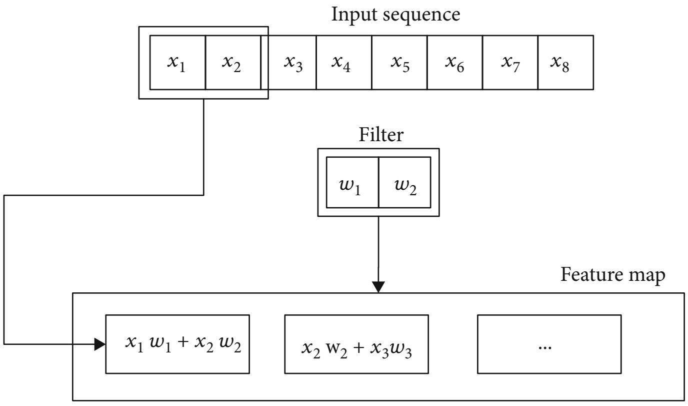

Figure 7: Basic principle of one-dimensional convolution.

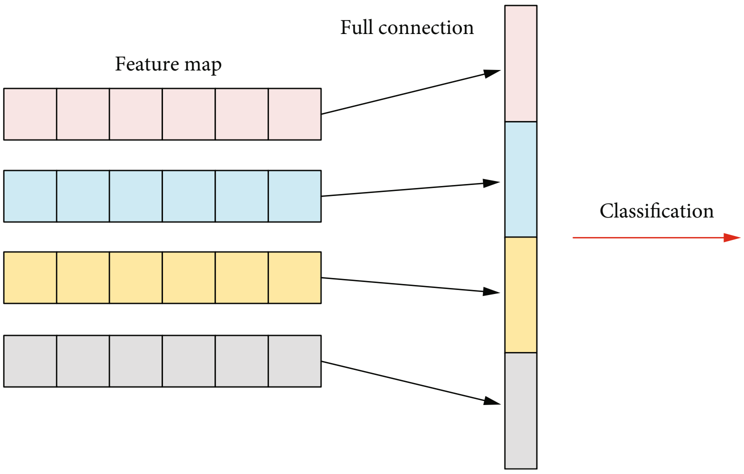

Figure 8: Principle of the flatten method.

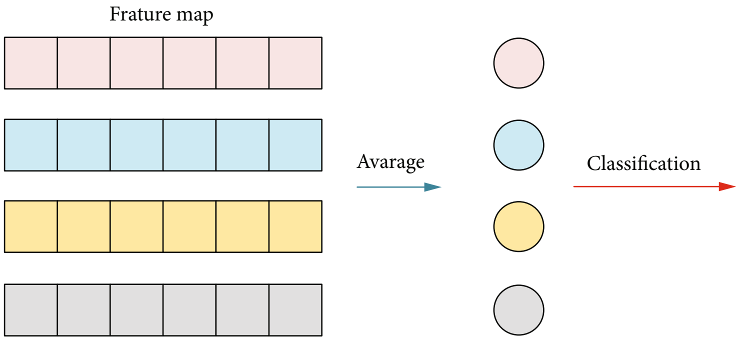

Figure 9: Principle of the global average pooling method.

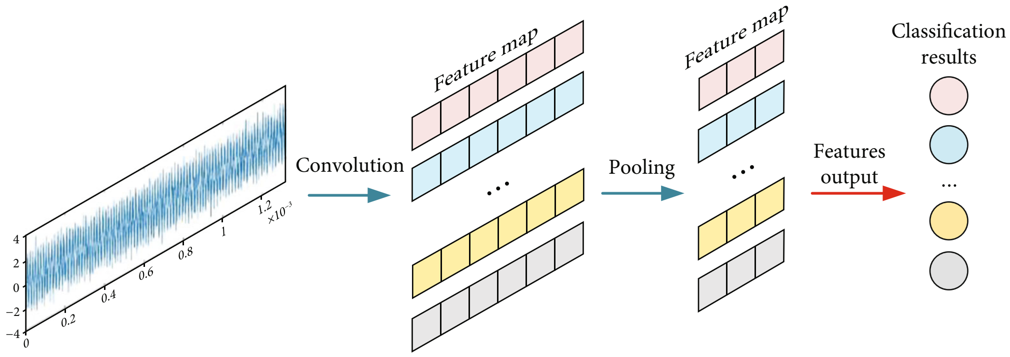

Figure 10: Schematic diagram of the one-dimensional CNN network structure.

