IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 6, 2021, accepted March 17, 2021, date of publication March 22, 2021, date of current version March 29, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3067734*

# Multi-User Secure Receiving Algorithm Based on Blind Recovery in MIMO Network

**YONGLI AN[1], CHENGMING ZHANG[1], ZHANLIN JI[1], AND ZHICHAO ZHOU[2]**
[1]Department of Artificial Intelligence, College of Artificial Intelligence, North China University of Science and Technology, Tangshan 063009, China
[2]Innovation Center of Smart Network, China Unicom Group, Beijing 100044, China

Corresponding author: Yongli An (tongxinayl@126.com)

This work was supported in part by the National Key Research and Development Project under Grant 2017YFE0135700, in part by the High Level Talent Support Project of Hebei Province under Grant A201903011, and in part by the Natural Science Foundation of Hebei Province under Grant F2018209358.

**ABSTRACT** In order to optimize the performance of data transmission in multiple input multiple output (MIMO) wireless communication systems, a spread spectrum self-interference system based on channel inverse matrix modulation is proposed. First of all, we improved the spread spectrum method and proposed the DIMMSS(channel inverse matrix modulation spread spectrum) spread spectrum method based on the channel inverse matrix. And a simulation comparison experiment was carried out for the anti-interference ability and anti-eavesdropping ability of this method. Secondly, this paper also proposes two blind despreading methods based on Walsh-hadamard algorithm and cluzeau algorithm. We studied the anti-jamming performance of these two algorithms, and optimized the blind despreading process according to their different characteristics of computational complexity. Experimental results show that compared with ordinary direct sequence spread spectrum, the spread spectrum self-interference system can not only improve the confidentiality and security of the transmitted signal, but also greatly simplify the receiving equipment. It has certain application value in the military and civilian fields.

**INDEX TERMS** MIMO, anti-eavesdropping, pseudo random sequence, spread spectrum method, reconstruction.

## I. INTRODUCTION

Today, wireless networks have been widely used in civilian and military applications, security issues have become a major issue in network research. Among them, the physical layer security is based on the information theory method to protect the confidentiality of data, and it has attracted extensive research interest because of its focus on the confidentiality in the communication process. Spread spectrum and despreading are important components in communication security, and also has important research value. Aiming at the problem of eavesdroppers stealing messages and interference between multi-user communications in wireless communication systems, this paper proposes a new spread spectrum method based on multiple input multiple output (MIMO) systems, which is channel inverse matrix modulation spread spectrum (CIMMSS).

The associate editor coordinating the review of this manuscript and approving it for publication was Stefan Schwarz.

There exist a large variety of methods about new spread spectrum in the existing research. Among them, walsh code soft spread spectrum signals are widely used. For example, the foreign military Mark VII Mode5 adopts (16,4) Walsh soft spread spectrum coding technology, and the new generation of Norwegian battlefield communication network also proposes to use (256,8) and (32,7) orthogonal matrix coding spread spectrum system. In addition, WCDMA applies (64,6) Walsh code soft spread spectrum coding technology. There is also a soft spread spectrum method that combines RS error correction coding and Walsh transform, which has good performance in orthogonality and error correction [1]. Literature [2] proposed the Massey algorithm to estimate pseudo-random sequences. This method can accurately estimate pseudo-random sequences, but this method requires no errors in the sequence, which results in very harsh calculation conditions for the algorithm. The matrix factorization algorithm is a common way of direct sequence spread spectrum (DSSS) despreading in recent years. For example, Burel and Bouder [3] calculated the covariance matrix based on

the feature analysis technique, and then reconstructed the spreading sequence through the feature vector. When the spreading code is too long, the calculation complexity of this method is too large, and it is difficult to apply in practical applications. Based on the feature analysis method, literature [4] combines the feature decomposition algorithm and the subspace tracking algorithm to realize the fast algorithm of feature decomposition, which greatly reduces the computational complexity, but has poor anti-noise performance. In [5], a double sliding window feature decomposition algorithm is also proposed. This method simplifies the problem of spreading code estimation under non-synchronization, but increases the computational complexity. There are also some articles proposed to estimate pseudo-code sequence respectively based on spreading code maximum likelihood estimation, neural network and average cross-correlation method, Although these algorithms have low computational complexity, but these methods have poor performance under low signal-to-noise ratio conditions [6], [7].

Regarding the problem that information in multi-user communication is easily disturbed and stolen, literature [8] proposed a single input multi output (SIMO) system that uses a neural network to achieve full-duplex legal receiver signals combination and self-interference Elimination scheme. The legal receiver sends artificial noise to interfere with the eavesdropper while receiving the signal for self-interference signal cancellation. Some articles studied the secure massive MIMO transmission for multi-cell and multi-user systems on independent and identically distributed Rayleigh fading channels, and proposed several matched filter precoding and Artificial noise (AN) generates a design to interfere with eavesdroppers' channels and protect user channels [9]. For the same system model, a regularized channel inversion and AN transmission scheme was designed in [9] to further improve the security performance. For eavesdroppers using massive MIMO antennas to steal information, a physical layer security method is proposed to prevent eavesdroppers, which is called the original data phase rotation secure transmission scheme. The method is to randomly rotate the phase of the base station before the original data transmission, so that a large number of MIMO eavesdroppers will be confused by intercepted signals that may not represent real information symbols [10].

This paper proposes a new spread spectrum method based on MIMO system, which uses the channel inverse matrix to modulate the spread spectrum code. The CIMMSS can effectively solve the problem of multi-user interference and eavesdropping. Compared with the method described above, it does not need to generate artificial noise to encrypt the transmission data, and only needs to detect the channel matrix between the transmitter and the receiver, we can realize point-to-point or many-to-many confidential data transmission. Since the information will be modulated by the channel matrix during the transmission process, The receiver only needs to despread by the method of DSSS. This operation can reduce the computational complexity of the receiver and greatly simplify the receiving device. And the use of blind despreading at the receiver can also enhance anti-interference and simplify the receiving device, to a certain extent.

