A Smart Tracking-based Jamming Scheme for Signals with Periodic Synchronization Sequences

Yuan Chen, Fei He, Jian Yan, Xiang Chen, Yuantao Gu
State Key Laboratory on Microwave and Digital Communications
Department of Electronic Engineering, TNList, Tsinghua University, Beijing 100084, P.R.China
{chenyuan05, chenxiang98}@mails.tsinghua.edu.cn

Abstract—**In this paper, a smart tracking-based jamming scheme is proposed for the signal with synchronization sequences. A different pseudo-random interference sequence, different from the signal's synchronization sequence, is used to track and interfere with the synchronization header in the original signal. With this known pseudo-random synchronization interference sequence, the interference overlapping on the original signal can be nearly cancelled, meanwhile the original signal can be successfully demodulated and decoded at the own receiver without severe interference. However, the other receivers, directly receiving the hybrid signal composed of the original and the pseudo-random interference signals, will fail to recover the original signal without the knowledge of the pseudo-random interference sequence. Compared with traditional full-band full-time noise blanket jamming in communication countermeasures, the advantages of this smart jamming scheme are its low power consumption and up to 100% chance of successful jamming. Simulation results and hardware implementation both show that this scheme can effectively and essentially interfere with the signal at low power consumption.**

Keywords- synchronization sequence; jamming; interference cancellation; m-sequence

I. INTRODUCTION

In the modern military confrontation, electronic countermeasures have become a very important way[1,2], which not only can detect and measure the specific technical parameters through the enemy's local radio or other electronic equipment, but also can effectively undermine and interfere with the enemy's local radio utilizing the measurement results. As an important part of electronic countermeasures, communication confrontation technology deprives the enemy of the acquisition of the signal power and signal transmission. It is a powerful weapon, and helps to firmly grasp the initiative in the battlefield.

For any communication signals, the traditional jamming scheme is to send an interference signal at the same frequency with that of the useful signal. However, the strength of this kind of interference signal should be equal to or even much more higher than that of the useful signal, and the duration of interference signal should be 100% duty cycle (the proportion of nonzero signal in the time domain) in order to guarantee effective interference performance, which is also called full-band full-time noise blanket jamming. This method is inefficient but very simple, because we only need to increase the transmission power to get better interference performance.

For some specific communication systems, such as relay communication systems with the periodic synchronized frame structure, we can expect the best interference performance at the minimum price if we adopt smarter jamming scheme based on the characteristic of the signal structure.

The new jamming scheme proposed in this paper is especially suitable for the signal with periodic synchronization sequences. In this scheme, the interference signal is not sent all the time in the time domain, but only at the particular time decided by the estimated transmission parameters (e.g., the position and the power level of periodic synchronization sequences). In addition, the structure of the interference sequence is tailored according to these estimated parameters. The enemy's normal communication process will be undermined, because their receivers could not complete the synchronization operations any more.

Though the scheme mentioned above can greatly reduce the transmitting power of the jamming station, there still is another limitation that it cannot interfere with the user terminals all the time. After in-depth study of the root cause of this limitation, we propose another scheme that allows us to track the original signal all the time, which enables us to interfere with the user terminals completely, ultimately enable us to achieve 100% chance of effective interference with low power consumption.

The rest of this paper is organized as follows. In Section II, the system structure and transmission scheme are described in detail. We analyze and discuss the problems in the traditional systems in Section III, and a new solution to these problems is proposed in Section IV. Computer simulation results and hardware implementation are given in Section V. Finally, conclusions are drawn in Section VI.

II. SYSTEM DESCRIPTION

Figure 1 shows the physical structure and interference model of a typical transparent relay communication system (for example, wireless repeater)，which is composed of an uplink station, a relay station, a jamming station and many other user terminals which want to receive the signal from the uplink station. In the normal communication process, communication from the uplink station to user terminals can be aided by the relay station: the uplink station sends signal to the relay station, then the relay station forwards the uplink signal to the user terminals in a transparent way; finally the user terminals can

This work is partially supported by National Basic Research Program of China (2007CB31060), China's Major Project (2010ZX03003-002), PCSIRT and China's 863 Project (2009AA011501).

