IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 January 2024, accepted 5 February 2024, date of publication 22 February 2024, date of current version 8 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3368868

RESEARCH ARTICLE

A Novel Voting Model Based on Parity Check Equations for Blind Detection of M-Sequences

PING WANG[1], QIANG YANG[2,3], YANGHENG HU[2], JIAN XIONG[1], YONG JIA[4], (Member, IEEE), AND DEQUAN GUO[2]

[1]School of Network and Communication Engineering, Chengdu Technological University, Chengdu, Sichuan 610731, China
[2]School of Automation, Chengdu University of Information Technology, Chengdu, Sichuan 610225, China
[3]Key Laboratory of Natural Disaster Monitoring and Early Warning and Assessment of Jiangxi Province, Jiangxi Normal University, Nanchang 330022, China
[4]School of Mechanical and Electrical Engineering, Chengdu University of Technology, Sichuan 610225, China

Corresponding author: Jian Xiong (jianxio1@sina.com)

This work was supported in part by the International Joint Research Center of Robots and Intelligence Program under Grant JQZN2022-001; in part by the School Project of Chengdu Technological University under Grant 2023ZR007, Grant 2023ZR006, and Grant 2023ZR008; in part by the Sichuan Science and Technology Program under Grant 2023YFN0009, Grant 2022YFN0020, Grant 2020YFG0177, Grant 2022YFG0360, and Grant 2021YFS0313; in part by the School Project of Chengdu University of Information Technology under Grant KYTZ202148; in part by the Chengdu Technical Innovation Research Program under Grant 2022-YF05-01134-SN; in part by Science and Technology of Xizang Autonomous Region under Grant CGZH2024000151; and in part by Opening Fund of Key Laboratory of Natural Disaster Monitoring, Early Warning and Assessment of Jiangxi Province (Jiangxi Normal University) under Grant JXZRZH202304.

ABSTRACT A novel acquisition scheme of pseudo-noise (PN) codes is proposed for spreading satellite communication systems relying on the proposed multi-voter model of this paper. Based on the proposed model, the acquisition of PN codes can be attributed to a voting and selecting mechanism to pick out the erroneous chips. Although message passing algorithm (MPA) is a feasible algorithm for decoding PN codes, MPA does not get good detection performance due to the limited number of parity check equations in the acquisition scheme. To overcome the negative impact of the limited number of parity check equations, this paper proposes single-voter and multi-voter models, which combine chip and sequence estimation on the basis of the chip-flipping (CF). It is known that the bit-flipping (BF), weighted-bit-flipping (WBF) and other algorithms based on BF are credible for low density parity check (LDPC) codes. Because of the lack of research, these algorithms have not been extended to the detection of PN codes. As the same as BF, the inputs of the proposed CF algorithm are the hard-decision samples. For the proposed CF, there exists an optimal flipping-threshold which is similar to the random weight of the WBF. Owing to the low computation complexity of CF, the unlimited number of parity check equations can be enabled in the voting model. The experimental results show that the detection performance of the proposed method of $N > 15$ is improved by 2 dB compared with MAP-based method and 4 dB compared with LEAP-based method at the detection probability 99%.

INDEX TERMS PN codes, voting model, detection algorithm, MPA.

I. INTRODUCTION

PN codes have been widely applied in the spreading satellite communications for unmanned aerial vehicles (UAVs), radar, vehicles and Internet-of-Things (IoT) [1], [2], [3], [4], [5]. The acquisition of PN codes is important for spreading communications because it is necessary for the receivers to accurately capture the PN codes [6]. Due to the good pseudo-random properties, m-sequences are considered as the basic PN codes [7].

Recently, some methods have been proposed for the blind detection of PN codes. Reference [27] blindly estimated the PN codes parameter and the characteristic polynomial with the repeated patterns, the linearity and the coidentity

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

of PN codes and the linear feedback shift register states. Reference [1] introduced a two-step PN codes estimation method based on sparse recovery. The proposed method is able to estimate PN codes from the BPSK signal in serious electromagnetic environments. Reference [28] proposed to exploit the finite symbol characteristics of information and spreading sequences. And then the iterative least square with projection method was adopted. Reference [29] proposed an improved estimation algorithm for the feedback polynomial of the linear PN codes constituting a search process and a verification process of feedback polynomial candidates to determine the correct feedback polynomial of the scrambler. However, these methods are designed for universal PN codes and the specific characteristics of m-sequences are not technically analyzed for the improvement.

The conventional method to detect m-sequences is that the receiver performs a sliding correlation between the received sequence and the local replica. The receiver synchronizes with the transmitter when the correlation value is greater than a given threshold [8], [9]. If the receiver does not save the local replica, the blind detection process is necessary. In fact, an m-sequence is a cyclic and linear code which is defined by a characteristic polynomial [10]. Suitable algorithms were designed to decode m-sequences blindly in [11], [12], and [13]. Some good algorithms were initially proposed in the cryptography [8], [14]. Then some improved algorithms were extended in wireless communications and navigation domains [13], [15], [16], [17], [18]. It is a necessary task for the receiver to decide whether an m-sequence is received, and if so, restore it [19]. Therefore, this is a joint problem of capturing and decoding the m-sequence [20]. By applying the parity check equations for iterations, the MPA-based method could achieve detecting m-sequence successfully [19], [20]. More specifically, [21] proposed an iterative MPA based on a redundant graphical model (RGM). In the algorithm, the parity check matrix E concatenates K elementary parity check matrices. Each elementary matrix is generated by consecutive cyclic shifts of one parity check equation [21]. With consideration of the computation complexity, the Hamming weight (number of non-zero coefficients), denoted by t, must be low. Actually, the detection performance deteriorates with the growing of t [8], [9], [24], which means that $t = 3$ is the best choice to decode m-sequences. In [22], a selection method of parity check equations of weight $t = 3$ was proposed. Several parity check equations are worked out and then applied to decode m-sequences based on MPA. M-sequences are Hamming codes represented by the characteristic polynomial $p(x)$, and contain many code words of weight $t = 3$. Reference [23] proposed a rapid code acquisition scheme based on MPA. This scheme is effective in low spreading factor satellite communication system.

However, the above MPA-based methods are mainly suitable for the limited decoding condition, in which only K elementary parity check matrix of m-sequences are enabled [22]. In fact, L-1 ($L \gg K$) elementary parity check matrix can be obtained [9], [26], which means that the above methods do not make full use of the correlation characteristic of m-sequences. In [24] and [25], an online supervised learning machine (LEAP) which aimed to make full use of the correlation characteristics of the PN sequence was proposed. However, the LEAP often fails to converge to the optimum performance and the large learning step may trigger the instability.