## II. SYSTEM MODEL

This article will construct and describe the system model based on the new spread spectrum method. Since CIMMSS is based on channel reciprocity conditions, and channel reciprocity is only established in time division duplex (TDD) working mode, this article only considers the use of CIMMSS in TDD mode.

### A. SYSTEM MODEL IN COOPERATIVE COMMUNICATION

In wireless communication, when a signal passes through a transmission channel, there will generally be fluctuations in signal strength and phase characteristics, which is called channel fading. Channel fading will reduce signal strength. This paper is based on MIMO technology to increase the diversity to achieve the effect of overcoming channel fading [11]. The data streams of the kth user in this system are $\{b_1^{(k)}\}$ and $\{b_2^{(k)}\}$.

Then the signals $\{b_1^{(k)}\}$ and $\{b_2^{(k)}\}$ of the kth user are modulated by the channel inverse matrix, in other words, multiplied by the channel inverse matrix.

$$\begin{bmatrix} \mathbf{z}_1^{(k)} \\ \mathbf{z}_2^{(k)} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \end{bmatrix}^{-1} \begin{bmatrix} b_1^{(k)} \\ b_2^{(k)} \end{bmatrix}, \tag{1}$$

where $h_{ij}, i, j \in \{1, 2\}$ is the independent Rayleigh attenuation coefficient from the base station transmitting antenna i to the k-th receiving antenna j. Thus, the baseband modulation signals $z_1^{(k)}$ and $z_2^{(k)}$ of the k-th user are obtained, k=1,...,K. The estimation of the channel matrix is usually realized by a pilot-based method, which is mainly used at the receiver. This article estimates CSI at the transmitter. This method is mainly to send the signal received by the receiver to the transmitter intact. The pilot signal received by the transmitter is equivalent to multiplying two identical channel matrices. So the channel state information can be restored by the transmitter [12].

The base station transmitter performs spread-spectrum modulation on the baseband modulation signals $z_1^{(k)}$ and $z_2^{(k)}$ to obtain spread-spectrum signals $t(z_1^{(k)})$ and $t(z_2^{(k)})$, which can be expressed as $x_1^{(k)}$ and $x_2^{(k)}$, and then transmit them by two antennas respectively.

The signals extracted by the k-th receiver are $y_1^{(k)}$ and $y_2^{(k)}$, where

$$\begin{bmatrix} y_1^{(k)} \\ y_2^{(k)} \end{bmatrix} = \begin{bmatrix} h_{11} & h_{21} \\ h_{12} & h_{22} \end{bmatrix} \begin{bmatrix} z_1^{(k)} \\ z_2^{(k)} \end{bmatrix} + \begin{bmatrix} n_1^{(k)} \\ n_2^{(k)} \end{bmatrix}, \tag{2}$$

where $n_1^{(k)}$ and $n_2^{(k)}$ are the baseband noise vectors of the antenna 1 and antenna 2 channels of the k-th receiver, respectively. It should be emphasized that the step of multiplying the channel matrix here is still valid for the signal after spreading;

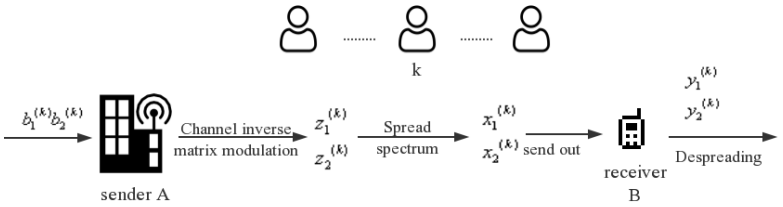



**FIGURE 1.** Communication system under CIMMSS.

Then the k-th receiver despreads the baseband signals $y_1^{(k)}$ and $y_2^{(k)}$, and extracts the base station transmit data streams $b_1^{(k)}$ and $b_2^{(k)}$. The specific communication process diagram is shown in Fig.1.

### B. SYSTEM MODEL FOR EAVESDROPPING EQUIPMENT

The system model contains three parts: transmitter A, receiver B and eavesdropper C. Assuming that A, B and C are all equipped with two antennas, there are four transmission paths between A and B. $h_{11}, h_{12}, h_{21}$, and $h_{22}$ respectively represent the attenuation coefficient of the independent Rayleigh path between A and B, which can also be generally represented by a matrix. $h_{1P}$, $h_{1Q}$, $h_{2P}$, $h_{2Q}$ represent the independent Rayleigh attenuation coefficients between A and C. The two antennas at A send the spread spectrum modulated information $x_1^{(k)}$ and $x_2^{(k)}$ to the two antennas at B. The data information received by the receiver is $y_1^{(k)}$ and $y_2^{(k)}$. If the Gaussian white noise during transmission is not considered, this process can be expressed as:

$$\begin{aligned} y_1^{(k)} &= h_{11}x_1^{(k)} + h_{21}x_2^{(k)} \\ y_2^{(k)} &= h_{12}x_1^{(k)} + h_{22}x_2^{(k)} \end{aligned} \tag{3}$$

We know that the data obtained after direct sequence spreading of $b_1^{(k)}$ and $b_2^{(k)}$ is the information received by B. B does not need to detect the channel state information (CSI) between the two ends, and data recovery can be achieved by directly despreading the received data, simplifying the receiving equipment.

Since A and the B both know the CSI, and the $x_1^{(k)}$ and $x_2^{(k)}$ of A are modulated by CSI, the information transmission in the transmission process can be realized by using CSI after despreading at the receiver.

