Secure OFDM System Design and Capacity Analysis Under Disguised Jamming

Yuan Liang, Jian Ren, *Senior Member, IEEE*, and Tongtong Li

***Abstract*— In this paper, we propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming, where the jammer intentionally misleads the receiver by mimicking the characteristics of the authorized signal and causes complete communication failure. More specifically, we bring off a dynamic constellation by introducing secure randomness shared between the legitimate transmitter and receiver, and hence, break the symmetricity between the authorized signal and the disguised jamming. We analyze the channel capacities of both the traditional OFDM and SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It is shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming. On the other hand, due to the secure randomness shared between the authorized transmitter and receiver, SP-OFDM can achieve a positive capacity under disguised jamming since the AVC channel corresponding to SP-OFDM is not symmetrizable. A remarkable feature of the proposed SP-OFDM scheme is that while achieving strong jamming resistance, it has roughly the same high spectral efficiency as the traditional OFDM system. The robustness of the proposed SP-OFDM scheme under disguised jamming is demonstrated through both theoretic and numerical analyses.**

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

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. Along with the wide spread of various wireless devices, especially with the advent of user configurable intelligent devices, jamming attack is no longer limited to battlefield or military related events, but has become an urgent and serious threat to civilian communications as well.

In literature [1]–[4], jamming has widely been modeled as Gaussian noise. Based on the noise jamming model and the Shannon capacity formula, $C = B\log(1 + SNR)$, an intuitive impression is that jamming is really harmful only when the jamming power is much higher than the signal power. However, this is only partially true. More recently, it has been found that disguised jamming [5]–[8], where the jamming is highly correlated with the signal, and has a power level close or equal to the signal power, can be much more destructive than the noise jamming; it can reduce the system capacity to zero even when the jamming power equals the signal power. Consider the following example:

$$R = S + J + N$$

where S is the authorized signal, J the jamming interference, N the noise independent of J and S, and R 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 [9, 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 [10], such as LTE and WiMax. However, unlike the spread spectrum techniques [11], OFDM mainly relies on channel coding for communication reliability under hostile jamming, and has very limited built-in resilience against jamming attacks [12]–[18]. For example, in [12], the bit error rate (BER) performance of the traditional OFDM was explored under full-band and partial band Gaussian jamming, as well as multitone jamming. It was shown that OFDM is quite fragile under jamming, as BER can go above 10^{-1} when the jamming power is the same as the signal power. In addition, OFDM systems have strict requirements on synchronization and channel estimation accuracy. As the OFDM signal formats of many popular communication standards are public, the attackers can utilize the public signal formats to paralyze the synchronization and channel estimation process of OFDM systems, e.g., the *protocol-aware jamming and RF spoofing attacks* [19]–[21]. For example, in [15]–[17], the jamming attacks aiming at the pilots in OFDM systems were studied. It was shown that when the system standard is public and no encryption is applied to the transmitted symbol sequence, pilot attacks can completely nullify the channel estimation and synchronization of OFDM, and hence result in complete communication failure.

To improve the accuracy of synchronization and channel estimation in OFDM, [22] proposed an adaptive synchronization algorithm to combat narrow-band noise jamming attacks in the context of LTE systems. To mitigate the jamming

Manuscript received January 25, 2019; revised June 3, 2019; accepted July 8, 2019. Date of publication July 17, 2019; date of current version September 24, 2019. This work was supported in part by NSF under Award ECCS 1744604. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Georges Kaddoum. *(Corresponding author: Tongtong Li.)*

The authors are with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824 USA (e-mail: liangy11@egr.msu.edu; renjian@egr.msu.edu; tongli@egr.msu.edu).

Digital Object Identifier 10.1109/TIFS.2019.2929449

interference on the pilot symbols in OFDM, [23] proposed a pilot randomization scheme and showed that under strong jamming power, the proposed scheme could outperform the existing OFDM. To combat the pilot spoofing attacks, [24], [25] proposed to use pilot precoding for channel estimation in multi-user OFDM systems. The pilot precoding schemes in [23]–[25] assumed perfect synchronization between the transmitter and receiver, which is, in fact, quite vulnerable to jamming or spoofing attacks [19], [20].