Inspired by the previous works, a novel estimation method based on CF is introduced for m-sequences. In summary, our main contribution are listed lie in the following folds:

(1) Based on the above methods, in this paper, we propose a voting model based on CF and apply it into the field of m-sequences estimation of spreading signals. Compared to the MPA, the voting model uses L-1 ($L \gg K$) elementary parity check matrix instead of K ones, which can greatly improve the detection performance of the network. Namely, the voting model make full use of the correlation characteristic with L-1 ($L \gg K$) elementary parity check matrix. In the model, the decoder generates $3(L\text{-}1)/2$ voters, who votes for the received chips. When one chip gets more than T votes, the chip will be flipped by the decoder.

(2) The optimum flipping threshold T determines the detection performance of the voting model, which is an important issue in this paper. Based on minimizing outputting error chip rate, the optimum flipping thresholds can be worked out.

(3) The proposed method is verified by Monte-Carlo simulations. Compared to the MPA and LEAP, the voting-model-based method has a better detection performance.

To make the novelty of the proposed method more clearly, the difference among our method and the majority works are given as follows:

(1) We believe that the abandoned check equations in the MPA-method be enable for the decoding, hence more priori information shall help the detection of m-sequences. In this paper, due the low computation complexity, the hard-decision chips are considered as the input of our method. Therefore, the abandoned check equations can be permitted to generate the parity check matrix in the iterative decoding work. We establish a single-voter model and a multi-voter model for enabling more priori information and the performance benefits are gained from the proposed model.

(2) The MPA-based method is an effective method for the detection of m-sequences. While applying such method, a large mount of soft information are necessary to be circularly renewed in the iterative decoding work, therefore the computation complexity is relatively high. Due to the computation complexity, only several check equations are employed to generate the parity check matrix in the MPA-based method in the works, like [22] and [23].

(3) The LEAP-based method is adaptive to non-stationary input and requires no priori information of statistical changes of the input. Since it requires a little of memory or data storage, the LEAP is very suitable for using in engineering. However, the small learning step also severely limits its performance.

(4) When the TCF-based method is applied for the detection, it is necessary for the peaks of the TCF to be accurately searched and this is really difficult to achieve in low SNR environments, and this method loses its detection performance compared with other method in the paper.

This paper is organized as follows. Several basic theories are presented in Section II and then some relevant conclusions are derived. The single-voter model and multi-voter model are established in Section III. Then the decoding scheme based on the multi-voter model is also proposed in this part. The Monte-Carlo simulations are performed in Section IV, in which the proposed method is compared with the baseline methods.

II. SEVERAL BASIC THEORIES OF THE M-SEQUENCE

An m-sequence can be generated by a linear feedback shift register (LFSR) sequence generator. The characteristic polynomial of r-stage LFSR can be expressed as follows [26]:

$$g(D) = g_r D^r + g_{r-1} D^{r-1} + \cdots + g_1 D + g_0, \quad g_i \in \{0, 1\}, 1 \le i \le r \tag{1}$$

where $g_0 = g_r = 1$. As indicated in [26], the m-sequence generated by the LFSR generator satisfies the constraint as follows:

$$g_r x_k \oplus g_{r-1} x_{k+1} \oplus \cdots \oplus x_{k+r} = 0 \tag{2}$$

where $\oplus$ indicates modulo-2 addition and x_k denotes the chip of the m-sequence at time k. The cycle period of the m-sequence is $L = 2^r - 1$.

The mentioned r-stage LFSR is shown in FIGURE 1. The feedback taps are given by the characteristic polynomial as formula (2) with $g_0 = g_r = 1$. More specifically, for the generated m-sequence $\boldsymbol{x} = [x_0, \ldots, x_{L-1}]$, $g(D)$ is a primitive polynomial of degree r, in which case the period of the m-sequence is $L = 2^r - 1$.

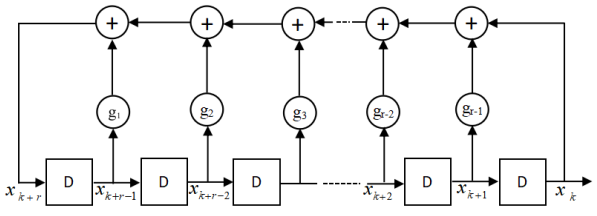


FIGURE 1. Fibonacci feedback generator of r-stage LFSR.

Triple correlation function (TCF) is usually used to work out the parity check equations of weight $t = 3$ [9], [26]. It is indicated in [26] that an m-sequence of length L is featured with L-1 parity check equations of weight $t = 3$.

Several basic properties of m-sequences are given as follows [9]:

1) The number of 1 in m-sequences is almost equal to the number of 0. More specifically, the number of 1 is one more than the number of 0.
2) The m-sequences are shift-addictive. An m-sequence can be noted as $C[n]$ and its replica with circle shift τ_1 can be noted as $C[n + \tau_1]$. Modulo-2 addition between $C[n]$ and $C[n + \tau_1]$ generates another shifted m-sequence $C[n + \tau_2]$. The shift-addictive property can be expressed as:

$$C[n] \oplus C[n + \tau_1] = C[n + \tau_2] \tag{3}$$

Formula (3) shows the check relationship of 3 replicas ($C[n]$, $C[n + \tau_1]$ and $C[n + \tau_2]$), which means that all the parity check equations of weight $t = 3$ can be represented by formula (3). In our paper, τ_1 and τ_2 in formula (3) are noted as (τ_1, τ_2), the number of which is L-1 [26].

All the (τ_1, τ_2) can be included in a collection, which is noted as set Ψ in this paper. According to the rule of modulo-2 addition, it can be performed to swap the place of τ_1 and τ_2, which means that (τ_1, τ_2) and (τ_2, τ_1) represent the same relationships. In order to avoid the repeated checks, (τ_1, τ_2) in set Ψ is constrained to $0 < \tau_1 < \tau_2 \le L$. Therefore, the number of valid check equations $(\tau_1, \tau_2) \in \Psi$ is reduced to $\frac{L-1}{2}$. Thus set Ψ has the form as:

$$\Psi = \left\{ (\tau_1, \tau_2) \,\middle|\, \begin{array}{l} 0 < \tau_1 < \tau_2 \le L, \text{and} \\ C[n] \oplus C[n + \tau_1] = C[n + \tau_2] \end{array} \right\} \tag{4}$$

For the reduction of the voting model in the following chapter, $C[n + \tau_2]$ in formula (3) and (4) on the right side can be moved to the left side, and then formula can be expressed as:

$$C[n] \oplus C[n + \tau_1] \oplus C[n + \tau_2] = 0 \tag{5}$$

According to the rule of modulo-2 addition, formula (5) is only applicable for 0/1 sequence. While the rule of formula (5) is applied to +1/-1 sequence, formula (5) can be equivalently replaced by the following form:

$$C[n]\, C[n + \tau_1]\, C[n + \tau_2] = 1 \tag{6}$$

For any τ_1 and τ_2 that do not satisfy formula (3), the relationship of them has the form as:

$$C[n]\, C[n + \tau_1]\, C[n + \tau_2] = -1 \text{ or} 1 \tag{7}$$

According to the [9], [25], the triple correlation of m-sequences can be expressed as follows:

$$\begin{aligned} &R(\tau_1, \tau_2) \\ &= \sum_{n=1}^{L} C[n]\, C[n + \tau_1]\, C[n + \tau_2] \\ &= \begin{cases} L, for\ (\tau_1, \tau_2) \in \Psi \\ -1, for\ (\tau_1, \tau_2) \notin \Psi \end{cases} (0 < \tau_1 < \tau_2 \le L) \end{aligned} \tag{8}$$