Table 1: Structural parameters of network.

Layer	Type	Parameter	Output
1	Conv1D	(80, 10, 3)	(334, 80)
2	MaxPooling1D	(2, 2)	(167, 80)
3	Conv1D	(40, 6, 2)	(84, 40)
4	MaxPooling1D	(2, 2)	(42, 40)
5	Conv1D	(40, 3, 3)	(14, 40)
6	MaxPooling1D	(2, 2)	(7, 40)
7	Conv1D	(60, 2, 1)	(7, 60)
8	MaxPooling1D	(2, 2)	(3, 60)
9	GlobalAveragerPooling1D	—	(1, 60)
10	Dense	60	3660
11	Dense	30	1830
12	Dense	12	372

obtained, the possible position of the signalling sequence is determined, and the carrier frequency, symbol rate, and other parameters related to the signal are combined to realize the location and interception of the signalling signal in the dehopping signal.

4. Signalling Recognition

Machine learning has a good performance in many types of recognition, because it can extract features from the input training data and reduce the incompleteness caused by artificial settings. The convolutional neural network (CNN) is a widely used machine learning structure. CNN is a feed-forward neural network whose artificial neurons can respond to surrounding units within a certain coverage area. In this paper, our network input is signalling signals, which are fixed-length time series. Since one-dimensional CNN has higher recognition accuracy when processing signals in large length, it is chosen for the recognition of signalling signals in this paper. Using the three characteristics of CNN (local perception, weight sharing, and maximum pooling), we can realize the type recognition of signalling signals. Figure 7 shows the basic principle of one-dimensional convolution.

After the feature map is obtained, in order to further refine the features, pooling technology is also used. Similar to the two-dimensional convolution technology, methods such as maximum pooling and average pooling are also used in one-dimensional convolution. Besides, before using the pooling technique, an activation function is also needed to increase the nonlinear factor.

After the refined features are obtained, the flatten method or the global average pooling method is also used to turn many feature maps into a feature vector so that the classification function can be used to classify the samples. The flatten method is to connect all the elements of each feature map to a single neuron. The principle is shown in Figure 8.

Although the flatten method looks simple, it has a big problem, namely, the amount of calculation. When the number and scale of feature maps are very large, adding a fully connected layer will increase the number of model

