Reliable and Secure Pre-Coding OFDM-DCSK Design for Practical Cognitive Radio Systems With the Carrier Frequency Offset

Zhaofeng Liu, Lin Zhang, *Member, IEEE*, and Zhiqiang Wu, *Senior Member, IEEE*

***Abstract*—In this paper, we present a pre-coding (PC) orthogonal frequency division multiplexing-aided differential chaos shift keying (OFDM-DCSK) scheme over non-contiguous (NC) spectrum bands for cognitive radio (CR) systems. In practical CR systems, the offset of fundamental clocks of transceivers or non-ideal components induce the carrier frequency offset (CFO), which will reduce the spectrum sensing accuracy and degrade reliability performances. Additionally, CR systems probably suffer from eavesdropping or malicious attacks due to the broadcasting property of wireless channels. With the aim to simultaneously combat the CFO and to enhance the security performance, in our OFDM-DCSK design, the information bits are modulated by reference chaotic sequences, then the data-bearing chaotic symbols and reference symbols are delivered to the pre-coding module, wherein we interleave chaotic chips, add the chaotic mask and duplicate chips. After OFDM modulations, the chaotic signals are transmitted over channels. At the receiver, reverse operations are performed. Moreover, we derive the theoretical bit error rate (BER) and information leakage expressions. Simulations are provided to verify the effectiveness of our derivations, and to demonstrate that more reliable and secure performances can be achieved by the presented system compared with counterpart systems.**

***Index Terms*—Bit error rate, carrier frequency offset, chaotic mask, non-contiguous bands, pre-coding orthogonal frequency division multiplexing-aided differential chaos shift keying.**

I. Introduction

COGNITIVE radio (CR) technologies can intelligently and identify unused and underused spectrum bands to allow the information transmission over non contiguous (NC) sub-bands [1], thus the spectrum utilization efficiency can be greatly improved. The CR technology can be further used in the fifth generation (5G) communication systems to provide services with the low latency, high coverage, high efficiency, etc. [2]–[4] over licensed and unlicensed bands.

In practical CR systems, the carrier frequency offset (CFO), which is generated by the offset of the fundamental clock of the transmitter and the receiver or the non-ideal components, will induce the transmission impairments to the signals. Thus the spectrum sensing accuracy will be reduced, thereby significantly degrading the transmission efficiency and bit error rate (BER) performances. Moreover, due to the broadcasting property of wireless channels, the information transmission over NC wireless bands may be easily eavesdropped and the security of wireless communication systems cannot be guaranteed.

Chaos is a natural non-periodic phenomenon, which can be hardly predicted. The chaotic sequences, which have properties such as non-periodic, noise-like and sensitive to initial value, can be utilized to combat interferences and to improve the security of communication systems [5], [6]. There are two types of chaotic modulation schemes, which are the coherent chaotic modulation and the non coherent chaotic modulation. The coherent chaotic modulation schemes like chaos shift keying (CSK) [7] can achieve good BER performances but have high complexity of chaos synchronization. By contrast, the non-coherent chaotic communication schemes such as the differential chaos shift keying (DCSK) [8] remove the chaos synchronization module, so that the complexity is acceptable for usage in practical systems.

Although DCSK can be implemented with the acceptable complexity [9],it has three main drawbacks. One is that the transmission efficiency is low because half of the duration of one DCSK symbol is used to transmit the reference sequences, which means that the transmission efficiency is 1/2. Another drawback is that the DCSK needs the delay line circuits, which can hardly be implemented. The third drawback is that the directive transmission of reference chaotic sequences degrades the security of DCSK systems since the transmitted data can be retrieved by malicious users with the received reference sequences.

In order to overcome these drawbacks, [10]–[14] propose to scramble chaotic chips to reduce the information leakage, which still retain the delay lines in the time domain. Then [15]–[18] utilize multiple carriers (MCs) to transmit reference sequences

Manuscript received May 13, 2019; revised October 1, 2019; accepted December 2, 2019. Date of publication December 13, 2019; date of current version March 6, 2020. This work was supported by the Project of National Natural Science Foundation of China under Grant 61602531, and in part supported by Key Research and Development and Transformation Plan of Science and Technology Program for Tibet Autonomous Region (No. XZ201901-GB-16). The associate editor coordinating the review of this article and approving it for publication was L. Wang. *(Corresponding author: Lin Zhang.)*

Z. Liu is with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China (e-mail: liuzhf5@mail2.sysu.edu.cn).

L. Zhang is with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China, and also with the Department of Science and Technology of Guangdong Province, Southern Marine Science and Engineering Guangdong Laboratory, Zhuhai 519000, China (e-mail: isszl@mail.sysu.edu.cn).

Z. Wu is with the Department of Electrical Engineering, Tibet University, Lhasa 850000, China, and also with the Department of Electrical Engineering, Wright State University, Dayton, OH 45435 USA (e-mail: zhiqiang.wu@wright.edu).

Digital Object Identifier 10.1109/TCCN.2019.2959332

to remove the delay lines. In orthogonal frequency-division multiplexing (OFDM) based DCSK systems, reference chaotic sequences and information-bearing sequences are delivered with different subcarriers. More explicitly, OFDM based DCSK system can deliver $N-1$ bits using N subcarriers in one OFDM symbol time slot, thus the transmission efficiency is improved while removing the delay lines. Notably, in OFDM-DCSK systems, since different sequences are distributed in different subcarriers, the receiver requires to know the exact subcarrier index which bears reference sequences to retrieve them for further demodulations of user data.

However, in practical MC-based CR systems, the CFO mentioned above will induce additional inter-carrier interferences (ICIs), which may induce the overlapping of signals from the primary user (PU) and secondary user (SU). Thus the spectrum sensing module cannot correctly identify the usage of spectrum bands, which will prevent the receiver from obtaining the reference sequence from the specific subcarrier with the correct subcarrier index. As a result, the reference sequences are improperly selected from received signals thus the demodulation errors increase, thereby bringing the issue of the reliability performance degradation. For example, the traditional OFDM-DCSK system [16] may have unacceptable BER performances when the CFO happens.

Research works have been done to suppress the CFO. Reference [18] proposes an OFDM-based code shifted (CS) DCSK to use the Walsh code to spread the information bits to suppress the CFO. Moreover, the CFO could be further suppressed with the combination of the robust optimal power control schemes [19], [20] to enhance system performances.

With the aid of the multi-carrier transmission and the CFO suppressing, the OFDM-DCSK scheme has provided the solution for the two problems of the lower efficiency as well as the delay lines for DCSK systems, yet the security issue remains not addressed. To be more explicit, the research progresses achieved in the improved DCSK schemes such as [16], [18] etc. have not taken the security performance into account.

In this paper, we propose a pre-coding (PC) chaos masking OFDM-DCSK scheme to improve the reliability and the security performances simultaneously for CR systems operating over NC bands. The novelty of the PC and chaos masking aided OFDM-DCSK design is that we propose a precoding module to utilize more subcarriers to transmit the information bits to combat the CFO and various channel conditions, with the aid of the chaos mask [21] to encrypt the information to enhance the security performances.

Different from our previous work [22], which proposes the frequency hopping aided OFDM-DCSK scheme to combat the frequency selective fading channel condition, in this paper, we propose a PC chaos masking OFDM-DCSK scheme, which can not only combat the channel fading but also suppress the CFO induced by imperfect operating conditions of the components in practical systems, to enhance the reliability performances. Moreover, we also propose to utilize the chaos mask to enhance the security performance, while [22] did not consider any security performance enhancement design. More explicitly, only the frequency selective fading scenario is considered, while in this paper, both the CFO and various channel fading conditions are taken into the modulation scheme design. Additionally, both reliability and security performances are enhanced with the improved pre-coding and chaos masking aided OFDM-DCSK design. Naturally, the theoretical and simulation results are also different.

In our design, at the transmitter, the binary phase shift keying (BPSK) symbols will be coherently modulated with the reference chaotic sequence. Then the data-bearing sequences and the reference sequence are precoded and masked by the chaotic sequence to combat the CFO and to enhance the security performances. After the inverse fast Fourier transform (IFFT) and the insertion of cyclic prefix (CP), the resultant signal is transmitted over wireless NC channels. At the legitimate receiver, reverse operations are carried out to retrieve the user data. After the CP removal and fast Fourier transform (FFT), the pre-decoding operation is performed, and the chaos mask is removed. Then correlation operations are performed on the received signals to remove the chaos mask and to obtain the reference sequence from the maximum likelihood detection. Subsequently, the correlation demodulation is carried out to recover the user data. Thanks to the chaos mask, eavesdroppers can hardly retrieve the user data without the knowledge of the chaos mask, thus the security performance can be improved.

Briefly, the main contributions include:

1) We present a PC-OFDM-DCSK scheme to defend against the adverse impact of CFO on BER performances, and prevent the malicious attack with the chaos mask, with the aim to simultaneously enhance reliability performances and security performances.
2) With the aid the pre-coding, both reference sequences and the data-bearing symbols are spread in the frequency domain, thus compared with the counterpart system, better BER performances can be achieved when there exist the CFO, and the robustness will be enhanced.
3) By exploiting the natural high security properties of chaotic sequences, after the masking, different chaotic sequences are weakly correlated with each other, thus the eavesdroppers can hardly recover the information by performing the correlation demodulation between the reference sequence and data bearing sequences directly. Accordingly, the security performance is enhanced.
4) We derive the theoretical BER performances for PC-OFDM-DCSK systems undergoing the CFO and the security performance, and provide simulation results for performance comparisons.