Formula (8) shows that all the $(\tau_1, \tau_2) \in \Psi$ can be worked out by searching the peak points of $R(\tau_1, \tau_2)$. In FIGURE 2, the triple correlation $R(\tau_1, \tau_2)$ of length $L = 2^7 - 1 = 127$ is showed. In order to avoid the repeated checks, (τ_1, τ_2) in set Ψ is constrained to $0 < \tau_1 < \tau_2 \le 127$. There are 63 peak points of triple correlation in the figure, which means that the check equations $(\tau_1, \tau_2) \in \Psi$ can been found with searching the peak points of $R(\tau_1, \tau_2)$.

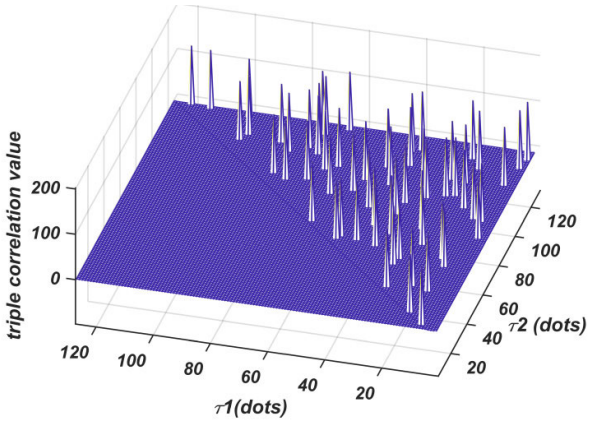


FIGURE 2. The triple correlation of the m-sequence with length L = 127.

III. THE DESIGN OF VOTING MODEL

A. THE DESIGN OF THE SINGLE-VOTER MODEL

In this section, variable X, called as a voter, is established in this paper. The special voter is empowered to propose flipping suggestion for each hard-decision chip. When chip $s[k]$ is correct, the voter ought to cast a do-not-flip vote, which is expressed as 0 in our pater. Similarly, when chip $s[k]$ is erroneous, the voter ought to cast a do-flip vote, which is expressed as 1. For the k^{th} hard-decision chip of the received sequence, the vote of X can be noted as:

$$X(k) = \begin{cases} 1, & \text{do flip} \\ 0, & \text{do not flip} \end{cases} \tag{9}$$

To generate voter X, it is necessary that variable Y should be established firstly. In our paper, variable Y is defined as:

$$Y(k) = s[k]\, s[k+\tau_1]\, s[k+\tau_2] \tag{10}$$

where $s[0]$, s [1], …, $s[k]$, …, $s[L\text{-}1]$ are the hard-decision chips of the received sequence over the wireless channel. Meanwhile, τ_1 and τ_2 satisfy $(\tau_1, \tau_2) \in \Psi$. Due to the basic properties of m-sequences, $Y(k)$ will equal 1 if the received sequence is an m-sequence and there is no erroneous chips in $s[k]$, $s[k+\tau_1]$ and $s[k+\tau_2]$. Otherwise if any one in $s[k]$, $s[k+\tau_1]$ and $s[k+\tau_2]$ is erroneous, $Y(k)$ will equal -1. Therefore, it is feasible to apply $Y(k)$ as an indicator to decide whether $s[k]$ is correct or not.

The mapping in formula (11) is performed in the paper and voter X is established.

$$X(k) = \begin{cases} 1, & for Y(k) = -1 \\ 0, & for Y(k) = 1 \end{cases} \tag{11}$$

Thus, the flipping suggestions of voter X for chip $s[k]$ are related to the 3 chips ($s[k]$, $s[k+\tau_1]$ and $s[k+\tau_2]$). The do-flip suggestion for chip $s[k]$ will be offered by $X(k)$, when any one of the 3 chips is erroneous. Therefore, the single-voter model probably propose a false suggestion for chip $s[k]$ because $s[k+\tau_1]$ and $s[k+\tau_2]$ also have extra impact on the suggestion as shown in formula (10). In order to avoid the false suggestions of single voter, the multi-voter model is derived in the next subsection.

First of all, it is necessary to analyze the efforts of false suggestions. When chip $s[k]$ is correct, voter X ought to cast a do-not-flip vote otherwise a false alarm occurs. Similarly, when chip $s[k]$ is erroneous, the voter ought to cast a do-flip vote otherwise an missed detection occurs. Either false alarms or missed detection causes erroneous output.

It is assumed that chip error rate of the hard-decision chips is p_0. According to the theories of the mathematical statistics, the error probability of an single chip equals to p_0. As demonstrated in formula (10) and (11), if one of the 2 chips ($s[k+\tau_1]$ and $s[k+\tau_2]$) is erroneous, voter X will equal to 1. And then the false alarm occurs although chip $s[k]$ is correct. The false alarm probability p_{fa} can be expressed as follows:

$$\begin{aligned} p_{fa} &= p(X(k) = 1 \,|\, s(k) \text{ is correct}) \\ &= C_2^1 \times p_0 \times (1 - p_0) \\ &= 2p_0(1 - p_0) \end{aligned} \tag{12}$$

Similarly, if one of 2 chips ($s[k+\tau_1]$ and $s[k+\tau_2]$) is erroneous, voter X will equal 0. And then the missed detection occurs although chip $s[k]$ is erroneous. The missed detection probability p_{miss} can be expressed as follows:

$$\begin{aligned} p_{miss} &= p(X(k) = 0 \,|\, s(k) \text{ is wrong}) \\ &= C_2^1 \times p_0 \times (1 - p_0) \\ &= 2p_0(1 - p_0) \end{aligned} \tag{13}$$

An interesting conclusion can be drawn in (12) and (13), the false alarm probability p_{fa} and the missed detection probability p_{miss} are equal.

B. THE DESIGN OF THE MULTI-VOTER MODEL

In this section, the multi-voter model will be derived. It can been seen from formula (10) in Section III-A that 3 voters of $s[k]$ can be worked out from the transformation of k. Besides (10), one voter $Y_2(k) = s[k-\tau_1]\, s[k]\, s[k+\tau_2-\tau_1]$ in the multi-voter model can be worked out from transformation $k = k - \tau_1$. Another voter $Y_3(k) = s[k-\tau_2]\, s[k+\tau_1-\tau_2]\, s[k]$ can be worked out from transformation $k = k - \tau_2$. As presented in the Section II, the number of $(\tau_1, \tau_2) \in \Psi$ is $\frac{L-1}{2}$ and then $\frac{3(L-1)}{2}$ voters can be obtained. If necessary, all of the voters can offer flipping suggestions for each received chip at the receiver.