978-1-4577-1010-0/11/$26.00 ©2011 IEEE

demodulate the received signal, and complete the normal communication process.

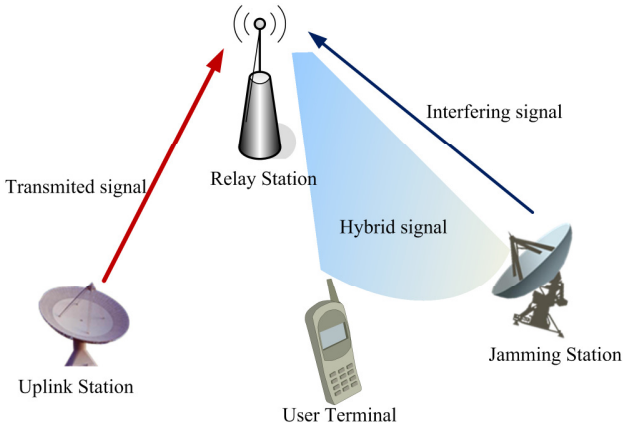

Figure 1. Interference Model of a Relay Communication System

In the presence of jammers, relay stations will receive the mixed signal composed of the useful signal and the interference signal sent from the jamming station. The mixed signal is also transferred by the relay station, and the jamming station and other user terminals will receive the mixed signal, which is used for the subsequent signal processing.

In modern communication systems, in order to recover the original signal quickly and effectively, the sender usually inserts a specific synchronization sequence in a specific position in the sent signal. With the help of the periodic synchronization sequence, the receiver can synchronize the signal and estimate channel parameters. This allows the whole communication system to resist external adverse factors, and to achieve better system performance. This approach is also used in this relay system, whose frame structure is shown in Figure 2.

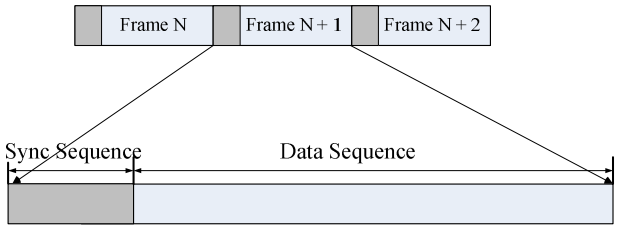

Figure 2. Frame structure with periodic synchronization sequences

In this system, the frames transmitted by the transmitter are continuous, not bursty. In each frame, there are many kinds of synchronization signals for different levels of synchronization, either for symbol synchronization or for frame synchronization. And the parameters of these sequences are also known at the jamming station.

For this relay communication system with synchronization sequence, apparently, we can interfere with it with the traditional full-band full-time noise blanket jamming approach, but we need to send a signal with adequate power so that we can obtain effective interference results, which is also not so cost-efficient. We can look at this from another point of view: if we send a signal sequence to interfere with just the synchronization sequence of the original signal, the user terminal cannot synchronize the original signal correctly, and will fail to get the desired information. The normal communication process is interrupted.

From the above analysis, we can see that: in the system with periodic synchronization sequence, the most effective and efficient way of interference is just to send a special interference signal to interfere with the normal function of the synchronization sequence in the original signal, and there is no need to completely suppress the original signal in power.

Therefore, we can consider another way to send interference sequences in Figure 1. After the jamming station have receive the downlink signal and complete the synchronization, it can locate the synchronization sequence in the downlink signal, and transmit some interference pulse with the feedback adjustment. The synchronization sequence and the interference pulse will overlap in time domain, which cause that the user terminal cannot distinguish the desired signal from the mixed signal.

We use the original signal's synchronization sequence to adjust the position of interference pulse. More accurately the synchronization sequence of the original signal and the interference pulse are overlapped, more inaccurate the feedback information for controlling the sending time of the interference pulse is. When the interference pulse is totally overlapped with the original signal, the jamming station also can't get the synchronization sequence as the other user terminals do, and lose the control of the emission time of interference pulse.

