2020 International Conference on Computing, Networking and Communications (ICNC): Communications and Information Security Symposium

Secure and Efficient OFDM System Design under Disguised Jamming

Yuan Liang Jian Ren Tongtong Li

Department of Electrical & Computer Engineering, Michigan State University, East Lansing, MI 48824, USA.
Email: {liangy11, renjian, tongli}@egr.msu.edu

***Abstract*—This paper proposes a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming. First, we bring off a dynamic constellation by introducing secure shared randomness between the legitimate transmitter and receiver, and hence break the symmetricity between the authorized signal and the disguised jamming. Second, using the arbitrarily varying channel (AVC) model, we prove that SP-OFDM can achieve a positive deterministic coding capacity under disguised jamming since the AVC channel corresponding to SP-OFDM is not symmetrizable. Finally, numerical examples are provided to demonstrate the effectiveness of the proposed scheme under disguised jamming attacks.**

***Index Terms*—OFDM, disguised jamming, precoding, arbitrarily varying channel.**

I. Introduction

In wireless systems, one of the most commonly used techniques for limiting the effectiveness of an opponent's communication is referred to as jamming, in which the authorized user's signal is deliberately interfered by the adversary. Recently, it was found that disguised jamming [1]–[3], where the jamming is highly correlated with the signal, can reduce the system capacity to zero. Consider channel $R = S+J+N$, where S is the authorized signal, J is the jamming interference, N is the noise independent of J and S, and R is the received signal. If the jammer is capable of eavesdropping on the symbol constellation and the codebook of the transmitter, it can simply replicate one of the sequences in the codebook of the legitimate transmitter, the receiver, then, would not be able to distinguish between the authorized sequence and the jamming sequence, resulting in a complete communication failure [4, ch 7.3].

Orthogonal frequency division multiplexing (OFDM), due to its high spectral efficiency and robustness under fading channels, has been widely used in modern high speed multimedia communication systems [5], such as LTE and WiMax. However, unlike the spread spectrum techniques [6], OFDM has very limited built-in resilience against jamming attacks, as it mainly relies on channel coding for communication reliability under hostile jamming. To enhance the jamming resistance of OFDM systems, in [7], a collision-free frequency hopping (CFFH) scheme was proposed. CFFH integrates the frequency hopping technique into OFDM transceiver design. The idea is to randomize the jamming interference through frequency domain interleaving based on secure, collision-free frequency hopping. It can improve the jamming resistance of OFDM significantly under partial jamming, without sacrificing the spectral efficiency. However, CFFH based OFDM is still fragile under *disguised jamming*. To combat disguised jamming in OFDM systems, a precoding scheme was proposed in [8], where extra redundancy is introduced to achieve jamming resistance. However, lack of plasticity in the precoding scheme results in inadequate reliability under cognitive disguised jamming.

In this paper, we propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming. First, we design a dynamic constellation by introducing shared randomness between the legitimate transmitter and receiver, which breaks the symmetricity between the authorized signal and the jamming interference, and hence ensures reliable performance under disguised jamming. Second, we analyze the channel capacity of the proposed SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model [9]. We prove that with the secure randomness shared between the authorized transmitter and receiver, the AVC channel corresponding to SP-OFDM is not symmetrizable, and hence SP-OFDM can achieve a positive deterministic coding capacity under disguised jamming. The channel capacity of the proposed system is also discussed. Finally, Numerical examples are provided to demonstrate the effectiveness of the proposed system under disguised jamming and frequency selective fading.

II. Secure OFDM System Design under Disguised Jamming

In this section, we introduce the proposed anti-jamming OFDM system with secure precoding and decoding, named as securely procoded OFDM (SP-OFDM).

A. Transmitter Design with Secure Precoding

The block diagram of the proposed system is shown in Fig. 1. Let N_c be the number of subcarriers in the OFDM system and Φ the alphabet of transmitted symbols. For $i = 0, 1, \cdots, N_c$ and $k = 0, 1, \cdots$, let $S_{k,i} \in \Phi$ denote the symbol transmitted on the i-th carrier of the k-th OFDM block. We denote the symbol vector of the k-th OFDM block by $\boldsymbol{S}_k = [S_{k,0}, S_{k,1}, \cdots, S_{k,N_c-1}]^T$. The input data stream is first fed to the channel encoder, mapped to the symbol vector $\boldsymbol{S}_k$, and then fed to the proposed symbol-level secure precoder.

978-1-7281-4905-9/20/$31.00 ©2020 IEEE

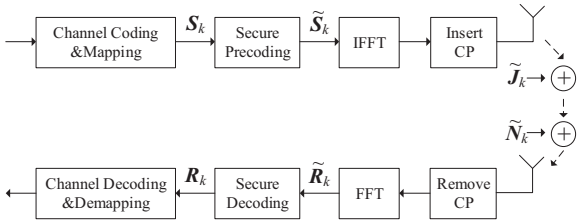

Fig. 1: Anti-jamming OFDM design through secure precoding and decoding.

