Research Article

A Method for Realizing Antifollower Jamming in Communication and Its Experimental Verification

Xinfeng Fan, Zhiliang Tan, and Peijiao Song

National Key Laboratory on Electromagnetic Environment Effects, Shijiazhuang Campus of Army Engineering University, Shijiazhuang 050003, China

Correspondence should be addressed to Xinfeng Fan; 1132544091@qq.com

Received 10 January 2020; Revised 23 March 2020; Accepted 16 April 2020; Published 14 May 2020

Academic Editor: Rafael Morales

Copyright © 2020 Xinfeng Fan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The technical difficulty of antifollower jamming in communication systems is a wide concern in the peer. In order to solve the problem of difficulty to achieve antifollower jamming, a new identification method of follower jamming is proposed in this paper based on the characteristics of it and then follower jamming is cancelled out. A hardware-in-the-loop simulation platform is built by using FPGA. Then, experimental verification for mitigating performance of follower jamming is conducted based on the platform and the proposed method. Results show that signal-interference ratio (SIR) promotion is different for different jamming frequencies and the jamming mitigation performance is affected by interference intensity. The average SIR promotion can reach 10 dB when variance of jamming signal is between 0.75 and 1.5. In other cases, average SIR promotion is less than 10 dB. The proposed suppression method provides a useful way to antifollower jamming in frequency hopping (FH) communication.

1. Introduction

FH [1, 2] communication is used extensively in military communications because of a series of unique advantages such as strong anti-jamming ability, low probability of interception, and easy networking [3]. But under the condition of complex electromagnetic environment, FH communication still faces the threat of multiple hostile jamming. The artificial and intentional jamming for FH communication is divided into follower jamming and barrage jamming. In follower jamming, the jammer intercepts the transmitter signal, trying to determine the frequency of the hop and generating jamming in a narrow range about this frequency. Thus, it is the most ideal jamming method for FH communication [4].

At present, effective utilization measures for follower jamming include improving the capability of FH networking, increasing the hop rate of FH, and adding the pattern complexity of FH [5]. Although the above method can mitigate the influence of follower jamming, it will increase the complexity and technical difficulty of equipment. New FH systems such as differential FH (DFH) [6], multisequence FH [7], and self-encoded spread spectrum [8] have certain capability of antifollower jamming, but they improve the FH principle and increase the difficulty of implementation. Although the spatial anti-jamming method [9, 10] can theoretically suppress the follower jamming, it is difficult to function with the current technical level. Thus, antifollower jamming is still a difficult problem.

Interference cancellation is an effective way to realize interference suppression [11–13]. It has been widely used because of its efficiency to solve the electromagnetic interference problem. According to the different forms of cancellation signals, interference cancellation is divided into radio frequency (RF) cancellation and digital cancellation. In terms of RF cancellation, Rome Air Development Centre had developed a wideband interference cancellation system [14], which was mainly used in short-range communication systems of air force and frequency-hopping transceivers. Jain [15] adopted the cancellation scheme that reference signal was extracted after RF power amplifier and noise elimination chip QHx220 was adopted to realize the adaptive RF interference cancellation. In terms of digital cancellation, a method of digital cancellation based on least
square estimation was proposed by Duarte [16]. The channel response was estimated by using the time-domain guidance sequence with equal intervals, and then, it was convolved with the known baseband signal to obtain the reconstructed jamming signal. The broadband jamming suppression in full duplex communication was realized ultimately. In [17], a digital self-cancellation method was proposed based on iterative variable step-size LMS, which achieved a high cancellation ratio. Compared with the existing cancellation method, the gain was more than 6 dB, but the nonlinear effect caused by ADC devices was not considered in this method. Although there is no public report about the application of interference cancellation for follower jamming, this method still provides the possibility to suppress follower jamming.

Motivated by this, a method of follower jamming suppression based on digital cancellation is proposed. According to characteristics of follower jamming and its tactics background, the follower jamming signal is first identified by digital cancellation and then further cancellation is conducted to mitigate the follower jamming signal. Results show that the method is effective for follower jamming suppression and there is a SIR promotion by 10 dB at some interference intensities.