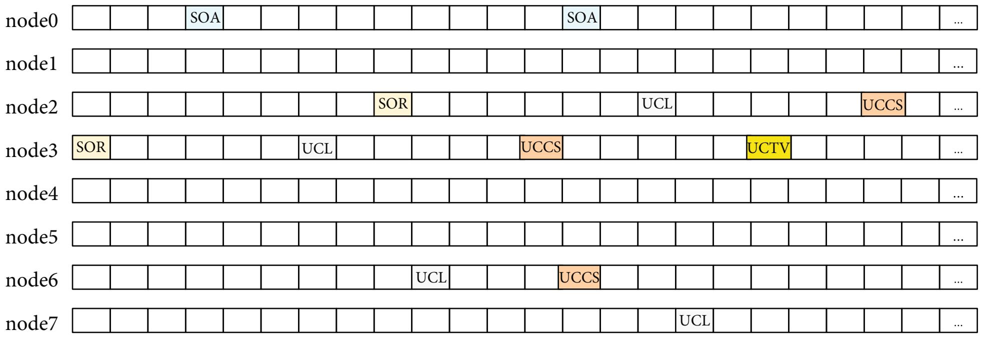

Figure 11: Schematic diagram of time slot signalling transfer between nodes.

```
$k = \{0, 1, \cdots N-1\} \longrightarrow N$ nodes of the network
$L^j \rightarrow$number of time slot signalling of the $j^{\text{th}}$ node
$S_{\text{SOR}} \rightarrow$SOR signalling search results
$S_{\text{UCL}} \rightarrow$UCL signalling search results
for $k = 1 : N$ do
    for $n = 1 : L^k$ do
        $i = 0$, search the SOR signalling
        $m = 0$, search the UCL signalling
        if *find the SOR signalling* then
            $S_{\text{SOR}}(i+1) = (k, n)$
        end
        if *find the UCL signalling* then
            $S_{\text{UCL}}(m+1) = (k, n)$
        end
    end
end
determine the central node and the calling node of voice transmission
based on $S_{\text{SOR}}$
determine the called node of voice transmission based on $S_{\text{UCL}}$
divide the three nodes(the calling node, the called node, and the central node)
for $k = C \rightarrow$the calling node number do
    for $n = 1 : L$ do
        $p = 0$, search the SOF signalling
            if *find the SOF signalling* then
            $S_{\text{SOF}}(p+1) = (C, n)$
            end
        end
end
based on $S_{\text{SOR}}$, $S_{\text{SOF}}$
intercept all the middle time slot signallings of the three nodes
```

Algorithm 1: Division and interception of time slot signallings

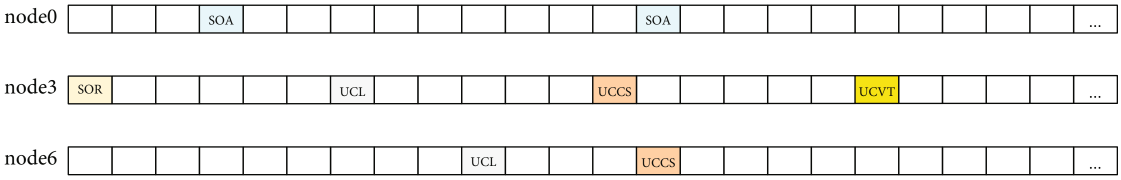

Figure 12: Time slot signalling division result 1.

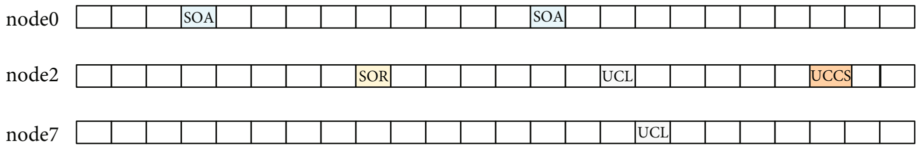

Figure 13: Time slot signalling division result 2.

Table 2: Parameters of simulation configuration.

Parameter	Value
Bit rate (R_b)	51200/3 bits/s
Bit interval (T_b)	3/51200 s
Frequency hopping rate (hopRate)	64000/105 s^{-1}
Number of bits per hop (bitsPerHop)	28
Number of samples per bit (sampNum)	354
Frequency hopping bandwidth (BW)	6 MHz
Frequency hopping frequency points (freqNum)	100
Frequency hopping interval (freqInterval)	60 KHz
Frequency hopping center frequency (f_c)	6 MHz
Number of signalling bits	19

parameters dramatically. In order to solve this problem, the global average pooling method can be used.

The global average pooling method is to form a feature vector by the average value of the elements in each feature map and then send the obtained feature vector to the classification function to obtain the classification result of the sample. Because the global average pooling method obtains the average value of each feature map without using a fully connected layer, it saves a lot of computing resources. The principle diagram of the global average pooling method is shown in Figure 9.

Before the data is input to the neural network, the data needs to be preprocessed. The main purpose of preprocessing is to reduce the dimensionality of the input signal data, making it easier to be processed by the neural network, while maintaining the information in the original signal, and improving the accuracy of network classification and recognition. Our convolutional network processes fixed-length signal sequences, so we need to perform fixed-length interception when intercepting signalling signals to make them have a uniform length. At the same time, the intercepted signals can be sampled at intervals to reduce the data dimension. If not preprocessed, the dimensionality of the input signal data will be quite large, which may contribute to long training time and low accuracy of network recognition. Therefore, the input of network is preprocessed IF signal which is converted from frequency hopping signal after dehopping and have a uniform length, while the output of network is the signalling type of the communication protocol. The one-dimensional CNN network structure is shown in Figure 10. And the structural parameters of the network are shown in Table 1.

5. Protocol Behavior Identification

During the positioning and recognition of signallings, types and time of arrival of signallings can be obtained. Next step is to identify the behavior of the emitter based on the signalling used. A schematic diagram of time slot signalling transmission of each node in the voice transmission process is shown in Figure 11.