More specifically, this interference process can be decomposed into three stages:

(1) Initial stage: in the initial period of the system, according to the received synchronization signal and the estimated channel delay, we can complete the coarse synchronization between the interference pulse and the synchronization sequence of the original signal;

(2) Adjusting stage: from the mixed signal we received, we can extract the timing difference between the synchronization sequence of original signal and the interference pulse, and form a feedback signal to correct the emission time of the interference pulse in order to synchronize with the synchronization sequence in the original signal at the relay station;

(3) Inertia stage: Once the interference pulses have been synchronized accurately with the original signal, we cannot make the feedback signal from the timing difference. However, with the fact that the original signal is a continuous frame with synchronization sequence, which appears periodically at both the user terminals and the jamming station, we can decide the next transmission time of the interference pulse with the estimated period parameter (the time length of one whole frame), i.e., the inertia of transmission.

III. Analysis And Remark

The jamming scheme mentioned in Section II can interfere with the original signal efficiently through destroying

the synchronization process at user terminals. However, this method still has the following problems:

(1) The interference feedback loop in the adjusting stage of this method is not convergence. When the synchronization sequence in the original signal is effectively interfered with, the jamming station also cannot recover the synchronization sequence, and fails to make the normal feedback signal for adjusting the transmission time of interference pulse; therefore, we need to use the inertia property of the continuous frame structure to decide the appropriate action to interfere with the original signal.

(2) The estimated periodic parameters used in the inertia stage are not accurate due to the estimation errors, which will cause the interference source at the jamming station cannot effectively interfere with the synchronization sequence; therefore, the jamming station will be out of synchronization after every successful interference operation, and it has to search for the synchronization sequence in the frame structure from scratch. We denote *the chance of jamming* as the probability of the exact synchronization between the synchronization sequence and the interference pulse. In this case, it allows the user terminals to get the original data under a certain probability, i.e., the chance of interference is less than 100%.

In order to further analyze the impact of inertia property, we assume the data clock offset jitter between the uplink station and the jamming station is δ ppm, the length of the synchronization sequence is $LenSyn$, the length of the interference pulse is L, and the symbol rate of the original signal was R Mbps. By definition, there will be one sample bias per $\delta \times 10^6$ samples. Without loss of generality, we just omit the other signal processing operation, such as Forward Error Correction (FEC). We assume that $L > LenSyn$, i.e., the synchronization sequence can be completely covered by the interference pulse. In this interference method, once the cumulative bias is up to $L - LenSyn$ symbols, the synchronization will be lost. The maximum length of time before jammer's desynchronization is bounded by $(L - LenSyn)/\delta R$.

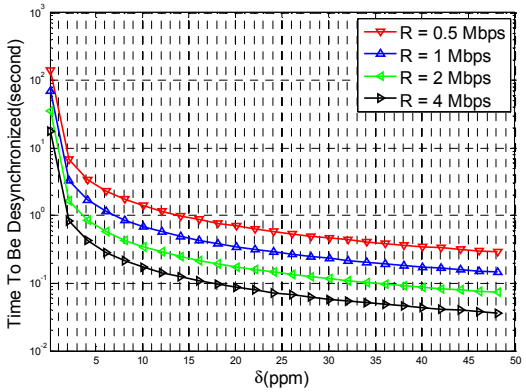

Figure 3. The maximum length of time before jammer's desynchronization

Figure 3 shows the theoretic upper bounds for the maximum length of time before jammer's desynchronization with different symbol rates and different data clock offsets. From this figure, we can see that though the data clock offset jitter is lower than 15ppm, the jammer can only keep synchronization less than 1s. It seems so easy to desynchronize the jammer from the uplink station. Therefore, we will further propose a smart tracking-based jamming scheme to overcome this desynchronization problem in the following section.

IV. Proposed Scheme

Based on the above analysis for the jamming scheme mentioned in Section II, the jammer is only synchronized with the original signal in the initial stage. Once the interference pulse is sent，the jamming station will be desynchronized, and it only can use the inertia property of the original signal to complete the interference operation. It shows that the whole system is not a closed-loop system, and instable. Sometimes, the original signal is able to be recovered by the user terminals due to the incomplete and inaccurate interference.