Suppose that C eavesdrops on the information sent by A to B, and c can obtain the complete transmitter data $x_1^{(k)}$ and $x_2^{(k)}$. According to the CSI between A and C, we get the information received by C as:

$$\begin{aligned} e_1 &= h_{1P}x_1^{(k)} + h_{2P}x_2^{(k)} \\ e_2 &= h_{1Q}x_1^{(k)} + h_{2Q}x_2^{(k)} \end{aligned} \tag{4}$$

As we can see from Fig.2, the eavesdropper C can estimate the channel matrix between A and C. Since the data at the transmitter is modulated by the channel inverse matrix between A and B, C does not know the channel information between A and C. If the eavesdropper wants to use some blind despreading algorithms to recover the data, they cannot recover the correct data. Even if C detects the CSI of cooperative communication, it does not know the communication mode between A and B, and ultimately cannot eavesdrop correctly. Through this method, the confidentiality and interference effects between multi-user communications can be realized.

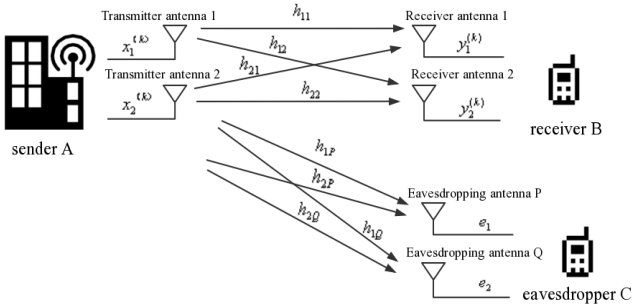



**FIGURE 2.** System model included eavesdropper.

## III. BLIND DESPREADING METHODS

The spreading code generally adopts pn code or gold code. This article uses the m sequence generated by the linear feedback shift register (LFSR) as the spreading code. Although the composite code sequence has stronger pseudo-random characteristics and is more complex than the m sequence, the low complexity of the m sequence has better performance in realizing the rapid recovery of information in the military and civilian fields. To realize the blind despreading process, we need to estimate the m sequence. The estimation of m-sequence is divided into two parts. First, we need to estimate feedback polynomial, and then estimate the initial state of LFSR. Assuming that the received demodulated signal sequences are $y_1^{(k)}$ and $y_2^{(k)}$, if you want to request the data streams $b_1^{(k)}$ and $b_2^{(k)}$ at the transmitter, you need to recover the LFSR sequence from $y_1^{(k)}$ and $y_2^{(k)}$.

### A. ORDER ESTIMATION

The demodulated signal at the antenna receiver has good autocorrelation. This article is based on a $2\times2$ MIMO system, so each user has two antennas. Two antennas correspond to two sets of data at the receiver. The operations of the two antennas are similar. Here, only one set of data is considered. Assume that the receiver of one of the antennas receives

data as $\{y\} = (y_1, y_2, y_3, ...y_n)$, and the transmitter information sequence is $\{b\}$. Because the information sequence is unbalanced, suppose the proportion of 0 in the information sequence is $0.5 + \varepsilon$, $0 < \varepsilon < 0.5$, in other words, the information sequence satisfies $p(b = 0) = 0.5+\varepsilon$. Given that there are only two numbers in the sequence $\{y\}$, 0 and 1, we first write 0 in the sequence as 1, and 1 as $-1$, and the sequence can be written as $y'_k = 1 - 2y_k$. The autocorrelation function is:

$$P(\tau) = \frac{1}{n}\sum_{k=0}^{n-1} y'_k * y'_{k+\tau}, (0 \le \tau \le M) \tag{5}$$

Because the period of the m sequence is $2^n - 1$, it is easy to know that when $\tau = k \times (2^n - 1)$, the autocorrelation function value can take the maximum value. After the generation of the autocorrelation function image, we can know the peak value of the function image, and then calculate the order of the feedback polynomial according to the period of $\tau$ corresponding to the peak value.

### B. USING WALSH-HADAMARD METHOD TO ESTIMATE FEEDBACK POLYNOMIAL

In this paper, a feedback polynomial estimation algorithm based on Walsh-Hadamard transform is used to recover the low-order feedback polynomial of the pseudo-random sequence. The principle of the algorithm is to use Walsh-Hadamard transformation to solve the error-containing equations, which extends to the use of Walsh-Hadamard transformation to solve the feedback polynomial of the m sequence. The coefficients transformed by this method can be expressed as the difference between the amount of data that makes the feedback relationship established and the amount of data that makes the feedback relationship not established. According to this principle, we only need to find the maximum value of the coefficient to know the feedback polynomial. This polynomial is the feedback polynomial with the maximum probability that it is correct [13].

The Walsh-Hadamard transformation mainly expresses that the Walsh function matrix can be easily obtained from the Hadamard matrix by using the corresponding relationship. The Walsh function matrix is a complete orthogonal function matrix that only takes 1 and $-1$. The Hadamard matrix is a square matrix with 1 and $-1$ as elements and any two rows orthogonal to each other. The lowest order square matrix is the second order square matrix, which can be expressed as

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{6}$$

For the nth order hadamard matrix, it can be expressed as

$$H_n = H_{\frac{n}{2}} \otimes H_2 \tag{7}$$

The Walsh-Hadamard transformation of $2^m$-dimensional row vector c can be expressed as

$$c^{wh} = cH_m \tag{8}$$

The specific steps of the algorithm are as follows:

1) First, we group the received information sequence a, assuming that L is the order of the feedback polynomial and N is the total length of the sequence. With L+1 data as a group, N data can be divided into N-L data groups, and then the data of each data group can be converted into decimal, we can get N-L decimal numbers, denote this sequence as b. The specific method is shown in Fig.3.
2) We convert L+1 binary numbers into decimal numbers respectively, so this decimal number has $2^{L+1}$ possibilities, Then the N-L decimal numbers are constructed into a $2^{L+1}$-dimensional vector c, and the value of each element of the vector c is equal to the number of occurrences of N-L decimal numbers.
3) Perform a Walsh-Hadamard transformation on c to generate $c^{wh}$. The position of the largest element in $c^{wh}$ is expressed in binary, and we can get the feedback polynomial. The largest element means that the error-containing equation is established the most times, and the polynomial represented by this position is most likely to be the correct feedback polynomial. The flowchart of walsh-hadamard algorithm is shown in Fig.4.