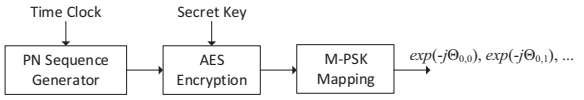

Fig. 2: Secure phase shift generator

As pointed out in [3], [10]–[12], a key enabling factor for reliable communication under disguised jamming is to introduce shared randomness between the transmitter and receiver, such that the symmetry between the authorized signal and the jamming interference is broken. To maintain full spectral efficiency of the traditional OFDM system, the precoding is performed by multiplying an *invertible* $N_c \times N_c$ precoding matrix $\boldsymbol{P}_k$ to the symbol vector $\boldsymbol{S}_k$, i.e.,

$$\tilde{\boldsymbol{S}}_k = \boldsymbol{P}_k \boldsymbol{S}_k. \tag{1}$$

In this paper, we design the precoding matrix $\boldsymbol{P}_k$ to be a diagonal matrix as

$$\boldsymbol{P}_k = diag(e^{-j\Theta_{k,0}}, e^{-j\Theta_{k,1}}, \cdots, e^{-j\Theta_{k,N_c-1}}). \tag{2}$$

That is, for $i = 0, 1, \cdots, N_c - 1$ and $k = 0, 1, \cdots$, a random phase shift is applied to each transmitted symbol; more specifically, a random phase shift $-\Theta_{k,i}$ is applied to the symbol transmitted on the i-th carrier of the k-th OFDM block. The phase shift changes randomly and independently across sub-carriers and OFDM blocks, and is encrypted so that the jammer has no access to it. More specifically, $\{\Theta_{k,i}\}$ is generated through a secure phase shift generator as shown in Fig. 2. The secure phase shift generator consists of three parts: (i) a PN sequence generator; (ii) an Advanced Encryption Standard (AES) [13] encryption module; and (iii) an M-PSK mapper.

The *PN sequence generator* generates a pseudo-random sequence, which is then encrypted with AES. The encrypted sequence is further converted to PSK symbols using an M-PSK mapper, where M is a power of 2, and every $\log_2 M$ bits are converted to a PSK symbol. The structure and the initial state of the PN sequence generator are public, so that the transmitter and the receiver can generate identical phase shift sequences as long as they share the same secret encryption key. The security, as well as the randomness of the generated phase shift sequence, are guaranteed by the AES encryption algorithm [13], for which the secret encryption key is only shared between the authorized transmitter and receiver. As a result, the phase shift sequence is random and unaccessible for the jammer.

The resulted symbol vector from the secure precoding, $\tilde{\boldsymbol{S}}_k$, is then used to generate the OFDM signals through IFFT, and transmitted to the receiver after inserting the cyclic prefix (CP), which eliminates the inter-symbol interference (ISI) introduced by the multipath channels.

B. Receiver Design with Secure Decoding

We consider an additive white Gaussian noise (AWGN) channel under hostile jamming. The transmitted OFDM signal is subject to an AWGN term, denoted by $\tilde{\boldsymbol{N}}_k$, and an additive jamming interference $\tilde{\boldsymbol{J}}_k$. Let $\tilde{\boldsymbol{N}}_k = [\tilde{N}_{k,0}, \tilde{N}_{k,1}, \cdots, \tilde{N}_{k,N_c-1}]$. We assume that the components in $\tilde{\boldsymbol{N}}_k$ are i.i.d. circularly symmetric complex Gaussian random variables. Note that in OFDM, the original symbol vectors $\{\boldsymbol{S}_k\}$ are considered to be in the frequency domain for $k = 0, 1, \cdots$, we also express the noise term $\tilde{\boldsymbol{N}}_k$ and the jamming signal $\tilde{\boldsymbol{J}}_k$ at the receiver input (please refer to Fig. 1) in terms of their frequency components as

$$\tilde{\boldsymbol{N}}_k = \boldsymbol{F}\bar{\boldsymbol{N}}_k, \text{ with } \bar{\boldsymbol{N}}_k = [\bar{N}_{k,0}, \bar{N}_{k,1}, \cdots, \bar{N}_{k,N_c-1}]^T, \tag{3}$$

$$\tilde{\boldsymbol{J}}_k = \boldsymbol{F}\boldsymbol{J}_k, \text{ with } \boldsymbol{J}_k = [J_{k,0}, J_{k,1}, \cdots, J_{k,N_c-1}]^T, \tag{4}$$

where $\bar{N}_{k,i}, J_{k,i} \in \mathbb{C}, i = 0, 1, \cdots, N_c - 1$, denote the noise and the jamming interference on the i-th subcarrier of the k-th OFDM block, respectively; $\boldsymbol{F}$ is the IFFT unitary matrix with $[\boldsymbol{F}]_{m,n} = \frac{1}{\sqrt{N_c}} e^{j2\pi mn/N_c}$, and $\mathbb{C}$ is the complex plane.

