An OFDM-Based Pre-Coded Chaos Shift Keying Transceiver for reliable V2V Transmission

Zuwei Chen, Lin Zhang, *Senior Member, IEEE*, Jian Zhang, *Member, IEEE*, Zhiqiang Wu, *Senior Member, IEEE*, and Danzeng Luobu

***Abstract*—In this correspondence, we propose a novel orthogonal frequency division multiplexing based pre-coded chaos shift keying (OFDM-PC-CSK) transceiver for reliable vehicle-to-vehicle (V2V) communications. In this design, different from traditional OFDM-aided differential chaos shift keying (OFDM-DCSK) systems, we remove the delivery of reference chaotic signals and utilize the diagonalization principle for information transmissions to achieve better reliability than the differential demodulation in OFDM-DCSK. At the transmitter, we construct the chaotic phase vector with chaotic sequences having different initial values, which are then combined with the discrete Fourier transform (DFT) matrix and a conjugate phase matrix of an eigenvalue matrix to compose a precoder. After precoding, the user data are modulated by the chaotic circulant matrix and transmitted over multiple subcarriers. At the receiver, reverse operations are conducted. Subsequently, we derive the theoretical bit error rate (BER) over V2V channels, the spectrum efficiency and the computational complexity. Simulation results validate the theoretical analysis, and demonstrate that the OFDM-PC-CSK system outperforms the counterpart schemes with better reliability and security performances over V2V channels.**

***Index Terms*—Circulant matrix, diagonalization, orthogonal frequency division multiplexing (OFDM), pre-coded chaos shift keying (PC-CSK), reliability performances.**

I. Introduction

In recent years, along with the growth of wireless technologies, intelligent transportation systems (ITSs) including Vehicular Ad Hoc Networks (VANETs) [1], vehicular cloud computing (VCC) [2], and Internet of vehicles (IoV) [3] becomes increasingly prosperous, which enable drivers to enjoy convenient and comprehensive services. However, ITSs suffer from potential reliable transmission issues due to the interferences induced by the high mobility of vehicles, and the security issues due to their inherent openness [1], [2].

Manuscript received July 1, 2021; revised October 28, 2021 and January 26, 2022; accepted March 6, 2022. Date of publication March 10, 2022; date of current version June 24, 2022. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB1802300, in part by National Science Foundation of China under grant U20A20162 and in part by Key Research and Development and Transformation Plan of Science and Technology Program for Tibet Autonomous Region under Grant XZ201901-GB-16. The review of this article was coordinated by Dr. Vuk Marojevic. *(Corresponding author: Lin Zhang.)*

Zuwei Chen is with the School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou, Guangdong Province 510006, China (e-mail: chenzw25@mail2.sysu.edu.cn).

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

Jian Zhang is with the Department of Traffic Engineering, Southeast University, Nanjing, Jiangsu 214135, China (e-mail: jianzhang@seu.edu.cn).

Zhiqiang Wu is with the Department of Electrical Engineering, Tibet University, Lhasa, Tibet 850000, China, and also with the Wright State University, Dayton, OH 45435 USA (e-mail: jianzhang@seu.edu.cn).

Danzeng Luobu is with the Department of Electrical and Electronic Engineering, University of Nottingham, Park NG72RD Nottingham, East Midlands, United Kingdom (e-mail: ezxd1@nottingham.ac.uk).

Digital Object Identifier 10.1109/TVT.2022.3158395

Chaos-based schemes [4], [5] have been applied in wireless systems thanks to the anti-interference capability and high security properties, including the ergodicity, the pseudo randomness and the high sensitivity to the initial values. Considering that the physical layer security [6], [7] can make vehicular network more secure against eavesdropping except for the authentication schemes [8], [9] and encryption schemes [10] in the media access control (MAC) layer, in this correspondence, we propose a novel chaotic modulation scheme to enhance the reliability of vehicle-to-vehicle (V2V) communications.

Although a lot of research works have been done on chaotic modulation methods, few research works have been on chaos-based transmission schemes over V2V channels. For example, the differential chaos shift keying (DCSK) scheme [11] has attracted more research interests due to the removal of complex chaotic synchronization circuits and the simplicity to be implemented. However, the noises contained in received reference chaotic signals undergoing imperfect transmissions lower the reliability performances. To enhance the performances, a noise reduction DCSK (NR-DCSK) method was proposed [12], which constructs a new reference signal by repeating the chaotic signals several times and the received signals are filtered to suppress the noises. In [13], repeated reference signals are spread by Walsh code and the receiver averages the noises of all reference signals for enhanced reliability performances. Moreover, in [14], [15], the researchers improved the receiver of the OFDM-DCSK schemes [16], which exploits the correlation between chaotic modulated signals to enhance reliability performances. Additionally, the protograph low-density parity-check (LDPC) code based scheme [17] was introduced, which applies error correction codes and in [18], the authors proposed a continuous-mobility DCSK (CM-DCSK) scheme with improved performances over fast fading channels.

In this correspondence, we propose a novel OFDM-based pre-coded chaos shift keying (OFDM-PC-CSK) transceiver with no need to deliver the reference chaotic signal or employ complex synchronization circuits. Different from traditional OFDM-DCSK schemes, the information transmissions based on the diagonalization of chaotic circulant matrix have no use for the noisy and interfered reference signals, which bring the improvement of reliability as well as the removal of reference signals avoids the exposure of signal characters and improves the security.