It is assumed that V check equations are extracted from set Ψ in one iterative loop, and then $N = 3V$ voters are generated through the above transformation. The voting model decides for each chip whether to flip or not. If chip $s[k]$ gets more than T do-flip votes, the voting model flips it. The do-flip thresholds T are worked out for different N below.

When chip $s[k]$ is correct the voter ought to cast a do-not-flip vote, otherwise the false alarm occurs. More specifically, a false alarm occurs in the multi-voter model if more than T voters cast do-flip votes for chip $s[k]$ when the chip is correct.

In the multi-voter model, when the correct chip is voted by N voters and the chip gets T do-flip votes, the false alarm occurs and the false alarm probability can be expressed as $C_N^T p_{fa}^T \left(1-p_{fa}\right)^{N-T}$, where p_{fa} is the false alarm probability of single-voter model in formula (12). Similarly, when the chip get m (more than T) votes, the false alarm probability can be expressed $C_N^m p_{fa}^m \left(1-p_{fa}\right)^{N-m}$. Therefore, the false alarm probability P_f in the multi-voter model can be expressed as:

$$P_f = \sum_{m=T}^{N} C_N^m p_{fa}^m \left(1-p_{fa}\right)^{N-m} \tag{14}$$

where p_{fa} is defined by (12), and T is the do-flip threshold, and $C_N^m = \frac{N!}{m!(N-m)!}$ is the formula of permutation and combination.

Similarly, when chip $s[k]$ is erroneous, the voter ought to cast a do-flip vote otherwise the missed detection occurs. More specifically, missed detection occurs if less than T voters cast do-flip votes for chip $s[k]$ when the chip is erroneous. In the multi-voter model, when the erroneous chip is voted by N voters and the chip gets T do-flip votes, the erroneous chip will be elected to flip and restore, the correct detection probability is $C_N^T \left(1-p_{miss}\right)^T p_{miss}^{N-T}$, where p_{miss} is the false alarm probability of single-voter model in formula (13), and so on. When the erroneous chip gets more T do-flip votes, the correct detection probability of erroneous chips is $\sum_{m=T}^{N} C_N^m \left(1-p_{miss}\right)^m p_{miss}^{N-m}$. Therefore, the missed detection probability P_m in the multi-voter model can be expressed as:

$$P_m = 1 - \sum_{m=T}^{N} C_N^m \left(1-p_{miss}\right)^m p_{miss}^{N-m} \tag{15}$$

where p_{miss} is defined by (13).

As demonstrated in (12), (13), (14) and (15), P_f and P_m are relevant to p_0, N and T.

FIGURE 3(a) shows P_f versus T with the configurations $N = 3, 6, 9, 12, 15$. FIGURE 3(b) shows P_m versus T with the same configurations for FIGURE 3(a). The chip error rate of the hard-decision chips is set to $p_0 = 10\%$. It can be seen that P_f increases with the growing of N. Contrarily, P_m decreases with the growing of N. It can be concluded that P_f and P_m can not reach the minimum simultaneously.

Since false alarms and missed detection probably introduce new erroneous chips, it is necessary to apply an suitable threshold for flipping the chips.

The do-flip threshold T is worked out by minimizing the chip error rate P_e, which can be expressed as:

$$P_e = P_f \times (1-p_0) + P_m \times p_0 \tag{16}$$

FIGURE 4 shows P_e versus T when the input chip error rate is set to $p_0 = 0.1, 0.2, 0.3, 0.4, 0.5$. The number of voters in one iteration is set to (a) $N = 15$, (b) $N = 30$, (c) $N = 60$.

Following conclusions can be drawn from FIGURE 4:

1) FIGURE 4(a) shows that P_e reaches its minimum at the point $T = 9$ for all the configurations $p_0 = 0.1, 0.2, 0.3, 0.4, 0.5$, when $N = 15$. It can be seen that P_e is probably greater than 0.5, when the do-flip threshold is not suitable and many correct chips are flipped. When $N = 15$, the convergence reaches its fastest at point $T = 9$, where the minimum of P_e is less than p_0. More specifically, the number of erroneous chips can be reduced after one voting event, which means that the erroneous chips can be restored by iterations. In this paper, the optimal configuration is noted as ($N = 15$, $T = 9$).
2) Similarly, FIGURE 4(b) (c) show that there are other optimal configurations, i.e., ($N = 30$, $T = 17$), ($N = 60$, $T = 32$). It can be summarized that the optimal configurations can be expressed as $T = \lfloor N/2 \rfloor + 2$. This conclusion of the multi-voter model can be applied to the proposed acquisition scheme of this paper.
3) FIGURE 4(a) (b) (c) show that the minimum of P_e decreases with the growing of N for a given p_0. It is demonstrated that fewer iterations are needed to restore the m-sequence when more voters are generated in one iteration. This will be even more visible in the simulation presented in Section IV.

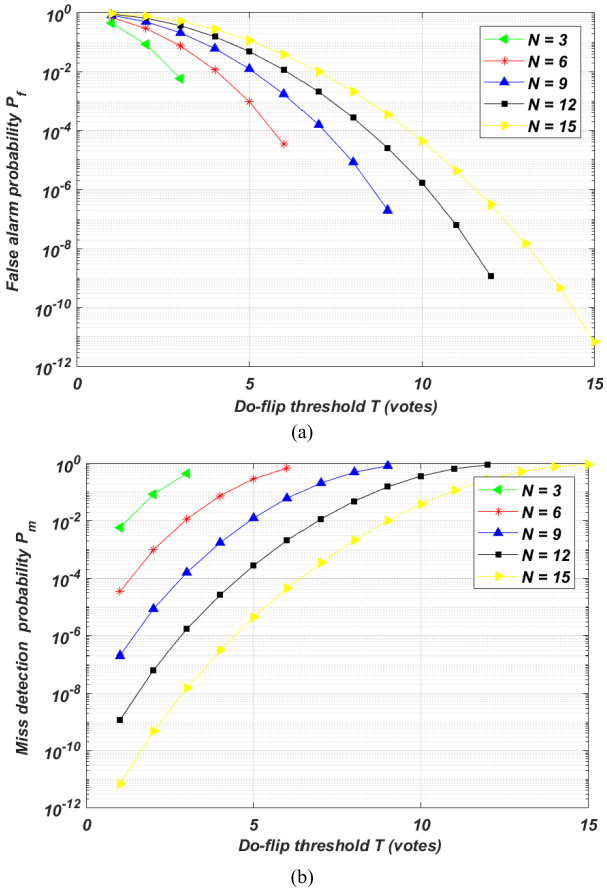


FIGURE 3. Specific performance of multi-voter model under different do-flip thresholds T with chip error rate $P_0 = 10\%$: (a) the false alarm probability P_f; (b) the missed detection probability P_m.