The time slots allocation of each node is different, and the occupancy of the node time slots in voice transmission is also different. At the same time, because the communication protocol supports two unidirectional voice transmissions at the same time, the time slot signallings between nodes are interleaved and mixed together. Therefore, it is more difficult to recognize the behavior of the emitter directly based on the time slot signalling types of all nodes in the entire network. It is necessary to further divide and intercept the time slot signallings based on the nodes participating in the communication. The specific division and interception steps are as Algorithm 1:

The results obtained by dividing the time slot signalling are shown in Figures 12 and 13.

Based on the characteristic signalling in the time slot signallings, the type of the emitter voice transmission is temporarily determined and then calculated the chronological matching degree between the intercepted time slot signallings and the theoretical signalling combination and use it as the correct identification rate of the emitter behavior. The calculation formula of the chronological matching degree is as follows:

$$P_{\text{match}} = \frac{\sum_{i=1}^{N} s_i}{N}. \tag{10}$$

In the above formula, s_i is the consistency between the time slot signalling type and the theoretical signalling type in the voice transmission process; if they are consistent, s_i is 1; otherwise, it is 0; and N is the total number of theoretical signallings from the beginning to the end of a voice transmission process.

The calculation of matching degree can guarantee high accuracy in protocol behavior recognition despite multiple signalling recognition results being incorrect. Even though multiple signalling recognition results are incorrect, we can still calculate the chronological matching degree, which is used as the correct identification rate of the protocol behavior. And by comparing the correct identification rate of different protocol behaviors, we can choose the maximum of them to ensure high accuracy in protocol behavior recognition.

6. Experiment and Analysis

In this section, we achieve frame length estimation and frame structure analysis using related algorithms, then achieve signalling signal positioning and interception based on the analysis results, and finally achieve the emitter behavior identification based on the signalling signal identification results.

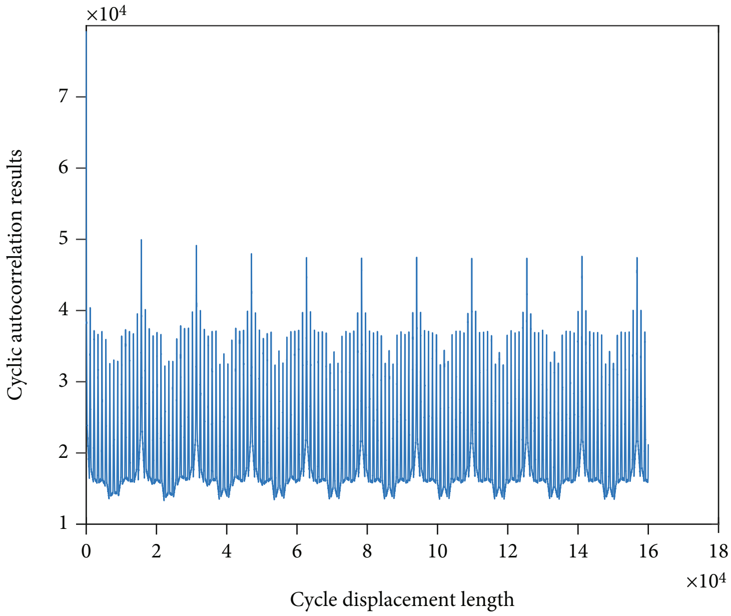

Figure 14: Partial cyclic autocorrelation curve.

