Efficient and Secure Non-Coherent OFDM-Based Overlapped Chaotic Chip Position Shift Keying System: Design and Performance Analysis

Lin Zhang, *Member, IEEE*, Zuwei Chen, Weiwei Rao, and Zhiqiang Wu, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a novel non-coherent orthogonal frequency division multiplex (OFDM) based overlapped chaotic chip position shift keying (OCCPSK) system. Different from traditional non coherent chaotic systems, this system endeavors to achieve efficient and secure performances with no need to transmit reference chaotic sequences. At the transmitter, information bits are grouped into multiple subsets and respectively modulated by the position of chaotic chips. Then iterative chaotically shift-aided shuffling and overlapping operations are performed on the resultant multi-ary signals to enhance the security. Subsequently, OFDM modulations are performed and information-bearing signals are transmitted. At the legitimate receiver, with the known key parameters, reverse operations are carried out. Then the positions used for modulations can be formulated out to recover information bits via maximizing the Euclidean norm of received symbols. Since no reference chaotic signals are required to be transmitted, both efficiency and security performances are improved. Moreover, we derive the analytical symbol error rate (SER) and bit error rate (BER) expressions over fading channels, and theoretical spectrum efficiency, energy efficiency and security performances are analyzed. Simulation results verify the effectiveness of derivations, and demonstrate the high efficiency and security of this design.**

***Index Terms*—Efficiency, non-coherent overlapped chaotic modulation, orthogonal frequency division multiplex, position shift keying, security.**

I. Introduction

CHAOTIC communication has been widely used for providing secure information transmissions by exploiting the natural high security properties such as being non-periodic and being sensitive to the initial value etc. [1], [2]. The potential applications include power line communication [3], ultra wide band systems [4] and cooperative networks [5], [6] etc. Additionally, the chaotic sequences have revealed the ability to minimize interferences for spreading code division multiple access (CDMA) systems [7]–[9].

In chaos-based communication systems, the information can be transmitted in the coherent or the non-coherent manner. The non-coherent chaotic transmission schemes have attracted a lot of research interests due to the low implementation complexity, while the coherent chaotic receivers require to use complex synchronization circuits to retrieve the chaotic basis sequences [10]. In non-coherent systems, the reference chaotic sequences are transmitted directly to the receiver and the synchronization circuits are removed [4], [11]–[14].

Among the non-coherent chaotic communication systems, the differential chaos shift keying (DCSK) [11] has been considered the most promising one because of its constant zero threshold, excellent bit error rate (BER) performance and low implementation complexity [4]. However, DCSK systems have two major drawbacks. As mentioned by [15], one drawback is the low energy and spectrum efficiency since only half of each symbol duration is used for information transmission. Another major drawback is that the delay line employed in the modulator is difficult to implement in practical systems.

In recent years, many researches have been done to remove the delay line and to improve performances for non-coherent chaotic modulation systems. On the one hand, in order to improve the spectrum efficiency and to remove the delay line, the signal extensions in different spaces such as the orthogonal basis space, the time space, the frequency space, the space constructed by the parameters and the amplitude space etc. are utilized to transmit more bits [12]–[14], [16]. For example, the space constructed by the orthogonal basis is utilized in [13], which employs the Hilbert transform to generate orthogonal basis signals for 2-dimension chaotic modulation schemes to transmit multiple bits in one time slot. For the time space extension, a high-efficiency DCSK (HE-DCSK) scheme is proposed in [12] which uses the same reference chaotic sequence in different time slots and transmits two data bits in one chaotic sample sequence by recycling each reference sample. Additionally, chaotic pulse is delayed by a certain time in [17] to modulate extra information bits with the time position of chaotic pulse, which is a hybrid modulation scheme of DCSK and chaotic pulse position modulation (PPM).

Manuscript received December 28, 2018; revised April 21, 2019 and August 1, 2019; accepted October 17, 2019. Date of publication November 8, 2019; date of current version January 15, 2020. This work was supported in part by the Project of National Natural Science Foundation of China under Grant 61602531, in part by the Key-Area Research and Development Project of Guangdong Province under Grant2018B010114001, in part by National Science Foundation under Grant 1323240, and in part by the Office of Naval Research under Contract N00024-14-C-4073. This article was recommended by Associate Editor J. Lota. *(Corresponding author: Lin Zhang.)*

L. Zhang and Z. Chen are with the School of Electronic and Information Technology, Sun Yat-sen University, Guangzhou 510006, China (e-mail: isszl@mail.sysu.edu.cn; chenzw25@mail2.sysu.edu.cn).

W. Rao is with Huawei Technologies Co., Ltd., Shenzhen 518219, China (e-mail: wwrao@qq.com).

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

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2019.2948789

In [18], chaotic PPM is combined with the orthogonal basis to further improve the date rate. Meanwhile, the frequency resources in the frequency space are utilized and many multi carrier aided DCSK scheme have been presented to utilize the orthogonality in the frequency space to remove the delay line and to improve the spectrum efficiency [19]–[22]. Moreover, the space constructed by the parameters of the signals is also exploited for higher efficiency. Reference [14] commutates the chaotic chips to generate different basis signals with distinct positions, and then exploits the index modulation of the commutations to increase the data rate, while in our previous work [16], we utilize the orthogonal signal index and amplitude space to modulate the extra information bits.

On the other hand, the security issue has also been investigated. Although the direct transmission of the reference chaotic sequences bring the benefit of the implementation simplicity, the security performances are degraded. Recently, researches have been done to improve the security by enhancing the randomness of the non-coherent chaotic transmissions [23]–[25]. Reference [23] proposes to interleave the chaotic chips to enhance the security, while in [24], the permutation index is utilized to hide the reference chaotic signals. In addition, in [25], the authors propose to shift the reference chaotic sequence, thus the eavesdroppers can not retrieve the data without the known shifting rule shared between the legitimate transceivers.

However, most of the presented schemes, which improve the efficiency or the security performances while removing the delay lines, still need to recover the information with the known reference chaotic sequence at the receiver. Naturally the transmission of the reference chaotic signals lowers the efficiency and increases the exposure chances to the malicious eavesdropping.

In this paper, we present an efficient and secure non-coherent orthogonal frequency division multiplex-based overlapped chaotic chip position shift keying (OCCPSK) to simultaneously enhance the spectrum efficiency and the security via utilizing multiple chip positions and the iterative chaotically shift-aided shuffling and overlapping. Thanks to the aperiodicity property and the outstanding self-correlation characteristic of the chaotic sequence, in our design, the presented OCCPSK receiver can recover the information by maximizing the Euclidean norm of the internal chips of the received symbols and then performing the chip position demodulation, thus the reference chaotic sequences are not required to be transmitted.

More explicitly, at the OCCPSK transmitter, after the serial to parallel (S/P) conversion, the information symbols are respectively modulated by different chips in chaotic sequences which may be generated by the same or different chaos generators. Each information symbol is modulated by the specific position of a chaotic chip in a chaotic sequence with the chip number of p. Thus the resultant information-bearing chip position shift keying modulated symbol can carry $log_2(p)$ bits, and a multi-ary modulation is realized. Then iterative chaotical shift aided shuffling and overlapping operations are carried out to process these $log_2(p)$-ary chaotic symbols. As a result, the information carried by the chaotic chip positions is interleaved with the chaotic scrambling, and the shuffled symbols are overlapped in pairs with a specific pattern. Therefore, the chaotic modulated symbols are hidden behind the overlapped signals to improve the security performance, which can be further enhanced by performing the combined iterative shift-aided shuffling and overlapping operations multiple times based on the user security demands. After the inverse fast Fourier transform (IFFT), the information-bearing orthogonal frequency division multiplex (OFDM) chaotic symbols are transmitted over the channels.

At the legitimate OCCPSK receiver, after the fast Fourier transform (FFT), inverse operations are performed on the received data. We firstly separate the overlapped received symbols, then with the known initial value and mapping method of chaotic sequences used for shuffling, the obtained symbols are re-shuffled to retrieve the position-modulated symbols, and the positions used for modulations are determined by calculating the Euclidean norm of the received symbols. Subsequently, the position demodulation can be performed. Then an index-to-bit mapping is performed and the estimates of the transmitted data can be derived.

Furthermore, we derive the symbol error rate (SER) and bit error rate (BER) performances for the OCCPSK system over the additive white Gaussian noise (AWGN) channel and the multipath flat fading channel, then we analyze the spectrum efficiency, the energy efficiency and the security performances theoretically.

Briefly, the main contributions of this paper include:

1) No reference chaotic signals are required for the non-coherent multi carrier transmissions. The OCCPSK receiver can retrieve the data via maximizing the Euclidean norm of the internal chips of the received symbols, thus both the efficiency and the security performance can be improved.
2) We propose a multi-ary chaotic chip position modulation scheme to modulate the information bits with the positions of the aperiodic chaotic sequence. Multiple bits can be transmitted with the positions of the aperiodic chaotic chips, thus the data rate, the spectrum efficiency and energy efficiency could be further enhanced.
3) We propose an iterative chaotical shift aided shuffling and overlapping algorithm to process the chaotic modulated symbols to hide the information behind the chaotic waveforms, wherein the iteration number is determined by user security demands. The legitimate receiver can recover the received symbols using the known shuffling and overlapping pattern, while the eavesdroppers could not retrieve the data without the knowledge of the key parameters, thereby improving the security performances.
4) Theoretical performances including the SER, the BER, the spectrum efficiency, the energy efficiency and the security are analyzed. We derive the SER and the BER over the AWGN channel and the flat fading channels, and utilize the wavelet transform to investigate the

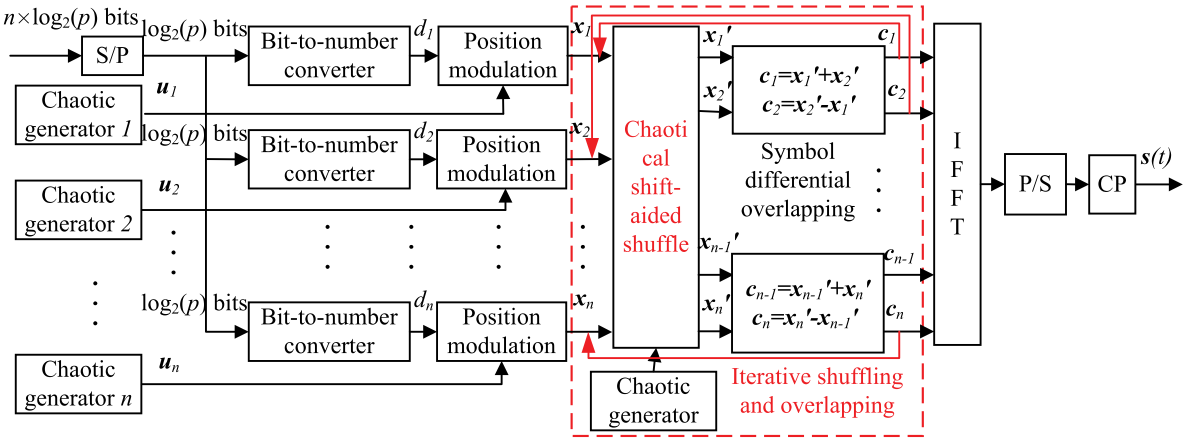


Fig. 1. Block diagram of the OCCPSK transmitter.

spectral characteristics of the signals for security performance analysis.