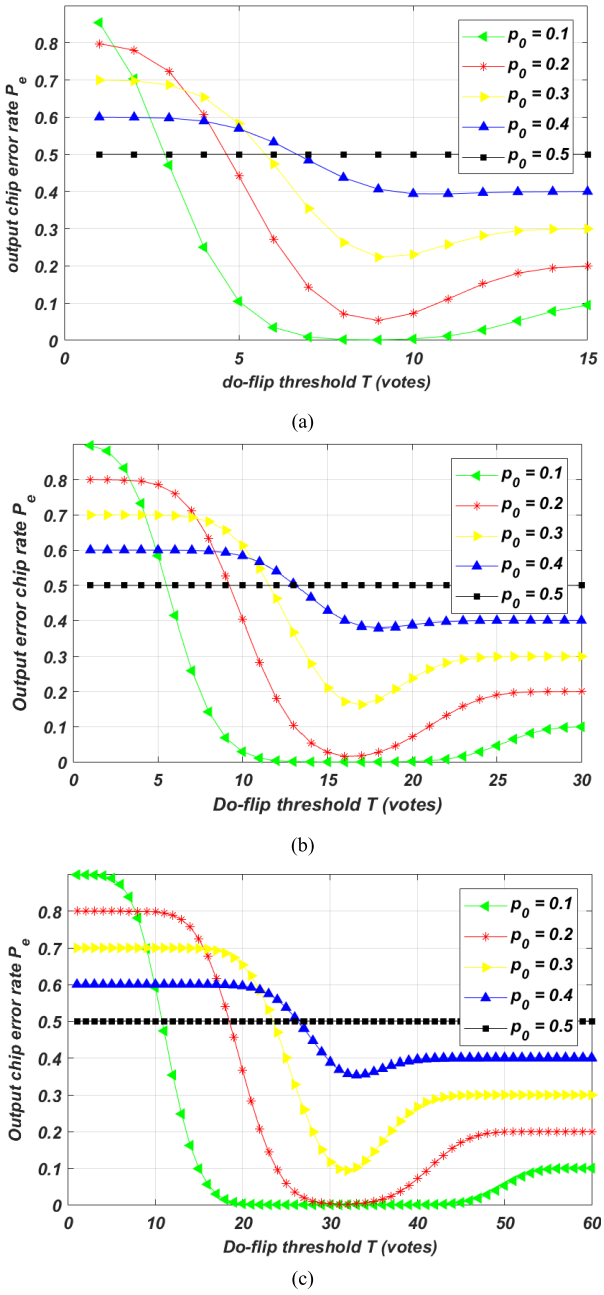


FIGURE 4. The output chip error rate P_e versus do-flip thresholds T with different number of voters: (a) the number of voters is set to $N = 15$; (b) the number of voters is set to $N = 30$; (c) the number of voters is set to $N = 60$.

4) FIGURE 4(a) (b) (c) demonstrate that the minimum of P_e is more faint with a higher p_0 for a given N and more obvious with a larger N for a given p_0. More specifically, a larger N means a faster convergence. The spreading spectrum system usually works in the low signal-to-noise ratio (SNR) environments. It can be concluded that a large N is more suitable for low SNR environments due to the high p_0. The above conclusion will help the design of the acquisition scheme based on the voting model.

The parity check matrix of the m-sequence $C[n]$ is a matrix E satisfying $Ey^T = 0$. The parity check matrix is established by concatenating K elementary parity check matrices as follows:

$$E = \left[E_0^T E_1^T \cdots E_{K-1}^T\right]^T \tag{17}$$

where $K = 3(L-1)/2$. Each matrix E_a is generated with a reference parity check polynomial $g_a(x) = \sum_{k=0}^{V} g_{a,k}x^k (a = 0, 1, \ldots, K\text{-}1)$, where $V = (L-1)/2$.

Matrix E_a ($a = 0, 1, \ldots, K\text{-}1$) can been expressed as follows:

$$E_a = \begin{bmatrix} g_{a,0} & g_{a,1} & \cdots & g_{a,V} & 0 & \cdots & \cdots & 0 \\ 0 & g_{a,0} & \cdots & \cdots & g_{a,V} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & & 0 \\ g_{a,V} & \cdots & \cdots & \cdots & 0 & g_{a,0} & \cdots & g_{a,V-1} \\ \vdots & \ddots & \cdots & \cdots & 0 & \ddots & \ddots & \vdots \\ g_{a,1} & \cdots & g_{a,V} & 0 & \cdots & \cdots & & g_{a,0} \end{bmatrix} \tag{18}$$

The factors of the reference parity check polynomial can been noted as $g_{a,0} = 1$, $g_{a,\tau_1} = 1$, $g_{a,\tau_2} = 1$ for (τ_1, τ_2). The matrix E_a is defined by the parity check equation (τ_1, τ_2). $g_a(x)$ belongs to set Ψ, hence E_a has a row weight equals to $t = 3$, which represents the 3 voters generated by the parity check equation (τ_1, τ_2). It is assumed that the receiver observes the sequence over its entire length $M = L$. As a consequence, E_a is circulant. This assumption will be helpful to derive the algorithm for generating $N = 3V$ voters. E is thus $VL \times L (V = 5, 10, \text{or } 20)$ sparse matrix in one iteration. The concatenation of V elementary matrices defines the graph on which the decoding algorithm is applied. While the row weight remains unchanged ($t = 3$), the V reference polynomials $g_0(x), \ldots, g_{V-1}(x)$ determine the structure of cycles.

C. THE DECODING ALGORITHM BASED THE MULTI-VOTER MODEL

Based on the multi-voter model, the acquisition scheme can be designed and the received sequence can be restored by such scheme.

The optimal algorithm of finding set Ψ is not addressed in this paper, because it has been deeply analyzed in references, such as [9], [22], and [26]. It is assumed in the paper that the receiver has already been configured with the optimal algorithm to find set Ψ.

Based on the previous derivation, the multi-voter model can been applied for the design of blind detection and the blind decoding algorithm can be realized as:

FIGURE 5 shows the voting and flipping process of the designed decoder. Erroneous chips are restored by the proposed algorithm based the multi-voter model. For one iteration, the number of parity check equations is set as $V = 20$, so the number of voters is $N = 3V = 60$. The do-flip threshold for the case can be set as $T = 32$ based on the optimal configurations. The transmitted m-sequence is shown

Blind Decoding Algorithm Based on Multi-Voter Model

Input: hard-decision chips of the received sequence over wireless channel are taken as the input.

Parameters: For one iteration, the number of parity check equations is set as V. So the number of voters, who are generated in one iteration, is $N = 3V$. The do-flip threshold T for different case is got from the derived optimal configurations, the maximum number of iterations is set as *IterMax*.