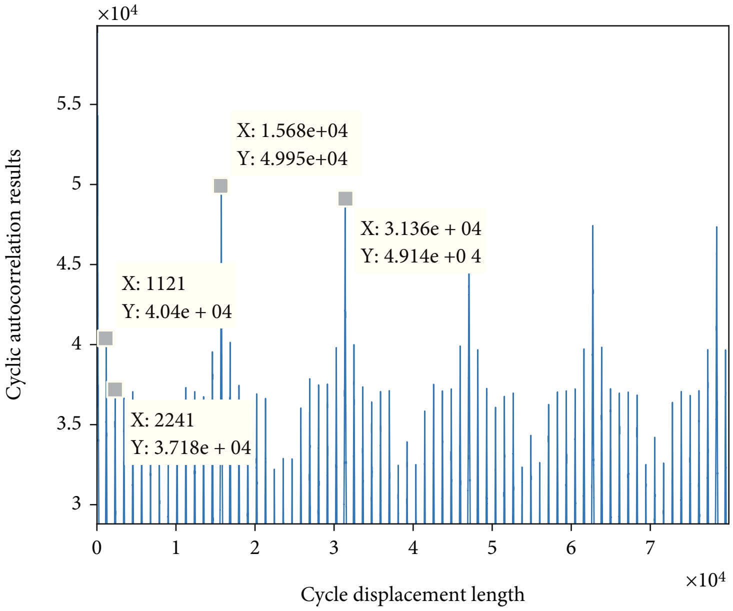

Figure 15: Partial enlargement of the cyclic autocorrelation curve.

Firstly, we consider a FH communication network with 8 nodes, including 1 master node and 7 ordinary nodes. It is assumed that the transmission of information between nodes follows the aforementioned FH radio TDMA networking protocol, and the digital modulation mode of baseband signal is MSK (minimum shift keying), which is a modulation method having good performance and widely used in communication systems. The relevant parameter settings for signalling signal simulation are shown in Table 2.

Next, we estimate the length of the time frame using cyclic autocorrelation, and the simulation results of the algorithm are shown in Figure 14. Periodic spikes appear in the cyclic autocorrelation results, with the continuous increase of the cyclic shift length. There are multiple secondary peaks between the highest spikes.

The results of the algorithm in Figure 14 are partially enlarged, and the distance between the highest peaks and the second peaks can be measured more accurately, as

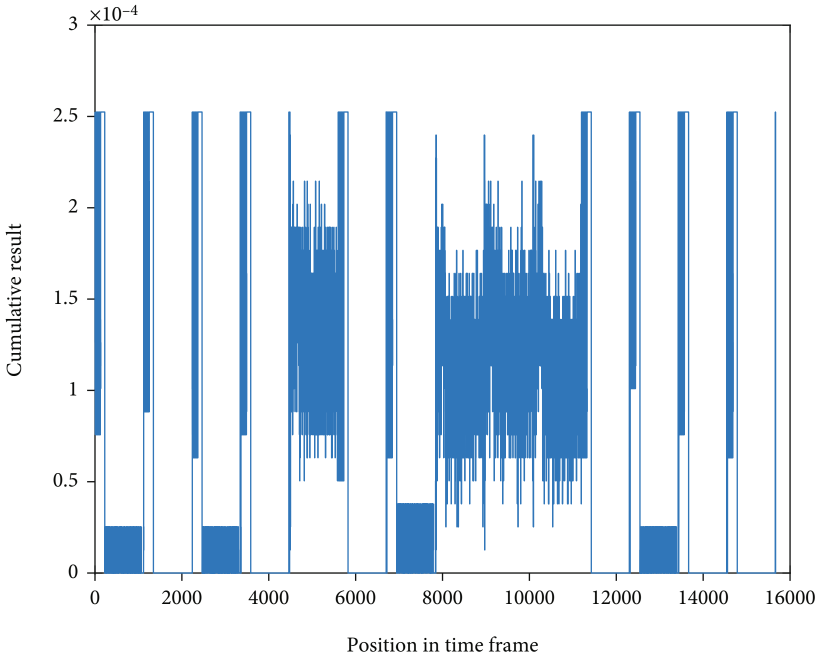

Figure 16: Simulation results of the frame structure analysis algorithm.