The novelty lies in that a diagnolization aided chaotic transceiver is proposed and the proposed chaos-based transceiver does not require to deliver the reference chaotic sequence. Thus both the reliability and security can be improved. In our design, at the transmitter, the chaotic sequences generated with the same of different initial values are cyclicly shifted to compose circulant matrices. Then we utilize the chaotic sequences with different initial values to construct chaotic phase vectors, which are combined with the discrete Fourier transform (DFT) matrix and a conjugate phase matrix of an eigenvalue matrix to constitute the precoder. The binary phase shift keying (BPSK) modulated symbols are precoded and modulated by circulant chaotic signals. Moreover, we prove that the chaotic circulant matrix can be diagonalized by the DFT matrix. Thus at the receiver, the received signals can be recovered and demodulated by Hermitian transposed DFT matrix with no need of the reference chaotic signals. Thanks to the diagonalization, the reliability performance can be enhanced. Meanwhile, since only the legitimate receiver with the known chaotic phase vectors can recover the data, the security performances can be improved.

Briefly, the main contributions include:

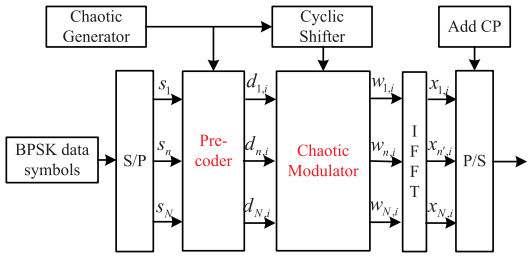

Fig. 1. The transmitter structure of OFDM-PC-CSK.

1) We propose a OFDM-PC-CSK transceiver to utilize the diagonalization of the circulant matrix to recover the user data, thus, the reliability performances are improved by the demodulation with no help of noisy reference signals in comparison to the differential demodulation.
2) We propose to construct the precoder with the chaotic phase vectors generated from chaotic sequences using different initial value for each subcarrier. Moreover, no reference chaotic signals are required. Hence the security performances are enhanced.
3) We derive the theoretical bit error rate (BER) expressions over V2V channels. Then, we analyze the spectrum efficiency and computational complexity.

II. OFDM-PC-CSK Transceiver

The OFDM-PC-CSK transceiver is presented as follows.

A. Transmitter

Fig. 1 illustrates the OFDM-PC-CSK transmitter. First, the information bits are modulated as BPSK symbols. Then after the serial to parallel (S/P) conversion, multiple BPSK symbol streams will be precoded, where the precoding matrix is constituted by combinations of the chaotic phase vector, the DFT matrix and the conjugate phase matrix of an eigenvalue matrix. Meanwhile, the chaotic generator outputs the chaotic sequences and then cyclic shifter produces chaotic circulant matrix. The chaotic circulant matrix is used to modulate the precoded information symbols. After inverse fast Fourier transform (IFFT), the resultant signal is transmitted over the wireless channel. More details are provided as below.

1) Chaotic Generator and Cyclic Shifter: In the chaotic generator, we use the improved logistic map to generate the chaotic sequence with different initial values for each subcarrier, which is represented by $c_{0,i+1}^{(n)} = 1 - 2(c_{0,i}^{(n)})^2$ [11], $i = 1, \ldots, \beta$ and $n = 1, \ldots, N$ where $c_{0,i}^{(n)}$ is the i_{th} chip over the n_{th} subcarrier and $c_{0,i}^{(n)} \in (-1, 0) \bigcup (0, 1)$. β denotes the length of the chaotic sequence and N denotes the number of the subcarriers. Then we have $\mathbf{c}_0^{(n)} = (c_{0,1}^{(n)}, \ldots, c_{0,\beta}^{(n)})^T$ where $(\cdot)^T$ is the transpose operator. Notably, without loss of generality, we assume that chaotic sequences are normalized such that their mean squared values are unity, i.e., $\mathrm{E}[(c_{0,i}^{(n)})^2] = \frac{1}{\beta}$.

Then the cyclic shifter performs the cyclic shifting operation on the reference chaotic vector $\mathbf{c}_0^{(n)}$ to generate the chaotic circulant matrix, which is expressed as

$$\mathbf{C}_n = \left[\mathbf{\Phi}_1 \mathbf{c}_0^{(n)}, \ldots, \mathbf{\Phi}_k \mathbf{c}_0^{(n)}, \ldots, \mathbf{\Phi}_\beta \mathbf{c}_0^{(n)}\right], \tag{1}$$

where $\mathbf{\Phi}_k$ $(k = 1, \ldots, \beta)$ is the cyclic shifting matrix. It's worth pointing out that $\mathbf{\Phi}_k$ is a square matrix with the size of $\beta \times \beta$, while both each row and column has only one element of 1 with all the other elements having the value of 0. Explicitly, $\mathbf{\Phi}_k$ can be represented by

$$\mathbf{\Phi}_k = \begin{bmatrix} \mathbf{0}_{(k-1)\times(\beta-k+1)} & \mathbf{I}_{(k-1)\times(k-1)} \\ \mathbf{I}_{(\beta-k+1)\times(\beta-k+1)} & \mathbf{0}_{(\beta-k+1)\times(k-1)} \end{bmatrix}, \tag{2}$$

where $\mathbf{I}_{(k-1)\times(k-1)}$ represents the unit matrix with the size of $(k-1) \times (k-1)$ and $\mathbf{0}_{(k-1)\times(\beta-k+1)}$ represents zeros with the size of $(k-1) \times (\beta-k+1)$.