In [14], the anti-jamming performance of Frequency Hopped (FH) OFDM system was explored. Like the traditional FH system, this approach achieves jamming resistance through large frequency diversity and sacrifices the spectral efficiency of OFDM. In [18], a collision-free frequency hopping (CFFH) scheme was proposed, where the basic idea was to randomize the jamming interference through frequency domain interleaving based on secure, collision-free frequency hopping. The most significant feature of CFFH based OFDM is that it is very effective under partial band jamming, and at the same time, has the same spectral efficiency as the original OFDM. However, CFFH based OFDM is still fragile under *disguised jamming* [6]–[8], [26].

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. As OFDM being identified as a major modulation technique for the 5G systems, there is an ever increasing need on the development of secure and efficient OFDM systems that are reliable under hostile jamming, especially the destructive disguised jamming.

If we examine disguised jamming carefully, we can see that the main issue there is the symmetricity between the authorized signal and the jamming interference. Intuitively, to design the corresponding anti-jamming system, the main task is to break the symmetricity between the authorized signal and the jamming interference, or make it impossible for the jammer to achieve this symmetricity. For this purpose, encryption or channel coding at the bit level will not really help, since the symmetricity appears at the symbol level. That is, instead of using a fixed symbol constellation, we have to introduce secure randomness to the constellation, and utilize a dynamic constellation scheme, such that the jammer can no longer mimic the authorized user's signal. At the same time, the authorized user does not have to sacrifice too much on the performance, efficiency and system complexity.

Motivated by the observations above and our previous research on anti-jamming system design [6]–[8], [18], [27], in this paper, we propose a securely precoded OFDM (SP-OFDM) system for efficient and reliable transmission under disguised jamming. By integrating advanced cryptographic techniques into OFDM transceiver design, 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. A remarkable feature of the proposed SP-OFDM scheme is that it achieves strong jamming resistance, but has the same high spectral efficiency as the traditional OFDM system. Moreover, the change to the physical layer transceivers is minimal, feasible and affordable. The robustness of the proposed SP-OFDM scheme under disguised jamming is demonstrated through both theoretic and numerical analyses.

More specifically, the main contributions of this paper can be summarized as follows:

- We design 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. The basic idea is to randomize the phases of transmitted symbols using the secure PN sequences generated from the Advanced Encryption Standard (AES) algorithm. The security is guaranteed by the secret key shared only between the legitimate transmitter and receiver. While SP-OFDM achieves strong jamming resistance, it does not introduce too much extra coding redundancy into the system and can achieve roughly the same spectral efficiency as the traditional OFDM system.
- We identify the vulnerability of the synchronization algorithm in the original OFDM system under disguised jamming, and propose a secure synchronization scheme for SP-OFDM which is robust against disguised jamming. In the proposed synchronization scheme, we design an encrypted cyclic prefix (CP) for SP-OFDM, and the synchronization algorithm utilizes the encrypted CP as well as the precoded pilot symbols to estimate time and frequency offsets in the presence of jamming.
- We analyze the channel capacity of the traditional OFDM and the proposed SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It is shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming. At the same time, 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 capacity under disguised jamming. Note that the authorized user aims to maximize the capacity while the jammer aims to minimize the capacity, we show that the maximin capacity for SP-OFDM under hostile jamming is given by $C = \log\left(1 + \frac{P_S}{P_J + P_N}\right)$ bits/symbol, where P_s denotes the signal power, P_J the jamming power and P_N the noise power.

Numerical examples are provided to demonstrate the effectiveness of the proposed system under disguised jamming and channel fading. Potentially, SP-OFDM is a promising modulation scheme for high-speed transmission under hostile environments. Moreover, it should be pointed out that the secure precoding scheme proposed in this paper can also be applied to modulation techniques other than OFDM.