1. Work out Ψ;
2. Work out the do-flip threshold T for the configured N;
3. $k = 0$;
4. While $k < IterMax$;
5. Extract V check equations from set Ψ;
6. Generate N voters according to (10) and (11);
7. Count the do-flip votes for each chip;
8. Flip the chips who get more than T do-flip votes;
9. Break out of the loop if every chip in the sequence get 0 vote or all the check equations have been extracted from set Ψ;
10. End.

in FIGURE 5(a); the received hard-decision m-sequence are shown in FIGURE 5(b); As showed in FIGURE 5(c), the do-flip vote of each chip are counted; the erroneous chips are found out in FIGURE 5(d) by comparing the do-flip votes of each chip with the threshold T; the erroneous chips are flipped in FIGURE 5(e). FIGURE 5 shows that the chips are completely restored after voting and flipping.

However, not all sequences can be correctly restored in the low SNR scenarios in one iteration. The iterative process is necessary for the received m-sequences when the chip error rate is high. One iteration process can be defined by one voting and flipping event as shown in FIGURE 5, and thus the decoder can restore the received m-sequence within several iterations.

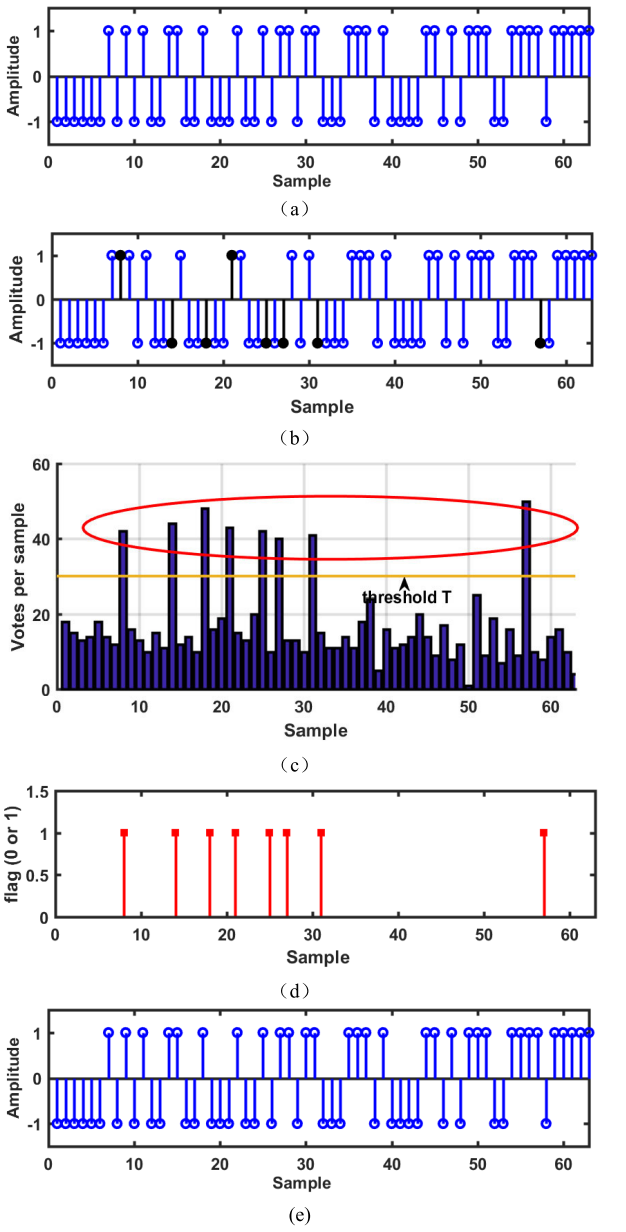


FIGURE 5. The illustration of voting-model-based method: (a) the original sequence; (b) the erroneous sequence at receiver; (c) the results of voting; (d) the tabs of the erroneous chips; (e) the restored sequence.

IV. PERFORMANCE

A. THE ANALYSIS OF THE DETECTION PERFORMANCE

In this section, the proposed method is compared with the MPA- [22], [23], the LEAP- [25] and the TCF-based [26] methods in the simulations.

The transmitter m-sequence is generated by LFSR of stage $p = 11$. The receiver observes L chips ($s[0]$, $s[1]$,..., $s[L-1]$) of the m-sequence and applies the proposed method for restoring the chips. To makes full use of the prior information of the m-sequence, all the check equations are allowed to be extracted sequentially from set Ψ unless the iterative detection is stopped. In one iteration, $V = 5$, 10, 20 parity check equations are extracted to generate $N = 3V = 15$, 30, 60 voters, who decide for chips whether to flip or not. For different N, the do-flip threshold T is set to the value derived in section III.

The voting-model-based method is defined in Section III. The iterations will stop when none of the voters cast any votes or the maximum number of iterations $IterMax = 50$ is reached. In this paper, the correct detection probability is noted as P_{CD}.

FIGURE 6 shows P_{CD} of these schemes versus the signal-to-noise (SNR).10000 Monte-Carlo simulations are performed for each scheme.

It can be seen in FIGURE 6 that P_{CD} of the voting-mode-based method increases with the growing of N and the method of configuration $N = 60$ achieves the best performance. Indeed, our voting-model- and the MPA- and the LEAP-based schemes can achieve equally good performance in high SNR environments. Further more, the voting-model-based method

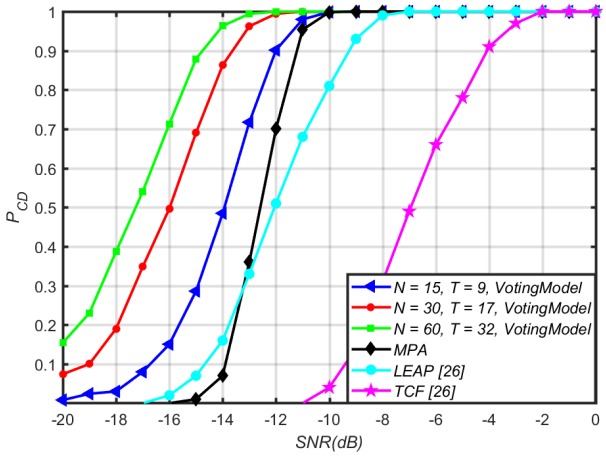


FIGURE 6. Comparison of different acquisition methods on detection probability under different SNRs.