On the receiver side, after removing the CP and performing OFDM demodulation (FFT) to the received signal, a symbol vector $\tilde{\boldsymbol{R}}_k = [\tilde{R}_{k,0}, \tilde{R}_{k,1}, \cdots, \tilde{R}_{k,N_c-1}]^T$ is obtained for the k-th transmitted OFDM block. That is,

$$\tilde{\boldsymbol{R}}_k = \boldsymbol{P}_k \boldsymbol{S}_k + \boldsymbol{J}_k + \bar{\boldsymbol{N}}_k. \tag{5}$$

Note that the noise vector $\tilde{\boldsymbol{N}}_k$ has zero mean and covariance matrix $\mathbb{E}\{\tilde{\boldsymbol{N}}_k^H \tilde{\boldsymbol{N}}_k\} = \sigma^2 \boldsymbol{I}$. It follows that the corresponding covariance matrix of $\bar{\boldsymbol{N}}_k$ is $\mathbb{E}\{\bar{\boldsymbol{N}}_k^H \bar{\boldsymbol{N}}_k\} = \sigma^2 \boldsymbol{I}$, since $\bar{\boldsymbol{N}}_k = F^H \tilde{\boldsymbol{N}}_k$ and F is a unitary matrix. Moreover, note that (i) for any circularly symmetric Gaussian random variable N, $e^{j\theta}N$ and N have the same distribution for any angle θ [14, p66]; (ii) linear combination of independent circularly symmetric Gaussian random variables is still circularly symmetric Gaussian. We can see that the components of noise $\bar{\boldsymbol{N}}_k$ are i.i.d. circularly symmetric complex Gaussian random variables with zeros mean and variance σ^2.

The secure decoding module multiplies the inverse matrix of $\boldsymbol{P}_k$ to $\tilde{\boldsymbol{R}}_k$, which results in the symbol vector

$$\boldsymbol{R}_k = \boldsymbol{S}_k + \boldsymbol{P}_k^{-1}\boldsymbol{J}_k + \boldsymbol{P}_k^{-1}\bar{\boldsymbol{N}}_k, \tag{6}$$

where $\boldsymbol{R}_k = [R_{k,0}, R_{k,1}, \cdots, R_{k,N_c-1}]^T$, with

$$R_{k,i} = S_{k,i} + e^{j\Theta_{k,i}} J_{k,i} + N_{k,i}, \tag{7}$$

where $N_{k,i} = e^{j\Theta_{k,i}} \bar{N}_{k,i}$, and $\Theta_{k,i}$ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, \cdots, M-1\}$. Again, the phase shift to the complex Gaussian noise $\bar{N}_{k,i}$ will not change its distribution. That is, $N_{k,i}$ is still a circular symmetric complex Gaussian

random variable of zero-mean and variance σ^2. For notation simplicity, from now on, we replace the double indices k, i of each symbol with a single index i, referring to the i-th symbol transmitted.

Taking the delay in the communication system into consideration, in this paper, we assume that the authorized user and the jammer do not have pre-knowledge on the sequence of each other. We do not assume any *a priori* information on the jamming signal, except a finite average power constraint of P_J, i.e., $\mathbb{E}\{|J_i|^2\} \leq P_J$, for any possible i.

C. PN Sequence Synchronization between the Secure Precoder and Decoder

A key issue in the secure precoding and decoding is the PN sequence synchronization. We ensure the synchronization between the PN sequences generated by the transmitter and the receiver using the following method: each party is equipped with a global time clock, and the PN sequence generators of the two parties are reinitialized at fixed intervals. The new state for reinitialization, for example, can be the elapsed time after a specific reference epoch in seconds for the time being, which is public. As the initial state changes with each reinitialization, no repeated PN sequence will be generated.

At the beginning of the reception, the PN sequences generated by the two parties may not be perfectly synchronized because of the mismatch between the time clocks and the possible delays in the transmission and reception. That is, the receiver may be unaware of the indices of the symbols at first.

This problem can be solved by inserting pilot symbols into the transmitted signal. Consider the random phase shifts introduced in the secure precoding, without loss of generality, we can assume the pilot symbol vector is $\boldsymbol{s}_p[1, 1, \cdots, 1]^T_{1\times m}$, where m is the length of pilot sequence. Suppose the received training sequence is denoted as $[\tilde{R}_{n_0}, \tilde{R}_{n_0+1}, ...\tilde{R}_{n_0+m-1}]^T$, where the staring index n_0 is unknown to the receiver, i.e,

$$\tilde{R}_{n_0+l} = \boldsymbol{s}_p e^{-j\Theta_{n_0+l}} + J_{n_0+l} + N_{n_0+l}, \quad l = 0, 1, \cdots, m-1. \tag{8}$$