The rest of the paper is organized as follows: the PC-OFDM-DCSK design is presented in Section II, then Section III describes the theoretical BER analysis and the security performance analysis. Simulation results are provided in Section IV to show the outstanding performances of our proposed system. Finally, we conclude the paper in Section V.

II. The PC-OFDM-DCSK Design

The details of the presented PC-OFDM-DCSK scheme are presented as follows.

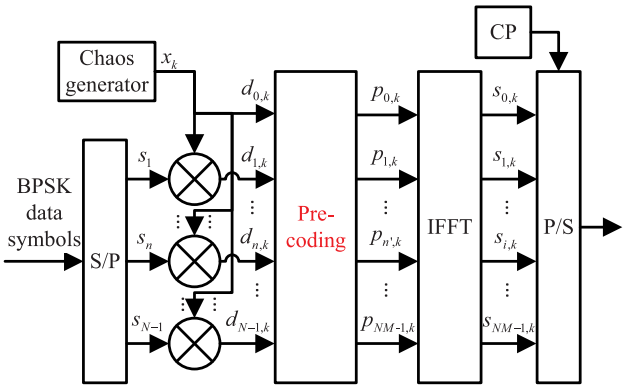

Fig. 1. The PC-OFDM-DCSK transmitter structure.

A. PC-OFDM-DCSK Transmitter Structure

Fig. 1 illustrates the transmitter structure of the presented PC-OFDM-DCSK scheme. Firstly, the information bits are modulated as BPSK symbols, then after the serial to parallel (S/P) conversion, multiple parallel BPSK data streams will be modulated by the reference chaotic sequence generated by the chaos generator. Then the pre-coding is performed on one reference sequence and $N-1$ data-bearing sequences, and the N data streams will be transformed to NM data streams, where M represent the subcarrier number of one chaos chip occupies. That is to say, the total subcarrier number required by the PC-OFDM-DCSK system is NM.

After the IFFT and adding the CP, the parallel to serial (P/S) conversion is performed and the resultant signals are transmitted over wireless NC channels. More details about the chaotic modulation and the pre-coding design are provided as below.

1) Chaotic Modulation: Let s_n denote the nth ($n = 1, 2, \ldots, N-1$) BPSK data symbol, which will be modulated with the kth chaotic chip x_k. Here we use the second order Chebyshev polynomial function (CPF) to generate x_k, i.e., $x_{k+1} = 1 - 2x_k^2$ where $x_k \in (-1, 0) \cup (0, 1)$, $0 \leq k \leq \beta - 1$ and β denotes the length of the chaotic sequence. After the chaotic modulation, the information-bearing chaotic modulated symbol $d_{n,k}$ is obtained as

$$d_{n,k} = s_n x_k. \tag{1}$$

Notably, for the sake of the brevity, here $d_{0,k} = x_k$ represents the kth chip of the reference chaotic sequences, and when $1 \leq n \leq N-1$, $d_{n,k}$ represents the kth chips in the nth data-bearing chaotic sequences. Next, all the sequences are delivered to the pre-coding module.

2) Pre-Coding Processing: In this module, the chaotic modulated symbols will be pre-coded to combat the CFO and to enhance the security. Without loss of generality, we assume β is the integral multiple of the number of chaotic sequences N or N is the integral multiple of β. That is to say, $\beta \bmod N = 0$ or $N \bmod \beta = 0$ is always satisfied, where mod is the modulo operator.

Let $\mathbf{D} = [\mathbf{d_0}^T, \mathbf{d_1}^T, \ldots, \mathbf{d_k}^T, \ldots, \mathbf{d}_{\beta-1}^T]$ represent the matrix input to the pre-coding module, where $(\cdot)^T$ denotes the transposition operation, and $\mathbf{d_k} = [d_{0,k}, d_{1,k}, \ldots, d_{n,k}, \ldots, d_{N-1,k}]$. Obviously, $\mathbf{D}$ has the dimension of $N \times \beta$.

Next, we reshape $\mathbf{D}$ as

$$\mathbf{D}' = \text{reshape}(\mathbf{D}, \beta, N). \tag{2}$$

More explicitly, after the reshaping operation, $\mathbf{D}'$ is obtained with the dimension of $\beta \times N$ which retains the column-wise ordering of $\mathbf{D}$.

Then $\mathbf{D}'$ is transformed to $\mathbf{R}'$ by

$$\mathbf{R}'(n,:) = \left(\text{circshift}\left(\mathbf{D}'(:,n), n\right)\right)^T \tag{3}$$

where $\mathbf{R}'(n,:)$ denotes the nth row of $\mathbf{R}'$, $\mathbf{D}'(:,n)$ denotes the nth column of $\mathbf{D}'$, and $\text{circshift}(\mathbf{v}, n)$ generates the n-chip-shifted version of the column vector $\mathbf{v}$.

Subsequently, we apply the chaos masking on $\mathbf{R}'$. To be more specific, with the aid of the second order CPF and a new initial value, we generate a new chaotic sequence $\mathbf{c}$ with the length of $N\beta$, which then constitutes the chaotic masking matrix $\mathbf{C}$ denoted by

$$\mathbf{C} = \exp(\text{reshape}(\mathbf{c}, N, \beta)) \tag{4}$$

where $\exp(\cdot)$ denotes the exponential function. Then the chaotic masking is carried out according to

$$\mathbf{P}' = \mathbf{R}' \circ \mathbf{C} \tag{5}$$

where $\circ$ denotes the element-wise multiplication operator of two matrices. Notably, during the information transmission, we can change $\mathbf{C}$ dynamically to further enhance the security performances.

After the chaotic masking, with the aim to combat the CFO, we propose use M subcarriers to transmit the duplicates of the matrix $\mathbf{P}'$, which formulates the matrix $\mathbf{P}$ as follows[23]

$$\mathbf{P}(nM - M + w, :) = \mathbf{P}'(n,:) \tag{6}$$

where $\mathbf{P} = [\mathbf{p_0}^T, \mathbf{p_1}^T, \ldots, \mathbf{p_{n'}}^T, \ldots, \mathbf{p_{NM-1}}^T]^T$, $0 \leq w \leq M-1$, $0 \leq n' \leq NM-1$, $\mathbf{p_{n'}}^T = [p_{n',0}, p_{n',1}, , \ldots, p_{n',k}, \ldots, p_{n',\beta-1}]^T$. The resultant matrix $\mathbf{P}$ is then sent to the IFFT module to perform the OFDM modulation.

3) OFDM Modulation: In the OFDM modulation processing, the IFFT are performed on $p_{n',k}$ as below

$$s_{i,k} = \frac{1}{\sqrt{N}} \sum_{n'=0}^{NM-1} p_{n',k} e^{j\frac{2\pi n' i}{N}} \tag{7}$$

where i is the index of IFFT-modulated chips.

It is worth pointing out that since multiple duplicates have been transmitted, the receiver can select the one with larger signal to noise ratio (SNR) for information retrieval, and thus the reliability performance can be enhanced with the improved security performances thanks to the chaotic masking.

B. Legitimate PC-OFDM-DCSK Receiver Structure

Fig. 2 illustrates the legitimate receiver structure of PC-OFDM-DCSK system. After the S/P transform and the removal of CP, the received data stream will be transformed to NM parallel streams.

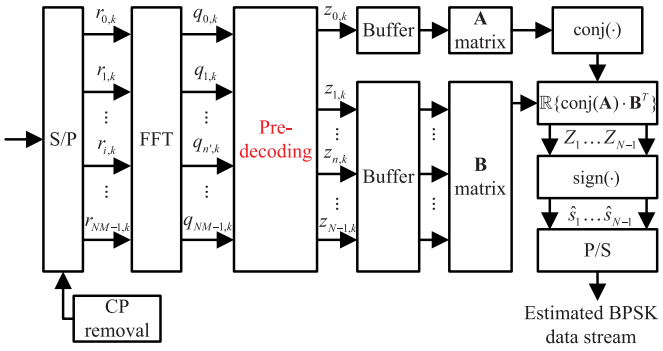

Fig. 2. The PC-OFDM-DCSK receiver structure.

Then the fast Fourier transform (FFT) is applied to perform the OFDM demodulation and the resultant symbols are sent to the pre-decoding module, wherein the maximum likehood detection is performed to optimally select N data stream from the NM data streams. Moreover, the chaos mask will be removed. Every resultant β pre-decoded symbols are performed correlation demodulations to recover the BPSK symbols. Finally, maximum likelihood method is used to recover transmitted information bits. More details about the OFDM demodulation, the pre-decoding, the detection and the estimation are given as below.

1) OFDM Demodulation: After the FFT, we obtain the symbol over the n'th subcarrier in the kth chaotic chip time slot denoted by $q_{n',k}$ as [24], [25]

$$\begin{aligned} q_{n',k} &= \frac{1}{\sqrt{NM}} \sum_{i=0}^{NM-1} r_{i,k} e^{-j\frac{2\pi n' i}{N}} \\ &= H_{n',k} p_{n',k} S_1 + \sum_{u=0,u\neq n'}^{NM-1} H_{u,k} p_{u,k} S_{u-n'+1} + \xi_{n',k} \end{aligned} \tag{8}$$

where $r_{i,k}$ denotes the ith chip of the OFDM symbol in the time slot of the ith chaotic chip, $\xi_{n',k}$ is the complex additive white Gaussian noise (AWGN) with zero mean and power spectral density of N_0, $H_{n',k}$ is the channel frequency response (CFR) over the n'th subcarrier and the kth chaotic chip. S_u represents the inter-carrier interference (ICI) induced by the CFO over the uth subcarrier as [24], [25]

$$S_u = \frac{\sin(\pi[u-1+\epsilon])}{NM \sin\left(\frac{\pi[u-1+\epsilon]}{NM}\right)} e^{j\pi\left(1-\frac{1}{NM}\right)(u-1+\epsilon)} \tag{9}$$

where ϵ is the normalized CFO, which is defined as $\epsilon = f_d/f_s$, f_d is the Doppler frequency shift, and f_s is the bandwidth occupied by the whole OFDM symbol.