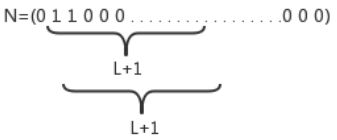



**FIGURE 3.** Sample about data grouping.

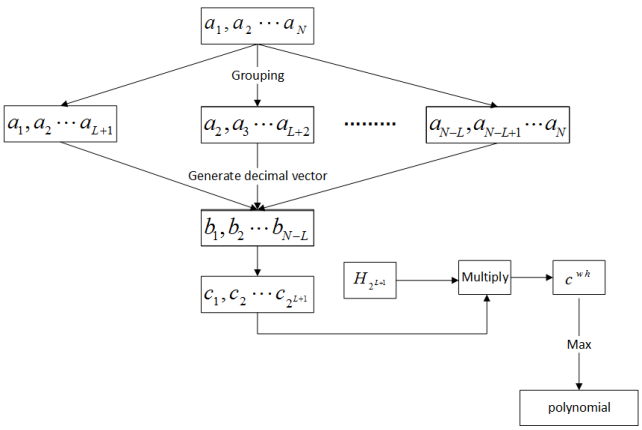



**FIGURE 4.** Walsh-Hadamard algorithm.

According to the physical meaning of the Walsh-Hadamard transformation, this method is called the maximum established quantity criterion, and this method requires the order of the feedback polynomial to be known.

### C. USING CLUZEAU ALGORITHM TO ESTIMATE FEEDBACK POLYNOMIAL

Compared with Walsh Hadamard algorithm, cluzeau algorithm does not need to determine the order of feedback polynomials first. It directly uses the demodulated sequence to

construct a random variable that obeys normal distribution, and transforms the determination of the generated polynomial into a binary hypothesis test problem [14].

Cluzeau algorithm does not search the feedback polynomial f(x) directly, but searches for the sparse multiple of f(x). When twice of f(x) is detected, it returns the nontrivial greatest common divisor (gcd) of the two detected multiples as the detected feedback polynomial. Judging whether the sparse polynomial is a multiple of f(x) is based on a statistical test of the absolute value of the variable Z, which is given by

$$Z = \sum_{t=i_{d-1}}^{N-1} (-1)^{z_t} \tag{9}$$

where $z_t$ is the modulo 2 summation of the sequence position of the corresponding order when the feedback polynomial length is d, which can be expressed as:

$$z_t = y_t \oplus \bigoplus_{j=1}^{d-1} y_{t-i_j} \tag{10}$$

Let $Q(X) = 1 + \sum_{j=1}^{d-1} X^{i_j}$, $(0 < i_1 < i_2 < \ldots < i_{d-1})$. When Q(X) is a multiple of f(x), we have

$$z_t = y_t \oplus \bigoplus_{j=1}^{d-1} y_{t-i_j} = x_t \oplus \bigoplus_{j=1}^{d-1} x_{t-i_j} \tag{11}$$

If the bias of the source is $P_r(x_t = 1) = \frac{1}{2} - \varepsilon$, we have

$$P_r(z_t = 1) = \frac{1}{2}[1 - (2\varepsilon)^{\mathrm{d}}]$$
$$Z = \sum_{t=i_{d-1}}^{N-1} (-1)^{z_t} = (N - i_{d-1}) - 2\sum_{t=i_{d-1}}^{N-1} z_t \tag{12}$$

And Z conforms to Gaussian distribution.

Obviously, when Q(X) is not a multiple of f(x),

$$P_{\mathrm{r}}(z_t = 0) = \frac{1}{2} \tag{13}$$

Regardless of whether Q(X) is a multiple of f(x), both obey the Gaussian distribution, but the average and variance of the Gaussian distribution are different. When Q(X) is not a multiple of f(x),

$$|Z| \sim N(0, N - i_{d-1}) \tag{14}$$

When Q(X) is a multiple of f(x),

$$|Z| \sim N(|\mu|, \sigma^2) \tag{15}$$

where $\mu = (N - i_{d-1})(2\varepsilon)^d$, and the normalized upper limit $\sigma^2$ of the variance is

$$(N - i_{d-1})[1 + 2d(d-1)](1 - (2\varepsilon)^{2d}) \tag{16}$$

Since Z has two different distributions, the threshold T can be used to determine whether Q(X) is a multiple of f(x), when |Z| <T, Q(X) is not a multiple of f(x); otherwise, Q(X) is a multiple of f(x). When Q(X) is not a multiple of f(x), T depends on the false alarm probability $P_{\mathrm{f}} = P_r(|Z| \geq T)$; when Q(X) is a multiple of f(x), T depends on the non-detection probability $P_n = P_r(|Z| \leq T)$.

The specific implementation steps of Cluzeau algorithm are as follows:

1) Calculate the threshold T

$$T = \frac{a(a + b\sigma)}{(2|\varepsilon|)^d} \tag{17}$$

where $a = \Phi^{-1}(1 - \frac{P_f}{2})$, $b = -\Phi^{-1}(P_n)$, $\Phi$ represents the standard normal distribution function;

2) We can calculate the required received sequence length according to the maximum order of the searched sparse multiples.

$$N = i_{L-1} + \frac{(a + b\sigma)^2}{(2\varepsilon)^{2d}} \tag{18}$$

3) Initialize Z with Z=0, take t from $i_{d-1}$ to N, calculate

$$z_t = y_t \oplus \bigoplus_{j=1}^{d-1} y_{t-i_j} \tag{19}$$

and

$$Z = Z + (-1)^{z_t} \tag{20}$$

4) If |Z| >T, then Q(X) is a sparse polynomial. Checking the first two sparse polynomials to find their gcd is the feedback polynomial.

The flowchart of cluzeau algorithm is shown in Fig.5.