To estimate the value of n_0, the receiver calculates its correlation with the known phase shifting sequence $e^{j\Theta_{n_1}}, e^{j\Theta_{n_1+1}}, ..., e^{j\Theta_{n_1+m-1}}$, i.e.,

$$\begin{aligned}&\frac{1}{m}\sum_{l=0}^{m-1}\tilde{R}_{n_0+l}e^{j\Theta_{n_1+l}}\\ =&\frac{1}{m}\sum_{l=0}^{m-1}\left[\boldsymbol{s}_p e^{-j(\Theta_{n_1+l}-\Theta_{n_0+l})} + J_{n_0+l}e^{j\Theta_{n_1+l}} + N_{n_0+l}\right].\end{aligned} \tag{9}$$

The receiver iterates n_1 over the candidate set of n_0, that is, all the possible values of n_0. Note that for $l_1 \neq l_2$, Θ_{l_1} and Θ_{l_2} are independent, and J_{l_1} and Θ_{l_2} are also independent, so we can get the mean and variance of the correlation coefficient as

$$\mathbb{E}\left[\frac{1}{m}\sum_{l=0}^{m-1}\tilde{R}_{n_0+l}e^{j\Theta_{n_1+l}}\right] = \begin{cases} 0, & n_0 \neq n_1 \\ \boldsymbol{s}_p, & n_0 = n_1 \end{cases}, \tag{10}$$

$$\mathbb{D}\left[\frac{1}{m}\sum_{l=0}^{m-1}\tilde{R}_{n_0+l}e^{j\Theta_{n_1+l}}\right] \leq \begin{cases} \frac{|\boldsymbol{s}_p|^2+P_J+\sigma_n^2}{m}, & n_0 \neq n_1 \\ \frac{P_J+\sigma_n^2}{m}, & n_0 = n_1 \end{cases}. \tag{11}$$

The value of n_0 can then be estimated through

$$\hat{n}_0 = \arg\max_{n_1} \left|\frac{1}{m}\sum_{l=0}^{m-1}\tilde{R}_{n_0+l}e^{j\Theta_{n_1+l}}\right|. \tag{12}$$

Note that from the design of the PN generator in section II-A, the receiver is able to have a rough estimation of n_0 from the time clock, so the candidate set of n_0 is finite. Under limited jamming power, the variance of the estimated correlation coefficient can be arbitrarily small as $m \to \infty$. Thus from the Chebychev inequality [15, Theorem 5.11], for any $n_1 \neq n_0$, the probability that

$$\Pr\left\{\left|\frac{1}{m}\sum_{l=0}^{m-1}\tilde{R}_{n_0+l}e^{j\Theta_{n_1+l}}\right| \geq \left|\frac{1}{m}\sum_{l=0}^{m-1}\tilde{R}_{n_0+l}e^{j\Theta_{n_0+l}}\right|\right\} \to 0, \tag{13}$$

as $m \to \infty$, which indicates we are able to get an accurate estimate of n_0.

Basing on the analysis above, in the following, we assume the PN sequences have been perfectly synchronized between the two parties. For notation simplicity, we further discard the indicies of symbol and rewrite the equivalent channel model as

$$R = S + e^{j\Theta}J + N, \tag{14}$$

where $S \in \Phi, J \in \mathbb{C}$, $N \sim \mathcal{CN}(0, \sigma^2)$, Θ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, ..., M-1\}$, and $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ denotes a circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and variance $\boldsymbol{\Sigma}$. We would like to point out that this model is used for system capacity evaluation under disguised jamming. The system performance with non-ideal carrier synchronization or channel estimation under fading channels will be demonstrated in Example 2 of section IV, where the error in carrier synchronization or channel estimation is modeled as the random channel gain under a Rician model.

III. Symmetricity and Capacity Analysis using the AVC Model

In this section, first, we will show that for the proposed SP-OFDM system, the equivalent arbitrarily varying channel (AVC) model is nonsymmetrizable under disguised jamming. We will further discuss the capacity of the proposed system under disguised jamming.

The arbitrarily varying channel (AVC) model, first introduced in [11], characterizes the communication channels with unknown states which may vary in arbitrary manners across time. For the jamming channel (14) of interest, the jamming symbol J can be viewed as the state of the channel under consideration. The channel capacity of AVC evaluates the data rate of the channel under the most adverse jamming interference among all the possibilities [9]. Note that unlike the jamming free model where the channel noise sequence is independent of the authorized signal and is independent and identically distributed (i.i.d.), the AVC model considers the possible correlation between the authorized signal and the jamming, as well as the possible temporal correlation among

the jamming symbols, which may cause much worse damages to the communication.

To prove the effectiveness of the proposed SP-OFDM under disguised jamming, we need to introduce some basic concepts and properties of the AVC model. First we revisit the definition of symmetrizable AVC channel.