2) The Pre-Coder: In this module, the information symbols are precoded to enhance the reliability and security. Based on the principle that the circulant matrix can be diagonalized by the DFT matrix, which are proved in Appendix A, we propose to compose the precoding matrix with the combined DFT matrix, the conjugate phase matrix of an eigenvalue matrix and a chaotic phase vector. To be explicit, the precoded vector over the n_{th} subcarrier is denoted by

$$\mathbf{d}_n = \mathbf{F}\mathbf{V}_n\mathbf{p}_n s_n, \tag{3}$$

where s_n is the information symbol over n_{th} subcarrier, $\mathbf{F}$ is the β-order DFT matrix whose entry in the i_{th} $(i = 1, \ldots, \beta)$ row and k_{th} $(k = 1, \ldots, \beta)$ column is $[\mathbf{F}]_{i,k} = \omega^{(i-1)(k-1)}, \omega = e^{-j\frac{2\pi}{\beta}}$ and j is the imaginary unit. $\mathbf{V}_n = diag(|\mathbf{v}_n|)^{-1} diag(\mathbf{v}_n)^H$ and $\mathbf{v}_n = \mathbf{F}^H \mathbf{c}_0^{(n)}$, where $diag(\cdot)$ is the diagonal matrix generation operator, $|\cdot|$ performs the absolute value operation on the element of a vector, $(\cdot)^{-1}$ is the matrix inversion operator and $(\cdot)^H$ is the Hermitian transpose operator. Besides, the i_{th} element of $\mathbf{d}_n$ is represented by $d_{n,i}$.

In addition, $\mathbf{p}_n$ denotes the chaotic phase vector, whose phase is decided by chaotic sequences. The i_{th} $(i = 1, \ldots, \beta)$ chip of $\mathbf{p}_n$ is denoted by

$$p_{n,i} = e^{j2\pi\phi_n} e^{j2\pi\theta_{n,i}}, \tag{4}$$

where e is the natural constant, $\theta_{n,i}$ and ϕ_n respectively represent the i_{th} and n_{th} chip of two different chaotic sequences, which are generated with different initial values or different chaotic mapping patterns.

3) Chaotic Modulator and OFDM Modulator: In the chaotic modulator, the precoded vector $\mathbf{d}_n$ is modulated by the chaotic circulant matrix $\mathbf{C}_n$, which is represented by

$$\mathbf{w}_n = \mathbf{C}_n \mathbf{d}_n, \tag{5}$$

whose i_{th} element is expressed as $w_{n,i}$.

Subsequently, the IFFT operation is conducted, and the resultant OFDM symbol can be expressed as

$$x_{n,'i} = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} w_{n,i} e^{j\frac{2\pi(n-1)\left(n'-1\right)}{N}}. \tag{6}$$

After adding cyclic prefix (CP) and parallel to serial (P/S) conversion, the signal is transmitted over the wireless V2V channel.

B. Receiver

As shown in Fig. 2, at the receiver, reverse operations are conducted. After the CP removal and S/P conversion, the fast Fourier transform (FFT) operations is conducted for OFDM demodulation. Then the chaotic demodulator and the de-precoder are used to obtain the estimates for information recovery.

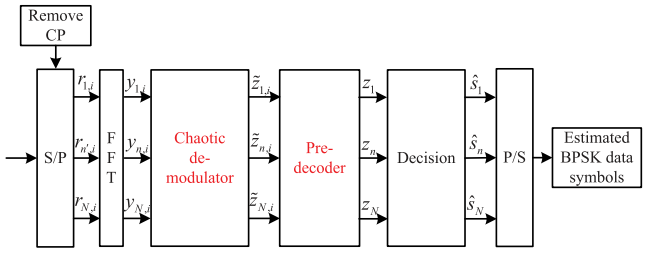

Fig. 2. The receiver structure of OFDM-PC-CSK.

1) OFDM Demodulator: Thanks to the timing and frequency synchronization achieved with training sequences, in OFDM systems, the timing and carrier frequency offsets can be neglected [19]. Additionally, without loss of generality, we assume that the length of CP is set as being longer than the maximum channel delay time, thus the negligible inter-symbol-interference (ISI) is not considered for demodulations. Accordingly, after the CP removal and FFT operations, the signals received over the n_{th} subcarrier at the i_{th} chaotic chip is denoted by

$$\begin{aligned} y_{n,i} &= \frac{1}{\sqrt{N}} \sum_{n'=1}^{N} r_{n,'i} e^{-j\frac{2\pi\left(n'-1\right)(n-1)}{N}} \\ &= H_{n,i} w_{n,i} + ICI_{n,i} + \xi_{n,i}, \end{aligned} \tag{7}$$

where $r_{n,'i}$ denotes the n'_{th} $(n' = 1, \ldots, N)$ chip of the i_{th} $(i = 1, \ldots, \beta)$ OFDM symbol in the received chaotic signal, $ICI_{n,i}$ represents the inter-carrier interference (ICI) and $\xi_{n,i}$ is the complex AWGN with zero mean and the power density of N_0. In addition, $H_{n,i}$ denotes the channel frequency response (CFR) over the n_{th} subcarrier and i_{th} chaotic chip.

Note that in practical V2V scenarios, $H_{n,i}$ might not be available due to the loss of pilot symbols. In this case, we can establish the channel model via real experiments to provide the evaluated $H_{n,i}$. For example, in [20], the nonstationary tapped delay line channel models for the 5-GHz band and 10-MHz bandwidth have been established. Then the CFR is given as

$$H_{n,i} = \sum_{l=1}^{L} \lambda_l \alpha_l e^{-j\frac{2\pi(n-1)\tau_l}{N}} \left(\frac{1}{N} \sum_{n'=1}^{N} e^{j\frac{2\pi f_{D,l}\left[n'+(i-1)T_s\right]}{T_s}} \right), \tag{8}$$

where λ_l represents the persistence process, α_l denotes the channel coefficient and l is the channel path index, L is the total number of fading channel paths and τ_l is the channel delay time. In addition, $ICI_{n,i}$ is denoted by

$$\begin{aligned} ICI_{n,i} = & \sum_{u=1,u\neq n}^{N} w_{u,i} \sum_{l=1}^{L} \lambda_l \alpha_l e^{-j\frac{2\pi(n-1)\tau_l}{N}} \\ & \left(\frac{1}{N} \sum_{n'=1}^{N} e^{j\frac{2\pi f_{D,l}\left[n'+(i-1)T_s\right]}{T_s}} e^{-j\frac{2\pi\left(n'-1\right)(n-u)}{N}} \right). \end{aligned} \tag{9}$$

It is worth mentioning that although the CFR given by (8) might not perfectly match the practical V2X channel conditions, in practical systems, we can modify the above parameters to adapt to the channel fluctuations.