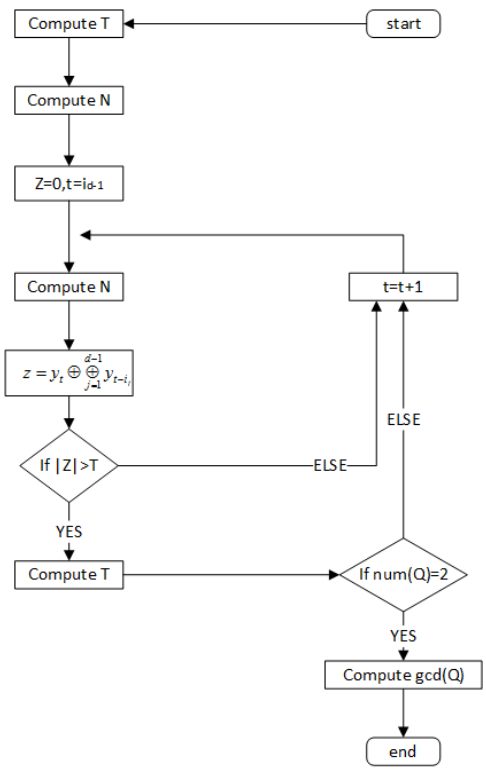



**FIGURE 5.** Cluzeau algorithm.

### D. LFSR INITIAL STATE RECOVERY

After the order of the LFSR and the feedback polynomial are determined, it is necessary to restore the initial state of the m-sequence in order to fully restore the m-sequence.

Johansson and Jonsson algorithm proposed a related attack method based on convolutional code to restore the initial state of LFSR, but this algorithm is time-consuming. This article uses the method of traversing all possible initial states and experimenting with each initial state through statistics and comparison to obtain the advantage value of sequence recovery. According to the advantage value, the initial state of the shift register is determined. When we use the wrong initial state to restore the information sequence, the ratio of 0 to 1 in the recovered sequence is almost equal, while the ratio of 0 to 1 obtained from the correct initial state to restore the information sequence is significantly different. The advantage value actually refers to the maximum value of the difference between the proportions of 0 and 1 after using different initial state recovery information sequences. For the L-level shift register, after identifying the order of the LFSR and the feedback polynomial, traverse $2^{L-1}$ initial states to recover the channel sequence, and count the advantage value of the recovered sequence. The initial state corresponding to the largest advantage value is the initial state of the LFSR.

## IV. EXPERIMENT RESULTS

In the simulation, a shorter sequence length sequence is used based on the idea of fast recovery. the rate of the transmitted signal and spreading code is known, all channels are Rayleigh flat fading channels, the number of antennas at the transmitter and the receiver are both 2, and the channel matrix between each antenna is generated by a complex Gaussian random variable with an average value of 0 and a variance of 0.01; The spreading code sequence used in the following experiments is generated by an LFSR whose initial state is 01011 and the feedback polynomial is $x^5 + x^2 + 1$. The initial information sequence is generated randomly, and the modulation method is bpsk modulation. The experimental results are also based on DIMMSS.

### A. SIMULATION OF FEEDBACK POLYNOMIAL ORDER ESTIMATION

First, autocorrelate the recovered sequence to get the result shown in Fig.6. We can see that the value of the peak position is (31, 62, 93, 124, 155, 186). According to this, the period of the judgment sequence is 31, which is the period of the pseudo-random sequence. Knowing that the period of the pseudo-random sequence of the feedback polynomial with the order of L is $2^L - 1$, the order can be calculated as 5.

This article also simulates the effect of SNR and $\varepsilon$ on the order recovery performance as shown in Fig.7, The number of Monte Carlo simulation is 500. From the image, it can be seen that the larger $\varepsilon$ is, the easier the recovery is. When $\varepsilon$ =0.4, 99% recovery of the order can be achieved when SNR>−30dB.

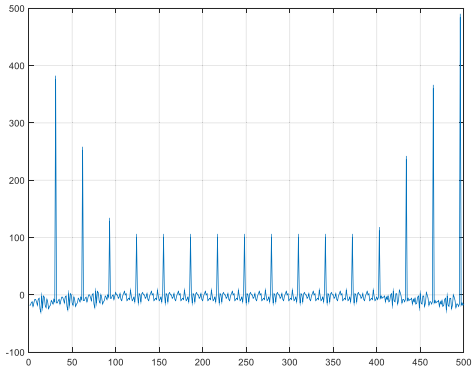



**FIGURE 6.** Autocorrelation function.

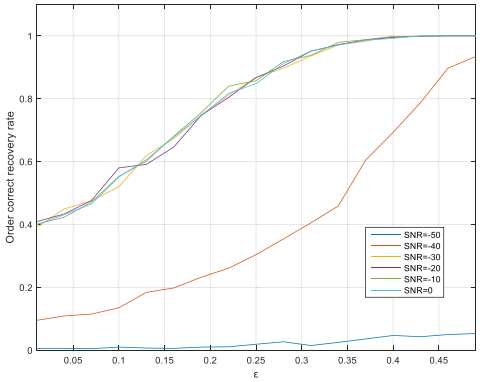



**FIGURE 7.** Order recovery performance.

### B. USING WALSH-HADAMARD ALGORITHM TO REALIZE FEEDBACK POLYNOMIAL ESTIMATION

The experiment simulates the relationship between the probability of correctly recovering the feedback polynomials by Walsh Hadamard algorithm and $\varepsilon$ under different SNR conditions. Fig.8 shows the recognition accuracy of Walsh Hadamard algorithm under different SNR values. The simulation uses a 5th-order polynomial $x^5+x^2+1$, $\varepsilon$ is changed from 0.05 to 0.45 in steps of 0.05, SNR is changed from −34dB to −22dB in steps of 3dB, and the number of Monte Carlo simulations is 1000.