Definition 1. *[9] [16] Let $W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{x})$ denote the conditional PDF of the received signal R given the transmitted symbol $\boldsymbol{s} \in \Phi$ and the jamming symbol $\boldsymbol{x} \in \mathbb{C}$. The AVC channel (14) is symmetrizable if and only if for some auxiliary channel $\pi : \Phi \to \mathbb{C}$, we have*

$$\int_{\mathbb{C}} W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{x}) dF_\pi(\boldsymbol{x}|\boldsymbol{s}') = \int_{\mathbb{C}} W(\boldsymbol{r} \mid \boldsymbol{s}', \boldsymbol{x}) dF_\pi(\boldsymbol{x}|\boldsymbol{s}), \quad (15)$$

$\forall \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C}$, where $F_\pi(\cdot|\cdot)$ is the probability measure of the output of π given the input, i.e., the conditional CDF

$$F_\pi(\boldsymbol{x}|\boldsymbol{s}) = \Pr\{Re(\pi(\boldsymbol{s})) \le Re(\boldsymbol{x}), Im(\pi(\boldsymbol{s})) \le Im(\boldsymbol{x})\}, \quad (16)$$

$\boldsymbol{x} \in \mathbb{C}, \boldsymbol{s} \in \Phi$, where $\pi(\boldsymbol{s})$ denotes the output of channel π given input symbol $\boldsymbol{s}$.

We denote the set of all the auxiliary channels, π's, that can symmetrize channel (14) by Π, that is,

$$\Pi = \{\pi \mid \pi \text{ satisfies (15) for any } \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C}\}. \quad (17)$$

With the average jamming power constraint considered in this paper, we further introduce the definition of l-symmetrizable channel.

Definition 2. *[16] The AVC channel (14) is called l-symmetrizable under average jamming power constraint if and only if (iff) there exists a $\pi \in \Pi$ such that*

$$\int_{\mathbb{C}} |\boldsymbol{x}|^2 dF_\pi(\boldsymbol{x}|\boldsymbol{s}) < \infty, \quad \forall \boldsymbol{s} \in \Phi. \quad (18)$$

In [16], it was shown that reliable communication can be achieved as long as the AVC channel is not l-symmetrizable.

Lemma 1. *[16] The deterministic coding capacity[1] of the AVC channel (14) is positive under any hostile jamming with finite average power constraint iff the AVC is not l-symmetrizable. Furthermore, given a specific average jamming power constraint P_J, the channel capacity C in this case equals*

$$\begin{aligned} C &= \max_{\mathcal{P}_S} \min_{F_J} I(S, R), \\ s.t. \quad & \int_{\mathbb{C}} |\boldsymbol{x}|^2 dF_J(\boldsymbol{x}) \le P_J, \end{aligned} \quad (19)$$

where $I(S, R)$ denotes the mutual information (MI) between the R and S in (14), $\mathcal{P}_S$ denotes the probability distribution of S over Φ and $F_J(\cdot)$ the CDF of J.

Next, we show that with the proposed secure precoding, it is impossible to l-symmetrize the AVC channel (14) corresponding to the SP-OFDM system.

[1]The deterministic coding capacity is defined by the capacity that can be achieved by a communication system, when it applies only one code pattern during the information transmission. In other words, the coding scheme is deterministic and can be readily repeated by other users [17].

Theorem 1. *The AVC channel of the proposed system is not l-symmetrizable.*

Proof. Suppose that there exists a channel $\pi \in \Pi$. Denote the output of channel π given input $\boldsymbol{x}$ by $\Pi(\boldsymbol{x})$, and define channel for inputs $\boldsymbol{s}$ and $\boldsymbol{s}'$ as

$$\hat{R}(\boldsymbol{s}, \boldsymbol{s}') = \boldsymbol{s} + \pi(\boldsymbol{s}')e^{j\Theta} + N, \quad (20)$$

where the channel output is denoted by $\hat{R}(\boldsymbol{s}, \boldsymbol{s}')$. From (15), the distribution of $\hat{R}(\boldsymbol{s}, \boldsymbol{s}')$ and $\hat{R}(\boldsymbol{s}', \boldsymbol{s})$ should be equal. Let $\varphi_X(\omega_1, \omega_2)$ denote the characteristic function (CF) for any complex random variable X. So we have

$$\varphi_{\hat{R}(\boldsymbol{s},\boldsymbol{s}')}(\omega_1, \omega_2) \equiv \varphi_{\hat{R}(\boldsymbol{s}',\boldsymbol{s})}(\omega_1, \omega_2), \quad (21)$$

and

$$\varphi_{\hat{R}(\boldsymbol{s},\boldsymbol{s}')}(\omega_1, \omega_2) = \varphi_{\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2)\varphi_N(\omega_1, \omega_2). \quad (22)$$

where, for the complex Gaussian noise, we have

$$\varphi_N(\omega_1, \omega_2) = e^{-\frac{\sigma^2}{4}(w_1^2+w_2^2)}, \quad \omega_1, \omega_2 \in (-\infty, +\infty), \quad (23)$$

which is non-zero over $\mathbb{R}^2$. Thus by eliminating the CFs of the Gaussian noises on both sides of equation (21), we have

$$\varphi_{\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2) = \varphi_{\boldsymbol{s}'+\pi(\boldsymbol{s})e^{j\Theta}}(\omega_1, \omega_2). \quad (24)$$