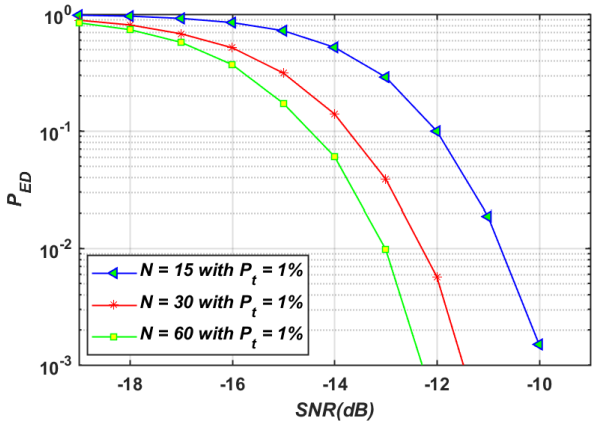


FIGURE 7. Comparison of different number of parity check equations V on the error detection probability P_{ED} under SNRs.

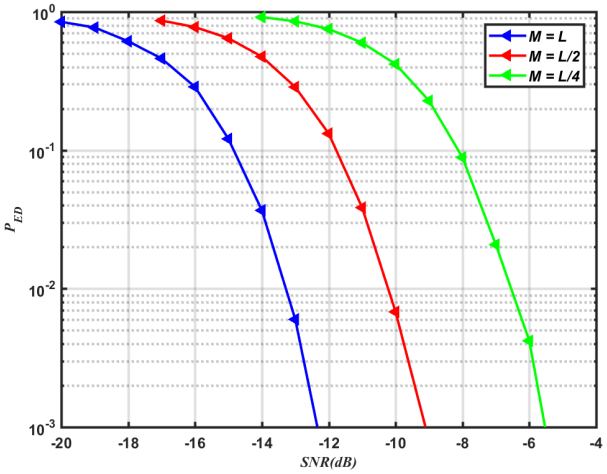


FIGURE 8. Comparison of different observation length M on the error detection probability P_{ED} under SNRs when $N = 60$.

of configuration $N = 15$ can not obviously outperform the MPA- and the LEAP- based method in low SNR environments. However, when compared with the MPA-based method in low SNR environments, the voting-model-based method of configuration $N > 15$ gets more than 2 dB gain at the detection probability 99%. The reason is that only one (in [23]) or several (in [22]) of parity check equations are used in MPA-based method in consideration of computation complexity. Thus the prior information of these parity check equations, which are not used in the detection, is abandoned. Similarly, the detection performance of the proposed method of configuration $N > 15$ is improved by 4 dB at the detection probability 99% compared with LEAP-based method. The reason is that whether the learning step is fixed or adjustable, it is difficult for LEAP-based method to convergent in the low SNR environments. The above results demonstrate that our method is better than MPA- and LEAP-based method when the SNR is low. The TCF-based method is also simulated. When the TCF-based method is applied for the detection, the peaks of the TCF are difficult to be accurately searched in low SNR environments [25], and this method shows bad detection performance.

As demonstrated in Figure 4 in the above Section III, if the number of the iteration is large enough, it is theoretically feasible that the received sequence can been completely restored in extremely harsh environment. However, the simulations in Figure 6 do not provide the ideal results as the theoretical ones. It is hypothesized that the erroneous rate of one chip is restricted to equal the chip error rate of the sequence. This hypothesis seems reasonable because the m-sequences are pseudo-noise. However, m-sequences can not be completely equivalent to noises, thus the algorithm shall divergence occasionally in iterative loops in the extremely harsh environment.

B. THE DETECTION PERFORMANCE OF REAL DETECTION SCENARIOS

In real detection scenarios, set Ψ is often found by the threshold algorithm [9]. It is inevitable that some false parity check equations are also collected into set Ψ. The probability of false parity check equations in set Ψ is noted as P_t in this paper. FIGURE 7 shows the error detection probability P_{ED} (P_{ED}=1 - P_{CD}) versus SNR with $P_t = 1\%$.

It can be seen that P_{ED} of the voting-model-based method can stably converge to 0.1%. Therefore, our proposed voting model for the detection of the m-sequences is suitable for real detection scenarios when some false parity check equations emerge in set.

In real detection scenarios, the number of the observed chips is variable. FIGURE 8 shows the error detection probability P_{ED} when the hard-decision samples are observed over different length $M = L$, $L/2$, $L/4$. The probability of false parity check equations is set to 0 and the number of voters is set to $N = 3V = 60$ ($V = 20$).

There is a 3 dB gap between the observed length $M = L$ and $M = L/2$ and 3.5 dB gap between $M = L/2$ and $M = L/4$ at 1% error detection probability. The reason is that the energy of the received sequence is decreased by 3 dB when the number of the observed chips is reduced by half.

V. CONCLUSION

The acquisition scheme based on multi-voter model is a simple but effective solution to restore the erroneous chips of the received m-sequence. In order to accomplish this target, the single-voter model and the multi-voter model are proposed in this paper. Firstly, one parity check equation of weight $t = 3$ is used to generate 3 voters in the voting model. In one iteration, N voters cast their votes for each chip and the receiver decides whether to flip or not, which is based on the do-flip threshold. Secondly, based on minimizing the chip error rate of the chips after one voting and flipping event, the optimal do-flip thresholds for different configurations are worked out in the paper. Finally, the voters are sequentially generated in the iterative loops and propose their flipping suggestions in decoding process. Due to the full use of prior information in set Ψ, The voting- model-based method outperforms the MPA-, the LEAP- and the TCF-based method.

It is known that the larger N is more efficient for improving the detection performance at a cost of more parallel computing time. It can be expected that parallel computing will become easier with the standardization of LDPC and the larger N can be enabled for the detection of m-sequences.

The case is not simulated when the number of voters in one iteration is set to $N > 60$ and such researches will be carried out in the future.

A novel concept is proposed for decoding PN codes in the paper. It can be seen that the proposed model is efficient for the codes which can been expressed by some parity check equations. It is possible that the voting model can be extended to other similar decoding scenarios in which the check matrix is generated by parity check equations. Notably, there are other excellent PN codes that have not been pointed out in this paper, such as Gold codes and Hadamard codes. Owning to shift-addictive characteristic, m-sequences featured with many parity check equations and the voting-model-based method are proposed based on this feature in the paper. However, the proposed method is not suitable for Gold codes and Hadamard codes, which are not shift-addictive. This paper provides an idea for other PN codes that the characteristics of a specific code type could be deeply analyzed and then new method could be derived.

ACKNOWLEDGMENT

The authors acknowledge the above funds for supporting this research and the editor and reviewers for their comments and suggestions.

REFERENCES

[1] B. Peng and Q. Chen, "PN codes estimation of binary phase shift keying signal based on sparse recovery for radar jammer," *Sensors*, vol. 23, no. 1, p. 554, Jan. 2023.

[2] S. Wang, C. Wang, W. Yuan, L. Wang, and J. Wang, "Secure echo-hiding audio watermarking method based on improved PN sequence and robust principal component analysis," *IET Signal Process.*, vol. 14, no. 4, pp. 229–242, Jun. 2020.

[3] Z. Qu, G. Zhang, H. Cao, and J. Xie, "LEO satellite constellation for Internet of Things," *IEEE Access*, vol. 5, pp. 18391–18401, 2017.