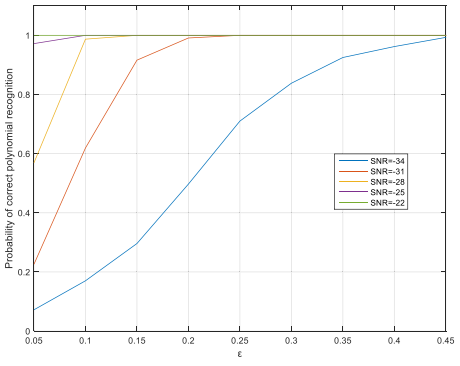



**FIGURE 8.** Restore feedback polynomial by Walsh-Hadamard algorithm with different SNR and $\varepsilon$.

When the SNR value is −22dB and $\varepsilon \geq 0.05$, the correct recovery probability of the feedback polynomial can reach 100%. When the SNR is lower than this value, the algorithm effect is reduced. It is easy to know from the image that the larger $\varepsilon$ is, the higher the probability of correct recovery of the feedback polynomial is, and the correct recovery of the feedback polynomial can be achieved even when the signal-to-noise ratio is low.

### C. USING CLUZEAU ALGORITHM TO REALIZE FEEDBACK POLYNOMIAL ESTIMATION

In this part, we mainly discuss the probability of cluzeau algorithm correctly identifying the feedback polynomial under different SNR conditions. First set the false alarm probability $p_f$ and the missed detection probability $p_n$. In this experiment, set $p_f = 2 \times 10^{-3}$ and $p_n = 10^{-3}$. This article only simulates the correct recovery rate of the feedback polynomial on the premise that the number of terms is 3, which can be written as d=3. Because the algorithm needs to know $\varepsilon$, here is set $\varepsilon = 0.25$. The simulation uses a 5th-order polynomial $x^5 + x^2 + 1$, the SNR changes from −50dB to 0dB in steps of 5dB, and the number of Monte Carlo simulations is 500 times. The simulation results are shown in the Fig.9.

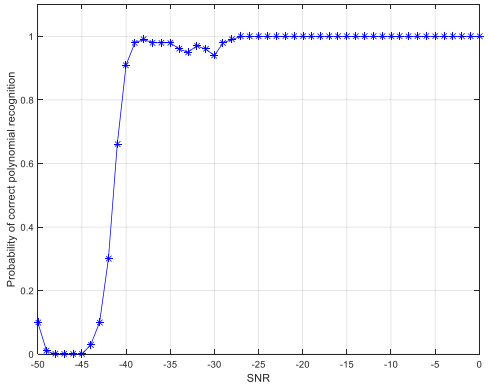



**FIGURE 9.** Restore feedback polynomial by cluzeau algorithm with different SNR.

As can be seen from the Fig.9, when the SNR is between −40dB and −35dB, the performance of the algorithm increases sharply. When the SNR is higher than −34dB, the correct recovery probability of the feedback polynomial is more than 95%, and when the SNR is higher than −27dB In this case, the probability of correct recovery of the feedback polynomial is more than 99%.

### D. COMPARISON OF TWO FEEDBACK POLYNOMIAL RECOVERY ALGORITHMS

For different two algorithms, the computational complexity of the two algorithms is compared. From the whole process of the Walsh-Hadamard algorithm, it can be seen that the calculation amount of the algorithm is mainly in the transformation of the hadamard matrix, and it can be obtained that the computational complexity of the algorithm is $O(2^{L+1} \cdot 2^{L+1})$. The computational complexity of cluzeau algorithm is mainly concentrated on traversing the various possible polynomials and then modulo two addition. The computational complexity is $O((N-L) \cdot 2^{L-2d}/\varepsilon^{2d})$. The specific simulation results are as follows.

Fig.10 and Fig.11 show the comparison of computational complexity when $\varepsilon$ is 0.05 and 0.25, the order of the feedback polynomial is from 3 to 50, and d=3 in the cluzeau algorithm. It can be seen from the image that when the order is lower than a certain value, the calculation complexity of the Walsh-hadamard algorithm is relatively low. With the increase of the order, the complexity of the algorithm increases exponentially. The complexity of cluzeau algorithm is lower than Walsh Hadamard algorithm. Among them, the computational complexity of the cluzeau algorithm is related to $\varepsilon$. The smaller the value, the higher the algorithm complexity, but in the increase of the order, the complexity of the Walsh-hadamard algorithm will always be much greater than the cluzeau algorithm. Therefore, in the process of blind despreading, one of the two different methods can be selected for operation with a lower complexity.

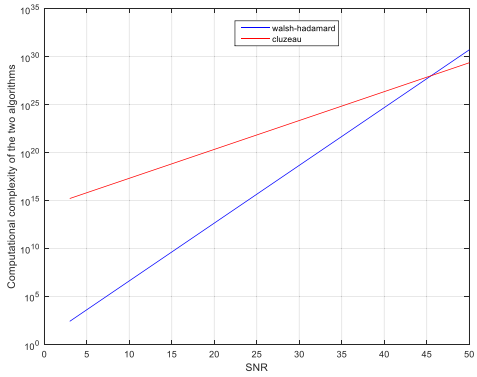



**FIGURE 10.** Computational complexity of the two algorithms when $\varepsilon$ is 0.05.

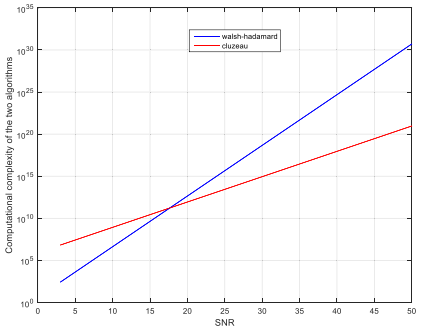



**FIGURE 11.** Computational complexity of the two algorithms when $\varepsilon$ is 0.25.

In order to more specifically illustrate the feasibility and correctness of the method proposed here, the two algorithms are compared with the algorithm in [15], The blind recovery capability of the cluzeau algorithm and the Walsh-hadamard algorithm for spreading codes under fixed a priori conditions is verified. Since the performance of the Walsh-Hadamard

algorithm is related to $\varepsilon$, the parameter $\varepsilon$ must be considered in the comparison process. The algorithm in the literature can realize the recovery of spreading code when the SNR is greater than $-22$, and the effect of the algorithm can be achieved when the Walsh-hadamard algorithm $\varepsilon$ is greater than 0.05. The cluzeau algorithm will not be affected by the parameter $\varepsilon$, and the cluzeau algorithm can recover the spreading code when the SNR is greater than $-28$dB. In summary, the two algorithms proposed in this paper have better performance when $\varepsilon$ is greater than a certain value.