for $\omega_1, \omega_2 \in (-\infty, +\infty)$. Let $\boldsymbol{s} = s_1 + js_2$, we can then express $\varphi_{\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2)$ as

$$\varphi_{\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2) = e^{js_1\omega_1 + js_2\omega_2}\varphi_{\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2), \quad (25)$$

and

$$\begin{aligned} \varphi_{\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2) &= \mathbb{E}\{e^{j\omega_1 Re(\pi(\boldsymbol{s}')e^{j\Theta}) + j\omega_2 Im(\pi(\boldsymbol{s}')e^{j\Theta})}\} \\ &= \int \mathbb{E}\{e^{j\omega_1 Re(\boldsymbol{x}e^{j\Theta}) + j\omega_2 Im(\boldsymbol{x}e^{j\Theta})}\} \mathrm{d}F_\pi(\boldsymbol{x}|\boldsymbol{s}'). \end{aligned} \quad (26)$$

Under the proposed secure precoding scheme, Θ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, ..., M-1\}$, where M is a power of 2. We have

$$\begin{aligned} & \mathbb{E}\{e^{j\omega_1 Re(\boldsymbol{x}e^{j\Theta}) + j\omega_2 Im(\boldsymbol{x}e^{j\Theta})}\} \\ &= \frac{1}{M} \sum_{i=0}^{M-1} e^{j\omega_1 |\boldsymbol{x}| \cos(\frac{2\pi i}{M} + \arg(\boldsymbol{x})) + j\omega_2 |\boldsymbol{x}| \sin(\frac{2\pi i}{M} + \arg(\boldsymbol{x}))} \\ &= \frac{2}{M} \sum_{i=0}^{M/2-1} \cos\Big(\omega_1 |\boldsymbol{x}| \cos(\frac{2\pi i}{M} + \arg(\boldsymbol{x})) + \\ &\qquad \omega_2 |\boldsymbol{x}| \sin(\frac{2\pi i}{M} + \arg(\boldsymbol{x}))\Big), \end{aligned} \quad (27)$$

which is of real value for $\omega_1, \omega_2 \in (-\infty, +\infty)$. So $\varphi_{\pi(\boldsymbol{s}')e^{j\Theta}}(\omega_1, \omega_2)$ and $\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}(\omega_1, \omega_2)$ are also of real values over $\mathbb{R}^2$. For $\boldsymbol{s} \neq \boldsymbol{s}'$, $\boldsymbol{s}' = s_1' + js_2'$, expression

$$e^{j[(s_1 - s_1')\omega_1 + (s_2 - s_2')\omega_2]}, \quad (28)$$

has non-zero imaginary part for $(s_1 - s_1')\omega_1 + (s_2 - s_2')\omega_2 \neq n\pi$, $n \in \mathbb{Z}$. Without loss of generality, we assume $s_1 \neq s_1'$. From (24), (25) and (27), we must have

$$\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}(\omega_1, \omega_2) = 0, \text{ for } \omega_1 + \frac{s_2 - s_2'}{s_1 - s_1'}\omega_2 \neq \frac{n\pi}{s_1 - s_1'}, n \in \mathbb{Z}. \quad (29)$$

On the other hand, the CF of a RV should be uniformly continuous in the real domain [15, Theorem 15.21]. So for any fixed $\omega_2 \in (-\infty, \infty)$, we should have

$$\begin{aligned}&\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}\left(\frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'},\omega_2\right)\\ =&\lim_{\omega_1\to\frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}}\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}(\omega_1,\omega_2),\ n\in\mathbb{Z}.\end{aligned}\tag{30}$$

For $\omega_1 \in \left(\frac{(n-1)\pi-(s_2-s_2')\omega_2}{s_1-s_1'}, \frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}\right) \cup \left(\frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}, \frac{(n+1)\pi-(s_2-s_2')\omega_2}{s_1-s_1'}\right)$, $\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}(\omega_1,\omega_2) \equiv 0$, so

$$\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}\left(\frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'},\omega_2\right)=0,\ n\in\mathbb{Z}.\tag{31}$$

Combining (29) and (31), we have

$$\varphi_{\pi(\boldsymbol{s})e^{j\Theta}}(\omega_1,\omega_2)=0,\quad \omega_1,\omega_2\in(-\infty,\infty).\tag{32}$$

However, (32) cannot be a valid CF for any RV. Thus channel π does not exist. Since Π is empty, the AVC channel is not l-symmerizable. □

From Lemma 1, the capacity of channel $R = S + e^{j\Theta}J + N$ is given by (19). It is hard to obtain a closed form solution of the channel capacity for a general discrete transmission alphabet Φ. However, if we relax the distribution of the transmitted symbol S from the discrete set Φ to the entire complex plane $\mathbb{C}$ under an average power constraint, we are able to obtain the following result on channel capacity.