[4] D. Zou, J. Liu, X. Cheng, J. Zhang, Y. Liu, and S. Ma, "Pseudo-noise code shifting signal for AI arranged UAV networking," *Mobile Netw. Appl.*, vol. 25, no. 5, pp. 1683–1693, Oct. 2020.

[5] V. Weerackody and E. G. Cuevas, "Technical challenges and performance of satellite communications on-the-move systems," *Johns Hopkins Apl Tech. Dig.*, vol. 30, no. 2, pp. 113–121, 2011.

[6] D. R. Cremons, X. Sun, J. B. Abshire, and E. Mazarico, "Small PN-code LiDAR for asteroid and comet missions—Receiver processing and performance simulations," *Remote Sens.*, vol. 13, no. 12, p. 2282, Jun. 2021.

[7] A. Polydoros and C. Weber, "A unified approach to serial search spread-spectrum code acquisition—Part I: General theory," *IEEE Trans. Commun.*, vol. COM-32, no. 5, pp. 542–549, May 1984.

[8] K. K. Chawla and D. V. Sarwate, "Parallel acquisition of PN sequences in DS/SS systems," *IEEE Trans. Commun.*, vol. 42, no. 5, pp. 2155–2164, May 1994.

[9] Y. Qio, "The estimation of spreading sequence in long-code expansion signals," M.S. dissertation, Univ. Electron. Sci. Technol. China, Chengdu, China, 2012.

[10] A. Ahmed, P. Botsinis, S. Won, L.-L. Yang, and L. Hanzo, "Primitive polynomials for iterative recursive soft sequential acquisition of concatenated sequences," *IEEE Access*, vol. 7, pp. 13882–13900, 2019.

[11] X. Jin, Z. Peng, Z. Ma, W. Zhang, Z. Xu, and Z. Jin, "PN code tracking based on sub-Nyquist and non-commensurate sampling," *Electron. Lett.*, vol. 56, no. 14, pp. 734–736, Jul. 2020.

[12] C. Ma, S. Ni, X. Tang, Z. Xiao, and G. Sun, "Zero-bias elimination with selective non-commensurate sampling for PN code tracking," *IET Radar, Sonar Navigat.*, vol. 14, no. 3, pp. 349–355, Mar. 2020.

[13] X. Jin, W. Zhang, S. Mo, Z. Xu, C. Zhang, and Z. Jin, "Optimal regenerative PN code tracking based on non-commensurate sampling and double-loop structure," *Electron. Lett.*, vol. 55, no. 23, pp. 1254–1255, Nov. 2019.

[14] A. Füster-Sabater and S. D. Cardell, "Linear complexity of generalized sequences by comparison of PN-sequences," *Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales A. Matematicas*, vol. 114, no. 2, pp. 1–18, Jan. 2020.

[15] R. Kerr and J. Lodge, "Iterative signal processing for blind code phase acquisition of CDMA 1x signals for radio spectrum monitoring," *J. Electr. Comput. Eng.*, vol. 2010, pp. 1–8, May 2010.

[16] M. Des Noes, V. Savin, J. M. Brossier, and L. Ros, "Blind identification of the scrambling code of a reverse link CDMA2000 transmission," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2013, pp. 4734–4739.

[17] M. Des Noes, V. Savin, J. M. Brossier, and L. Ros, "Blind identification of the uplink scrambling code index of a WCDMA transmission and application to femtocell networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2013, pp. 4530–4535.

[18] M. Des Noes, V. Savin, J. M. Brossier, and L. Ros, "Iterative decoding of Gold sequences," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 4840–4845.

[19] M. des Noes, V. Savin, L. Ros, and J. M. Brossier, "Improving the decoding of M-sequences by exploiting their decimation property," *Proc. IEEE 21st Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2013, pp. 1–5.

[20] N. Weinberger and N. Merhav, "Codeword or noise? Exact random coding exponents for joint detection and decoding," *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5077–5094, Sep. 2014.

[21] O. W. Yeung and K. M. Chugg, "An iterative algorithm and low complexity hardware architecture for fast acquisition of long PN codes in UWB systems," *J. VLSI signal Process. Syst. Signal, Image Video Technol.*, vol. 43, no. 1, pp. 25–42, Apr. 2006.

[22] M. des Noes, V. Savin, L. Ros, and J.-M. Brossier, "Selection of parity check equations for the iterative message-passing detection of M-sequences," *IEEE Trans. Commun.*, vol. 65, no. 8, pp. 3214–3225, Aug. 2017, doi: 10.1109/TCOMM.2017.2706724.

[23] Z. Lin, Z. Ni, L. Kuang, C. Jiang, B. Liu, and Z. Huang, "A rapid PN code acquisition method for low spreading factor satellite communication systems," *IEEE Commun. Lett.*, vol. 25, no. 11, pp. 3664–3668, Nov. 2021.

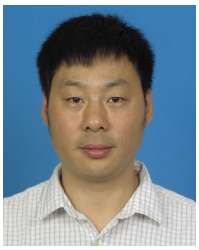
[24] H. Chen and R.-W. Lin, "An on-line unsupervised learning machine for adaptive feature extraction," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 41, no. 2, pp. 87–98, Feb. 1994.

[25] Y. Wei, S. Fang, X. Wang, and S. Huang, "Blind estimation of the PN sequence of a DSSS signal using a modified online unsupervised learning machine," *Sensors*, vol. 19, no. 2, p. 354, Jan. 2019.
[26] X. Gu, Z. Zhao, and L. Shen, "Blind estimation of pseudo-random codes in periodic long code direct sequence spread spectrum signals," *IET Commun.*, vol. 10, no. 11, pp. 1273–1281, Jul. 2016.
[27] D. Kim and D. Yoon, "Blind estimation of self-synchronous scrambler in DSSS systems," *IEEE Access*, vol. 9, pp. 76976–76982, 2021.
[28] L. Li, H. Zhang, S. Du, T. Liang, and L. Gao, "Blind despreading and deconvolution of asynchronous multiuser direct sequence spread spectrum signals under multipath channels," *IET Signal Process.*, vol. 17, no. 5, p. e1222, May 2023.
[29] D. Kim and D. Yoon, "Novel algorithm for blind estimation of scramblers in DSSS systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2292–2302, 2023.

PING WANG, photograph and biography not available at the time of publication.

QIANG YANG, photograph and biography not available at the time of publication.

YANGHENG HU, photograph and biography not available at the time of publication.



JIAN XIONG received the Ph.D. degree in automation engineering science from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2017. He is currently an Associate Professor with the School of Network and Communication Engineering, Chengdu Technological University. His current research interests include wireless communication diagnostics, prognostics for circuits and systems, and classification and identification of communication signals.

YONG JIA, photograph and biography not available at the time of publication.

DEQUAN GUO, photograph and biography not available at the time of publication.