The rest of this paper is organized as follows. The design of the proposed SP-OFDM system is described in Section II. The synchronization procedure of SP-OFDM is presented in Section III. The symmetricity analysis and capacity evaluation

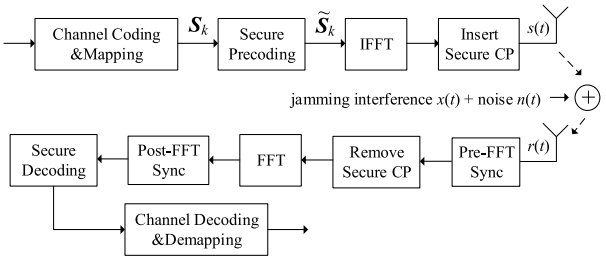

Fig. 1. Anti-jamming OFDM design through secure precoding and decoding.

of SP-OFDM are presented in Section IV. Numerical examples are provided in Section V and we conclude in Section VI.

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 $i = 0, 1, \cdots, N_c - 1$ and $k \in \mathbb{Z}$, let $S_{k,i} \in \Phi$ denote the symbol transmitted on the i-th carrier of the k-th OFDM block.[1] 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.

As pointed out in [7], [27]–[29], 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.,

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

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, a random phase shift is applied to each transmitted symbol; more specifically, for $i = 0, 1, \cdots, N_c - 1$ and $k \in \mathbb{Z}$, 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

[1] In literature, the term *OFDM symbol* is often used to denote the symbol block transmitted in one OFDM symbol period. In this paper, to avoid the ambiguity with the data symbols transmitted at each subcarrier, we choose to use the term *OFDM block* instead.

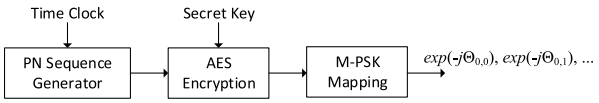

Fig. 2. Secure phase shift generator.

phase shift generator consists of three parts: (i) a pseudo-noise (PN) sequence generator; (ii) an Advanced Encryption Standard (AES) [30] 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. To facilitate the synchronization process, the PN sequence generator is initialized in the following way: each party is equipped with a global time clock, and the PN sequence generators 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. The security, as well as the randomness of the generated phase shift sequence, are guaranteed by the AES encryption algorithm [30], for which the secret encryption key is only shared between the authorized transmitter and receiver. Hence, 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 body of OFDM block through IFFT, whose duration is T_s. The security of the proposed system lies in the privacy of the secret key. Therefore, for best jamming resilience, the secret key should be updated regularly; the secret key can be delivered either through an independent and secure channel or in the data flow of the proposed system with encryption applied in the upper layers.

In OFDM transceiver design, the synchronization module plays a crucial role: OFDM requires both accurate time and frequency synchronization to avoid inter-symbol interference (ISI) and inter-carrier interference (ICI). In SP-OFDM, we propose a cyclic prefix (CP) based synchronization algorithm, as in traditional OFDM. However, SP-OFDM differs in that its CP is encrypted to ensure the security under disguised jamming.

B. Cyclic Prefix Design With Secure Precoding

In traditional OFDM, CP has three major functions: (i) eliminating the ISI between neighboring blocks; (ii) converting the linear convolution of OFDM block body with the channel impulse response into circular convolution under multi-path channel fading; and (iii) eliminating the ICI introduced by multipath propagation. As CP is a copy of the tail of OFDM block body, we can calculate the correlation between CP and the tail of OFDM block to estimate the starting point of each OFDM block [31] when disguised jamming is absent.

However, as to be shown in Section III, the traditional CP based synchronization is fragile under disguised jamming.

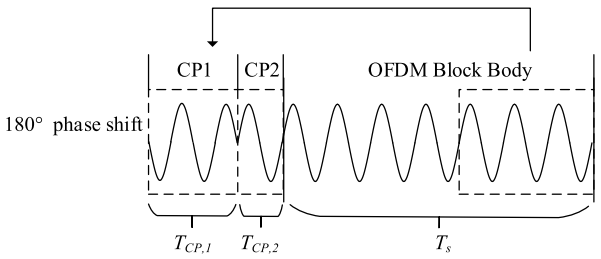

Fig. 3. An OFDM waveform example with secure cyclic prefix, illustrated with a 180° phase shift on CP1.