The remainder of the paper is organized as follows. In Section II, the details of the OCCPSK modulation as well as the demodulation are presented. Section III derives the SER and the BER expression over the flat multipath Rayleigh fading channel, then the spectrum efficiency, energy efficiency and security performances are analyzed for the proposed scheme. Subsequently, Section IV provides the simulation results and numerical analysis. Finally, Section V concludes our findings.

II. The OCCPSK Transceiver

In this section, the modulation and demodulation architectures of the proposed OCCPSK scheme are presented.

A. OCCPSK Modulation

Fig. 1 illustrates the block diagram of the proposed OCCPSK transmitter. The information bits are converted from the serial bit stream to the parallel information subsets. Then they are respectively modulated with the chip positions of the chaotic sequence output from the chaos generator. The resultant information-bearing chaotic modulated symbols are chaotically shifted and shuffled to enhance the security by utilizing the natural high secure property of the chaotic sequence being sensitive to the initial value non-repetitive. Subsequently, the neighboring pairs are overlapped mutually and then transformed by the IFFT module.

Specifically, let n denote the number of chaotic generators used for chaotic modulation, which also represents the number of generated chaotic sequences in one time slot, and p denote the number of chaotic chips contained in one chaotic sequence, then the number of the parallel information subsets, which are obtained after the serial to parallel (S/P) conversion, should be equal to the number of the chaotic sequence n. In addition, for the binary data, the chaotic positions numbered p can be used to modulate $log_2(p)$ bits. Accordingly, in one time slot, the total number of $n \times log_2(p)$ binary data bits can be modulated.

The procedure of the OCCPSK modulation for these binary bits is presented as follows.

1) Binary Bit to Decimal Number Conversion: For the multiple parallel streams, each binary data stream is fed into a bit-to-number converter to produce the corresponding decimal number. Let d_i denote the decimal number obtained from the ith input bit subset, then for a specific input stream including $log_2(p)$ bits, the range of values of the obtained decimal number d_i should be $0, 1, 2, \ldots, p-1$.

2) The Chaotic Chip Position Shift Keying: As illustrated in Fig.1, let $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots \boldsymbol{u}_n$ denote the n chaotic sequence vectors, where each vector has the length of M. These chaotic vectors can be generated using different chaotic maps or the same chaotic map with different initial values. In this paper, we use the following Logistic map with different initial values to generate the n chaotic vectors, i.e., we have

$$u_{i,q+1} = 1 - 2 \times u_{i,q}^2, \quad 1 \le i \le n, \ 1 \le q \le M \qquad (1)$$

where $u_{i,q}$ denotes the q_{th} element of the chaotic vector $\boldsymbol{u}_i$.

Subsequently, the ith p-ary number d_i is modulated by the position of the chaotic sequence generated from the chaos generator numbered from 1 to n. The resultant position shift keying modulated symbol obtained from the information d_i and the chaotic vector $\boldsymbol{u}_i$ is represented by $\boldsymbol{x}_i$, which has the length of $\beta(\beta = p \times M)$. More explicitly, the $(d_i \times M + q)_{th}$ element of $\boldsymbol{x}_i'$ will become the q_{th} element of $\boldsymbol{u}_i$ $(q = 1, 2, \ldots M)$, namely we have

$$x_{i,d_i \times M+q} = u_{i,q} (q = 1, 2, \ldots M) \qquad (2)$$

where $x_{i,d_i \times M+q}$ denotes the $(d_i \times M + q)_{th}$ element of $\boldsymbol{x}_i$, $u_{i,q}$ denotes the q_{th} element of $\boldsymbol{u}_i$, and the other elements of $\boldsymbol{x}_i$ are zeros.

For example, assuming that there are $p = 4$ chips in one chaotic sequence, and the length of each chip is $M = 20$, thus each symbol has the length of 80 $(p \times M = 4 \times 20)$. In each symbol, $log_2(p) = 2$ information bits will be modulated by the position shift keying scheme. Take the information bits "11" as an example. For the ith bit subset "11", the corresponding decimal number is $d_i = 3$. Then the $(d_i + 1) = 4_{th}$ chip of is modulated and equals to $\boldsymbol{u}_i$, namely we have $x_{i,3\times20+q} = u_{i,q}(q = 1, 2, \ldots 20)$.

3) The Chaos-Based Shuffling and Symbol Differential Overlapping: Next, the n position shift keying modulated symbols $\boldsymbol{x}_i$ are shuffled aided with chaotical shifting. To be more specific, the shuffling rule is determined by the chaotic sequence, and a specific shift pattern dependent on the resultant chaotic sequence.

More explicitly, let $\boldsymbol{v} = [v_1, v_1, \ldots, v_n]$ denote the chaotic sequence generated by the chaotic generator with the length of n, $\boldsymbol{x} = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_n]$ denote the collection of the modulated symbols, and $\boldsymbol{x}' = \left[\boldsymbol{x}'_1, \ldots, \boldsymbol{x}'_i, \ldots, \boldsymbol{x}'_n\right]$ represent the shuffled symbols, we define the shuffling rule as $f(\boldsymbol{x})$, which shuffle the symbols aided with the chaotical shift according to Algorithm I. Then after shuffling, we obtain $\boldsymbol{x}' = f(\boldsymbol{x})$. In the 9_{th} step of Algorithm I, $\lceil\cdot\rceil$ is the rounding function and % is the modulo operator.

Algorithm 1 Shuffling $\boldsymbol{x}$

```
Input: $x$
Output: $x'$
    Initialization :
    LOOP Process
 1: for $i = 1$ to $n$ do
 2:     $j = 0$
 3:     for $g = 1$ to $n$ do
 4:         if $(v_i > v_g)$ then
 5:             $j = j + 1$
 6:         end if
 7:     end for
        Shifting Process
 8:     for $m = 0$ to $p \times M - 1$ do
 9:         $x'_{i,m+1} = x_{i,(m+j\times\lceil\frac{p\times M}{n}\rceil)\%(p\times M)+1}$
10:     end for
11: end for
12: return $x'$
```

Notably, thanks to the non repetitive property of chaotic sequences, the shifting will also be non repetitive when $n \leqslant p \times M$. If $n > p \times M$, we would divide the subcarriers into several groups, each group including less than $p \times M$ subcarriers. Then the shuffling operations will be performed on each group respectively, thus the security could be further enhanced. For legitimate users, the key parameters including the initial value and the mapping structure for the chaotic sequence generation, and the chaotical shift aided shuffling algorithm are notified before the information transmission. By contrast, the malicious user can not retrieve the information without the knowledge of these secret keys. Thus with the aid of the chaotical shift-aided shuffling, which scrambles the symbols chaotically in the time domain, the security performance of DCSK systems can be greatly improved.

After the shuffling, as indicated by Fig.1, the neighboring pairs of symbols are overlapped with each other in a differential way. To be more explicit, performing the differential overlapping operation on the paired $i_{th}(i = 1, \ldots, n)$ and the $(i+1)_{th}$ symbol, which are respectively expressed as $\boldsymbol{x}'_i$ and $\boldsymbol{x}'_{i+1}$, we obtain the overlapped symbol $\boldsymbol{c}_i$ and $\boldsymbol{c}_{i+1}$ as

$$\begin{bmatrix} \boldsymbol{c}_i \\ \boldsymbol{c}_{i+1} \end{bmatrix} = \boldsymbol{B}_{overlap} \begin{bmatrix} \boldsymbol{x}'_i \\ \boldsymbol{x}'_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{x}'_i \\ \boldsymbol{x}'_{i+1} \end{bmatrix} \tag{3}$$

where $\boldsymbol{B}_{overlap}$ represents the overlapping method. In fact, for the matrix $\boldsymbol{B}_{overlap}$ with the dimension of 2×2, the elements can be any real number on the premise that the constructed $\boldsymbol{B}_{overlap}$ is invertible, since at the receiver, the inverse matrix $\boldsymbol{B}_{overlap}^{-1}$ is required for recovering the transmitted information. Here with considerations of the energy efficiency and the brevity of the theoretical derivations, we use the matrix $\boldsymbol{B}_{overlap} = \left[\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right]$. In this case, Eq.(3) can be rewritten as

$$\boldsymbol{c}_i = \begin{cases} \boldsymbol{x}'_i + \boldsymbol{x}'_{i+1}, & if\ i\%2 = 1 \\ \boldsymbol{x}'_i - \boldsymbol{x}'_{i-1}, & if\ i\%2 = 0 \end{cases} \tag{4}$$

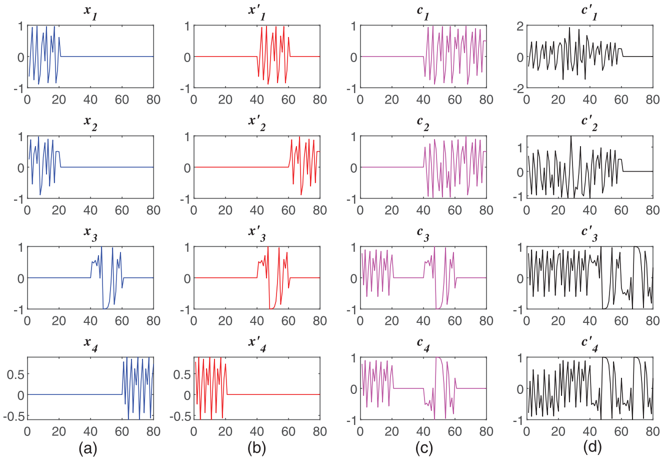


Fig. 2. An example of the waveform of $\boldsymbol{x}_i$, $\boldsymbol{x}'_i$, $\boldsymbol{c}_i$ and $\boldsymbol{c}'_i$.