There are two basic goals for the performance of our expected interference schemes :

(1) Achieve the 100% chance of interference, and avoid the user terminals to obtain original information effectively;

(2) Keep the duty cycles as less as possible to reduce the average transmit power of the jamming station.

In order to achieve the first goal, we must guarantee that the jamming station is synchronized with the original signal all the time, so it can calculate all the parameters that it needs to make the right jamming choice, and ensure that the user terminals cannot accurately capture the synchronization sequence. For the second goal, we can select a different interference waveform, which achieves full interference performance while keeping its transmit power as low as possible.

Therefore, we propose a new kind of jamming scheme. In this scheme, the jammer can restore and eliminate the known interference sequence, then effectively recover the original signal with the synchronization sequence. The diagram of the proposed jamming scheme is shown in Figure 4. The detailed steps are as following:

Step 1): The interference signal is sent at the same frequency and the same position of the original periodic synchronization sequence;

Step 2): After the mixed (hybrid) signal has been transparent forward, the jamming station will perform interference estimation and cancellation as in [3] to recover the original signal for tracking:

2-a) Based on the match filter by restored interference sequences, the jamming station estimates the channel response parameters, including the amplitude, the phase and the transmission delay of the channel;

2-b) Recover the interference signal by the estimated channel parameters;

2-c) Remove the interference signal form the hybrid signal, and get the synchronization tracking on the original signal at jamming station.

Step 3): Finally, based on the estimated transmission delay, the jamming station adjusts the time to send the jamming signal, which is used to interfere with the synchronization of the original signal.

Based on the above interference cancellation at jamming station receiver, it can synchronize with the original signal with the probability up to 100%, which allows the jamming station to do accurate calculation of the location of the synchronization sequence in the original signal. Therefore, the jammer's signal processing loop is convergent now, because it can get all the information in this system and be in the synchronization status all the time. Meanwhile, the user terminals are completely interfered with by the interference sequence, which avoids them to complete the synchronization operation. So it reaches the first goal.

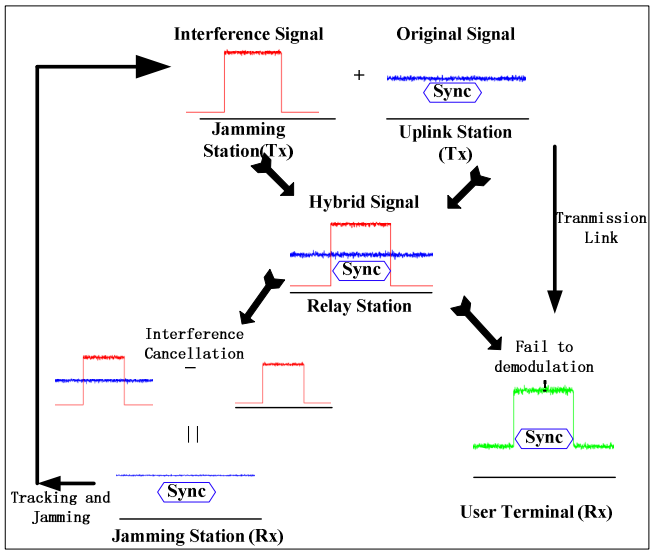

Figure 4.Diagram of proposed tracking-based jamming scheme

On the other hand, in order to reduce the interference signal duty cycle and have fast detection method, there are two basic requirements for the interference signal:

(1) The autocorrelation property of the interference sequence is good;

(2) The cross-correlation property between the interference sequence and the original periodic synchronization sequence is good.