In the special case that the information transmission undergoes the flat fading, i.e., the CFR remains constant in the time domain, we have $H_{n,k} = H_n$ for $\forall k$.

2) Pre-Decoding for Legitimate Receivers: At the legitimate receiver, the reverse pre-decoding operation is performed. Let $\mathbf{q}_{\mathbf{n}'}^T$ denote the matrix consists of $q_{n',0}$ given by Eq. (8), namely we have $\mathbf{q}_{\mathbf{n}'}^T = [q_{n',0}, q_{n',1}, \ldots, q_{n',k}, \ldots, q_{n',\beta-1}]^T$, which further constitutes the matrix $\mathbf{Q} = [\mathbf{q_0}^T, \mathbf{q_1}^T, \ldots, \mathbf{q_{n'}}^T, \ldots, \mathbf{q_{NM-1}}^T]^T$.

Next, we remove the chaos mask from the received signals with the known chaos masking pattern. It is worth pointing out that in the proposed PC-OFDM-DCSK system, we use the uncoordinate direct sequence spread spectrum (UDSSS) technique [26], [27] to transmit the chaos mask pattern to the legitimate receiver. With the aid of the chaos masking pattern learned from the specific control channel at receivers, we remove the chaos mask by

$$\mathbf{Q}' = \mathbf{Q} \circ \mathrm{conj}(\mathbf{C}') \tag{10}$$

where $\mathrm{conj}(\cdot)$ performs the conjunction calculation, and similar to Eq. (5), $\mathbf{C}'(nM - M + w, :) = \mathbf{C}(n, :)$ where $0 \leq w \leq M-1$.

After removing the chaos mask, we recover the reference chaotic sequence from the symbols potentially undergoing the CFO with the aid of $\mathbf{Q}'$. Define $\mathbf{R_m} = \mathbf{Q}'((0 : N-1) \times M + m, :)$, then the optimal value of $\mathbf{R_{m^*}}$ will be determined by

$$m^* = \arg\max_m \ \mathrm{tr}\Big(\mathrm{conj}(\mathbf{R_m}) \cdot (\mathbf{R_m})^T\Big) \tag{11}$$

where $\mathrm{tr}(\cdot)$ denotes the trace of a matrix. For a given m^*, the $N \times \beta$-dimension matrix $\mathbf{R_{m^*}}$ can be determined.

Subsequently, similar to Eq. (3), $\mathbf{R_{m^*}}$ will be firstly shifted as

$$\mathbf{Z}'(:, n) = \mathrm{circshift}\Big((\mathbf{R_{m^*}}(n, :))^T, -n\Big). \tag{12}$$

Then the reshaping reverse to Eq. (2) is performed on $\mathbf{Z}'(:, n)$, which can be denoted as

$$\mathbf{Z} = \mathrm{reshape}(\mathbf{Z}', N, \beta) \tag{13}$$

where $\mathbf{Z} = [\mathbf{z_0}^T, \mathbf{z_1}^T, \ldots, \mathbf{z_k}^T, \ldots, \mathbf{z_{\beta-1}}^T]$, and $\mathbf{z_k} = [z_{0,k}, z_{1,k}, \ldots, z_{n,k}, \ldots, z_{N-1,k}]$.

3) Detection and Estimation: After the pre-decoding, the buffers will store the resultant chip $z_{n,k}$. If $z_{n,k}$ is buffered β times, the stored sequences will be released to perform the correlation demodulation as

$$Z_n = \Re\left\{\sum_{k=0}^{\beta-1} \mathrm{conj}(z_{0,k}) \cdot z_{n,k}\right\} \tag{14}$$

where $\Re\{\cdot\}$ takes the real part, $z_{0,k}$ is the kth element of the reference chaotic sequence, and Z_n is the demodulated nth BPSK symbol.

At last, the maximum likelihood estimation of transmitted symbols is carried out on Z_n, namely, we have $\hat{s}_n = \mathrm{sgn}(Z_n)$ where $\mathrm{sgn}(\cdot)$ denotes the sign function.

III. Performance Analysis

In this section, we will analyze BER and security performances for the PC-OFDM-DCSK scheme.

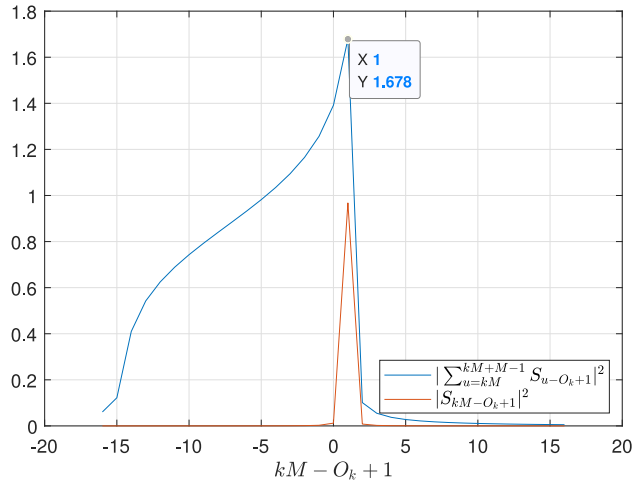

Fig. 3. The value of $|\sum_{u=kM}^{kM+M-1} S_{u-O_k+1}|^2$ and $kM - O_k + 1$. $N = 128$, $\beta = 128$, $M = 16$ and $\epsilon = 0.1$.

A. BER Performance

1) BER for Legitimate Users: Using Gaussian approximation (GA) [28] method, we can derive the theoretical BER expressions for the PC-OFDM-DCSK system undergoing the CFO. Without loss of generalization, we assume that β is large enough and equal to the number of chaotic data streams N. In addition, we also assume that the CFO will not change with time and the symbols will not be shifted by Eq. (3) or de-shifted by Eq. (12).

Firstly, according to Eq. (2), Eq. (5) and Eq. (8), received symbols can be re-expressed as

$$\begin{aligned} q_{n',k} &= \sum_{u=0}^{NM-1} H_{u,k} p_{u,k} S_{u-n'+1} + \xi_{n',k} \\ &= \sum_{u=0}^{NM-1} H_{u,k} d_{k,y} c_{y,k} S_{u-n'+1} + \xi_{n',k} \end{aligned} \tag{15}$$

where $y = \text{floor}(u/M)$, $\text{floor}(u/M)$ defines the largest integer which is not larger than u/M, and $c_{y,k}$ denotes the yth row and kth column element in the chaos mask matrix $\mathbf{C}$.

After the pre-decoding, we obtain

$$z_{n,k} = q_{O_k,n} \cdot c^*_{\text{floor}(O_k/M),n} \tag{16}$$

where O_k is the optimal number provided by Eq. (11) and ranged from kM to $kM + M - 1$. When $n' = O_k$, according to Eq. (15), we have

$$q_{O_k,n} = \sum_{u=0}^{NM-1} H_{u,n} p_{u,n} S_{u-O_k+1} + \xi_{O_k,n} \tag{17}$$

Notably, in this equation, when $kM \le u \le kM + M - 1$, $p_{u,n}$ remains the same. Considering that the channel response $H_{u,n}$ and the noises $\xi_{O_k,n}$ are weakly correlated with the received signals, the optimization problem given in Eq. (11) can be transformed to the problem of selecting the optimal O_k for $p_{k,n} \sum_{u=kM}^{kM+M-1} S_{u-O_k+1}$ $(kM \le O_k \le kM + M - 1)$.

Fig. 3 illustrates the value of $|\sum_{u=kM}^{kM+M-1} S_{u-O_k+1}|^2$ versus $kM - O_k + 1$. It can be observed that when $kM - O_k + 1 = 1$, $|\sum_{u=kM}^{kM+M-1} S_{u-O_k+1}|^2$ attains the largest value, therefore we obtain the optimal value of O_k as $O_k = kM$.

According to Eq. (15) and Eq. (16), we have

$$z_{n,k} = \left(\sum_{u=0}^{NM-1} H_{u,n} d_{n,y} c_{y,n} S_{u-kM+1} + \xi_{kM,n} \right) \cdot c^*_{k,n} \tag{18}$$

where $z_{0,k}$ denotes the kth chip of reference chaotic chip when $n = 0$, when $n \ge 1$, $z_{n,k}$ denotes the kth chip of the nth information bearing chaotic sequences, the complex CFR $H_{u,n}$ with zero mean and power spectral density of 1 and $\xi_{kM,n}$ is the noise. Since $H_{u,n}$ and $\xi_{kM,n}$ are random variables and the chip of chaos mask $c_{y,n}$ has the amplitude of 1 and uniform distributed phase, it is reasonable to assume that the multiplication of chaos mask chips will not change the distribution of CFR and noise. Therefore, according to Eq. (1), we obtain

$$\begin{aligned} z_{n,k} &= \sum_{u=0}^{NM-1} \hat{H}_{u,n} s_n x_y S_{u-kM+1} + \hat{\xi}_{kM,n} \\ &= s_n g_k + \hat{\xi}_{kM,n} \end{aligned} \tag{19}$$

where $\hat{H}_{u,n} = H_{u,n} c_{y,n} c^*_{k,n}$ has the same distribution as $H_{u,n}$, $\hat{\xi}_{kM,n} = \xi_{kM,n} c^*_{k,n}$ has the same distribution as $\xi_{kM,n}$ and $g_k = \sum_{u=0}^{NM-1} \hat{H}_{u,n} x_y S_{u-kM+1}$.