It is noticeable that the security performances can be further enhanced by performing iterative chaotic shift-aided shuffling and overlapping for multiple times, wherein the iteration number is dependent on the user security demands. More explicitly, the overlapped $\boldsymbol{c}_i$ and $\boldsymbol{c}_{i+1}$ are fed back as the input $\boldsymbol{x}_i$ and $\boldsymbol{x}_{i+1}$ iteratively. Hence, the proposed OCCPSK design can provide multiple fold chaotical shift-aided shuffling and overlapping protections for security enhancements.

Take an OCCPSK system using one iteration as an example. In this system, $\boldsymbol{x}_i$, $\boldsymbol{x}'_i$ and $\boldsymbol{c}_i$ are the waveforms obtained at the first round shuffling and the overlapping. Then $\boldsymbol{c}_i$ is fed back as $\boldsymbol{x}_i$ for the second round shuffling and overlapping. Let $\boldsymbol{c}'_i$ represent the overlapped symbol.

Assuming that $n = 4$, $p = 4$, $M = 20$ and the chaotic sequence used for the shift-aided shuffling is $v_1 = 0.2, v_2 = 0.92, v_3 = -0.6928, v_4 = 0.0401$, then we have $\boldsymbol{x}'_1 = roll(\boldsymbol{x}_1, 40)$, $\boldsymbol{x}'_2 = roll(\boldsymbol{x}_2, 60)$, $\boldsymbol{x}'_3 = roll(\boldsymbol{x}_3, 0)$, $\boldsymbol{x}'_4 = roll(\boldsymbol{x}_4, 20)$, $\boldsymbol{c}_1 = \boldsymbol{x}'_1 + \boldsymbol{x}'_2$, $\boldsymbol{c}_2 = \boldsymbol{x}'_2 - \boldsymbol{x}'_1$, $\boldsymbol{c}_3 = \boldsymbol{x}'_3 + \boldsymbol{x}'_4$, $\boldsymbol{c}_4 = \boldsymbol{x}'_4 - \boldsymbol{x}'_3$, while after the feedback and the second shift-aided shuffling as well as the overlapping, we have $\boldsymbol{c}'_1 = roll(\boldsymbol{c}_1, 40) + roll(\boldsymbol{c}_2, 60)$, $\boldsymbol{c}'_2 = roll(\boldsymbol{c}_2, 60) - roll(\boldsymbol{c}_1, 40)$, $\boldsymbol{c}'_3 = roll(\boldsymbol{c}_3, 0) + roll(\boldsymbol{c}_4, 20)$ and $\boldsymbol{c}'_4 = roll(\boldsymbol{c}_4, 20) - roll(\boldsymbol{c}_3, 0)$ where $roll(\boldsymbol{c}_i, s)$ denotes the function rolling $\boldsymbol{c}_i$ to the right s units.

Fig. 2 illustrates the waveforms of $\boldsymbol{x}_i$, $\boldsymbol{x}'_i$, $\boldsymbol{c}_i$ and $\boldsymbol{c}'_i$ when the position information is $d_1 = 0, d_2 = 0, d_3 = 2$, $d_4 = 3$. It can be observed that the shuffled symbols $\boldsymbol{x}'_i$ can be identified if the malicious users apply the energy detection method. In addition, in the special case that the neighboring pair has the value of 0 such as $d_1 = d_2 = 0$, $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$

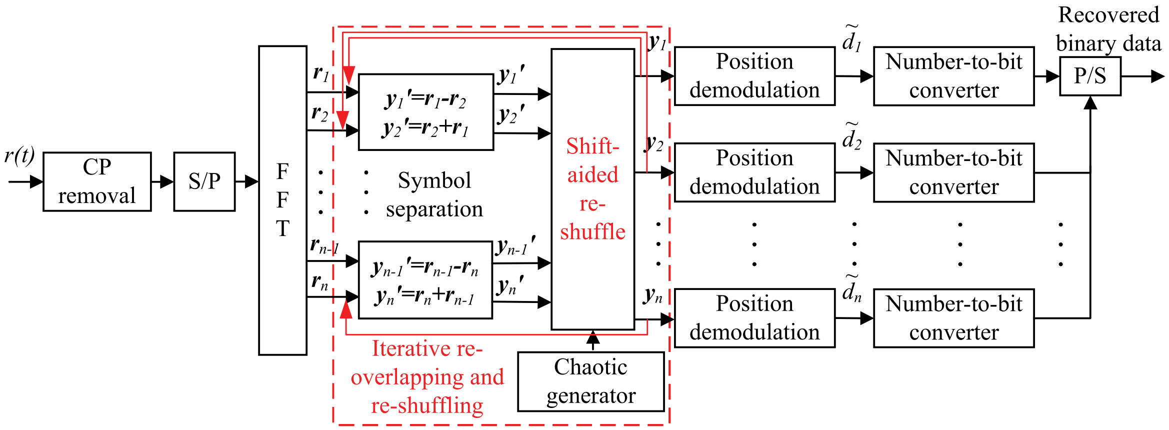


Fig. 3. Block diagram of the OCCPSK receiver.

would not reveal the user information when using the energy detection.

By contrast, after 1 iteration, thanks to one more shift aided shuffling and overlapping operation, the randomness of the symbols $\boldsymbol{c}_i'$ is enhanced and they could hardly be identified by applying the energy detection. Moreover, the randomness could be further improved via the iterative chaotical shift-aided shuffling and overlapping operations. In practical systems, we could select an appropriate iteration number based on the user security demands.

Notably, in the following descriptions and performance analysis, as shown in Fig. 1 and Fig. 3, we only consider the case of one-time overlapping for the sake of brevity.

4) OFDM Modulation: The resultant overlapped chaotic signals are then transformed by the IFFT module for transmission over multiple subcarriers. Notably, in order to accommodate the paired overlapping, the total number of subcarriers should be an even number. Then the OFDM symbols are converted by the parallel to serial (P/S) module. After adding the cyclic prefix (CP) that is longer than the maximum channel delay time to eliminate the inter symbol interference and to allow a simpler frequency domain processing at the receiver, the OCCPSK symbols are sequentially transmitted over the channel to the receiver.

After the modulation, the symbol is switched from frequency domain to the time domain, and the sequential OFDM signal in the time domain can be expressed as

$$s(t)=\sum_{q=1}^{\beta}\sum_{i=1}^{n}c_{i,q}e^{2\pi jf_it},\quad 0\le t\le \beta T_o \tag{5}$$

where $c_{i,q}$ denotes the q_{th} element of $\boldsymbol{c}_i$, $f_i=i/T_o$ is the subcarrier frequency, T_o is one OFDM symbol duration, and $s(t)$ represents the transmitted OCCPSK signal. It is worth pointing out that for each overlapped symbol $\boldsymbol{c}_i$ having the length of β, the spreading operations performed in the time domain will require β number of IFFT operations to transmit all the $n\times log_2(p)$ bits, where the spreading factor is β.

B. The Channel Model

We employ the following channel model to represent the multipath fading, and the channel impulse response is expressed as

$$h(t)=\sum_{l=1}^{L_p}\sum_{q=1}^{\beta}\alpha_{l,\lceil\frac{qT_o}{T_h}\rceil}\delta(t-\tau_{l,\lceil\frac{qT_o}{T_h}\rceil}) \tag{6}$$

where L_p is the total number of fading channel paths, l is the channel path index, $\tau_{l,\lceil\frac{qT_o}{T_h}\rceil}$ is the channel delay time, T_O is the OFDM symbol duration time and $T_h=\theta T_o$ is the time duration when the channel coefficient α_l maintains constant during the transmission of θ OFDM symbols and $\lceil\boldsymbol{.}\rceil$ is the ceiling operator.

When the statistics characteristics of the fading channel follows the Rayleigh distribution, the probability density function (PDF) of α_l is

$$f_{\mathrm{Rayleigh}}(\alpha|\sigma)=\left(\frac{\alpha}{\sigma^2}\right)\exp\left(-\frac{\alpha^2}{2\sigma^2}\right),\quad \alpha>0 \tag{7}$$

where σ is the scale parameter of the distribution representing the root-mean-square value of the received voltage signal.

C. Demodulation

At the receiver, the received OCCPSK signal over the multipath fading channel is given by

$$r(t)=h(t)\bigotimes s(t)+\xi(t) \tag{8}$$

where $\bigotimes$ is the convolution operator and $\xi(t)$ is a circularly symmetric Gaussian noise with zero mean and power spectral density of $N_0/2$.

Fig. 3 illustrates the information recovery procedure of the OCCPSK receiver. After the removal of the CP, FFT operations are performed on the received data. Then we derive the positions used for the chaotic chip position keying by maximizing the Euclidean norm of the symbols for estimations of the transmitted data. For the proposed OCCPSK legitimate receiver, with the known shuffling algorithm, the known key parameters and the same iteration number as that used at the transmitter, the iterative multiple chaotical shift aided re-shuffling and overlapping operations are carried out to recover the user data. More details are provided as below.