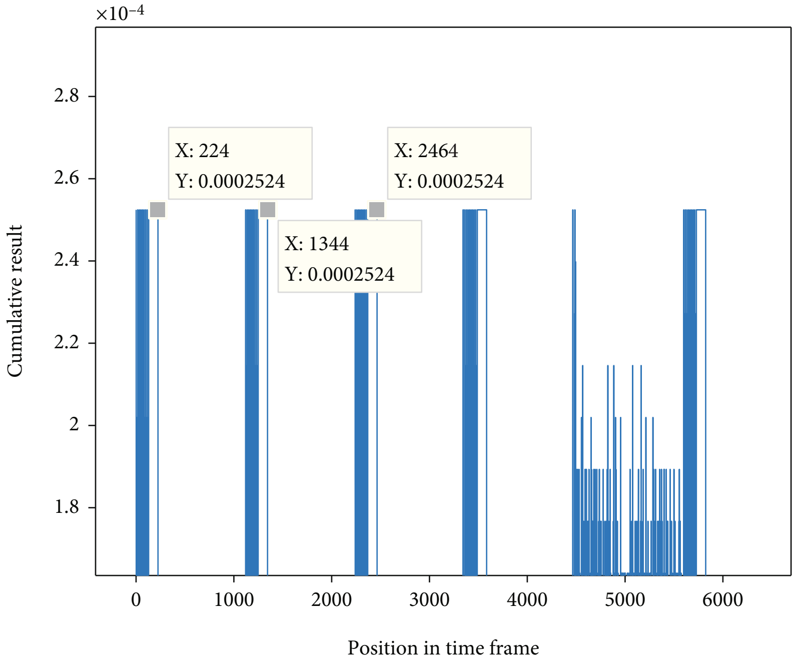

Figure 17: Partially enlarged results of algorithm simulation.

shown in Figure 15. Taking the average of multiple measurements of the peak distance in the amplified cyclic autocorrelation results, the distance between the highest peaks is about 15680, and the distance between the second peaks is about 1120, which is exactly consistent with the hypothetical communication protocol, indicating that the simulation results of the algorithm are completely correct.

Then, based on the estimation result of the time frame length, we achieve the analysis of the frame structure using the cumulative filtering algorithm, and the simulation result of the algorithm is shown in Figure 16. It can be found that there is a periodic structure inside the time frame. The number of the periodic structure in a time frame is about 14, which is in full compliance with the hypothetical communication protocol.

Similarly, the analysis result of the frame structure is further partially enlarged to more accurately determine the length of the periodic structure and the length of the initial

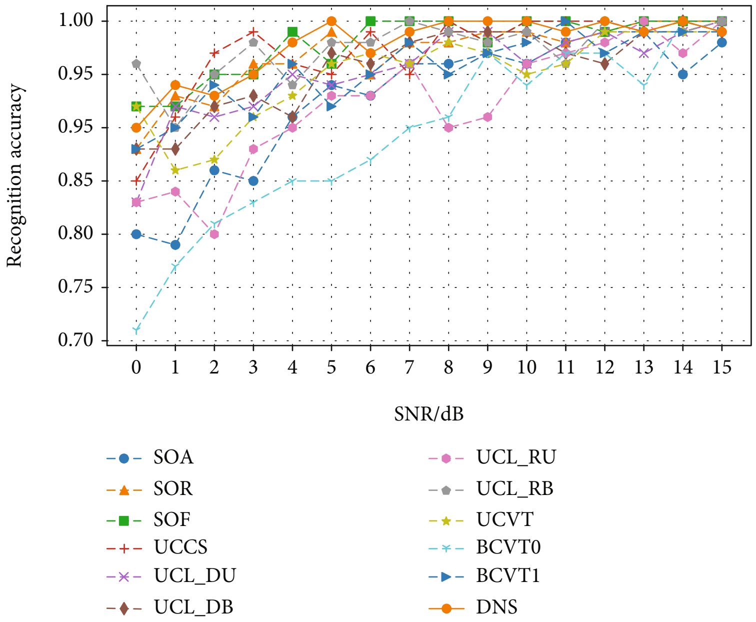

Figure 18: The recognition accuracy rate of 12 kinds of signalling under different signal-to-noise ratio conditions.