Then after the equalization, we have $\hat{y}_n = w_{n,i} + \frac{H^*_{n,i}}{|H_{n,i}|^2} ICI_{n,i} + \frac{H^*_{n,i}}{|H_{n,i}|^2} \xi_{n,i}$ where $(\cdot)^*$ is the conjugate operator. The signal vector over the n_{th} subcarrier $\hat{\mathbf{y}}_n$ consists of $[\hat{y}_{n,1}, \ldots, \hat{y}_{n,i}, \ldots, \hat{y}_{n,\beta}]^T$. Thus, we have $\hat{\mathbf{y}}_n = \mathbf{w}_n + \mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n + \hat{\boldsymbol{\xi}}_n$ where $\mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n$ and $\boldsymbol{\xi}_n$ are both the vectors with the length of β and the i_{th} entry of $\mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n$ and $\boldsymbol{\xi}_n$ are respectively $\frac{H^*_{n,i}}{|H_{n,i}|^2} ICI_{n,i}$ and $\frac{H^*_{n,i}}{|H_{n,i}|^2} \xi_{n,i}$.

2) The Chaotic Demodulator: Next, using the Hermitian transposed DFT matrix $\mathbf{F}^H$ to perform the chaotic demodulation, the resultant vector is denoted by

$$\begin{aligned} \tilde{\mathbf{z}}_n &= \mathbf{F}^H \hat{\mathbf{y}}_n = \mathbf{F}^H \mathbf{w}_n + \mathbf{F}^H \mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n + \mathbf{F}^H \hat{\boldsymbol{\xi}}_n \\ &= \mathbf{F}^H \mathbf{C}_n \mathbf{F} \mathbf{V}_n \mathbf{p}_n s_n + \mathbf{F}^H \mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n + \mathbf{F}^H \boldsymbol{\xi}_n \\ &= \beta diag\left(|\mathbf{v}_n|\right) \mathbf{p}_n s_n + \mathbf{F}^H \mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n + \mathbf{F}^H \boldsymbol{\xi}_n. \end{aligned} \tag{10}$$

As proved in Appendix A, by applying the DFT matrix, the circulant matrix can be diagonalized. Since $\mathbf{F}^H \mathbf{C}_n \mathbf{F} = \beta diag(\mathbf{v}_n)$, we have $\mathbf{F}^H \mathbf{C}_n \mathbf{F} \mathbf{V}_n = \beta diag(\mathbf{v}_n) diag(|\mathbf{v}_n|)^{-1} diag(\mathbf{v}_n)^H = \beta diag(|\mathbf{v}_n|)$. Thus, by using $\mathbf{F}^H$, the information-bearing chaotic signals can be demodulated with no need of the reference chaotic signals.

3) Pre-Decoder and Decision Module: Subsequently, we pre-decode the demodulated symbol. Note that only legitimate receivers know the chaotic phase vectors learned form the specific secure control channel [21], thus the security can be enhanced and the pre-decoded symbols are expressed as

$$z_n = \mathbf{p}_n^H \tilde{\mathbf{z}}_n = \beta ||\mathbf{v}_n||_1 s_n + \mathbf{p}_n^H \mathbf{F}^H \mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n + \mathbf{p}_n^H \mathbf{F}^H \boldsymbol{\xi}_n, \tag{11}$$

where $||\cdot||_1$ is the 1-norm operator and $||\mathbf{v}_n||_1 = \sum_{i=1}^{\beta} |v_{n,i}|$. $v_{n,i}$ is the i_{th} element of $\mathbf{v}_n$. Finally, in the decision module, we can obtain the estimated BPSK symbol $\hat{s}_n$ by detecting the sign of z_n.

III. Performance Analysis

In this section, the BER expression is derived using the Gaussian approximation (GA) method [21], then the spectrum efficiency and computational complexity are analyzed.

A. BER Derivations

According to (11), the decision variable is expressed as

$$z_n = \mathbf{p}_n^H \tilde{\mathbf{z}}_n = \beta ||\mathbf{v}_n||_1 s_n + \mathbf{p}_n^H \mathbf{F}^H \mathbf{I}\hat{\mathbf{C}}\mathbf{I}_n + \mathbf{p}_n^H \mathbf{F}^H \boldsymbol{\xi}_n. \tag{12}$$

The statistical characteristics of z_n is determined by

$$\begin{aligned} &\mathrm{E}\left[z_n | s_n = +1\right] = -\mathrm{E}\left[z_n | s_n = -1\right] = \beta \mathrm{E}\left[||\mathbf{v}_n||_1\right], \\ &\mathrm{Var}\left[z_n | s_n = \pm 1\right] = \beta \sum_{i=1}^{\beta} \frac{|ICI_{n,i}|^2 + N_0}{2\left|H_{n,i}\right|^2}. \end{aligned} \tag{13}$$