1) FFT Operation: For each received symbol stored in a shared buffer, which contain n samples, we perform β successive FFT operations, then we can obtain n symbols with the length of β. For the i_{th} symbol corresponding to the transmitted vector $\boldsymbol{c}_i$ over the ith subcarrier, the samples in this symbol denoted by $\boldsymbol{r}_i$ are given by

$$r_{i,q} = H_{i,q} c_{i,q} + \xi_{i,q} \tag{9}$$

where $\xi_{i,q}$ is the AWGN with zero mean and variance of $N_0/2$, and $H_{i,q}$ is the frequency channel response for the i_{th} subcarrier obtained from by the q_{th} FFT operation based on Eq.(6), namely we have

$$H_{i,q} = \sum_{l=1}^{L_p} \alpha_{l,\lceil \frac{qT_o}{T_h} \rceil} e^{-2\pi j f_i \tau_{l,\lceil \frac{qT_o}{T_h} \rceil}} \tag{10}$$

Since CP has been added at the transmitter, in the case that the maximum channel delay time is much lower than the OFDM symbol intervals, namely $\tau_{l,\lceil \frac{qT_o}{T_h} \rceil} << T_o$, the multipath interferences at the receiver become negligible, then we have $e^{-2\pi j f_i \tau_{l,\lceil \frac{qT_o}{T_h} \rceil}} = e^{-2\pi j i \tau_{l,\lceil \frac{qT_o}{T_h} \rceil}/T_o} \approx 1$. Accordingly, Eq. (10) can be simplified as

$$H_{i,q} = \sum_{l=1}^{L_p} \alpha_{l,\lceil \frac{qT_o}{T_h} \rceil} \tag{11}$$

which is uncorrelated to the subcarrier index i. For the sake of expressing brevity, in the following sections, the channel response is represented by H_q. Considering that the paired overlapped symbols are correlated to each other, and can be transmitted over two neighboring subcarriers, which means that the condition that $\tau_{l,\lceil \frac{qT_o}{T_h} \rceil} << T_o$ can be satisfied, the overlapped two symbols will undergo similar channel conditions within the coherence bandwidth.

Accordingly, over the two subchannels with the channel response of H_q, by substituting Eq. (3) into Eq. (9), the received symbol $r_{i,q}$ will be reexpressed as

$$\begin{aligned} r_{i,q} &= H_q c_{i,q} + \xi_{i,q} \\ &= \begin{cases} H_q(x'_{i,q} + x'_{i+1,q}) + \xi_{i,q}, & if\ i\%2 = 1 \\ H_q(x'_{i,q} - x'_{i-1,q}) + \xi_{i,q}, & if\ i\%2 = 0 \end{cases} \end{aligned} \tag{12}$$

2) Separation of Overlapped Symbols: Subsequently, as indicated by Fig.3, every two paired neighboring vectors $\boldsymbol{r}_i (i = 1, 2, \ldots n)$ are firstly separated to recover the i_{th} position-modulated vector $\boldsymbol{y}'_i (i = 1, 2, \ldots n)$, which is an inverse process of the overlapping at the transmitter represented by Eq. (3). After the symbol separation, we obtain

$$\boldsymbol{y}'_i = \begin{cases} \boldsymbol{r}_i - \boldsymbol{r}_{i+1}, & if\ i\%2 = 1 \\ \boldsymbol{r}_i + \boldsymbol{r}_{i-1}, & if\ i\%2 = 0 \end{cases} \tag{13}$$

Then we substitute Eq. (12) into Eq. (13), the q_{th} element in the position-modulated vector $\boldsymbol{y}'_i$ can be unfolded as

$$\begin{aligned} y'_{i,q} &= \begin{cases} r_{i,q} - r_{i+1,q}, & if\ i\%2 = 1 \\ r_{i,q} + r_{i-1,q}, & if\ i\%2 = 0 \end{cases} \\ &= \begin{cases} 2H_q x'_{i,q} + \zeta_{i,q}, & if\ i\%2 = 1 \\ 2H_q x'_{i,q} + \zeta_{i,q}, & if\ i\%2 = 0 \end{cases} \end{aligned} \tag{14}$$

where $\zeta_{i,q} = \xi_{i,q} - \xi_{i+1,q}$ when $i\%2 = 1$, and $\zeta_{i,q} = \xi_{i,q} + \xi_{i-1,q}$ when $i\%2 = 0$, which are Gaussian noises with zero mean and variance of N_0.

It can be seen from Eq. (14) that the decision symbol $y'_{i,q}$ is composed of two terms. For the position demodulation, the first term $2H_q x'_{i,q}$ is the desirable information-bearing part, while the second term $\zeta_{i,q}$ is AWGN.

As an example, given $n = 4$, we have

$$\begin{aligned} r_{1,q} &= H_q c_{1,q} + \xi_{1,q} = H_q(x'_{1,q} + x'_{2,q}) + \xi_{1,q} \\ r_{2,q} &= H_q c_{2,q} + \xi_{2,q} = H_q(x'_{2,q} - x'_{1,q}) + \xi_{2,q} \\ r_{3,q} &= H_q c_{3,q} + \xi_{3,q} = H_q(x'_{3,q} + x'_{4,q}) + \xi_{3,q} \\ r_{4,q} &= H_q c_{4,q} + \xi_{4,q} = H_q(x'_{4,q} - x'_{3,q}) + \xi_{4,q} \end{aligned} \tag{15}$$

Then based on Eq. (13) and Eq. (15), we retrieve the four position modulated symbols as $\boldsymbol{y}_i (i = 1, \ldots, 4)$ as

$$\begin{aligned} y'_{1,q} &= r_{1,q} - r_{2,q} = 2H_q x'_{1,q} + \zeta_{1,q} \\ y'_{2,q} &= r_{2,q} + r_{1,q} = 2H_q x'_{2,q} + \zeta_{2,q} \\ y'_{3,q} &= r_{3,q} - r_{4,q} = 2H_q x'_{3,q} + \zeta_{3,q} \\ y'_{4,q} &= r_{4,q} + r_{3,q} = 2H_q x'_{4,q} + \zeta_{4,q} \end{aligned} \tag{16}$$

From Eq.(16), we can see that the information-bearing part of each $\boldsymbol{y}'_i$ has the performance gain of 2. Thus although the overlapping operations consume more energy at the transmitter, the effective energy of information-bearing symbols correspondingly increases at the receiver. Hence, the presented design would enhance the system security without lowering the energy efficiency and the spectrum efficiency.

3) Symbol Re-Shuffle: As mentioned above, at the stage of the re-shuffling, the separate symbols $\boldsymbol{y}'_i (i = 1, 2, \ldots n)$ are descrambled chaotically with the known initial value and known chaotic sequence generation mapping method. The resultant recovered symbols are represented as $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \ldots, \boldsymbol{y}_n\}$, whose elements are expressed based on Eq. (14) as

$$y_{i,q} = \begin{cases} 2H_q x_{i,q} + \zeta_{i,q}, & if\ i\%2 = 1 \\ 2H_q x_{i,q} + \zeta_{i,q}, & if\ i\%2 = 0 \end{cases} \tag{17}$$

4) Decisions: Subsequently, the re-shuffled position-bearing signal $\boldsymbol{y}_i$ is fed into the position demodulator for the retrieval of the p-ary number $\widetilde{d}_i$, which is represented as

$$\widetilde{d}_i = \arg\max_{w} || \frac{y_{i,w\times M+1:(w+1)\times M}}{2} || \tag{18}$$

where $w = 0, 1, 2, \ldots, p-1$ denotes the chip number, and $y_{i,w\times M+1:(w+1)\times M}$ denotes the w_{th} chip of $\boldsymbol{y}_i$, which consists of the $(w \times M + 1)_{th}$ element to the $((w+1) \times M)_{th}$ element in $\boldsymbol{y}_i$, the denominator 2 is used to normalize the desirable part $2H_q x'_{i,q}$ as given by Eq. (14), and $||\frac{y_{i,w\times M+1:(w+1)\times M}}{2}||$ denotes the Euclidean norm of $y_{i,w\times M+1:(w+1)\times M}/2$.

Finally the decisions $\widetilde{d}_i$ are passed to a number-to-bit converter to retrieve the estimated binary data.

III. Theoretical Analysis

In this section, we analyze the error probability of the OCCPSK scheme with one shuffling and overlapping operation over the multipath Rayleigh flat fading channel, then the spectrum efficiency and the energy efficiency of the proposed scheme is evaluated and compared with its counterparts, finally the physical layer security is studied in terms of the wavelet transform.

A. Error Probability Analysis

1) SER Derivation: According to the decision making expressed by Eq. (18), the symbol error occurs when the Euclidean norm of the $(d_i+1)_{th}$ chip of $\boldsymbol{y}_i$ is less than the Euclidean norm of any one of the other chips of $\boldsymbol{y}_i$. Then we derive the SER as follows.

Considering that the position demodulation requires the computation of the Euclidean norm of the chips, we decompose the decision vectors $\boldsymbol{y}_i/2$ into multiple sub-variables which are the Euclidean norm of the inner chips of $\boldsymbol{y}_i/2$, namely $||\frac{y_{i,w\times M+1:(w+1)\times M}}{2}||$ $(w=0,1,2,\ldots p-1)$.

According to Eq. (17), the re-shuffled $\boldsymbol{y}_i$ is a linear combination of $\boldsymbol{x}_i$ and $\boldsymbol{\zeta}_i$. In addition, as mentioned above, for the ith $log_2(p)$-ary number d_i which has the possible value of $0,1,2,\ldots,p-1$, the $(d_i+1)_{th}$ chip of $\boldsymbol{x}_i$ is modulated by $\boldsymbol{u}_i$ and other $(p-1)$ chips are occupied by zeros.

Therefore, the p sub-variables $||\frac{y_{i,w\times M+1:(w+1)\times M}}{2}||$ $(w=0,1,2,\ldots p-1)$ are further decomposed into two parts. One part corresponds to the Euclidean norm of the element-wise linear combination of $\boldsymbol{u}_i$ and one chip of $\boldsymbol{\zeta}_i$, which is denoted as ϕ, namely

$$\begin{aligned}\phi &= ||\frac{y_{i,d_i\times M+1:(d_i+1)\times M}}{2}|| \\ &= ||H_{d_i\times M+1:(d_i+1)\times M}\circ \boldsymbol{u}_i + \frac{\zeta_{i,d_i\times M+1:(d_i+1)\times M}}{2}|| \end{aligned} \tag{19}$$

where $H_{d_i\times M+1:(d_i+1)\times M}$ denotes the vector composed of the elements from $H_{d_i\times M+1}$ to $H_{(d_i+1)\times M}$, and $\circ$ is the Hadamard product operator which denotes the element-wise product of two vectors.