Theorem 2. *The deterministic coding capacity of SP-OFDM is positive under any hostile jamming. More specifically, let the alphabet $\Phi = \mathbb{C}$ and the average power of S being upper bounded by P_S, then the maximin channel capacity in (19) under average jamming power constraint P_J and noise power $P_N = \sigma^2$ is*

$$C=\log\left(1+\frac{P_S}{P_J+P_N}\right).\tag{33}$$

The capacity is achieved at input distribution $\mathcal{CN}(0, P_S)$ and jamming distribution $\mathcal{CN}(0, P_J)$.

Proof. By replacing the support of S, Φ, with the complex plane $\mathbb{C}$, the maximin optimization problem is reformulated as

$$\begin{aligned}C\quad&=\max_{F_S}\min_{F_J} I(R;S),\\ s.t.\quad&\int|\boldsymbol{x}|^2\mathrm{d}F_S(\boldsymbol{x})\le P_S,\\ &\int|\boldsymbol{x}|^2\mathrm{d}F_J(\boldsymbol{x})\le P_J,\end{aligned}\tag{34}$$

where $F_S(\cdot)$ denotes the CDF function of S defined on $\mathbb{C}$.

Mutual information $I(S, R)$ is concave w.r.t. $F_S(\cdot)$ and convex w.r.t. $F_J(\cdot)$ [16, Lemma 4]. We denote $I(S, R)$ for input distribution $F_S(\cdot)$ and jamming distribution $F_J(\cdot)$ by $\phi(F_S, F_J)$. As is noted in [18], if we can find input distribution F_S^* and jamming distribution F_J^* such that

$$\phi(F_S,F_J^*)\le\phi(F_S^*,F_J^*)\le\phi(F_S^*,F_J),\tag{35}$$

for any F_S and F_J under the average power constraints. Then

$$\phi(F_S^*,F_J^*)=C.\tag{36}$$

Pair (F_S^*, F_J^*) is the saddle point of the max-min problem [19].

Note that: (i) phase shift would not change the distribution of a circularly symmetric complex Gaussian RV, (ii) the capacity achieving input distribution of a Gaussian channel is Gaussian, and (iii) the worst noise in terms of capacity for Gaussian input is Gaussian [4]. So the saddle point (F_S^*, F_J^*) is achieved at $(\mathcal{CN}(0, P_S), \mathcal{CN}(0, P_J))$, where the corresponding channel capacity is

$$C=\log\left(1+\frac{P_S}{P_J+P_N}\right),\tag{37}$$

which completes the proof. □

IV. Numerical Results

In this section, we evaluate the performance of the proposed system under disguised jamming attacks through simulation examples.

Example 1: System performance under disguised jamming in AWGN channels: In this example, we analyze the bit error rates (BERs) of the proposed system under disguised jamming in AWGN channels. We use the low density parity check (LDPC) codes for channel coding, and adopt the parity check matrices from the DVB-S.2 standard [20]. The coded bits are mapped into QPSK symbols. The random phase shifts in the proposed secure precoding are approximated as i.i.d. continuous RVs uniformly distributed over $[0, 2\pi)$. We observe that such an approximation has negligible difference on BER performance compared with a sufficiently large M. The jammer randomly selects one of the codewords in the LDPC codebook and sends it to the receiver after the mapping and modulation. On the receiver side, we use a soft decoder for the LDPC codes, where the belief propagation (BP) algorithm [21] is employed. The likelihood information in the BP algorithm is calculated using the likelihood function of a general Gaussian channel, where the noise power is set to $1 + \sigma^2$ considering the existence of jamming signal, and σ^2 is the noise power. That is, the signal to jamming power ratio (SJR) is set to be 0 dB. It should be noted that for more complicated jamming distribution or mapping schemes, customized likelihood functions basing on the jamming distribution will be needed for the optimal performance. Fig. 3 compares the BERs of the communication system studied with and without the proposed secure precoding under different code rates and SNRs. It can be observed that: (i) under the disguised jamming, in the traditional OFDM system, the BER cannot really be reduced by decreasing the code rate or the noise power, which indicates that without appropriate anti-jamming procedures, we are not able to communicate reliably under disguised jamming; (ii) with the proposed SP-OFDM scheme, when the code rates are below certain thresholds, the BERs can be significantly reduced with the decrease of code rates using the proposed secure precoding.

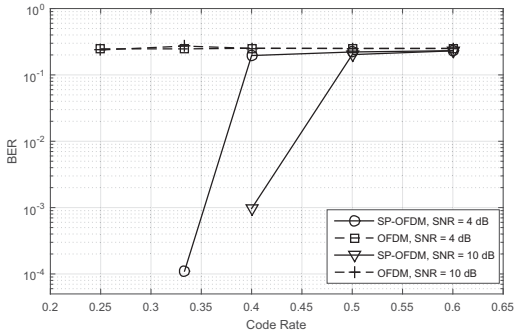

Fig. 3: BER performance comparison under disguised jamming in AWGN channels: SP-OFDM versus the traditional OFDM system, signal to jamming power ratio (SJR) = 0 dB.