Then, according to Eq. (14) and Eq. (19), the demodulated symbol Z_n for $n \ge 1$ can be derived as

$$\begin{aligned} Z_n &= \Re\left\{ \sum_{k=0}^{\beta-1} \left(s_0 g_k + \hat{\xi}_{kM,0} \right)^* \left(s_n g_k + \hat{\xi}_{kM,n} \right) \right\} \\ &= \underbrace{\Re\left\{ \sum_{k=0}^{\beta-1} s_n |g_k|^2 \right\}}_{P_1} + \underbrace{\Re\left\{ \sum_{k=0}^{\beta-1} \hat{\xi}^*_{kM,0} \hat{\xi}_{kM,n} \right\}}_{P_2} \\ &\quad + \underbrace{\Re\left\{ \sum_{k=0}^{\beta-1} \left(g^*_k \hat{\xi}_{kM,n} + s_n g_k \hat{\xi}^*_{kM,0} \right) \right\}}_{P_3} \end{aligned} \tag{20}$$

where P_1 contains the desired signal, P_2 and P_3 denote the disturbance components. Because P_1, P_2 and P_3 are statistically independent, the expectation and variance of Z_n can be naturally obtained as

$$\begin{aligned} \text{E}\{Z_n | (s_n = \pm 1)\} &= \sum_{w=1}^{3} \text{E}\{P_w | (s_n = \pm 1)\} \\ \text{var}\{Z_n | (s_n = \pm 1)\} &= \sum_{w=1}^{3} \text{var}\{P_w | (s_n = \pm 1)\} \end{aligned} \tag{21}$$

where $\text{E}\{\cdot\}$ takes the expectation and $\text{var}\{\cdot\}$ takes the variance. Thus the signal-to-noise-plus-interference ratio (SINR) expression can be represented by

$$\begin{aligned} \Gamma &= (\text{E}\{Z_n | (s_n = \pm 1)\})^2 / \text{var}\{Z_n | (s_n = \pm 1)\} \\ &= \frac{\sum_{w=1}^{3} \text{E}\{P_w | (s_n = \pm 1)\}}{\sum_{w=1}^{3} \text{var}\{P_w | (s_n = \pm 1)\}}. \end{aligned} \tag{22}$$

Furthermore, using the central limit theorem, we can evaluate the statistical characteristics of P_1, P_2 and P_3 as

$$\begin{aligned}
&\mathrm{E}\{P_1|s_n=+1\} = -\mathrm{E}\{P_1|s_n=-1\} = \beta\mathrm{E}\Big\{|g_k|^2\Big\}\\
&\mathrm{E}\{P_2|s_n=\pm1\} = \mathrm{E}\{P_3|s_n=\pm1\} = 0\\
&\mathrm{var}\{P_1|s_n=\pm1\} = \beta\mathrm{var}\Big\{|g_k|^2\Big\}\\
&\mathrm{var}\{P_2|s_n=\pm1\} = \frac{1}{2}\beta N_0^2\\
&\mathrm{var}\{P_3|s_n=\pm1\} = \beta\mathrm{E}\Big\{|g_k|^2\Big\}N_0.
\end{aligned} \tag{23}$$

Then we could derive the BER expression for the presented PC-OFDM-DCSK system as

$$\begin{aligned}
BER &= \mathrm{erfc}\Big(\sqrt{\Gamma/2}\Big)/2\\
&= \frac{1}{2}\mathrm{erfc}\left[\left(\frac{2\mathrm{var}\{|g_k|^2\}}{\beta\mathrm{E}\{|g_k|^2\}^2} + \frac{2\gamma NN_0}{E_b(N-1)} + \frac{\gamma^2N^2N_0^2\beta}{E_b^2(N-1)^2}\right)^{-\frac{1}{2}}\right]
\end{aligned} \tag{24}$$

where $E_b = N\beta\mathrm{E}\{x_k^2\}/(N-1)$ is the average bit energy, $\gamma = \mathrm{E}\{x_k^2\}/\mathrm{E}\{|g_k|^2\}$.

To elaborate a bit further, with the assumption that β is large enough [28], the term $2\mathrm{var}\{|g_k|^2\}/(\beta\mathrm{E}\{|g_k|^2\}^2)$ in Eq. (24) is approximately equal to 0. Thus from Eq. (22), Eq. (23) and Eq. (24), we can see that the BER is determined by $\mathrm{E}\{|g_k|^2\}$. Next, we will evaluate $\mathrm{E}\{|g_k|^2\}$.

Firstly, without loss of generality, we assume that the CFRs of M adjacent subcarriers over frequency selective fading channels remains constant by selecting the appropriate M, and that x_y over M adjacent subcarriers are also constant. Define two (NM)-dimension vector columns as $\mathbf{h} = [\overline{H}_0, \overline{H}_1, \ldots, \overline{H}_u, \ldots, \overline{H}_{NM-1}]^T = [\hat{H}_{0,n}\hat{x}_0, \hat{H}_{1,n}\hat{x}_1, \ldots, \hat{H}_{u,n}\hat{x}_u, \ldots, \hat{H}_{NM-1,n}\hat{x}_{NM-1}]^T$ and $\mathbf{s_k} = [S_{0-kM+1}, S_{1-kM+1}, \ldots, S_{u-kM+1}, \ldots, S_{NM-1-kM+1}]^T$, where $\hat{x}_u = x_{\mathrm{floor}(u/M)} = x_y$, $\overline{H}_u = \hat{H}_{u,n}\hat{x}_u$, then g_k can be represented by $g_k = \mathbf{s_k}^T\mathbf{h} = \mathbf{h}^T\mathbf{s_k}$, and $\mathrm{E}\{|g_k|^2\}$ is expressed as

$$\begin{aligned}
\mathrm{E}\Big\{|g_k|^2\Big\} &= \mathrm{E}\{g_k^*g_k\} = \mathrm{E}\Big\{\mathbf{s_k}^H\mathbf{h}^*\mathbf{h}^T\mathbf{s_k}\Big\}\\
&= \mathbf{s_k}^H\mathrm{E}\Big\{\mathbf{h}^*\mathbf{h}^T\Big\}\mathbf{s_k}
\end{aligned} \tag{25}$$

where $(\cdot)^H$ denotes the Hermitian transpose.

Obviously, $\mathrm{E}\{|g_k|^2\}$ depends on the distribution of CFR and chaotic chips. For chaotic chips generated by the second CPF, the distribution of x_k is $\mathrm{E}\{x_y^2\} = 1/2$. When the channel is identically and independently distributed (i.i.d.), the CFR will be independent with each other and the distribution is $\mathrm{E}\{|\hat{H}_{u,n}|^2\} = 1$. Thus $\mathrm{E}\{|\overline{H}_u|^2\} = \mathrm{E}\{x_y^2\}\mathrm{E}\{|\hat{H}_{u,n}|^2\} = 1/2$ and we have

$$\mathrm{E}\Big\{\overline{H}_{u1}^*\overline{H}_{u2}\Big\} = \begin{cases} 1/2, & \text{if } \overline{H}_{u1} = \overline{H}_{u2} \\ 0, & \text{otherwise} \end{cases}. \tag{26}$$

Considering that we assume that the channel fading and noises remain constant over M subcarriers, $\mathbf{h}$ can be divided into M-dimension sub-vector, $\mathrm{E}\{\mathbf{h}^*\mathbf{h}^T\}$ can be expressed as

$$\mathrm{E}\Big\{\mathbf{h}^*\mathbf{h}^T\Big\} = \frac{1}{2}\begin{bmatrix} \mathbf{1_M} & \mathbf{0_M} & \cdots & \mathbf{0_M} \\ \mathbf{0_M} & \mathbf{1_M} & \cdots & \mathbf{0_M} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0_M} & \mathbf{0_M} & \cdots & \mathbf{1_M} \end{bmatrix} \tag{27}$$

where $\mathbf{1_M}$ denotes the $M \times M$-dimension matrix whose all elements are 1 and $\mathbf{0_M}$ denotes the $M \times M$-dimension matrix whose all elements are 0. Therefore, according to Eq. (25) and Eq. (27), the $\mathrm{E}\{|g_k|^2\}$ is derived as

$$\begin{aligned}
\mathrm{E}\Big\{|g_k|^2\Big\} &= \frac{1}{2}\mathbf{s_k}^H\begin{bmatrix} \mathbf{1_M} & \mathbf{0_M} & \cdots & \mathbf{0_M} \\ \mathbf{0_M} & \mathbf{1_M} & \cdots & \mathbf{0_M} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0_M} & \mathbf{0_M} & \cdots & \mathbf{1_M} \end{bmatrix}\mathbf{s_k}\\
&= \frac{1}{2}\sum_{n=0}^{N-1}\sum_{u_1=0}^{M-1}\sum_{u_2=0}^{M-1}\\
&\quad\times S_{u_1+nM-kM+1}^*S_{u_2+nM-kM+1}
\end{aligned} \tag{28}$$

From Fig. 3, we can learn that S_u can have a large value only when $u = 1$. Substituting Eq. (9) into Eq. (28), we can see that the value of $\mathrm{E}\{|g_k|^2\}$ is dependent on k, M and ϵ. For example, when $N = 128$, $\beta = 128$ and $\epsilon = 0.1$, Table I shows the value of $\mathrm{E}\{|g_k|^2\}$ increases with larger M, which means that lower BER and better reliability performances can be provided for the presented PC-OFDM-DCSK system.