Another part of the $(p-1)$ sub-variables are the Euclidean norms of the remaining chips of $\boldsymbol{\zeta}_i$, which is denoted as ϵ and given by

$$\begin{aligned}\epsilon &= ||\frac{y_{i,w\times M+1:(w+1)\times M}}{2}|| \quad (w\neq d_i) \\ &= ||\frac{\zeta_{i,w\times M+1:(w+1)\times M}}{2}|| \quad (w\neq d_i) \end{aligned} \tag{20}$$

where the $(p-1)$ remaining sub-variables are denoted as $\epsilon_1,\epsilon_2,\ldots,\epsilon_{p-1}$, and the maximum value is denoted as ϵ_{max}, namely $\epsilon_{max}=max\{\epsilon_1,\epsilon_2,\ldots,\epsilon_{p-1}\}$.

Next, we derive the statistical characteristics for the decision variables ϕ and ϵ.

For the first part, with the aid of the channel response expression, ϕ can be further unfolded as

$$\phi=\sum_{q=1}^{M}\left[\sum_{l=1}^{L}\alpha_{l,\lceil\frac{(q+d_i\times M)T_o}{T_h}\rceil}u_{i,q}+\frac{\zeta_{i,(q+d_i\times M)}}{2}\right]^2 \tag{21}$$

As mentioned in Section II-C, over slow and flat fading channels, the channel coefficient stays constant during $\theta=T_h/T_o$ OFDM symbols, hence $\alpha_{l,\lceil\frac{(q+d_i\times M)T_o}{T_h}\rceil}(1\leq q\leq M)$ is uncorrelated to the index i when $M<<\theta$. In this case, Eq. (21) can be further expressed as

$$\phi=\sum_{q=1}^{M}\left[\sum_{l=1}^{L}\alpha_l u_{i,q}+\frac{\zeta_{i,(q+d_i\times M)}}{2}\right]^2 \tag{22}$$

It can be seen that ϕ is the square accumulation of the sum of Gauss variables and chaotic samples. Note that the Gauss variable $\frac{\zeta_{i,(q+w\times M)}}{2}$ has zero mean and variance of $N_0/4$, hence by normalizing the variance of the Gauss variable in ϕ, the normalized variable $\phi_{norm}=\frac{\phi}{N_0/4}$ is distributed according to the non-central chi-squared distribution with its possibility density function (PDF) given by

$$f_{\phi_{norm}}(x)=\frac{1}{2}e^{-(x+\lambda)/2}\left(\frac{x}{\lambda}\right)^{M/4-1/2}I_{M/2-1}\left(\sqrt{\lambda x}\right) \tag{23}$$

where $I_{\upsilon}(x)=(x/2)^{\upsilon}\sum\limits_{j=0}^{\infty}\frac{(x^2/4)^j}{j!\Gamma(\upsilon+j+1)}$, and $\lambda=\frac{4\left(\sum\limits_{l=1}^{L}\alpha_l\right)^2\sum\limits_{q=1}^{M}u_{i,q}^2}{N_0}$.

For another part represented by ϵ, we have

$$\epsilon=\sum_{q=1}^{M}\left[\frac{\zeta_{i,(q+w\times M)}}{2}\right]^2 \tag{24}$$

We can see that ϵ is the sum of squares of Gauss variables. Similarly, by normalizing the variance of the Gauss variable in ϵ, the normalized variable $\epsilon_{norm}=\frac{\epsilon}{N_0/4}$ is distributed according to the chi-squared distribution with its cumulative distribution function (CDF) given by

$$F_{\epsilon_{norm}}(x)=\frac{\gamma(M/2,x/2)}{\Gamma(M/2)} \tag{25}$$

where $\Gamma(z)=\int_0^{\infty}x^{z-1}e^{-x}dx$, $\gamma(s,x)=\int_0^{x}t^{s-1}e^{-t}dt$. For the maximum ϵ_{max}, since $\epsilon_1,\epsilon_2,\ldots,\epsilon_{p-1}$ are independent distributed random variables, the CDF of $\frac{\epsilon_{max}}{N_0/4}$ can be given in a form of successive multiplication of $F_{\epsilon_{norm}}(x)$ with $(p-1)$ times, namely $F_{max(\epsilon)}(x)=F_{\epsilon_{norm}}(x)^{p-1}$.

Subsequently, with the aid of the derived PDF of ϕ expressed by Eq. (23) and the CDF of ϵ given by Eq. (25), we derive the SER as follows.

Without loss of generality, the symbol energy E_s can be computed as

$$\begin{aligned}E_s &= \sum_{q=1}^{\beta}c_{i,q}^2 \\ &= \begin{cases}\sum\limits_{q=1}^{\beta}x_{i,q}^{\prime 2}+\sum\limits_{q=1}^{\beta}x_{i+1,q}^{\prime 2}+\sum\limits_{q=1}^{\beta}2x_{i,q}^{\prime}x_{i+1,q}^{\prime}, & if\ i\%2=1 \\ \sum\limits_{q=1}^{\beta}x_{i,q}^{\prime 2}+\sum\limits_{q=1}^{\beta}x_{i-1,q}^{\prime 2}-\sum\limits_{q=1}^{\beta}2x_{i,q}^{\prime}x_{i-1,q}^{\prime}, & if\ i\%2=0\end{cases}\end{aligned} \tag{26}$$

Due to the low cross-correlation value of chaotic sequences, for large β and M, the terms $\sum\limits_{q=1}^{\beta}2x_{i,q}^{\prime}x_{i+1,q}^{\prime}$ and

$\sum_{q=1}^{\beta} 2x'_{i,q}x'_{i-1,q}$ are small valued compared with other terms in Eq. (26) and can be approximated as 0, thus E_s can be approximated as

$$E_s \approx \begin{cases} \sum_{q=1}^{M} u'^2_{i,q} + \sum_{q=1}^{M} u'^2_{i+1,q}, & if\ i\%2 = 1 \\ \sum_{q=1}^{M} u'^2_{i,q} + \sum_{q=1}^{M} u'^2_{i-1,q}, & if\ i\%2 = 0 \end{cases} = 2\sum_{q=1}^{M} u^2_{i,q} \tag{27}$$

Based on the above equation, λ in Eq. (23) can be reexpressed as $\lambda = \frac{2\left(\sum_{l=1}^{L}\alpha_l\right)^2 E_s}{N_0} = \frac{2k\left(\sum_{l=1}^{L}\alpha_l\right)^2 E_b}{N_0}$, where E_b is the energy for transmitting per information bit and $k = log_2(p)$ denotes the number of bits modulated in each subcarrier symbol.

Finally, the error probability of $\widetilde{d_i}$, namely the SER, can be derived as follows

$$\begin{aligned} SER(d_i) &= 1 - P(\widetilde{d_i} = d_i) \\ &= 1 - P\big(\phi > \epsilon_{max}\big) \\ &= 1 - P\big(\frac{\phi}{N_0/4} > \frac{\epsilon_{max}}{N_0/4}\big) \\ &= \int_{-\infty}^{+\infty} \big(1 - \big(F_{max(\epsilon)}(x)\big)\big) \times f_{\phi_{norm}}(x)\,dx \\ &= \int_{-\infty}^{+\infty} \Big(1 - \big(F_{\epsilon_{norm}}(x)\big)^{p-1}\Big) \times f_{\phi_{norm}}(x)\,dx \end{aligned} \tag{28}$$

2) BER Derivation: With considerations that $\epsilon_1, \epsilon_2, \ldots, \epsilon_{p-1}$ are independent distributed variables, and that the probability of misjudging d_i would be the same, which is equal to $\frac{1}{p-1}$, the BER of the proposed scheme can be derived directly from the SER as

$$BER = SER(d_i) \times \frac{\sum_{j=0}^{(log_2 p-1)} (log_2 p - j)\mathrm{C}^j_{log_2 p}}{(p-1)log_2 p} \tag{29}$$

where $\mathrm{C}^j_{log_2 p}$ represents the number of possibilities of selecting j elements from $log_2 p$ elements.

B. Spectrum Efficiency Analysis

According to the definition of spectrum efficiency given in [26], which is the ratio of the bit rate to the total bandwidth, the spectrum efficiency of the OCCPSK scheme is derived as below

$$\eta_{\mathrm{OCCPSK}} = \frac{\frac{log_2(p)\times n}{pMT_s}}{B_c \times (1+n)} = \frac{nlog_2(p)}{(1+n)pM} \tag{30}$$

where p is the number of chips and $log_2(p)$ is the number of modulated bits transmitted over each subcarrier, M is the chip size, T_s denotes the duration of each chaotic sample (which is equal to the OFDM symbol duration T_o in this paper), thus pMT_s represents the sequence duration. In addition, $B_c = \frac{1}{T_s}$ represents half of the bandwidth occupied by each subcarrier under the assumption of ideal filtering.

TABLE I

SPECTRUM EFFICIENCY COMPARISON

Scheme	OCCPSK	CCI-DCSK [14]	PPM-DCSK [17]	DIM-DCSK-I [18]
η	$\frac{nlog_2(p)}{(1+n)pM}$	$\frac{n(log_2(p)+1)}{(1+n)pM}$	$\frac{n(log_2(p)+1)}{(1+n)(p+1)M}$	$\frac{n(2log_2(p)+2)}{(1+n)(p+1)M}$

TABLE II

ENERGY EFFICIENCY COMPARISON

Scheme	OCCPSK	DCSK [11]	CCI-DCSK [14]
Ψ	$log_2(p)$	$\frac{1}{2}$	$log_2(p)+1$
Scheme	PPM-DCSK [17]	DIM-DCSK-I [18]	
Ψ	$(log_2(p-1)+1)$	$(2log_2(p-1)+2)$	

For the OCCPSK scheme, which operates over multiple subcarriers, let n represent the total number of subcarriers, then the total number of modulated bits is $log_2(p) \times n$ and the total bandwidth of the OCCPSK symbol is $(n+1)B_c$ instead of 2 nB_c because OFDM allows the spectrum aliasing.