The average BER can thereby be obtained as

$$\begin{aligned} \mathrm{BER} = & \sum_{i_1,\ldots,i_L \in \{0,1\}} \prod_{l=1}^{L} P_{i_l,l} \\ & \int_0^{\infty} \frac{1}{2} \mathrm{erfc}\left(\sqrt{\frac{\left(\mathrm{E}\left[z_n | s_n = \pm 1\right]\right)^2}{2\mathrm{Var}\left[z_n | s_n = \pm 1\right]}} \right) f(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} \\ = & \sum_{i_1,\ldots,i_L \in \{0,1\}} \prod_{l=1}^{L} P_{i_l,l} \\ & \int_0^{\infty} \frac{1}{2} \mathrm{erfc}\left(\frac{\mathrm{E}\left[||\mathbf{v}_n||_1\right]}{\beta} \sqrt{\gamma_b} \right) f(\boldsymbol{\alpha})\, d\boldsymbol{\alpha}, \end{aligned} \tag{14}$$

where $\gamma_b = \frac{E_b}{\frac{1}{\beta}\sum_{i=1}^{\beta}(|ICI_{n,i}|^2 + N_0)/|H_{n,i}|^2}$, $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_L]$ is the tap amplitude vector, $\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^{\infty} e^{-\eta^2} d\eta$ is the complementary error function and the average bit energy is denoted by $E_b =$

TABLE I
THE SPECTRUM EFFICIENCY AND COMPUTATION COMPLEXITY COMPARISONS

System	Spectrum efficiency	Complexity
proposed OFDM-PC-CSK	$\frac{N}{B\beta T_s}$	$\Theta\left(N\beta^2\right)+\Theta\left(N\beta\log_2\beta\right)+\Theta\left(N\beta\log_2 N\right)$
OFDM-DCSK [16]	$\frac{N-1}{B\beta T_s}$	$\Theta\left(N\beta\log_2 N\right)$
LRAM-MC-DCSK with SVD [15]	$\frac{N-1}{B\beta T_s}$	$\Theta\left(N\beta\log_2 N\right)+\Theta\left(N\beta^2\right)$
CM-DCSK [18]	$\frac{N}{2B\beta T_s}$	$\Theta\left(\beta\right)$

$\beta^3\mathrm{E}[(c_{0,i}^{(n)})^2]=\beta^2$. Additionally, e is the natural constant. For the L-path V2V channel [20], $\boldsymbol{\alpha}$ follows the correlated multivariate Weibull distribution and λ_l $(l=1,\ldots,L)$ is a first-order two-state Markov chains where $P_{i_l,l}$ is the steady-state probability associated with the state i_l ($i_l\in\{0,1\}$) and $P_{i_lk_l,l}$ is the transition probability of going from state i_l ($i_l\in\{0,1\}$) to state k_l ($k_l\in\{0,1\}$).

Notably, since $||\mathbf{v}_n||_1=\sum_{i=1}^{\beta}|v_{n,i}|$, for larger value of β, $\frac{\mathrm{E}[||\mathbf{v}_n||_1]}{\beta}$ approaches a constant and γ_b becomes uncorrelated with β. Thus when the chaotic sequence has larger length of β, thanks to the diagonalization of the chaotic circulant matrix, the proposed system can keep similar BER performances. Hence the anti-interference capability is enhanced. By contrast, in traditional OFDM-DCSK systems [16], when β increases and the reference chaotic sequences containing larger interferences are used for the differential demodulation, the reliability performances degrade accordingly. Therefore, the diagonalized demodulation in our design can improve the reliability performance.

B. Spectrum Efficiency

The spectral efficiency can be measured by the ratio of the symbol rate to total bandwidth [16]. For the fairness of comparisons, we assume that considered schemes occupy the same bandwidth of B and the OFDM symbol duration is T_s. In addition, the CM-DCSK [18] scheme is applied in the OFDM system. Then spectrum efficiency of the proposed scheme is calculated by $\frac{data\ rate}{total\ bandwidth}=\frac{N}{BT_s}$ and Table I compares the performances of the spectrum efficiency, which shows that our proposed scheme attains the highest spectrum efficiency.

C. Computational Complexity Comparisons

Next we evaluate the computational complexity of the proposed scheme in terms of the times of multiplexing operations [21]. For the proposed system, the computational complexity is determined by the cyclic shifting, pre-coding and pre-decoding, modulation and demodulation, as well as IFFT and FFT operations. Firstly, the complexity of the cyclic shifting operations is $\Theta(N\beta^2)$ since the large number of elements valued "0" in (1) will greatly reduce the matrix multiplication complexity. Then we apply the fast Fourier transform (FFT) to realize the DFT matrix multiplexing, thus the complexity of pre-coding is $\Theta(N\beta^2)+\Theta(N\beta\log_2\beta)+\Theta(N\beta)$, while the complexity of the de-precoding operations is $\Theta(N\beta)$. Besides, the complexity of the chaotic modulation is $\Theta(N\beta^2)$ and that of the demodulation is $\Theta(N\beta\log_2\beta)$. The complexity of the IFFT and FFT are both $\Theta(N\beta\log_2 N)$. Therefore, ignoring the low order term, we can derive that the complexity of the proposed OFDM-PC-CSK transmitter is $\Theta(N\beta^2)+\Theta(N\beta\log_2\beta)+\Theta(N\beta\log_2 N)$. TABLE I compares the computational complexity, which shows that the complexity of our scheme is higher than that of counterpart schemes.

IV. SIMULATION RESULTS

In this section, we provide simulation results to validate our design and the theoretical analysis. Moreover, the reliability performances are compared with those of the counterpart systems including CM-DCSK [18], NR-DCSK [12], OFDM-DCSK [16] and LRAM-MC-DCSK with SVD [15]. For the fairness of comparison, single-subcarrier schemes [12], [18] are applied into a OFDM-based version and the user number in multi-user OFDM-DCSK [16] is one. In addition, the parameter settings are referred to benchmark schemes to facilitate the performance comparisons. The channel models [20] can be classified into two types: Urban-Antenna Outside Car (UOC) and Open-Area High Traffic Density (OHT), where open areas are highways and their parameter settings are given in Table II. Thereinto, $f_{D,max}$ represents the maximum Doppler shift and $\Gamma(\cdot)$ denotes the gamma function.