### E. ESTIMATION OF THE INITIAL STATE OF PSEUDO-RANDOM SEQUENCE

The experiment also simulated the relationship between the probability of correct restoration of the initial state and $\varepsilon$ under different SNR conditions. $\varepsilon$ changed from 0.01 to 0.49 with a step length of 0.03, and the SNR changed from $-50$dB to 0dB with a step length of 10dB. The number of Monte Carlo simulations was 300. The simulation results are shown in Fig.12.

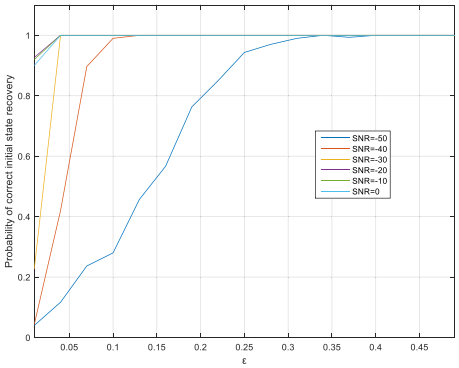



**FIGURE 12.** Initial state recovery with different SNR and $\varepsilon$.

As we can see from the Fig.12, when the SNR is greater than $-30$dB and the value of $\varepsilon$ is greater than 0.04, the algorithm can correctly restore the initial state. When the SNR is less than this value, the smaller the signal-to-noise ratio, the greater the requirement for the value of $\varepsilon$ to restore the initial state correctly.

### F. COMPARISON BETWEEN NEW SPREAD SPECTRUM AND DIRECT SEQUENCE SPREAD SPECTRUM

Spread spectrum gain is an important factor that measures and affects the anti-interference ability in the communication process. Generally, when the spreading gain is higher, the anti-interference ability during transmission is stronger. This section mainly simulates the performance of DIMMSS under different expansion gains, where the expansion gains are respectively taken as gain=5 and gain=50. In order to obtain the comparison of the performance of DIMMSS and DSSS under different spread spectrum gains, a comparative experiment will be carried out on these two methods. The number of Monte Carlo simulation is 1000, and the specific simulation results are shown in Fig.13 and Fig.14.

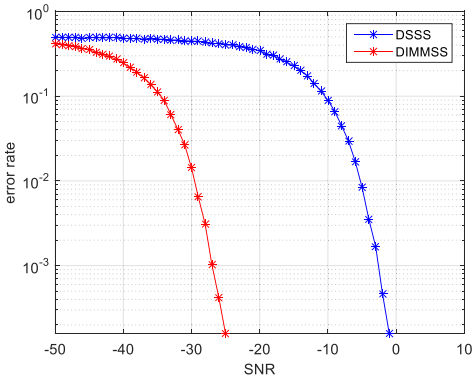



**FIGURE 13.** Comparison of anti-interference ability of DIMMSS and DSSS when gain=5.

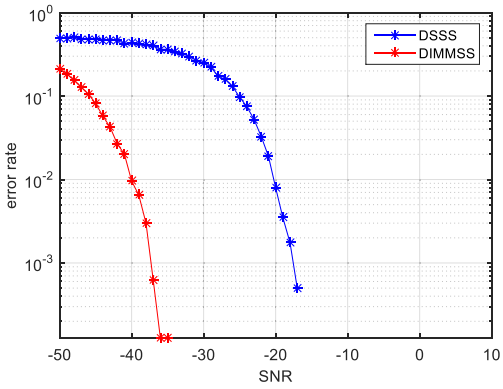



**FIGURE 14.** Comparison of anti-interference ability of DIMMSS and DSSS when gain=50.

It can be seen that when the spreading gain is 5 and SNR=$-25$dB, DIMMSS can achieve low bit error rate transmission; when the spreading gain is 50, DIMMSS only needs SNR greater than about $-35$dB to achieve low Bit error rate transmission. It can be proved that with the increase of spread spectrum gain, the anti-interference ability of DIMMSS will increase. The experiment also carried out DSSS performance simulation under the same conditions. It can be seen from Fig.13 and Fig.14 that although increasing the spread spectrum gain can improve the anti-interference ability of DSSS, no matter how the spread spectrum gain changes, the anti-interference performance of DIMMSS is better than DSSS. According to [16], the existing spread spectrum technology generally achieves performance of $-10\lg$ (gain), that is to say, when gain=5, SNR=$-7$dB can realize transmission; when gain=50, SNR=$-17$dB can realize transmission. But it can be seen that DIMMSS performs better.

We also compared the anti-eavesdropping ability of DIMMSS under the condition of gain=50. In the simulation comparison between cooperative communication and non-cooperative communication, the main difference is that the CSI through the channel is different, as shown in Fig.15.

The experimental simulation shows that since the eavesdropper does not know the CSI in the cooperative communication, the information sequence cannot be recovered correctly.

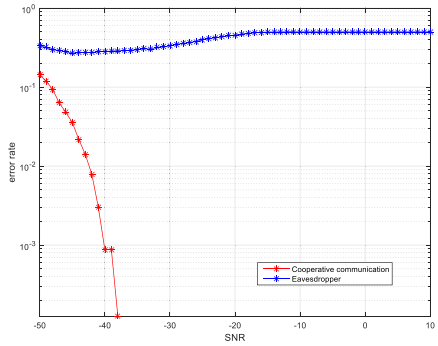



**FIGURE 15.** Anti-eavesdropping performance.

## V. CONCLUSION

For the MIMO system, this article first proposes a new spread spectrum method for channel inverse matrix modulation. This new spread spectrum method can not only simplify the receiving equipment, but also improve the anti-eavesdropping ability in MIMO wireless communication. Through simulation experiments, the use of this spread spectrum method can also improve the anti-interference ability of the system, and can be used to restore the information sequence in the case of a lower signal-to-noise ratio. This paper also proposes to apply the Walsh-hadamard algorithm and the cluzeau algorithm to despreading. These two methods have advantages for lower-order and higher-order feedback polynomial recovery. Effective use of these two methods at the receiver can realize fast calculation of the blind despreading process. However, this method does not perform channel coding, so there may be several bits of error. The more errors, the greater the impact on the algorithm performance.