Next, we compare the spectrum efficiency of the OCCPSK scheme with the counterpart position-related chaos-modulated schemes, including commutation code index DCSK (CCI-DCSK) [14], pulse position modulation DCSK (PPM-DCSK) [17] and dual-index modulation DCSK I (DIM-DCSK-I) [18]. For the comparison fairness, we assume that PPM-DCSK and DIM-DCSK-I modulation schemes are combined with multi-carrier OFDM transmissions.

As shown in Table I, wherein η represents the spectrum efficiency, we can observe that the presented OCCPSK scheme achieves the similar spectrum efficiency to that of PPM-DCSK aided OFDM systems, which is slightly lower than that of the CCI-DCSK and DIM-DCSK-I scheme.

C. Energy Efficiency Analysis

According to the definition of the energy efficiency given as below [20]

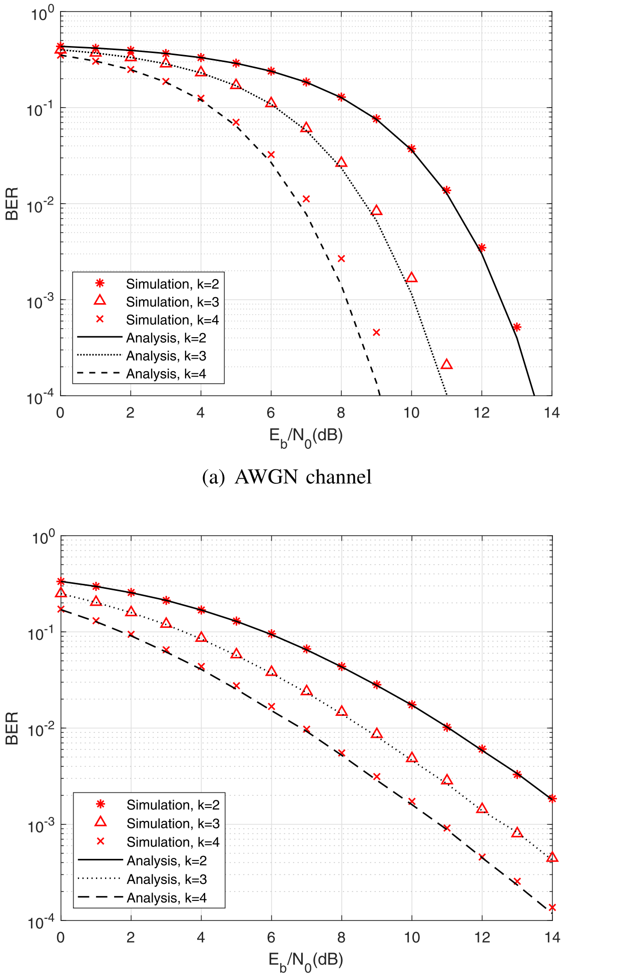
$$\Psi = \frac{E_{data}}{E_b} \tag{31}$$

where E_{data} is the energy of data and E_b represents the transmitted energy for each bit. Note that no reference signal is transmitted, thus E_{data} is equal to the symbol energy E_s given by Eq. (26). Since the symbol has p positions for modulation. $k = log_2(p)$ bits of information are modulated, hence $E_b = E_s/log_2(p)$. Therefore, for the presented OCCPSK system, the energy efficiency is $\Psi = E_{data}/E_b = log_2(p)$.

Then we compare the energy efficiency in Table II. It can be seen that compared with the conventional DCSK systems with the Ψ of 1/2, the energy efficiency of the proposed OCCPSK system is satisfactory and is close to that of PPM-DCSK [17], which is determined by p, although slightly lower than the energy efficiency of CCI-DCSK [14] and DIM-DCSK-I [18].

D. Physical Layer Security Evaluation

Moreover, we use the wavelet transform to quantitatively analyze the characteristics of the OCCPSK modulated signals in the time-frequency domain.



(a) AWGN channel

(b) Three-path flat fading channel with equal average power gain $E(\alpha_l^2) = 1/3$

Fig. 4. Comparisons of the simulated and analytical BER of OCCPSK with $\beta = 256$ over AWGN channel and flat multipath Rayleigh fading channel with different k.

Using the definition of the wavelet transform given as below [27]

$$WT_x^{\psi}(\sigma, \upsilon) = \frac{1}{\sqrt{|\upsilon|}} \int x(t)\psi^*(\frac{t-\sigma}{\upsilon})dt \qquad (32)$$

where $\psi(t)$ is the transforming window function, σ is related to the location of the window which corresponds to time information in the transform domain, and υ is the scale parameter which is defined as the reciprocal of the frequency. The results of the wavelet transform of the proposed OCCPSK modulated signals will be provided in Section IV.

IV. Numerical Results

In this section, numerical results are given to evaluate the performances of the proposed OCCPSK scheme which uses 4 subcarriers, i.e., $n = 4$.

A. BER Performances

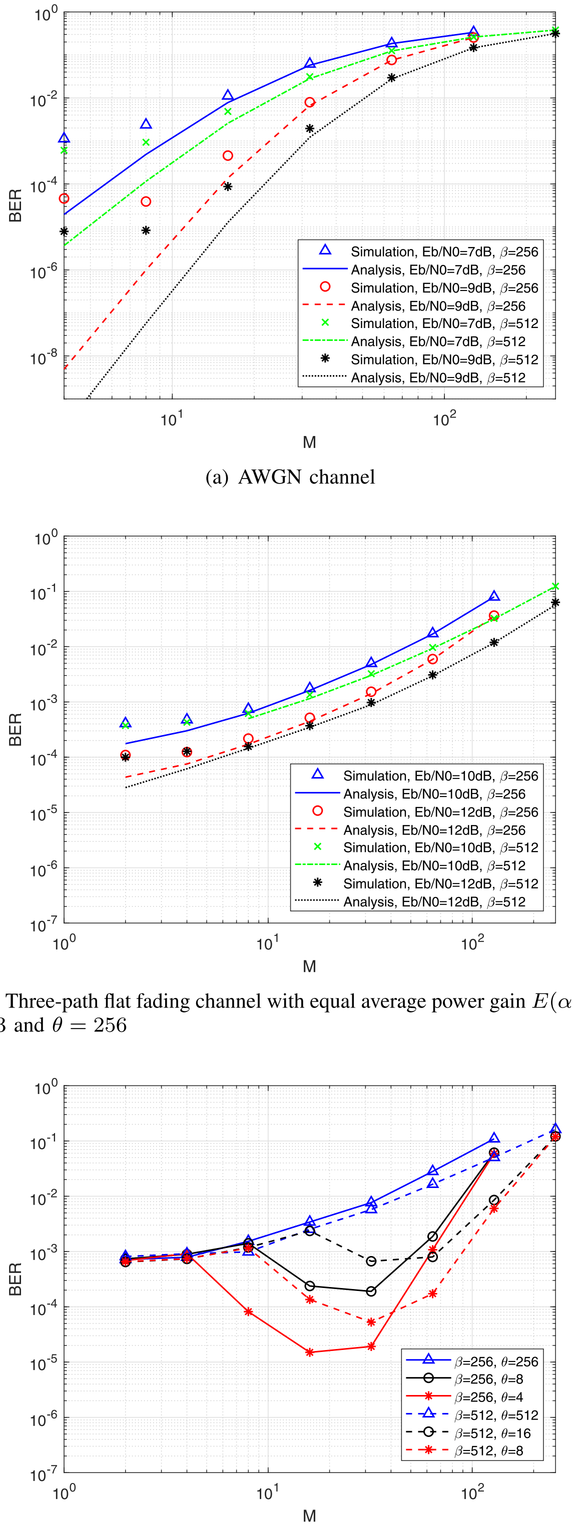
Fig. 4(a) and Fig. 4(b) respectively compare the simulated BER of OCCPSK with the analytical BER given by Eq. (29) over the AWGN channel and the flat multipath Rayleigh fading channel when the number of modulated bits carried in one symbol over each subcarrier, which is represented by $k = log_2(p)$, is different. It can be seen that the analytical results match the simulations, and the differences become smaller when k decreases. The reason is that for bigger k, the chip size $M = \frac{\beta}{2^k}$ becomes smaller, thus the approximation error of $\sum_{q=1}^{\beta} 2x'_{i,q}x'_{i+1,q}/E_s \approx 0$ or $\sum_{q=1}^{\beta} 2x'_{i,q}x'_{i-1,q}/E_s \approx 0$ in Eq. (26) increases, leading to larger variance of E_s, thereby bringing less accurate analytical BER. Moreover, we can observe that no matter what channel condition is, the BER performances are improved when k increases thanks to the equivalently suppressed noises as indicated in Eq. (29).

In the following Fig. 5, the influences of the chip size M on the performances of the proposed scheme over the AWGN channel and the flat multipath Rayleigh fading channel are further evaluated. Similar to the observations drawn from Fig. 4, for smaller M, the differences between the analytical BER and the simulated BER are larger. In addition, it is noticeable that with smaller M, the presented OCCPSK systems achieve better BER performances thanks to larger value of $\frac{E_s}{N_0}$ over AWGN channel and Rayleigh channel with the invariant $\theta = 256$, as respectively shown in 5(a) and Fig. 5(b).

From Fig. 5(c), we can observe that when the parameter θ corresponding to different channel conditions of Rayleigh fading is as small as $\theta = 4$ and $\theta = 8$, the BER performances would not always become worse when M increases. Further, we can see from Fig. 5(c) that M should be larger than θ, thus the time diversity of the fading channel can be utilized to improve BER performances. Hence for transmissions over flat multipath fading channels, there should be a trade-off between the energy intensity and the channel time diversity when selecting the chip size M. Additionally, when θ is 4 and 8, we can see that with the best selected M, the presented OCCPSK system can achieve better performances because more channel variations among different time slots are embedded into the symbols and more time diversity gain could be exploited. Moreover, in another case that $\theta = \beta = 256$, since the transmitted data could not experience different channel fading in different time slots, thus no time diversity gain is available and we can observe that the OCCPSK have the worst BER performance in this scenario.