Requirement (1) is to make us be able to detect the pseudo-random interference sequence effectively; Requirement (2) makes us be able to interfere with the original signal effectively with transmit power as low as possible. So, it is necessary to select proper interference sequence to meet the above requirements. Without loss of generality, we assume the original signal is random BPSK modulation sequence. We take the M sequences and Chu sequences as candidate interference sequences. We use synchronous interference cancellation technique (as **Step 2-a) to 2-c)** show) to remove the known pseudo-random interference sequence from the mixed signal[3]. We denote the residual interference signal as the difference between the sent interference signal and the estimated interference signal at the given signal to interference ratio. We compare **the absolute residual interference signal** ($20\log_{10}|S\text{-}S'|$, S and S' are original and estimated signals respectively) with M sequences and that of Chu sequences, respectively, at different SIRs in Figure 5. From the simulation results, we can find that the performance of M sequences is much better than that of Chu sequences when the interference power is low. The advantage of the Chu sequence[4] is the low complexity of implementation in hardware circuit, especially when the length of sequence is very long. But we choose the length of M sequence is not too long. Therefore, we select the M sequence as the synchronization interference signal.

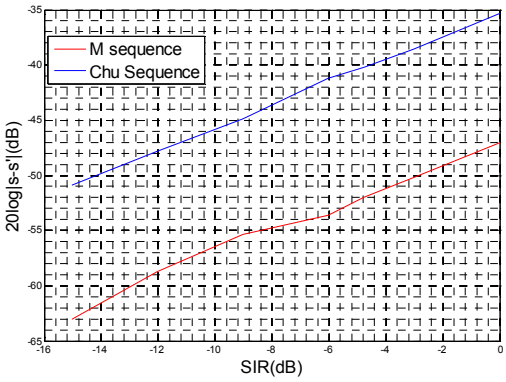

Figure 5. The residual interference performance based on different pseudo-random sequences

V. Simulation Results and Hardware Implementation

In this section, we will give some simulation results and a hardware implementation to verify the effectiveness of our proposed scheme.

Firstly, we will evaluate the interference cancellation performance at our own receiver through estimating our sent pseudo-random interference signal by simulations. Here, we denote the useful signal as S, the synchronization interference sequence as I (here is the M sequences), and the additive white Gaussian noise as N, then the mixed receiving signal has the form

$$R = S + I + N .$$

We estimate the pseudo-random interference signal $\alpha e^{j\theta} I$ by the synchronous interference cancellation techniques (**Step 2-a) to 2-c)**), in which we denote α, θ as the amplitude and phase of the estimated pseudo-random interference sequence respectively. Then the actual signal used for subsequent demodulation and decoding is

$$R' = S + I + N - \alpha e^{j\theta} I = S + \left(1 - \alpha e^{j\theta}\right) I + N .$$

Furthermore, in order to simply evaluate the impact of residual interference signal to the normal receivers, we just consider the

estimated amplitude α without the error of θ. Then we set the instant $SIR = -6dB$,the parameters of the original signal Frame length = 204bytes, periodic synchronization header's byte length = 1byte, M sequence length = 31 bits, and use (2,1,7)convolution code as the FEC. In the reference relay system, the simulation results for the bit error rate of R' are shown in Figure 6.

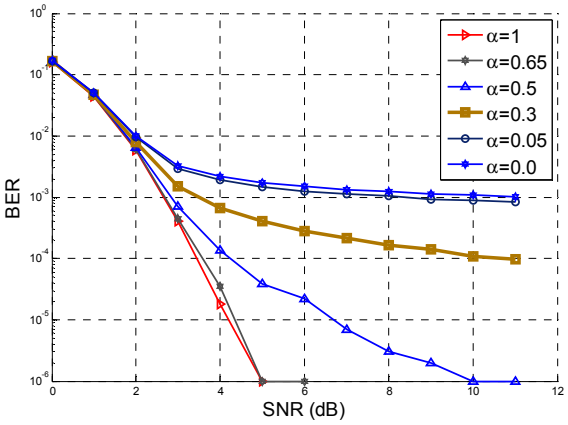

Figure 6. The BER of with different α

From Figure 6, it can be noted that the similar performance can be achieved as the original (2,1,7) convolution code(α=1),when estimated α is larger than 0.65. This condition can be satisfied easily according to the simulation results shown in Figure 5. Meanwhile, in Figure 6 we can also see that how well the other receivers are interfered with. Actually, when α=0, it means that the pseudo-random interference signal is not eliminated totally just as in normal receivers for original signal, then the BER becomes constant even when SNR is higher than 10dB. Therefore, the periodic synchronization sequence of other receivers can be effectively interfered with when the pseudo-random interference sequence overlaps on the synchronization sequence in the original signal.