2. Characteristics of Follower Jamming

Generally, follower jamming includes waveform follower jamming, guidance follower jamming, and forwarding follower jamming [5]. Jamming effects are shown in Figures 1 and 2. The effect of forwarding follower jamming is similar to multipath jamming, so it is ignored here. Waveform follower jamming is an ideal jammer, so follower jamming refers to guidance follower jamming in practice. As seen in Figure 2, the follower jamming signal has a certain delay relative to the starting point of the frequency-hopping signal in each frequency-hopping period, and the delay is within a frequency-hopping period. Follower jamming signals are similar to the FH signal in time domain and frequency domain, but their modulation information is generally different. The modulated signal of follower jamming can be noise, pulse, or single tone, while the modulated signal of FH signal is the effective information.

Although follower jamming is the best jamming form for FH communication, limitations of speed and distance make it work in a certain geographical area [18]. It is pointed out that the geometric model of this area is an ellipse as shown in Figure 3 [19].

For the follower jamming to be effective, inequality (1) can be deduced where $c$ is the speed of an electromagnetic wave, $d_1$ is the distance between the transmitter and jammer; $d_2$ is the distance between the receiver and jammer; $L$ is the distance between the transmitter and receiver; $T_r$ is the processing time required by the jammer; $\eta$ is a jamming ratio fraction; and $T_{d}$ is the hopping duration. Equation (1) states that the arrival-time delay of the jamming relative to the desired signal at the receiver must not exceed a certain fraction of the hopping duration if the jamming is to be effective. The value of $\eta$ is determined by the jamming power at the receiver and the details of receive design, etc. as follows:

$$\frac{d_1 + d_2}{c} + T_r \leq \frac{L}{c} + \eta T_d. \quad (1)$$

Equation (1) yields to inequality (2), which defines an ellipse with the transmitter and the receiver at the two focal because that $d_1 + d_2$ can be regarded as a constant. The jamming cannot be effective when the follower jammer is outside this ellipse:

$$d_1 + d_2 \leq L + (\eta T_d - T_r) c. \quad (2)$$

3. Suppression Method for Follower Jamming

3.1. Principle of Digital Cancellation. Principle diagram of digital cancellation is shown in Figure 4. The basic input $d(n)$ includes the desired signal $S(n)$ and the jamming signal $u(n)$. The reference input $X(n)$ is the signal associated with $u(n)$. All inputs are obtained by sampling. The adaptive filter realizes the optimal estimation of the jamming signal under the action of the adaptive algorithm, making $y(n)$ the optimal estimation of $u(n)$, and then, $y(n)$ is compared with
In practice, it needs at least 2 times of signal detection, indicating that the jamming signal is completely cancelled out. Thus, the signal processing time is about 80 μs, and it is possible to intercept 100 μs unjammed FH signal if the starting point of one hop is known.

In summary, the identification of follower jamming signal mainly includes the following steps:

(A) Sampling the mixed signal and detecting frequency
(B) The time delay is calculated according to the prior condition, and then, the FH signal of a certain length is intercepted and stored
(C) The stored signal in B and the sampled mixed signal are sent to the digital canceller for cancellation, and the follower jamming signal is identified in a certain frequency
(D) When the next frequency point is detected, steps B and C are repeated

In the following experimental verification, some marks are set in the FH signal at each frequency point, so it is easy to intercept unjammed FH signal. When a mark comes, it needs to start intercepting the signal. In practical situation, it is essential to adopt some methods to detect the different frequency points of a real FH signal and know when the frequency changes.

3.3. Realization of Follower Jamming Suppression. After follower jamming signal is identified, it should be used as a reference signal to cancel the mixed signal again to realize jamming suppression. The cancellation scheme of follower jamming suppression is shown in Figure 5. C canceller 1 is used to identify the follower jamming signal, and canceller 2 is used to obtain the original FH signal. The basic input of two cancellers is all input by the mixed signal d (n). The reference input of canceller 1 is the intercepted signal St(n), and the reference input of canceller 2 is the system output of canceller 1. The output signal of the system is theoretically the desired signal S(n) with two cancellations, indicating the follower jamming is suppressed.

In conclusion, the designed cancellation scheme is summarized in Algorithm 1.