B. BER Comparisons With Counterpart Schemes

Then we compare the BER performances of OCCPSK with three counterpart position-related chaos-modulated schemes including the CCI-DCSK [14], the PPM-DCSK [17], the DIM-DCSK-I [18] over the AWGN channel and the flat multipath Rayleigh fading channel. Note that the proposed OCCPSK scheme transmits the information via multiple subcarriers, while the other three counterpart systems are single carrier transmission systems. Let k denote the number of bits in one symbol period transmitted over each carrier, and k_{total} denote the total number of bits transmitted in one symbol period. Accordingly, for three counterpart single carrier systems, we have $k_{total} = k$, while for the proposed multicarrier



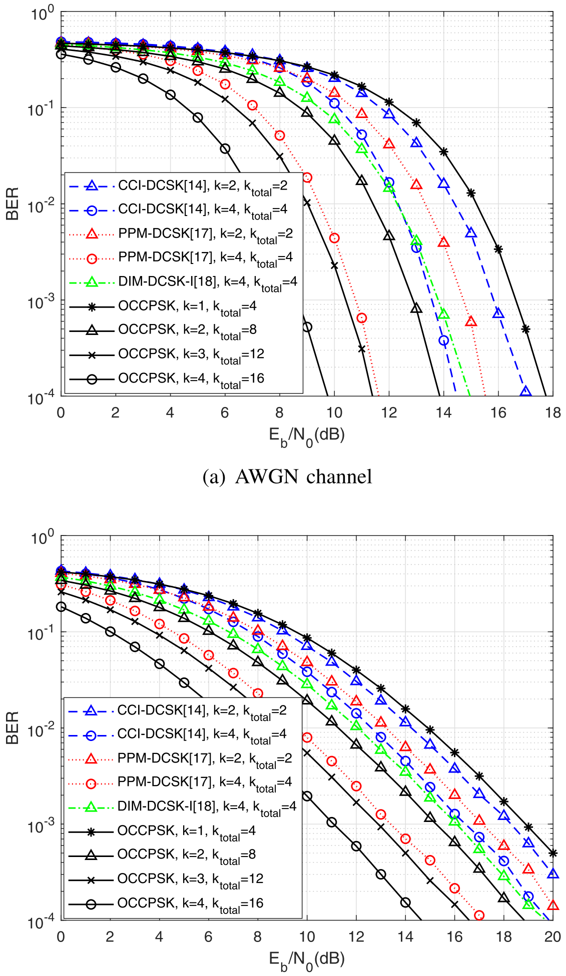
(a) AWGN channel

(b) Three-path flat fading channel with equal average power gain $E(\alpha_l^2) = 1/3$ and $\theta = 256$

(c) Three-path flat fading channel with equal average power gain $E(\alpha_l^2) = 1/3$ and different θ

Fig. 5. BER performances of the OCCPSK system in terms of M.

OCCPSK system, $k_{total} = n \times k$. It could be observed from Fig. 6 that the BER performances of the proposed OCCPSK system and the counterpart systems become better when k increases.



(a) AWGN channel

(b) Three-path flat fading channel with equal average power gain $E(\alpha_l^2) = 1/3$

Fig. 6. BER comparisons of the CCI-DCSK [14], PPM-DCSK [17], DIM-DCSK-I [18] and the OCCPSK systems with $\beta = 288$, $k = 1, 2, 3, 4$ and $k_{total} = 2, 4, 8, 12$.

Moreover, in Fig. 6, we compare the BER performances not only for the same number of bits per carrier but also for the same number of bits per symbol. For fairness of comparisons, we have chosen $\beta = 288$ in Fig. 6 to ensure the same spreading factor is applied on different schemes, while their chip size M may be different. According to Table I, since the spreading factor for CCI-DCSK, PPM-DCSK, DIM-DCSK-I and the proposed OCCPSK schemes are $2^k M$, $(2^{k-1}+1)M$, $(2^{(k-2)/2}+1)M$, $2^k M$, respectively, thus we could derive the common value of k for these schemes, which is $k = 4$. In addition, we also consider the cases that $k = 1, 2, 3$ in Fig. 6(a) and Fig. 6(b).

To be more explicit, when $k = 4$, i.e., all the systems have the same number of bits per carrier, we could observe from Fig. 6(a) and Fig. 6(b) that the proposed OCCPSK design achieves better BER performances than the benchmark schemes over the AWGN channel and the flat multipath fading channel with the same k.

On the other hand, when $k_{total} = 4$, i.e., all the considered systems have the same number of bits per symbol. In this case, for the proposed multicarrier OCCPSK system with

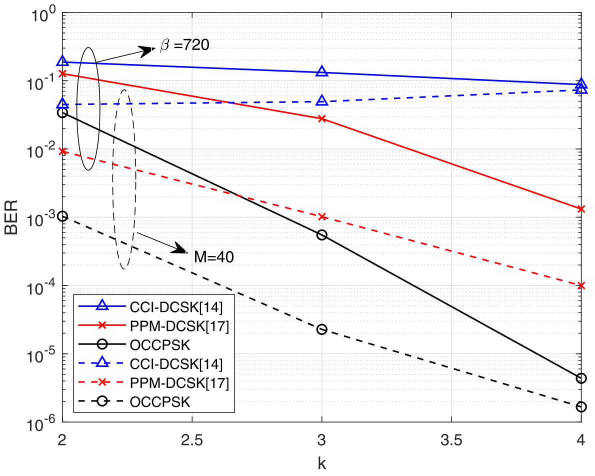


Fig. 7. BER comparisons of the CCI-DCSK [14], PPM-DCSK [17] and the OCCPSK systems in terms of different k over AWGN channel with $E_b/N_0 = 12dB$, $M = 40$ and $\beta = 720$.

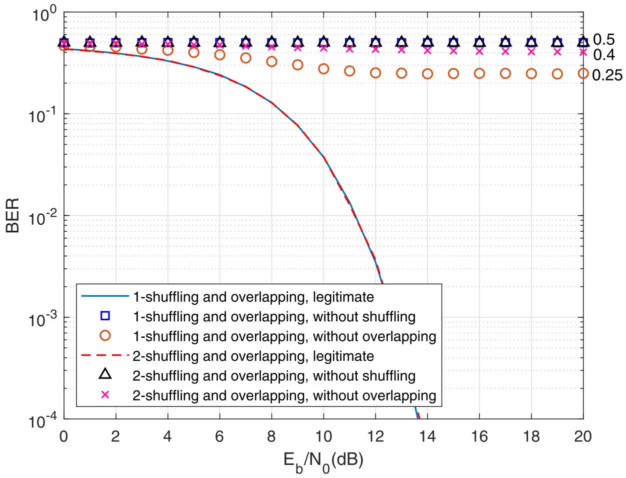


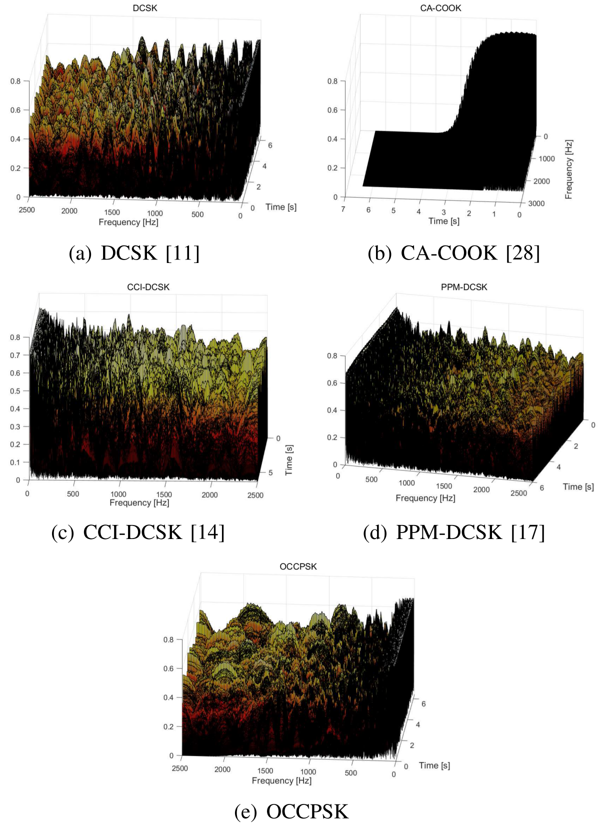
Fig. 8. BER comparisons of the eavesdropper and the legitimate receiver over the AWGN channel with $p = 4$ and $\beta = 256$.

4 subcarriers, only 1 bit is transmitted per carrier, i.e., $k = 1$. We can observe that the BER performances of the proposed OCCPSK system are worse than those of counterpart systems due to the decreased signal to noise ratio per carrier as indicated in Eq. (29) and observed from Fig. 4.

Furthermore, Fig. 7 demonstrates the BER performances of CCI-DCSK [14], PPM-DCSK [17], and the proposed OCCPSK scheme in terms of different k with the same spreading factor β or with the same chip size M. In this figure, we would not compare the performances with those of the DIM-DCSK-I scheme [18] since the number of bits modulated by the DIM-DCSK-I symbol is required to be a even number that is no less than 4. From Fig 7, we can observe that the OCCPSK scheme achieves better BER performances than those of the other two counterpart schemes with the same parameters, hence our scheme can provide more reliable transmissions than the counterpart schemes.

C. Security Performances

In Fig. 8, we investigate the BER performances for the eavesdroppers and the legitimate receivers. It can be seen that due to the high BER, the eavesdroppers can not retrieve the information without the knowledge of the overlapping pattern and the key parameters used in the chaotical shift-aided shuffling operations, while the legitimate receivers can recover the data reliably with the satisfactory BER. With the aid of the iterative shuffling and overlapping design, after one more overlapping, the BER of eavesdroppers increase from about 0.25 ($\approx 1/p$) to 0.4. Moreover, after the second shuffling, the BER approaches to 0.5, which means that it's impossible for the eavesdroppers to retrieve the transmitted data. Thus the system security can be greatly enhanced by using the iterative chaotical shift-aided shuffling and overlapping design.