TABLE I
$\mathrm{E}\{|g_k|^2\}$ VERSUS M

M	1	2	4	8	16
$\mathrm{E}\{\lvert g_k\rvert^2\}$	0.498	0.596	0.695	0.797	0.908

In the special case when the PC-OFDM-DCSK system operates over AWGN channel, by setting $S_u = 1$ and $H_{u,n} = 1$, the BER over AWGN channel can be derived based on Eq. (24) and Eq. (28) as

$$\begin{aligned}
&BER_{AWGN}\\
&= \frac{1}{2}\mathrm{erfc}\left[\left(\frac{1}{\beta} + \frac{2NN_0}{E_b(N-1)} + \frac{N^2N_0^2\beta}{E_b^2(N-1)^2}\right)^{-\frac{1}{2}}\right].
\end{aligned} \tag{29}$$

It is worth pointing out that from Eq. (9) and Eq. (28), we can notice that for the practical CR systems with the CFO, the CFO will induce the interferences from signals transmitting over other subcarriers. Moreover, S_u will bring the phase offset of the symbols, thereby degrading the BER performances of the conventional OFDM-DCSK system [16]. By contrast, with our pre-coding design, the chaos chips can be transmitted via all available subcarriers, thus the receiver can select the best chaos chips which are not affected by the ICI to retrieve the received data, thus the BER performances can be improved. Moreover, different chaos chips can be distributed in different subcarriers, then the channel frequency response information can be collected and extracted from these chaos chips in one chaotic sequence. Thus the frequency diversity gain can be exploited to improve the BER performances. Except for

the analytical analysis, the simulated BER results provided in Section IV can also validate the better BER performances achieved by our design.

2) BER for Eavesdroppers: As mentioned above, the eavesdroppers cannot recover the information without the knowledge of the chaotic masking. In this scenario, similar to Eq. (24), we derive the BER of the eavesdroppers as

$$BER_{eavesdroppers} = \frac{1}{2}\mathrm{erfc}\left[\left(\frac{2\mathrm{var}\{|\tilde{g}_k|^2\}}{\beta \mathrm{E}\{|\tilde{g}_k|^2\}^2} + \frac{2\tilde{\gamma}NN_0}{E_b(N-1)} + \frac{\tilde{\gamma}^2N^2N_0^2\beta}{E_b^2(N-1)^2}\right)^{-\frac{1}{2}}\right] \tag{30}$$

where $\tilde{\gamma} = \mathrm{E}\{|x_k|^2\}/\mathrm{E}\{|\tilde{g}_k|^2\}$, $\tilde{g}_k = \sum_{u=0}^{NM-1} \tilde{H}_{u,n} x_y S_{u-kM+1}$ and $\tilde{H}_{u,n} = H_{u,n} c_{y,n}$.

It is noticeable that the equivalent CFR of legitimate users and eavesdroppers are represented by $\hat{H}_{u,n}$ and $\tilde{H}_{u,n}$ respectively, which satisfies $\hat{H}_{u,n} = \tilde{H}_{u,n} \cdot c_{k,n}^*$, $c_{k,n}^*$. Different from the legitimate users, for eavesdroppers, $\tilde{H}_{u,n}$ contains the element $c_{y,n}$, which is independent with other chaos mask chips when n is different, thus different data streams received by the eavesdroppers will be independent with each other. Using the similar derivation method to Eq. (28), due to the statistical independent characteristics of received signals, we can derive that $\mathrm{E}\{|\tilde{g}_k|^2\} \approx 0$. Accordingly, $BER_{eavesdroppers}$ is large and the eavesdroppers can hardly retrieve the transmitted data.

B. Security Performance

In order to evaluate the theoretical security performances, we calculate the information leakage as follows [29], [30].

Assuming that the binary bits 0 and 1 for the transmission are generated with the identical probability, the mutual information between the transmitted data X and the data Y_E retrieved by eavesdroppers can be derived as

$$\begin{aligned} I_n(Y_E;X) &= H_n(Y_E) - H_n(Y_E|X) \\ &= 1 + p_n \log_2 p_n + (1-p_n)\log_2(1-p_n) \end{aligned} \tag{31}$$

where $H_n(\cdot)$ calculates the entropy and p_n is the BER given in Eq. (30).

Since at the eavedropping receivers, the $N-1$ PC-OFDM-DCSK information bearing data streams are independent from each other, the information leakage can be obtained as [30]

$$L = \frac{1}{N-1}\sum_{n=1}^{N-1} I_n(Y_E;X). \tag{32}$$

For practical CR systems, thanks to the non-periodicity property of the chaotic sequence, it is too difficult for eavesdroppers to recover the transmitted data by time-consuming brute force cracking methods, thus the information leakage of real time communications for legitimate PC-OFDM-DCSK receivers is very low and hence the security performance can be enhanced.

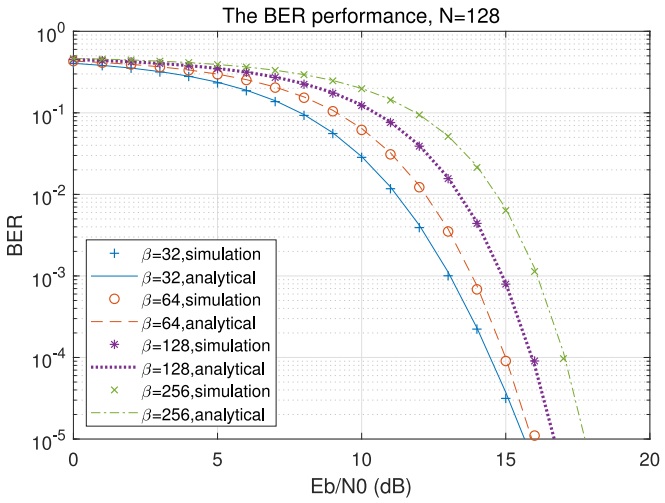

Fig. 4. The theoretical and simulated BER performances of PC-OFDM-DCSK systems over AWGN channel when $N = 128$.

IV. Simulation Results

In this section, with the motivation to validate the main contributions of the proposed scheme, including the improved security and reliability performances in the scenario wherein the CFO exists as well as the theoretical analysis, the simulation results are provided. To be more explicit, we first compare the analytical results with the simulated BER performances to verify the effectiveness of theoretical derivations. Then we compare the simulated BER performances of the presented PC-OFDM-DCSK systems with counterpart schemes including the conventional OFDM-DCSK [16] system and the OFDM-CS-DCSK system [18] to validate the enhanced performances achieved by our design.

A. BER Performances of PC-OFDM-DCSK System

Firstly, Fig. 4 demonstrates that for the legitimate PC-OFDM-DCSK receiver, the theoretical BER performances match the simulated BER performances over AWGN channel when $\beta = 32, 64, 128, 256$, which verifies the effectiveness of our derivations. In addition, it can be seen that the BER performances are better for smaller β due to fewer interferences, which is in accordance with the observations obtained in [16].

Furthermore, Fig. 5 investigates the BER performances of the proposed system with different β when the E_b/N_0 varies from 10dB to 16dB. It can be observed that when the value of E_b/N_0 becomes larger, there emerges an optimal value of β with which the proposed system could achieve the best performance. Moreover, when β becomes larger, the BER performances degrade faster. The reason is that when β is relatively small, the BER performances could be improved since chaotic transmissions could help to combat the channel fading. However, when β increases, the interferences induced by chaotic sequences would degrade the BER performances. In particular, when the signal energy increases, the interferences also increase accordingly, thereby bringing deeper impact to the BER performances. Hence we could select an appropriate β for a specific practical system based on the user demands and transmission conditions.

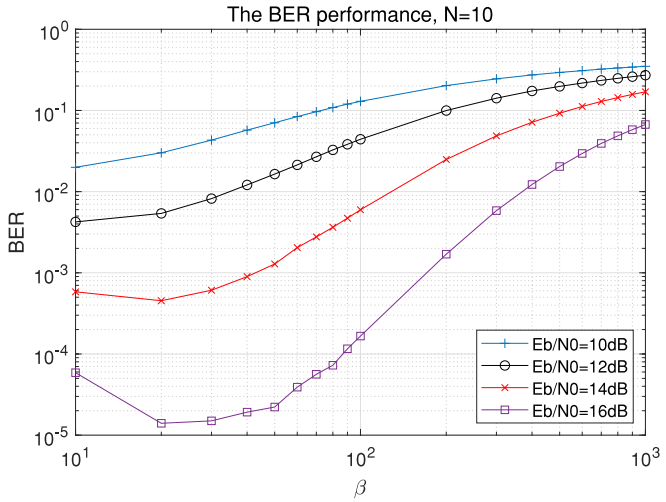

Fig. 5. The BER performances versus β of PC-OFDM-DCSK systems over AWGN channel when $N = 10$.