## REFERENCES

[1] D.-Y. Tang, "Soft spectrum spreading technique combining RS error-correction coding and Walsh transforming," *Telecommun. Eng.*, vol. 52, no. 6, pp. 943–947, 2012.

[2] P. C. J. Hill and M. E. Ridley, "Blind estimation of direct-sequence spread spectrum m-sequence chip codes," in *Proc. IEEE 6th Int. Symp. Spread Spectr. Techn. Appl.*, Sep. 2000, pp. 305–309.

[3] G. Burel and C. Bouder, "Blind estimation of the pseudo-random sequence of a direct sequence spread spectrum signal," in *Proc. 21st Century Mil. Commun. Archit. Technol. Inf. Superiority (MILCOM)*, Oct. 2000, pp. 967–970.

[4] C. Ma, L. M. Zhang, and J. X. Wang, "Blind estimation of long code DSSS signal based on subspace tracking," *Appl. Mech. Mater.*, vols. 484–485, pp. 976–981, Mar. 2014.

[5] T. Zhang, S. Dai, G. Ma, W. Zhanq, and P. Miao, "Approach to blind estimation of the PN sequence in DS-SS signals with residual carrier," *J. Syst. Eng. Electron.*, vol. 21, no. 1, pp. 1–8, Feb. 2010.

[6] S. Mehboodi, M. Farhang, and A. Jamshidi, "Maximum likelihood estimation of pseudo-noise sequences in non-cooperative direct-sequence spread-spectrum communication systems," in *Proc. 24th Iranian Conf. Electr. Eng. (ICEE)*, May 2016, pp. 119–123.

[7] L. Xiao, G. Xuan, and Y. Wu, "Blind estimation of chaotic spread spectrum sequences by neural network," in *Proc. 11th Int. Congr. Image Signal Process., Biomed. Eng. Inform. (CISP-BMEI)*, Oct. 2018, pp. 1–9.

[8] L. Wei-jia and L. Huan, "Signal combining and self-interference cancellation scheme based on linear neural network in a full-duplex receiver cooperative jamming system," *J. Beijing Univ. Posts Telecommun.*, vol. 43, no. 1, p. 61, 2020, doi: 10.13190/j.jbupt.2019-067.

[9] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 4766–4781, Sep. 2014.

[10] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[11] W.-H. Wu, Y.-H. Cao, S.-H. Wang, T.-S. Yeo, and M. Wang, "MIMO waveform design combined with constellation mapping for the integrated system of radar and communication," *Signal Process.*, vol. 170, May 2020, Art. no. 107443.

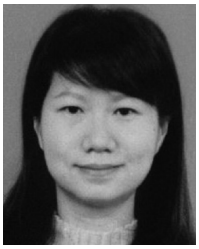
[12] H. Huang, J. Yang, H. Huang, Y. Song, and G. Gui, "Deep learning for super-resolution channel estimation and DOA estimation based massive MIMO system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8549–8560, Sep. 2018.

[13] Y. Ma and L. M. Zhang, "Reconstruction of scrambler with real-time test," *J. Electron. Inf. Technol.*, vol. 38, no. 7, pp. 1794–1799, 2016, doi: 10.11999/JEIT151068.

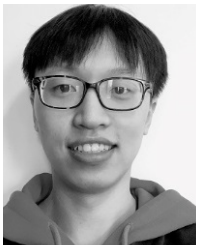
[14] X.-B. Liu, S. N. Koh, X.-W. Wu, and C.-C. Chui, "Reconstructing a linear scrambler with improved detection capability and in the presence of noise," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 208–218, Feb. 2012.

[15] Y. Qiang and S. Yulong, "Similarity based blind despread method of DS-SS signal," *Syst. Eng. Electron.* vol. 39, no. 7, pp. 1451–1456, 2017.

[16] Z. Li, W. Tan, C. Kang, and J. Cheng, "Research on anti-interference ability of direct sequence spread spectrum system," *J. Electron. Inf. Technol.*, vol. 43, no. 1, pp. 116–123, 2021.



**YONGLI AN** received the Ph.D. degree in information science from Beijing Jiaotong University, Beijing, China, in 2015. She is currently with the College of Information Engineering, North China University of Science and Technology, Tangshan, China. Her current research interests include multi-antenna processing technology, metamaterial antenna, interference cancellation technology, and large-scale MIMO technology.



**CHENGMING ZHANG** was born in 1995. He received the bachelor's degree from the Nanjing University of Posts and Telecommunications, in 2017. He is currently pursuing the master's degree with the North China University of Technology.

**ZHANLIN JI** received the M.Eng. degree from Dublin City University, in 2006, and the Ph.D. degree from the University of Limerick, Ireland, in 2010. He is currently a Professor with the North China University of Science and Technology, China, and a Researcher with the Telecommunications Research Centre (TRC), University of Limerick. He has authored/coauthored 70 research papers in refereed journals and conferences. His research interests include UCWW, the Internet of Things (IoT), cloud computing, big data management, and data mining.

**ZHICHAO ZHOU** was born in 1989. He received the master's and Ph.D. degrees from the Institute of Information Science, Beijing Jiaotong University, in 2013 and 2017, respectively. He is currently working with the 5G Innovation Center, Network Technology Research Institute, China Unicom. He has published 16 articles as corresponding author and 14 of them have been cited by SCI and EI. His research interests include beamforming in 5G, signal processing, wireless resource allocations, pilot contamination reduction in massive MIMO, V2X, and positioning based on mobile communication networks.