(a) DCSK [11]

(b) CA-COOK [28]

(c) CCI-DCSK [14]

(d) PPM-DCSK [17]

(e) OCCPSK

Fig. 9. Wavelet transformation comparisons.

Moreover, we use the wavelet transform to investigate the physical features of signals, which determines the physical layer security performance [29]. The wavelet transform provides the time-frequency representation of signals with multiple resolutions [27]. For instance, it has been used in [30] to extract features for the physical layer signals.

Fig. 9 illustrates the signal time-frequency features of the OCCPSK system and counterpart systems with the sampling frequency $f_s = 5$kHz. As shown in Fig. 9(a) and Fig. 9(b), the DCSK and the CA-COOK modulated signals exhibit distinct patterns like the peaks along the frequency axis and the cliffs along the time axis. These patterns are not desirable in physical layers because it exposes the existence of the information and imperils the physical layer security.

By contrast, the wavelet transform of the CCI-DCSK, PPM-DCSK and the proposed OCCPSK modulated signal reveals nothing but direct current components. Meanwhile, even if the OCCPSK signal feature has been unfortunately identified, the OCCPSK modulated information is still hardly to be cracked through brute force algorithm if the shuffling and overlapping pattern is unknown. Therefore, the OCCPSK scheme can provide high security transmission scheme thanks to the smooth signal features as well as the large space of the chaotical shuffling and overlapping possibilities.

V. Conclusion

In this paper, we present a non-coherent OCCPSK scheme to transmit information with high efficiency and enhanced physical layer security. In our design, no reference chaotic signal are required to be transmitted. The information bits are modulated by the chip position of the chaotic signal, then each position-modulated sequence is shuffled and overlapped iteratively with the other specified sequences. Using this method, multiple bits can be carried using one chaotic sequence, thus high spectrum efficiency can be achieved. Moreover, thanks to the iterative chaotical shift-aided shuffling and overlapping operations, the information is hidden in the overlapped symbols, thus the security can also be improved. Furthermore, we derive the SER and the BER expression over the flat multipath Rayleigh fading channel. Simulations results verify the effectiveness of the theoretical analysis. Furthermore, the performance comparisons among the presented scheme and counterpart schemes over AWGN channel and flat multipath fading channels demonstrate that our presented OCCPSK scheme can achieve better BER than the counterpart systems while retaining high security performances. Hence, with the aid of the high order position modulation, the chaotical shift-aided shuffling and the overlapping, the requirement for the reference chaotic signals is removed and the users can be served with more efficient, reliable and secure performances.

Acknowledgements

The authors want to thank the editor and all the reviewers' for their precious time and helpful comments.

References

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

[2] S. Hayes, C. Grebogi, and E. Ott, "Communicating with chaos," *Phys. Rev. Lett.*, vol. 70, no. 20, p. 3031, 1993.

[3] G. Kaddoum and N. Tadayon, "Differential chaos shift keying: A robust modulation scheme for power-line communications," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 64, no. 1, pp. 31–35, Jan. 2017.

[4] 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.

[5] P. Chen, Y. Fang, G. Han, and G. Chen, "An efficient transmission scheme for DCSK cooperative communication over multipath fading channels," *IEEE Access*, vol. 4, pp. 6364–6373, 2016.

[6] G. Cai, Y. Fang, G. Han, J. Xu, and G. Chen, "Design and analysis of relay-selection strategies for two-way relay network-coded DCSK systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1258–1271, Feb. 2018.

[7] R. Rovatti and G. Mazzini, "Interference in DS-CDMA systems with exponentially vanishing autocorrelations: Chaos-based spreading is optimal," *Electron. Lett.*, vol. 34, no. 20, pp. 1911–1913, Oct. 1998.

[8] G. Mazzini, R. Rovatti, and G. Setti, "Interference minimisation by autocorrelation shaping in asynchronous DS-CDMA systems: Chaos-based spreading is nearly optimal," *Electron. Lett.*, vol. 35, no. 13, pp. 1054–1055, 1999.

[9] A. P. Kurian, S. Puthusserypady, and S. M. Htut, "Performance enhancement of DS/CDMA system using chaotic complex spreading sequence," *IEEE Trans. Wireless Commun.*, vol. 4, no. 3, pp. 984–989, May 2005.

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

[11] G. Kolumbán, B. Vizvári, W. Schwarz, and A. Abel, "Differential chaos shift keying: A robust coding for chaos communication," in *Proc. Int. Workshop Nonlinear Dyn. Electron. Syst.*, Seville, Spain, Jun. 1996, pp. 87–92.

[12] H. Yang and G.-P. Jiang, "High-efficiency differential-chaos-shift-keying scheme for chaos-based noncoherent communication," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 59, no. 5, pp. 312–316, May 2012.

[13] G. Cai, Y. Fang, G. Han, F. C. M. Lau, and L. Wang, "A square-constellation-based M-ary DCSK communication system," *IEEE Access*, vol. 4, pp. 6295–6303, 2016.

[14] M. Herceg, D. Vranješ, G. Kaddoum, and E. Soujeri, "Commutation code index DCSK modulation technique for high-data-rate communication systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 12, pp. 1954–1958, Dec. 2018.

[15] T. Huang, L. Wang, W. Xu, and G. Chen, "A multi-carrier M-ary differential chaos shift keying system with low PAPR," *IEEE Access*, vol. 5, pp. 18793–18803, 2017.

[16] W. Rao, L. Zhang, Z. Liu, and Z. Wu, "Efficient amplitude shift keying-aided orthogonal chaotic vector position shift keying scheme with QoS considerations," *IEEE Access*, vol. 5, pp. 14706–14715, 2017.

[17] M. Miao, L. Wang, M. Katz, and W. Xu, "Hybrid modulation scheme combining PPM with differential chaos shift keying modulation," *IEEE Wireless Commun. Lett.*, vol. 8, no. 2, pp. 340–343, Apr. 2019, doi: 10.1109/LWC.2018.2871137.

[18] X. Cai, W. Xu, L. Wang, and F. Xu, "Design and performance analysis of differential chaos shift keying system with dual-index modulation," *IEEE Access*, vol. 7, pp. 26867–26880, 2019.

[19] G. Kaddoum, F. 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.

[20] S. Li, Y. Zhao, and Z. Wu, "Design and analysis of an OFDM-based differential chaos shift keying communication system," *J. Commun.*, vol. 10, no. 3, pp. 199–205, 2015.

[21] H. Yang, W. K. S. Tang, G. Chen, and G.-P. Jiang, "Multi-carrier chaos shift keying: System design and performance analysis," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 64, no. 8, pp. 2182–2194, Aug. 2017.

[22] 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.

[23] G. Kaddoum, F. Gagnon, and F.-D. Richardson, "Design of a secure multi-carrier DCSK system," in *Proc. Int. Symp. Wireless Commun. Syst.*, Aug. 2012, pp. 964–968.

[24] 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. Technol.*, vol. 67, no. 4, pp. 2997–3011, Apr. 2018.

[25] 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)*, Jan. 2017, pp. 1073–1076.

[26] S. Benedetto and E. Biglieri, *Principles of Digital Transmission: With Wireless Applications*. Boston, MA, USA: Springer, 1999.

[27] R. Polikar, *The Wavelet Tutorial: Part III—Multiresolution Analysis and THG Continuous Wavelet Transform*. Accessed: Jan. 12, 2001. [Online]. Available: http://users.rowan.edu/polikar/WAVELETS/WTpart3.html

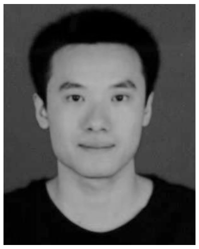
[28] A. Mesloub, A. Boukhelifa, O. Merad, S. Saddoudi, A. Younsi, and M. Djeddou, "Chip averaging chaotic ON–OFF keying: A new non-coherent modulation for ultra wide band direct chaotic communication," *IEEE Commun. Lett.*, vol. 21, no. 10, pp. 2166–2169, Oct. 2017.

[29] H. Li, "Physical-layer security enhancement in wireless communication systems," M.S. thesis, Dept. Elect. Comput. Eng., Univ. Western Ontario, London, U.K., 2013.

[30] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *J. Commun. Netw.*, vol. 11, no. 6, pp. 544–555, Dec. 2009.

Lin Zhang (M'16) received the B.S. and M.S. degrees from Shanghai University, in 1997 and 2000, and the Ph.D. degree from Sun Yat-sen University, in 2003, all in electrical engineering. She joined the Department of Electronic Engineering, Sun Yat-sen University, in 2003, where she has been 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. Her research has been supported by the National Natural Science Foundation of China, the Guangdong Provincial Key Laboratory of Information Security Technology, and the Science and Technology Program Project of Guangdong Province. Her current research interest includes signal processing and its applications to wireless communication systems.

Zuwei Chen received the B.S. degree from the School of Electronic Information Science and Technology, Sun Yat-sen University, Guangzhou, China, in 2019, where he is currently pursuing the master's degree with the School of Information and Communication Engineering. His research interest includes chaotic communication and its application to wireless communication systems.



Weiwei Rao received the B.S. and M.S. degrees from the School of Electronic Information Science and Technology, Sun Yat-sen University, Guangzhou, China, in 2016 and 2019, respectively. He is currently with Huawei Company, Shenzhen, China. His current research interest includes signal processing and its applications to wireless communication systems.

Zhiqiang Wu (M'02–SM'17) received the B.S. degree from the Beijing University of Posts and Telecommunications in 1993, the M.S. degree from Peking University in 1996, and the Ph.D. degree from Colorado State University in 2002, all in electrical engineering. He has also held visiting positions at Peking University, Harbin Engineering University, Guizhou Normal University, and Tibet University. He was an Assistant Professor with the Department of Electrical and computer Engineering, West Virginia University Institute of Technology, from 2003 to 2005. He joined 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 the NSF, the AFRL, the ONR, the AFOSR, and the OFRN.