TABLE II
CHANNEL MODELS

Type	UOC	OHT
Center frequency	$5GHz$	$5GHz$
Sampling rate	$10MHz$	$10MHz$
Maximum relative vehicle speed	$24m/s$ ($f_{D,max}=400Hz$)	$52m/s$ ($f_{D,max}=880Hz$)
Intervehicle distance	$<100m$	$<1000m$
Tap Doppler spectra	low pass	low pass
Tap delay τ_l	$[0,1,2,3]$	$[0,1,2]$
Averaged tap energy	$[0.88,0.08,0.03,0.001]$	$[0.95,0.04,0.01]$
Tap Weibull shape factors b_l	$[3.19,1.61,1.63,1.73]$	$[4.3,1.64,1.89]$
Tap Weibull scale factors a_l	$a_l=\sqrt{1/\Gamma\left(\frac{2}{b_l}+1\right)}$	$a_l=\sqrt{1/\Gamma\left(\frac{2}{b_l}+1\right)}$
Tap correlation coefficient matrix	$\begin{bmatrix}1 & 0.6898 & 0.6518 & 0.5772\\ 0.6898 & 1 & 0.4922 & 0.5142\\ 0.6518 & 0.4922 & 1 & 0.8479\\ 0.5772 & 0.5142 & 0.8479 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 0.5441 & 0.4157\\ 0.5441 & 1 & 0.1707\\ 0.4157 & 0.1707 & 1\end{bmatrix}$
Tap transition probability $P_{00,l}$	$[0,0.2717,0.4401,0.5571]$	$[0,0.3625,0.5999]$
Tap transition probability $P_{11,l}$	$[1,0.9150,0.8171,0.7488]$	$[1,0.8366,0.6973]$
Tap steady-state probability $P_{1,l}$	$[1,0.8956,0.7538,0.6382]$	$[1,0.7960,0.5696]$

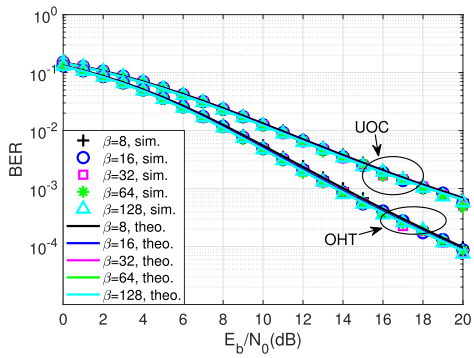

Fig. 3. The theoretical and simulated BER performance comparisons of the proposed OFDM-PC-CSK system for different β and $N=64$.

A. Theoretical and Simulated BER Performance Comparisons

Fig. 3 illustrates the simulated (Sim.) and theoretical (Theo.) BER results of the OFDM-PC-CSK system with different β over the UOC and OHT channels respectively. In Fig. 3, it can be observed that in accordance with the theoretical analysis of the BER, when β increases, the performances of the proposed system almost not change with different β. In addition, we can notice that the theoretical performances match simulated ones well.

B. BER Performance Comparisons With Counterpart Schemes

In Fig. 4(a), we compare our scheme with counterpart schemes including NR-DCSK [12], OFDM-DCSK [16], and LRAM-MC-DCSK with SVD [15] over the UOC and OHT channels. Considering that in practical systems, the channel state information (CSI) might contain errors, we investigate the performances in two cases of the perfect CSI (pCSI) and the imperfect CSI (iCSI). Note that for fairness of comparisons, the NR-DCSK [12] has replicated times of 2. From Fig. 4(a), we

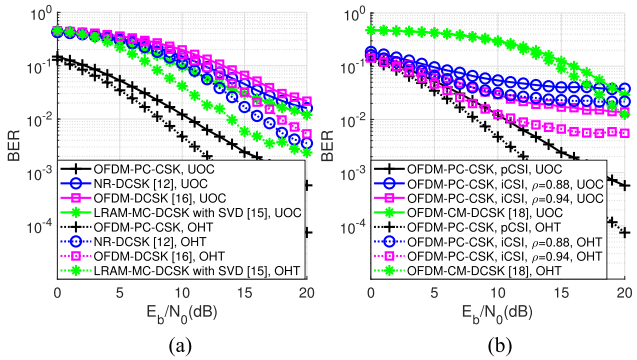

Fig. 4. The BER performance comparison of OFDM-PC-CSK and benchmark schemes for $\beta = 128$ and $N = 64$. (a) Perfect CSI. (b) Imperfect CSI.

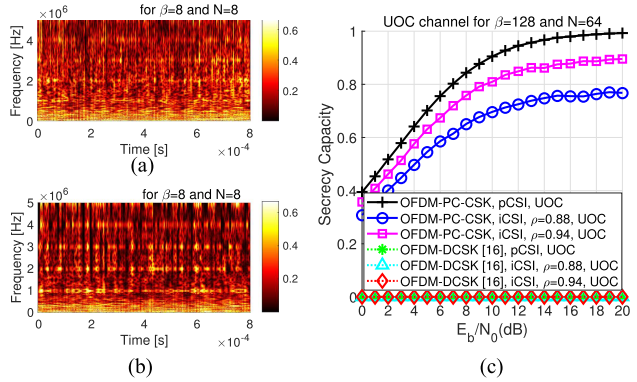

Fig. 5. The security performance comparisons. (a) OFDM-PC-DCSK. (b) OFDM-DCSK [16]. (c) Secrecy capacity performance over.

can see that our scheme achieves the best BER performances over both UOC and OHT channels.