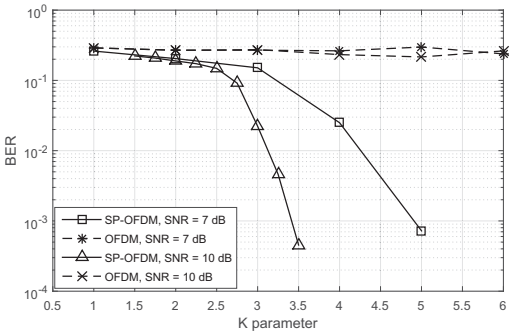

Fig. 4: BER performance comparison under disguised jamming in Rician channels: code rate $= 1/3$, SJR = 0 dB. Here the K parameter refers to the power ratio between the direct path and the scattered path.

This demonstrates that the proposed SP-OFDM system can achieve a positive deterministic channel coding capacity under disguised jamming.

Example 2: System performance under disguised jamming in Rician channels: In this example, we verify the effectiveness of the proposed system in fading channels. We consider a Rician channel, where the multipath interference is introduced and a strong line of sight (LOS) signal exists. The fading effect is slow enough so that the channel remains unchanged for one OFDM symbol duration. In the simulation, we set the power of the direct path of Rician channel to be 1 and vary the K parameter, which is the ratio between the power of the direct path and that of the scattered path. Fig. 4 shows the BERs for LDPC code rate $1/3$ under disguised jamming. It can be observed that the proposed system is still effective under the fading channel with a sufficient large K parameter. For a small K parameter, i.e., when the fading is severe, channel estimation and equalization will be needed to guarantee a reliable communication.

V. Conclusions

In this paper, we designed a highly secure and efficient OFDM system under disguised jamming, named securely precoded OFDM (SP-OFDM), by exploiting secure symbol-level precoding basing on phase randomization. We showed that, with the secure randomness shared between the authorized transmitter and receiver, the AVC channel corresponding to SP-OFDM is not symmetrizable, and hence SP-OFDM can achieve a positive deterministic coding capacity under disguised jamming. Both our theoretical and numerical results demonstrated that SP-OFDM is robust under disguised jamming and frequency selective fading.

References

[1] A. Lapidoth and P. Narayan, "Reliable communication under channel uncertainty," *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2148–2177, Oct 1998.

[2] T. Song, K. Zhou, and T. Li, "CDMA system design and capacity analysis under disguised jamming," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2487–2498, Nov 2016.

[3] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping-part ii: Capacity analysis under disguised jamming," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 80–88, January 2013.

[4] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[5] T. Hwang, C. Yang, G. Wu, S. Li, and G. Y. Li, "OFDM and its wireless applications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 4, pp. 1673–1694, May 2009.

[6] A. J. Viterbi, *CDMA: Principles of Spread Spectrum Communication*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1995.

[7] L. Lightfoot, L. Zhang, J. Ren, and T. Li, "Secure collision-free frequency hopping for OFDMA-based wireless networks," *EURASIP J. Adv. Signal Process*, vol. 2009, pp. 1:1–1:11, Mar. 2009.

[8] T. Song, Z. Fang, J. Ren, and T. Li, "Precoding for OFDM under disguised jamming," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 3958–3963.

[9] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: positivity, constraints," *IEEE Transactions on Information Theory*, vol. 34, no. 2, pp. 181–193, Mar 1988.

[10] R. Ahlswede, "Elimination of correlation in random codes for arbitrarily varying channels," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 44, no. 2, pp. 159–175, 1978.

[11] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacities of certain channel classes under random coding," *Ann. Math. Statist.*, vol. 31, no. 3, pp. 558–567, 09 1960.

[12] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping-part i: System design," *IEEE Transactions on Wireless Communications*, vol. 12, no. 1, pp. 70–79, January 2013.

[13] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Alpha Press, 2009.

[14] J. R. Barry, D. G. Messerschmitt, and E. A. Lee, *Digital Communication: Third Edition*. Norwell, MA, USA: Kluwer Academic Publishers, 2003.

[15] A. Klenke, *Probability Theory: A Comprehensive Course*. Springer, 2008.

[16] I. Csiszar, "Arbitrarily varying channels with general alphabets and states," *IEEE Transactions on Information Theory*, vol. 38, no. 6, pp. 1725–1742, Nov 1992.

[17] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Transactions on Information Theory*, vol. 31, no. 1, pp. 42–48, Jan 1985.

[18] J. M. Borden, D. M. Mason, and R. J. McEliece, "Some information theoretic saddlepoints," *SIAM Journal on Control and Optimization*, vol. 23, no. 1, pp. 129–143, 1985.

[19] D. Du and P. Pardalos, *Minimax and Applications*. Springer US, 1995.

[20] A. Morello and V. Mignone, "DVB-S2: The second generation standard for satellite broad-band services," *Proceedings of the IEEE*, vol. 94, no. 1, pp. 210–227, Jan 2006.

[21] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of sum-product decoding of low-density parity-check codes using a Gaussian approximation," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 657–670, Feb 2001.