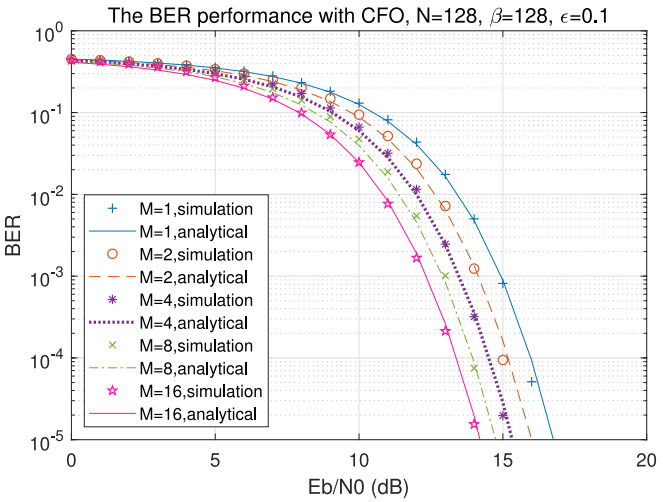

Fig. 7. The BER performances of PC-OFDM-DCSK systems undergoing the CFO when $N = 128$, $\beta = 128$ and $\epsilon = 0.1$.

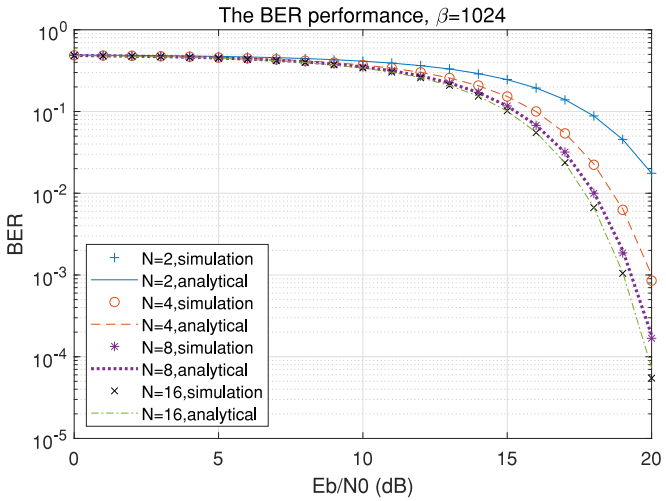

Fig. 6. The theoretical and simulated BER performances of PC-OFDM-DCSK systems over AWGN channel when $\beta = 1024$.

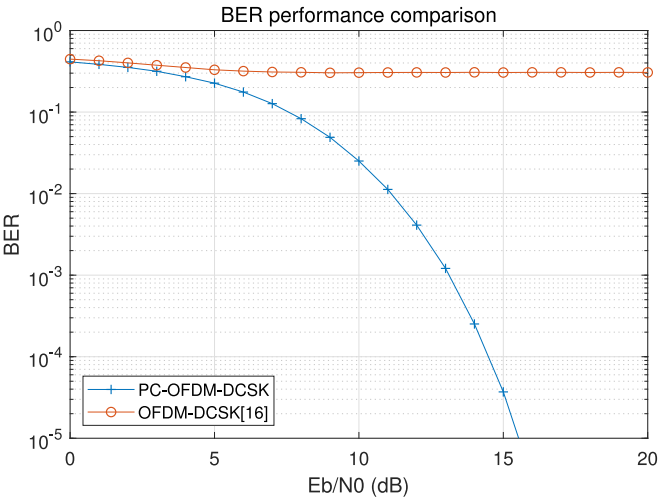

Fig. 8. The simulated BER performance comparison between PC-OFDM-DCSK and OFDM-DCSK [16] systems undergoing the CFO.

Then, Fig. 6 provides the analytical BER and simulated BER performances over AWGN channel when $\beta = 1024$. It can be seen that better BER performances can be achieved by using more subcarriers. Moreover, for larger N, the theoretical BER performances match the simulated BER performances better due to the smaller approximation error when using the Gaussian approximation methods. Notably, since the analytical result are obtained using the Gaussian approximation method, the distribution of Z_n defined by Eq. (20) may be slightly different from Gaussian distribution, which induces the approximation errors and brings the slight deviations of the simulated results from the analytical results. Moreover, we can observe that the BER performance gain increases more slowly when N increases. The reason is that it can be seen from Eq. (24) that the value of the fraction $N/(N-1)$ approaches 1 when N becomes larger.

Fig. 7 illustrates the BER performances of the presented PC-OFDM-DCSK system over the channel with the CFO. We can conclude from Fig. 7 that thanks to the pre-coding, when $N = 128$, $\beta = 128$ and the CFO is set as $\epsilon = 0.1$, the BER performances of PC-OFDM-DCSK system become better when the subcarrier expansion factor M increases. It can also be seen that the simulation results match the analytical results evaluated from Eq. (24) and Eq. (28), which means that our derivations are effective.

B. BER Performance Comparisons of PC-OFDM-DCSK Systems and Counterpart Systems

For the fairness of performance comparisons, in the following performance comparisons, the same parameter settings are employed in the presented and the counterpart systems.

1) BER Performance Comparison Between PC-OFDM-DCSK and OFDM-DCSK: Fig. 8 compares the simulated BER performances over the channels wherein there exist CFO environment between the presented PC-OFDM-DCSK and conventional OFDM-DCSK [16]. It can be observed that the PC-OFDM-DCSK design can effectively combat the CFO, and achieves much lower BER than the conventional

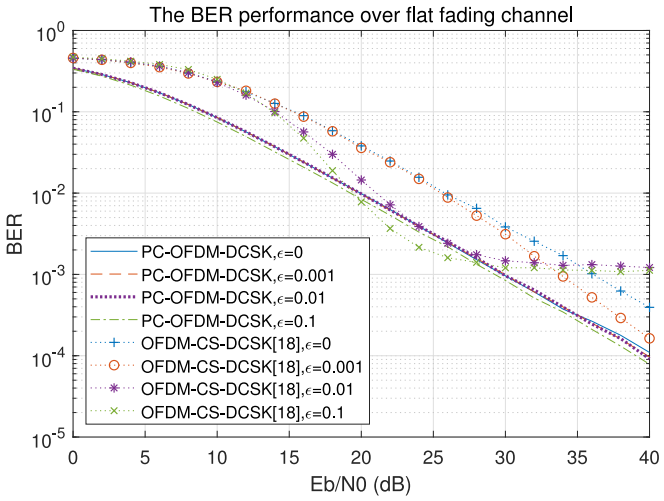

Fig. 9. The BER performance comparison of the PC-OFDM-DCSK system and the OFDM-CS-DCSK system [18] over flat fading channels with CFO when the length of CP is 8.

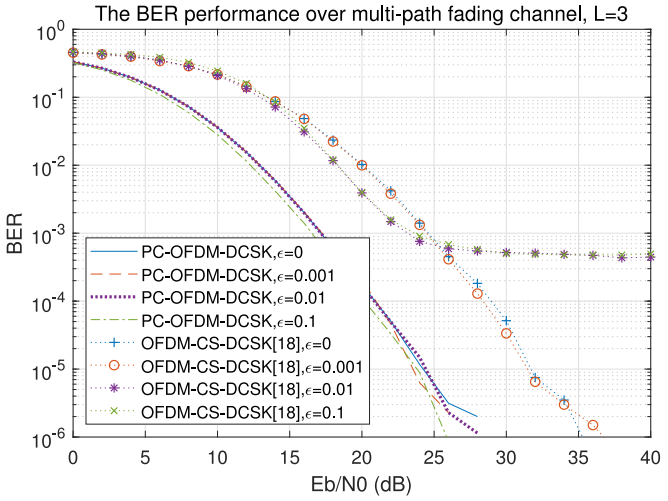

Fig. 10. The BER performance comparison of the PC-OFDM-DCSK system and the OFDM-CS-DCSK system [18] over multi-path fading channels with CFO and $L = 3$ when CP length is 8.

OFDM-DCSK system [16]. The reason is that with the precoding module, the chaos chips could be transmitted via different subcarriers, thus the channel impulse response naturally embedded into these chaos chips can be collected for information retrieval. Thus the receiver can select chaos chips over subcarriers with fewer ICI or collect the chaos chips over different subcarriers to utilize the frequency diversity gain to improve the BER performances for the proposed system.

2) BER Performance Comparison Between PC-OFDM-DCSK and OFDM-CS-DCSK: Subsequently, we compare the BER performances of PC-OFDM-DCSK and OFDM-CS-DCSK [18] over flat fading channels and multi-path fading channels. In the following comparisons, the number of the chaotic sequence is $N = 8$, and each chaotic sequence has the length of $\beta = 8$. In addition, for the PC-OFDM-DCSK system, the parameter M is set as 16.

Fig. 9 illustrates the BER performance comparisons of the PC-OFDM-DCSK system and the OFDM-CS-DCSK system [18] over flat fading channels with CFO. We can conclude from Fig. 9 that our presented system achieves lower BER when the E_b/N_0 is low. Besides, we can notice that when E_b/N_0 increases, the BER performances of the OFDM-CS-OFDM system have an error floor although the BER of OFDM-CS-DCSK is lower than the BER of our system when $20\text{dB} \leq E_b/N_0 \leq 28\text{dB}$ and $\epsilon = 0.1$. Moreover, with the absence of the error floor, our system can reach a much lower BER bound in the scenario where the CFO exists.

Then we compare the BER performances between the PC-OFDM-DCSK system and the OFDM-CS-DCSK system over the multi-path fading channel with the CFO. In the simulations, the multi-path fading channel has L paths whose average power are $\mathrm{E}\{h_l^2\}$ where $\mathrm{E}\{h_l^2\} = \mathrm{E}\{h_1^2\}\exp[-\nu(l-1)]$ and $l = 1, 2, \ldots, L$, and the power of each path will be normalized to guarantee $\sum_{i=1}^{L} \mathrm{E}\{h_l^2\} = 1$. The channel fading parameter ν is set as 1.