In Fig. 4(b), the iCSI is obtained via the channel estimation module given by $\hat{H}_{n,i} = \rho H_{n,i} + \sqrt{1-\rho^2}\epsilon_{n.k}$ [22] where $\hat{H}_{n,i}$ is the estimated CFR and the estimation error $\epsilon_{n.k}$ is a Gaussian random variable independent from $H_{n,i}$ and has 0 mean and the unit variance which equals to the power of errors, and the correlation coefficient ρ determines the quality of channel estimations. From Fig. 4(b), we can observe that our proposed scheme can perform better than the CM-DCSK system [18] when the CSI has fewer errors. For example, when $\rho = 0.88$ and $E_b/N_0 < 19\ dB$, our scheme attains better BER performances.

C. Security Performance Comparisons of OFDM-PC-CSK

Finally, in Fig. 5(a-b), we use the wavelet transform to quantitatively analyze the security performances in terms of the time-frequency characteristics of the OFDM-PC-CSK and OFDM-DCSK [16] signal power with the sampling frequency $f_s = 10$ MHz. The wavelet transform is defined as $WT_x^{\psi}(\sigma, v) = \frac{1}{\sqrt{|v|}} \int x(t)\psi^*(\frac{t-\sigma}{v})dt$ where $\psi(t)$ is the mother wavelet function, σ is the translation parameter which corresponds to the time information, and v is the scale parameter defined as the reciprocal of the frequency. It can be seen that the OFDM-DCSK [16] signals exhibit distinct peaks along the frequency axis which expose the existence of the information-bearing subcarriers and imperil the physical layer security due to the similarity of reference and data-bearing signals. By contrast, the OFDM-PC-CSK modulated signals have more random waveforms.

Moreover, even if the OFDM-PC-CSK signal feature has been unfortunately identified, the OFDM-PC-CSK modulated signal is still hardly to be eavesdropped since the chaotic phase vector is secret and shared between legitimate transceivers before the information transmission begins. We consider a wiretap channel where the transmitter Alice communicates with a legitimate receiver Bob while an eavesdropper Eve hears the confidential data signal transmitted by Alice [23]. Notably, with considerations that eavesdroppers might be smart to occasionally learn the diagonalization models, we assume that the only thing the eavesdropper does not know is the secret chaotic phase vector. In addition, the channel between Alice and Bob is independent of the eavesdropper channel but has the same distribution and path-loss.

To evaluate the security performances quantitatively, the secrecy capacity performances are compared in Fig. 5(c). The security capacity is calculated by $C_{secrecy} = I(Y_B|X) - I(Y_E|X)$ [21] where $I(Y_B|X)$ and $I(Y_E|B)$ respectively evaluates the mutual information between the transmitted data X and the received data Y_B of legitimate users and Y_E of eavesdroppers. It can be seen that, with different quality of CSI, our proposed scheme always achieves much higher secured data rate than the benchmark OFDM-DCSK system [16] whose secured information rate approaches to 0. That is because in OFDM-DCSK system [16], the reference chaotic signal is transmitted directly over specific subcarriers, thus eavesdroppers can easily retrieve the information. By contrast, the unknown irregular chaotic phase vector guarantee the security of the information delivery in the proposed system.

V. Conclusion

In this correspondence, we propose a reliable OFDM-PC-CSK transceiver, which removes the reference chaotic signal and utilizes the diagonalization principle of the chaotic circulant matrix. At the transmitter, the chaotic phase vectors are generated with different chaotic sequences using different initial values, which are then combined with the DFT matrix and the conjugate phase matrix of an eigenvalue matrix to compose a chaotic precoder. At the receiver, based on the circulant matrix diagonalization principle, the user data can be recovered with no need of reference chaotic signals. Furthermore, we derive the theoretical BER over the V2V channel, the spectrum efficiency and computational complexity. Simulation results validate the effectiveness of our derivations, and demonstrate that our scheme can achieve better BER and security performances than counterpart schemes over V2V channels. Therefore, our scheme provides a better candidate for reliable and secure vehicular communications.

Appendix A
Proof of the Diagonalization

We prove that the chaotic circulant matrix $\mathbf{C}_n$ can be diagonalized by a β-order DFT matrix $\mathbf{F}$ [24]. Namely, $\mathbf{F}^H\mathbf{C}_n\mathbf{F} = \beta diag(\mathbf{F}^H\mathbf{c}_0^{(n)})$.

We first define the downshift matrix $\mathbf{D}$ as

$$\mathbf{D} = \begin{bmatrix} \mathbf{0}_{1\times(\beta-1)} & 1 \\ \mathbf{I}_{(\beta-1)\times(\beta-1)} & \mathbf{0}_{(\beta-1)\times 1} \end{bmatrix} \tag{15}$$

Then we decompose $\mathbf{C}_n$ as $\mathbf{C}_n = \sum_{i=1}^{\beta} c_{0,i}^{(n)}(\mathbf{D})^{i-1}$. Note that $(\mathbf{D})^0 = \mathbf{I}_{\beta\times\beta}$.

Subsequently, utilizing the DFT matrix $\mathbf{F}$, we obtain

$$\mathbf{F}^H\mathbf{C}_n\mathbf{F} = \sum_{i=1}^{\beta} c_{0,i}^{(n)} \left(\mathbf{F}^H(\mathbf{D})^{i-1}\mathbf{F}\right) \tag{16}$$

Since for all i_1 and i_2 that satisfy $1 \le i_1 \le \beta$ and $1 \le i_2 \le \beta$, the i_{1th} row and the i_{2th} column entry of the matrix in (16) is $[\mathbf{F}^H\mathbf{D}\mathbf{F}]_{i_1,i_2} =$

$\omega^{-(i_2-1)}\sum_{i=1}^{\beta}\omega^{(i-1)(i_2-i_1)}$ where $\omega = e^{-j\frac{2\pi}{\beta}}$ while

$$\sum_{i=1}^{\beta}\omega^{(i-1)(i_2-i_1)}=\begin{cases}\beta\omega^0 = \beta, i_1 = i_2\\ \frac{1-\omega^{\beta(i_2-i_1)}}{1-\omega^{i_2-i_1}} = 0, i_1 \neq i_2\end{cases} \tag{17}$$