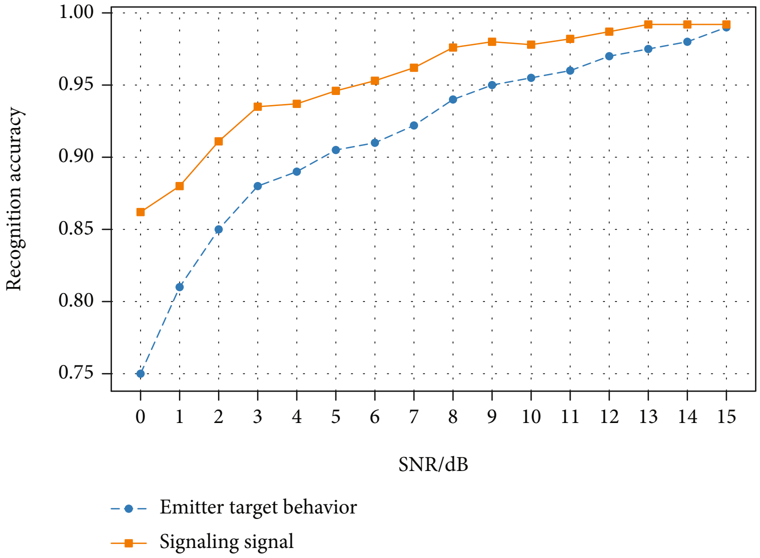

Figure 19: The average recognition accuracy of signalling signals and the target behavior recognition accuracy of the radiation source under different signal-to-noise ratio conditions.

sequence. The analysis result of the partially enlarged frame structure is shown in Figure 17. In the time frame analysis result, the length of the periodic structure is about 1240, and the length of the beginning sequence is about 224. Based on this, the position of the signalling sequence in the time frame is determined, and the positioning and interception of the signalling signal is realized combining the signal-related parameters.

After that, we identify the intercepted signalling signals using the convolutional neural network to obtain the signalling type of each signalling signal. The variation of the recognition accuracy of the 12 signalling signals with the signal-to-noise ratio is shown in Figure 18. The average recognition accuracy of 12 types of signalling is calculated to be 95.2% according to the single signalling recognition accuracy under the condition of single signal-to-noise ratio. In addition, we made statistics on the misidentification of each signalling signal under the condition of single signal-to-noise ratio. It is found that identification confusion among several types of signalling signal is prone to occur, and error detection and correction of signalling signal recognition can be realized based on this.

At the same time, the stability and robustness of the neural network have been verified. We have generated signals in different lengths by other digital modulation methods to verify the stability and robustness of the neural network. The digital modulation methods include BPSK, FSK, ASK, and MSK. The accuracies of signal recognition for the four modulation methods are all above 90% on average, and longer signal data can also be well recognized by the neural network, which indicate the stability and robustness of the neural networks we used in this paper.

At last, we realize the behavior recognition of the emitter by logical inversion according to the protocol, based on the recognition result of the signalling signal. Figure 19 shows the average recognition accuracy of the signalling signal and the emitter behavior under the condition of 0-15 dB signal-to-noise ratio. It can be seen from the figure that when the signal-to-noise ratio is 3 dB, the average behavior recognition accuracy has reached over 85%.

7. Conclusions

Based on the existing related technologies and theories of frequency hopping communication, this paper focuses on solving the two major technical problems of signalling signal positioning and signalling signal recognition. Finally, by identifying the type of the time slot signalling signal, the FH communication emitter behavior recognition is realized. This paper is oriented to the intelligent reconnaissance needs of FH communication stations and explores the cognitive mechanism and methods of the FH communication emitter behavior. According to the electromagnetic signal law formed by the FH communication emitter performing specific functions, the method of identifying the behavior of the emitter based on the signalling signal identification is studied. This paper focuses on the realization of key technologies such as signalling signal positioning and interception and signalling type recognition, lays a foundation for the emitter cognition of related information such as the behavior and tasks in complex electromagnetic environments, and is of great significance to improve the intelligent countermeasures in the electromagnetic spectrum domain.

Data Availability

The data used in this study is generated by simulation according to frequency hopping communication TDMA protocol. The [MAT] data used to support the findings of this study are included within the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest

References

[1] Q. Liu and M. P. Fok, “Ultrafast and wideband microwave photonic frequency-hopping systems: a review,” *Applied Sciences*, vol. 10, no. 2, p. 521, 2020.

[2] W. Lu, Y. Ding, Y. Gao et al., “Resource and trajectory optimization for secure communications in dual unmanned aerial vehicle mobile edge computing systems,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2704–2713, 2022.

[3] R. Zhi, L. Zhang, and Z. Zhou, “Cognitive frequency hopping,” in *2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, pp. 1–4, Singapore, 2008.

[4] W. Hu, D. Willkomm, M. Abusubaih et al., “Cognitive radios for dynamic spectrum access - dynamic frequency hopping communities for efficient IEEE 802.22 operation,” *IEEE Communications Magazine*, vol. 45, no. 5, pp. 80–87, 2007.