As shown in Fig. 10, it can be observed that in the OFDM-CS-DCSK system, similar to the case of flat fading channels,

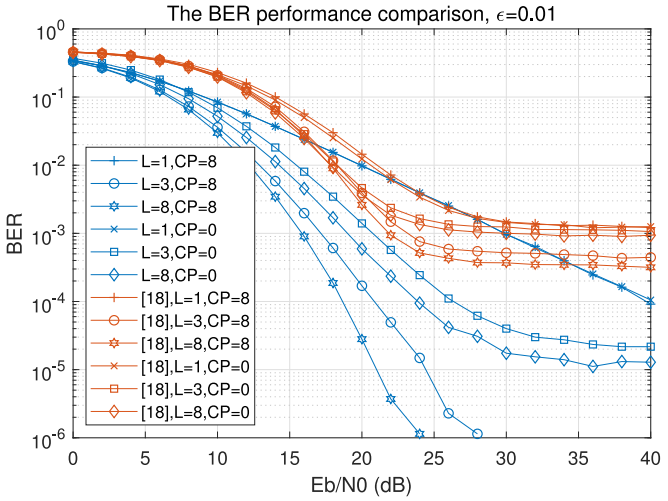

Fig. 11. The BER performance comparison of the PC-OFDM-DCSK system and the OFDM-CS-DCSK system [18] over multi-path fading channels with $L = 1,3,8$, $\epsilon = 0.01$ and CP length $= 0, 8$.

the BER error floor appears above 10^{-4} when $\epsilon = 0.01$ and $\epsilon = 0.1$. By contrast, our presented PC-OFDM-DCSK system can provide better BER performances over the channels with the CFO of different ϵ, and achieve the BER lower than 10^{-5} when $\epsilon = 0.01$ and $\epsilon = 0.1$. Thus the presented design can effectively combat the CFO and the multi-path fading to provide reliable transmission for the users over multi-path fading channels.

Fig. 11 provides the BER performance comparison results between the presented PC-OFDM-DCSK system and the OFDM-CS-DCSK system [18] over multi-path fading channels with different number of paths and CP length when ϵ is set as 0.01. Similar to the observations in Fig. 9 and Fig. 10, the OFDM-CS-DCSK system has the BER error floor.

Furthermore, we can conclude that our PC-OFDM-DCSK system performs well in the CFO environment no matter whether the CP is added or not, however, it is noticeable that the lack of CP will result in the error floor above 10^{-5}. Hence,

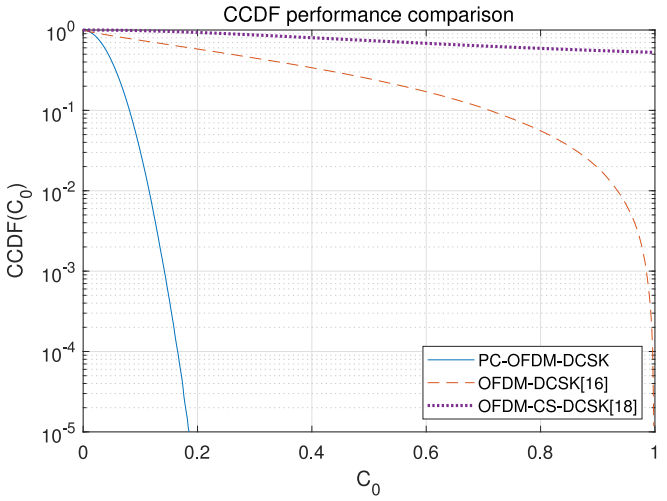

Fig. 12. The CCDF performance comparison between the PC-OFDM-DCSK system and other counterpart systems when $N = 128$ and $\beta = 128$.

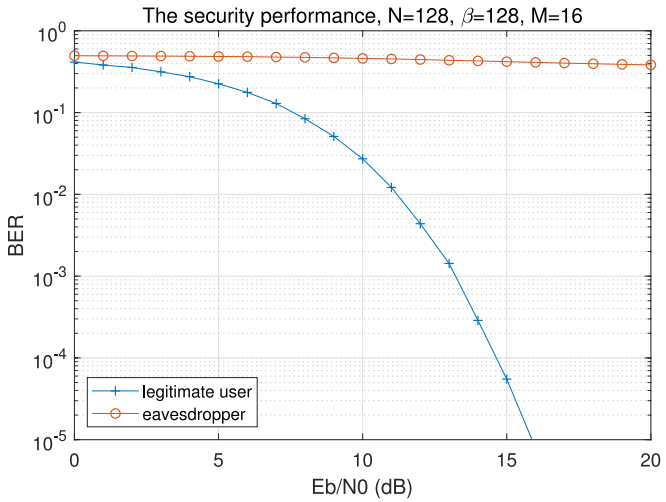

Fig. 13. The BER performance comparison of legitimate users and eavesdroppers when $N = 128$, $\beta = 128$ and $M = 16$.

the CP can help the presented PC-OFDM-DCSK system to defend against the multi-path fading. Moreover, it can be also be seen that for larger number of path, better BER performances can be achieved by our presented system. The reason is that when L increases, more frequency diversity can be utilized and thus the BER performances are improved.

C. Security Performance

Here we propose to investigate the correlation degree among the transmitted symbols, and compare the information leakage among the presented PC-OFDM-DCSK system and counterpart systems. In the following simulation, the number of eavesdroppers is set as 1, the number of subcarriers N is set as 128, the length of chaotic sequences β is set as 128, the subcarrier expansion factor M is set as *16*, and the average power of each path $\mathrm{E}\{h_l^2\}$ over multipath fading channel is set as $\mathrm{E}\{h_l^2\} = \mathrm{E}\{h_1^2\}\exp\left[-\nu(l-1)\right]$, where $l = 1, 2, \ldots, L$, L is the number of paths, $\nu = 1$ and the power of each path is normalized to $\sum_{i=1}^{L}\mathrm{E}\{h_l^2\} = 1$.

Besides, we assume that the eavesdropper can receive all the data from the legitimate users due to the broadcasting property of wireless channels, and that the channel state information of both the legitimate channel and the eavesdropping channel can be obtained from the pilot symbols, thus the data of legitimate users can be fed back, decoded and retrieved [31]. Notably, it is reasonable to assume that the only thing the eavesdropper does not know is the chaos mask pattern due to the chaos mask employed at the proposed PC-OFDM-DCSK transmitter.

1) CCDF Performance Comparison: In Fig. 12, we firstly investigate the correlations among the OFDM symbols among the presented PC-OFDM-DCSK system, OFDM-DCSK system [16] and OFDM-CS-DCSK system [18]. The correlation of OFDM symbols in different time slots indicates the security performance since the eavesdroppers may retrieve the information by performing the correlation demodulation between different OFDM symbols. Therefore, if the correlation is weak, the eavesdroppers can hardly obtain the information.

Here we evaluate the correlations by $C_{j,k} = \Re\{\sum_{i=0}^{NM-1}\mathrm{conj}(s_{i,j}) \cdot s_{i,k}\}/N_f$, where $s_{i,j}$ is the ith chip of the jth OFDM symbol transmitted by the transmitter, $s_{i,k}$ is the ith chip of the kth OFDM symbol and N_f is the constant normalization factor. Furthermore, we evaluate the distribution of $C_{j,k}$ using the complementary cumulative distribution function (CCDF), which is defined as

$$CCDF(C_0) = Pr\big(C_{j,k} > C_0\big) \tag{33}$$

where C_0 is the threshold of $C_{j,k}$ and $Pr(C_{j,k} > C_0)$ denotes the probability that $C_{j,k}$ is larger than the threshold.

From Fig. 12, we can conclude that the CCDF of the PC-OFDM-DCSK system is much lower than that of the other two systems, including the OFDM-DCSK system [16] and the OFDM-CS-DCSK system [18], which means that thanks to the chaos mask, the correlation between reference chaotic sequences and information bearing sequences is weakened and the eavesdroppers cannot recover the information by simply performing the correlation demodulations.

Fig. 13 compares the BER performances for legitimate users and eavesdroppers. Simulation results show that the legitimate users can successfully demodulate the information since they can recover the symbols from the masked signals with the knowledge of chaos mask. By contrast, the eavesdroppers receiver can not recover the transmitted data due to the high BER since the chaos mask are unknown to them.

Finally, Fig. 14 shows the information leakage performances for eavesdropping between the PC-OFDM-DCSK system and the OFDM-DCSK system [16] according to Eq. (31) and Eq. (32). Here we assume that the eavesdroppers could learn all the key parameters at the transmitter [29], except the chaos mask. It can be concluded from Fig. 14 that thanks to the chaos mask, it is nearly impossible for the eavesdroppers to recover the transmitted data from the masked symbols in the PC-OFDM-DCSK system, and the information leakage is much lower than the corresponding performance of OFDM-DCSK systems. Moreover, when E_b/N_0 is large enough, the eavesdroppers can easily obtain all information transmitted

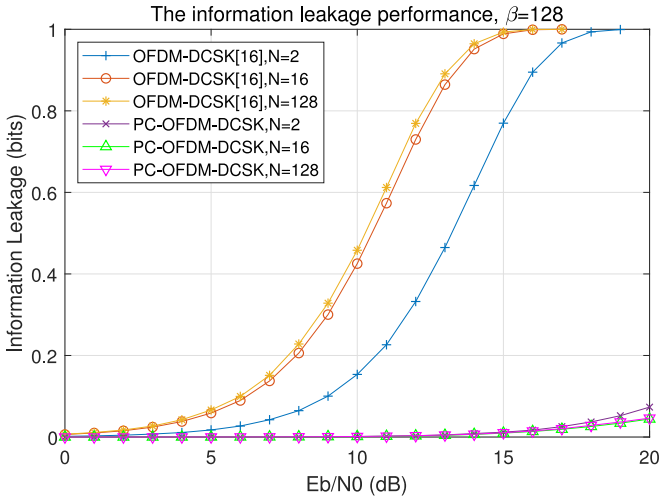

Fig. 14. Information leakage performance comparison between the presented PC-OFDM-DCSK system and the OFDM-DCSK system [16].

by OFDM-DCSK systems. On the contrary, for PC-OFDM-DCSK systems, even when the E_b/N_0 is large, the number of leaked bits remains few. We can also conclude from Fig. 14 that for the information leakage will increase with larger N. The reason is that more information can be extracted from more received data.