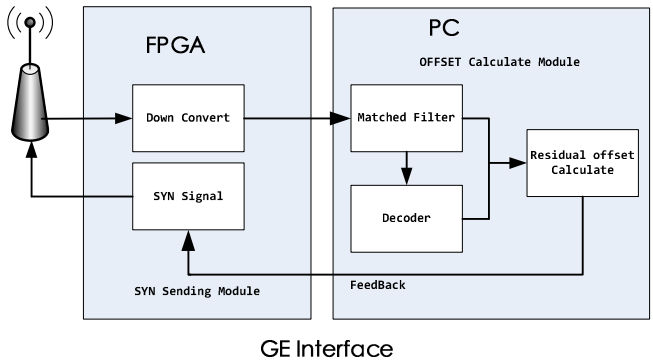

Figure 7.Diagram of hardware implementation for jamming station

Furthermore, we give a hardware implementation of the jamming station to test the proposed scheme. The basic diagram is shown in Figure 7. There are two main modules in this figure, the synchronization interference (SYN) sending Module implemented on a field-programmable gate array (FPGA), and the OFFSET Calculate Module implemented on a personal computer (PC). They exchange information through Gigabit Ethernet (GE) interface.

In our hardware implementation, we use FPGA to receive the mixed (hybrid) signal and down convert it to baseband. Then the baseband signal is sent from FPGA to the PC module through the GE interface. On the PC, a match filter is used to detect the amplitude and phase of the sending pseudo-random interference signal. Based on the estimated amplitude and phase, the pseudo-random interference signal can be removed from the mixed signal. In these processes [5,6], we can calculate the time difference between the synchronization sequence of the original signal and the pseudo-random interference signal, which can be used to control the sending time of the SYN signal module. At last, we use the reference implementation to synchronize the mixed signal and can demodulate the original signal correctly, but other receivers are always out of synchronization.

VI. CONCLUSION

In this paper, we propose a smart tracking-based jamming scheme to interfere signal with periodic synchronization sequences. For our own receiver, the used pseudo-random interference sequence can be completely canceled by proper parameter estimations and interference signal recovery. Consequently, the smart jammer (our own transmitter) can continuously interfere with the original receivers by accurately tracking the demodulation signal nearly without interference. Using this scheme, we can achieve low power consumption and up to 100% chance of successful jamming. Simulation results and hardware implementation both verify this scheme's validity.

REFERENCES

[1] Lixia Liu, "Research on communication countermeasure simulation training system", International conference on computer technology and development, 2009 (ICCTD'09), pp.93-97

[2] Yashang Liang, Lechang Sun, Chunsheng Liu,Ning Xu, Simulation study of communication confrontation, (in Chinese), Radio Engineering of China,Vol S1, 2001, pp.220-223.

[3] Fei He, Xiang Chen, Jian Yan, Ming Zhao, Shidong Zhou, "Low Overhead Pilot-Aided Parameter Estimation Scheme for Asymmetric PCMA Systems," in Proc. 5th International ICST Conference on Communications and Networking in China (CHINACOM'10), pp.1-5, Aug. 2010.

[4] M.G. Parker, K.G. Paterson and C. Tellambura, "Golay complementary sequences," in *Wiley Encyclopedia of Telecommunications*, John G. Proakis, ed. Wiley, 2003.

[5] H. Meyr, M. Moeneclaey, and S. A. Fletchel, *Digital Communication Receivers: Synchronization, Channel Estimation and Signal Processing*. John Wiley & Sons, 1997.

[6] Floyd M.Gardner,A BPSK/QPSK Timing-Error Detector for Sampled Receivers,IEEE Trans. on comm. Vol 34, Issue 5, 1986, pp.423-429.