4. Experimental Verification and Result Discussion

4.1. Experimental Platform. The function principle diagram of the designed cancellation scheme for follower jamming is shown in Figure 6. The Simulink model generates source simulation data, including FH signal and mixed signal with superimposed jamming, which is then attached with the top, tail, and frequency mark to package as simulation packet. The simulation packet is transmitted to the data-parsing module of FPGA through USB communication and transferred to the cancellation algorithm module of FPGA with some process. The cancellation algorithm module receives the iteration coefficient sent by the upper computer program. The processed data are sent back to the upper computer program via USB, stored as a Hex file and
completed data waveform display. Finally, the M file in Matlab analyzes the data to obtain the mitigated performance. The built hardware-in-the-loop experimental platform is shown in Figure 7. In the waveform display interface, waveform before and after cancellation are respectively shown.

4.2. Parameter Settings. The main parameters of source simulation data are set as follows:

(A) Hopping rate: 100hop/s; modulation: FH/2FSK

(B) FH frequency points: (1 kHz, 2 kHz, 3 kHz, 4 kHz, 5 kHz, 6 kHz, 7 kHz, 8 kHz, 9 kHz); sampling frequency: \(1 \times 10^6\) Hz

(C) Modulated signal of follower jamming is pseudo-random jamming with zero mean and variance of \(\sigma_w^2\); time delay is 0.001 s

(D) Filter 1 and Filter 2 have the same parameters: \(W_1(0) = W_2(0) = 0\) and \(\mu_1 = \mu_2 = 0.001\); the length of each filter is 8
For the convenience of processing, the length of the intercepted FH signal is 0.001 s at each frequency point.

Figure 8: SIR curves of three different FH frequency points. (a) 3 kHz; (b) 6 kHz; (c) 9 kHz.

Figure 9: SIR promotion curves of all FH frequency points.

4.3. Result Discussion. To facilitate the jamming mitigation performance, SIRs before and after cancellation are respectively calculated in M file. The SIR promotion is taken as the evaluation index to analyze the effect of follower jamming suppression with different interference intensities and frequency points.

Figure 8 shows SIR curves of three different FH frequency points (3 kHz, 6 kHz, and 9 kHz). In each subfigure, the above curve represents SIR after cancellation, and the below curve represents SIR before cancellation. It is clear to see that SIR after cancellation has obvious increase compared to SIR before cancellation, indicating that the proposed method can effectively suppress jamming. In fact, the variance of modulated pseudo-random jamming represents power, determining the interference intensity. The bigger the variance, the stronger the interference intensity. Therefore, it can also be seen that a stronger interference intensity (or bigger variance) makes a smaller SIR before cancellation. Comparing Figure 8(a) with Figures 8(b) and 8(c), it can be found that SIR after cancellation is not the same for different FH frequencies, indicating that frequency has slight influence on jamming mitigation performance.

The SIR promotion of all FH frequency points is shown in Figure 9. It is clear to see that SIR promotion has some difference for different frequency points. Meanwhile, the effect of follower jamming suppression has some difference for different interference intensities. As shown by the black line in Figure 9, average SIR promotion can achieve 10 dB when variance is between 0.75 and 1.5. When variance is larger than 1.5 or less than 0.75, average SIR promotion is less than 10 dB, indicating jamming mitigation performance is slightly worse. In a bad manner, average SIR promotion is less than 8 dB when variance is 2 or 0.25. Therefore, the performance of the proposed follower jamming suppression method is affected by the interference intensity of the jamming signal, and it has obvious mitigation performance with a 10 dB SIR promotion when the variance is between 0.75 and 1.5.

5. Conclusion

Aiming at the existing problems of antifollower jamming, an identification method of follower jamming is proposed in this paper according to the characteristics of follower jamming and formation condition. Then, the identified jamming signal is input as the reference signal of cancellation and follower jamming is suppressed. The corresponding cancellation experiment platform is built based on FPGA, and the effectiveness of the suppression method is preliminarily verified. Experimental results show that the suppression method is effective in mitigating the influence of follower jamming. SIR after cancellation decreases with the decrease of SIR before cancellation. SIR promotion has some difference for different frequency points. Meanwhile, the performance of the suppression method is affected by the
interference intensity. It has obvious mitigation performance with a 10 dB SIR promotion at some interference intensities. In the experiment, the frequency of FH signal is set low to intercept the unjammed FH signal. However, the unjammed FH signal is not easy to obtain at high-frequency condition, so the proposed method may lose efficacy. Nevertheless, the proposed follower jamming suppression method still provides a useful way to antifollower jamming, and further research needs to be conducted for more types of modulated signals of follower jamming and higher frequency condition.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Key Pre-research Fund with grant no. 914OC87030413JB34001.

References