V. Conclusion

In this paper, we propose a novel pre-coding OFDM-DCSK scheme to simultaneously improve both the reliability and the security performances for practical CR systems undergoing the CFO. In our design, the chaotic chips are interleaved and spread in the frequency domain, then the chaos mask is added. Thanks the pre-coding with chaotic masking, the average energy of the desired signal is increased, and thus the BER performances can be improved. Moreover, the eavesdroppers can hardly retrieve the pre-coded symbol without the knowledge of the trace of the chaos mask, which enhances the security performances. Furthermore, we derive the theoretical BER and information leakage expressions. Simulations are performed to verify the effectiveness of our derivations, and to investigate the reliability and security performances. The results demonstrate that our presented system achieves better BER and more secure performances over AWGN channel, the flat fading channel and the multipath fading channel than the counterpart state-of-the-art designs. Therefore, the presented PC-OFDM-DCSK scheme can provide services with high reliability and security over contiguous or NC bands for practical CR systems potentially operating with the CFO induced by the clock offset or non-ideal electronic components.

Acknowledgment

The authors want to thank Prof. L. Wang and Prof. W. Xu for their invaluable support.

References

[1] D. Cabrić, S. M. Mishra, D. Willkomm, R. Brodersen, and A. Wolisz, "A cognitive radio approach for usage of virtual unlicensed spectrum," in *Proc. 14th IST Mobile Wireless Commun. Summit*, Dresden, Germany, Jun. 2005, pp. 1–4.

[2] S. Sasipriya and R. Vigneshram, "An overview of cognitive radio in 5G wireless communications," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Chennai, India, Dec. 2016, pp. 1–5.

[3] X. Hong, J. Wang, C.-X. Wang, and J. Shi, "Cognitive radio in 5G: A perspective on energy-spectral efficiency trade-off," *IEEE Commun. Mag.*, vol. 52, no. 7, pp. 46–53, Jul. 2014.

[4] H. Bogucka, P. Kryszkiewicz, and A. Kliks, "Dynamic spectrum aggregation for future 5G communications," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 35–43, May 2015.

[5] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems*. New York, NY, USA: Springer, 2003.

[6] J. C. Feng, *Reconstruction of Chaotic Signals With Applications to Chaos-Based Communications*. Singapore: World Sci., 2008.

[7] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-sychronizing Chua's circuits," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 10, pp. 634–642, Oct. 1993.

[8] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. NDES*, 1996, pp. 87–92.

[9] Y. Fang, G. Han, P. Chen, F. C. M. Lau, G. Chen, and L. Wang, "A survey on DCSK-based communication systems and their application to UWB scenarios," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1804–1837, 3rd Quart., 2016.

[10] H. Yang, G. Jiang, L. Xia, and X. Tu, "Reference-shifted DCSK modulation scheme for secure communication," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Santa Clara, CA, USA, Jan. 2017, pp. 1073–1076.

[11] F. C. M. Lau, K. Y. Cheong, and C. K. Tse, "Permutation-based DCSK and multiple-access DCSK systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 6, pp. 733–742, Jun. 2003.

[12] M. Herceg, G. Kaddoum, D. Vranješ, and E. Soujeri, "Permutation index DCSK modulation technique for secure multiuser high-data-rate communication systems," *IEEE Trans. Veh. Tech.*, vol. 67, no. 4, pp. 2997–3011, Apr. 2018.

[13] W. Ma, J. Du, and H. Xue, "Design of reverse-DCSK for chaos based communication system," in *Proc. 3rd IEEE Int. Conf. Comput. Commun. (ICCC)*, Dec. 2017, pp. 743–747.

[14] H. Cai, Z. Hua, and H. Huang, "A novel differential-chaos-shift-keying secure communication scheme," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, Miyazaki, Japan, Oct. 2018, pp. 1794–1798.

[15] G. Kaddoum, F.-D. Richardson, and F. Gagnon, "Design and analysis of a multi-carrier differential chaos shift keying communication system," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3281–3291, Aug. 2013.

[16] S. Li, Y. Zhao, and Z. Wu, "Design and analysis of an OFDM-based differential chaos shift keying communication system," *J. Commun.*, vol. 10, pp. 199–205, Mar. 2015.

[17] G. Kaddoum, "Design and performance analysis of a multiuser OFDM based differential chaos shift keying communication system," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 249–260, Jan. 2016.

[18] M. Chen, W. Xu, D. Wang, and L. Wang, "Design of a multi-carrier different chaos shift keying communication system in doubly selective fading channels," in *Proc. 23rd Asia–Pac. Conf. Commun. (APCC)*, Dec. 2017, pp. 1–6.

[19] S. Gong, P. Wang, and L. Duan, "A game theoretic approach for robust power control in cognitive radio networks," in *Proc. IEEE Glob. Commun. Conf.*, Austin, TX, USA, Dec. 2014, pp. 1053–1058.

[20] S. Gong, P. Wang, and L. Duan, "Distributed power control with robust protection for PUs in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3247–3258, Jun. 2015.

[21] Z. He, K. Li, L. Yang, and Y. Shi, "A robust digital secure communication scheme based on sporadic coupling chaos synchronization," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 47, no. 3, pp. 397–403, Mar. 2000.

[22] Z. Liu, L. Zhang, and Z. Wu, "Non contiguous frequency hopping aided OFDM-DCSK design without requiring CSI," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[23] S.-H. Tsai, Y.-P. Lin, and C.-C. J. Kuo, "An approximately MAI-free multiaccess OFDM system in carrier frequency offset environment," *IEEE Trans. Signal Process.*, vol. 53, no. 11, pp. 4339–4353, Nov. 2005.

[24] P. Dharmawansa, N. Rajatheva, and H. Minn, "An exact error probability analysis of OFDM systems with frequency offset," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 26–31, Jan. 2009.

[25] R. U. Mahesh and A. K. Chaturvedi, "Closed form BER expressions for BPSK OFDM systems with frequency offset," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 731–733, Aug. 2010.

[26] C. Popper, M. Strasser, and S. Capkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 703–715, Jun. 2010.
[27] B. Chen, L. Zhang, and H. Lu, "High security differential chaos-based modulation with channel scrambling for WDM-aided VLC system," *IEEE Photon. J.*, vol. 8, no. 5, Oct. 2016, Art. no. 7804513.
[28] Y. Xia, C. K. Tse, and F. C. M. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 51, no. 12, pp. 680–684, Dec. 2004.
[29] H. Lu, L. Zhang, M. Jiang, and Z. Wu, "High-security chaotic cognitive radio system with subcarrier shifting," *IEEE Commun. Lett.*, vol. 19, no. 10, pp. 1726–1729, Oct. 2015.
[30] H. Li, X. Wang, and Y. Zou, "Dynamic subcarrier coordinate interleaving for eavesdropping prevention in OFDM systems," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 1059–1062, Jun. 2014.
[31] J. Kim, J. Kim, J. Lee, and J. P. Choi, "Physical-layer security against smart eavesdroppers: Exploiting full-duplex receivers," *IEEE Access*, vol. 6, pp. 32945–32957, 2018.

Zhaofeng Liu received the B.S. degree in communication engineering from Sun Yat-sen University, Guangzhou, China, in 2017, where he is currently pursuing the master's degree in electronics and communication engineering. His research interests include chaotic communication, multicarrier communication, cognitive radio, and Internet of Things.

Lin Zhang (M'16) received the B.S. and M.S. degrees in electrical engineering from Shanghai University in 1997 and 2000, respectively, and the Ph.D. degree in electrical engineering from Sun Yat-sen University in 2003, where she joined the Department of Electrical Engineering in 2003 and has been served as an Associate Professor since 2007. From 2008 to 2009, she was a Visiting Researcher with the Electrical and Computer Engineering Department, University of Maryland, College Park, USA, for one year. In 2019, she joined Southern Marine Science and Engineering Guangdong Laboratory, where she served as a Researcher. Her research has been supported by National Natural Science Foundation of China and the Science and Technology Program Project of Guangdong Province. Her current research interests are in the area of signal processing and their applications to wireless communication systems.

Zhiqiang Wu (M'02–SM'17) received the B.S. degree in electrical engineering from the Beijing University of Posts and Telecommunications in 1993, the M.S. degree in electrical engineering from Peking University in 1996, and the Ph.D. degree in electrical engineering from Colorado State University in 2002. He served as an Assistant Professor with the Department of Electrical and Computer Engineering, West Virginia University Institute of Technology, from 2003 to 2005. He joined the Wright State University in 2005, where he currently serves as a Full Professor with the Department of Electrical Engineering. His research has been supported by NSF, AFRL, ONR, AFOSR, and OFRN. He has also held visiting positions with Peking University, Harbin Engineering University, Guizhou Normal University, and Tibet University.