Thus, we obtain $\mathbf{F}^H\mathbf{D}\mathbf{F} = \beta diag(1, \omega^{-1}, \ldots, \omega^{-(\beta-1)})$. Substituting it into (16), we derive that

$$\begin{aligned}\mathbf{F}^H\mathbf{C}_n\mathbf{F} &= \sum_{i=1}^{\beta} c_{0,i}^{(n)}\left(\mathbf{F}^H\mathbf{D}^{i-1}\mathbf{F}\right) = \sum_{i=1}^{\beta} c_{0,i}^{(n)}\frac{\left(\mathbf{F}^H\mathbf{D}\mathbf{F}\right)^{i-1}}{\beta^{i-2}}\\ &= \beta\sum_{i=1}^{\beta} c_{0,i}^{(n)} diag\left(1, \omega^{-(i-1)}, \ldots, \omega^{-(i-1)(\beta-1)}\right)\\ &= \beta diag\left(\mathbf{F}^H\mathbf{c}_0^{(n)}\right)\end{aligned} \tag{18}$$

The proof is completed.

REFERENCES

[1] F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[2] A. Masood, D. S. Lakew, and S. Cho, "Security and privacy challenges in connected vehicular cloud computing," *IEEE Commun. Surv. Tuts.*, vol. 22, no. 4, pp. 2725–2764, Sep.-Dec. 2020.

[3] J. Cheng *et al.*, "Accessibility analysis and modeling for IoV in an urban scene," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4246–4256, Apr. 2020.

[4] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, "Chaos-based partial transmit sequence technique for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 27, no. 23, pp. 2429–2432, Dec. 2015.

[5] A. A. E. Hajomer, X. Yang, and W. Hu, "Chaotic walsh-hadamard transform for physical layer security in OFDM-PON," *IEEE Photon. Technol. Lett.*, vol. 29, no. 6, pp. 527–530, Mar. 2017.

[6] M. Rice *et al.*, "Physical-layer security for vehicle-to-everything networks: Increasing security while maintaining reliable communications," *IEEE Veh. Technol. Mag.*, vol. 15, no. 3, pp. 68–76, Sep. 2020.

[7] Q. Liu, H. Li, S. Ding, and Y. Wang, "Lightweight secure data exchange in decentralized VANETs with physical layer security," in *Proc. 2020 IEEE 92nd Veh. Technol. Conf.*, 2020, pp. 1–5.

[8] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[9] L. Wu *et al.*, "An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 55050–55063, 2019.

[10] T. Limbasiya and D. Das, "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication," *IEEE Syst. J.*, vol. 14, no. 1, pp. 520–529, Mar. 2020.

[11] 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. Surv. Tuts.*, vol. 18, no. 3, pp. 1804–1837, Jul.-Sep. 2016.

[12] G. Kaddoum and E. Soujeri, "NR-DCSK: A noise reduction differential chaos shift keying system," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 63, no. 7, pp. 648–652, Jul. 2016.

[13] G. Cai, Y. Fang, J. Wen, S. Mumtaz, Y. Song, and V. Frascolla, "Multi-carrier M-ary DCSK system with code index modulation: An efficient solution for chaotic communications," *IEEE J. Sel. Top. Signal Process.*, vol. 13, no. 6, pp. 1375–1386, Oct. 2019.

[14] L. Zhang, H. Zhang, Y. Jiang, and Z. Wu, "Intelligent and reliable deep learning LSTM neural networks-based OFDM-DCSK demodulation design," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 16163–16167, Dec. 2020.

[15] L. Zhang, J. Zheng, B. Chen, and Z. Wu, "Reliable low-rank approximation of matrices detection aided multicarrier DCSK receiver design," *IEEE Syst. J.*, vol. 15, no. 4, pp. 5277–5288, Dec. 2021.

[16] 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.

[17] P. Chen, L. Shi, Y. Fang, G. Cai, L. Wang, and G. Chen, "A coded DCSK modulation system over rayleigh fading channels," *IEEE Trans. Commun.*, vol. 66, no. 9, pp. 3930–3942, Sep. 2018.

[18] F. J. Escribano, G. Kaddoum, A. Wagemakers, and P. Giard, "Design of a new differential chaos-shift-keying system for continuous mobility," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2066–2078, May 2016.

[19] M. M. U. Gul, X. Ma, and S. Lee, "Timing and frequency synchronization for OFDM downlink transmissions using zadoff-chu sequences," *IEEE Trans. Wireless Commun.*, vol. 14, no. 3, pp. 1716–1729, Mar. 2015.

[20] I. Sen and D. W. Matolak, "Vehicle-vehicle channel models for the 5-GHz band," *IEEE Trans. Intell. Transp. Syst.*, vol. 9, no. 2, pp. 235–245, Jun. 2008.

[21] Z. Liu, L. Zhang, Z. Wu, and J. Bian, "A secure and robust frequency and time diversity aided OFDM-DCSK modulation system not requiring channel state information," *IEEE Trans. Commun.*, vol. 68, no. 3, pp. 1684–1697, Mar. 2020.

[22] A. Pascual-Iserte, D. P. Palomar, A. I. Perez-Neira, and M.A. Lagunas, "A robust maximin approach for MIMO communications with imperfect channel state information based on convex optimization," *IEEE Trans. Signal Process.*, vol. 54, no. 1, pp. 346–360, Jan. 2006.

[23] 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.

[24] G. H. Golub and C. F. V. Loan, *Matrix Computations*, 4th ed. Baltimore, Maryland, Americal: Johns Hopkins University Press, 2013.