[5] M. Liu, Z. Liu, L. Weidang, Y. Chen, X. Gao, and N. Zhao, “Distributed few-shot learning for intelligent recognition of communication jamming,” *IEEE Journal of Selected Topics in Signal Processing*, p. 1, 2021.

[6] B. R. Mahafza, *Introduction to Radar Analysis*, Chapman and Hall/CRC, Second Edition edition, 2017.

[7] N. J. Muller, *Bluetooth Demystified*, McGraw Hill, 2001.

[8] M. Liu, J. Wang, N. Zhao, Y. Chen, H. Song, and Y. Richard, “Radio frequency fingerprint collaborative intelligent identification using incremental learning,” *IEEE Transactions on Network Science and Engineering*, 2021.

[9] M. Liu, C. Liu, M. Li, Y. Chen, S. Zheng, and N. Zhao, “Intelligent passive detection of aerial target in space-air-ground integrated networks,” *China Communications*, vol. 19, no. 1, pp. 52–63, 2022.

[10] D. A. Fritz, D. W. Moy, and R. A. Nichols, “Modeling and simulation of advanced EHF efficiency enhancements,” in *MILCOM 1999. IEEE Military Communications. Conference Proceedings*, Atlantic City, NJ, USA, 2002.

[11] J. P. Montgomery, D. L. Runyon, and J. A. Fuller, “Large multibeam lens antennas for EHF SATCOM,” in *MILCOM 88, 21st Century Military Communications - What's Possible?'. Conference record. Military Communications Conference*, San Diego, CA, USA, 1988.

[12] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications Handbook*, The McGraw-Hill Companies, Inc., 1994.

[13] V. Bezruk, “Methods of random signals recognition,” in *2006 International Conference - Modern Problems of Radio Engineering, Telecommunications, and Computer Science*, Lviv, UKraine, 2007.

[14] Q. Wen, “An overview of the study of the complexity of the complex electromagnetic environments,” in *2015 8th International Symposium on Computational Intelligence and Design (ISCID)*, Hangzhou, China, 2015.

[15] Q. Liu, X. Zhai, Z. Bao, Y. Liu, and Y. Wang, “Electromagnetic compatibility design of a certain information system command vehicle in complex electromagnetic environment,” *Engineering*, vol. 576, pp. 707–713, 2020.

[16] F. Yang, Z. Dong, and X. Duan, “Research on computation and simulation technology of battlefield complex electromagnetic environment,” *IOP Conference Series Materials Science and Engineering*, vol. 635, no. 1, article 012018, 2019.

[17] X. Li, Z. Nan, S. Yi, and F. R. Yu, “Interference alignment based on antenna selection with imperfect channel state information in cognitive radio networks,” *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 5497–5511, 2016.

[18] B. Zhao, L. Xin, J. Liu, and Q. Ding, “Research on narrowband interference suppression and diversity characteristics in fast frequency-hopping communication systems,” *International*

Journal of Future Generation Communication and Networking, vol. 9, no. 4, pp. 315–322, 2016.

[19] S. Dean, A. A. Khuder, and M. N. Abdullah, “Comparison and investigation of hopping rate estimation processes,” in *International Conference on Information and Communication Technologies: from Theory to Applications*, Damascus, Syria, 2008.

[20] D. Peng, T. Peng, X. Tang, and X. Niu, “A class of optimal frequency hopping sequences based upon the theory of power residues,” in *Sequences and Their Applications - SETA 2008, 5th International Conference*, Lexington, KY, USA, September 2008.

[21] X. U. Shanding, X. W. Cao, and X. U. Guangkui, “A Class of Frequency-Hopping Sequences Set with a Multiple of Prime Number Length,” *Acta Electronica Sinica*, no. 10, pp. 1930–1935, 2015.

[22] J. Wang, X. Yang, and X. Peng, “A linear method for TDOA estimation of frequency-hopping signal,” in *Wireless Communications, Networking and Mobile Computing (WiCOM), 2012 8th International Conference*, Shanghai, China, 2012.

[23] J. T. Guo, “Time-frequency analysis of frequency hopping signals based on particle swarm optimization,” *Applied Mechanics and Materials*, vol. 195, pp. 265–269, 2012.