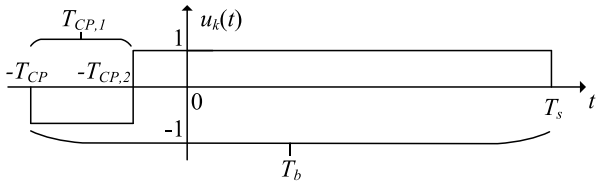

Fig. 4. The waveform of $u_k(t)$ with $C_k = -1$.

As shown in Fig. 3, to ensure the robustness of synchronization, in SP-OFDM, we apply a secure phase shift to part of the CP for each OFDM block. More specifically, the CP of each OFDM block is divided into two parts: for the first part, with a duration of $T_{CP,1}$, a secure phase shift is applied to the signal. We name this part of CP as CP1; while for the second part, which is of length $T_{CP,2}$, no special processing is applied. We name the second part as CP2. CP1 is used for effective synchronization under disguised jamming; CP2 maintains the functions of the original CP. To avoid ISI and ICI, both $T_{CP,1}$ and $T_{CP,2}$ are chosen to be longer than the maximum delay spread of the channel.

To ensure the security, the phase shift applied to CP1 is encrypted and varies for each OFDM block. The corresponding secure phase shift sequence can be generated using the same phase shift generator proposed in Fig. 2, with a much lower generation rate, since only one phase shift symbol is needed per OFDM block. Let $s_k(t)$ denote signal of the k-th OFDM block in the time domain by aligning the beginning of the OFDM block body at $t = 0$, and C_k denote the phase shift symbol applied to its CP1; let $u(t)$ be the unit step function, $T_{CP} = T_{CP,1} + T_{CP,2}$ and T_s denote the duration of OFDM block body. Define function $u_k(t)$ as

$$u_k(t) \triangleq C_k[u(t + T_{CP}) - u(t + T_{CP,2})] + u(t + T_{CP,2}) - u(t - T_s). \quad (3)$$

An example of $u_k(t)$ with $C_k = -1$ is plotted in Fig. 4. For SP-OFDM with secure CP, $s_k(t)$ can be expressed as

$$s_k(t) = \frac{1}{N_c} \sum_{i=0}^{N_c-1} \tilde{S}_{k,i} e^{j\frac{2\pi i}{T_s}t} u_k(t), \quad (4)$$

where $\tilde{S}_{k,i} = S_{k,i} e^{-j\Theta_{k,i}}$. Let $T_b = T_s + T_{CP}$ denote the duration of an OFDM block. Then the entire OFDM signal in the time domain can be expressed as

$$s(t) = \sum_{k=-\infty}^{\infty} s_k(t - kT_b). \quad (5)$$

Even though the receiver can generate identical phase shift sequences used in CP1 generation from the design of Fig. 2, there will still be an offset between the two generated sequences considering the delays in communication and the mismatch between the time clocks. Let C_k and $\tilde{C}_k$ denote the phase shift symbols generated at the transmitter and receiver respectively, and we have

$$C_k = \tilde{C}_{k+k_0}, \quad \forall k. \quad (6)$$

Since the phase shift sequences are generated from the global time clock, the offset k_0 is bounded. The offset k_0 can be estimated by the synchronization module at the receiver. Note that synchronization is needed for the precoding matrix sequence $\boldsymbol{P}_k$ as well; for the ease of synchronization, we pair the CP phase shift symbol C_k with the precoding matrix $\boldsymbol{P}_k$ for each OFDM block k; that is, for each CP phase shift symbol generated, we generate N_c phase shift symbols in parallel as the sub-carrier phase shifts. In this way, the two phase shift sequences are synchronized, in the sense that once the synchronization on the CP phase shift sequence is obtained, the synchronization on the precoding matrices is achieved automatically.

C. 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 $n(t)$, and an additive jamming interference $x(t)$. The received OFDM signal can be expressed as

$$r(t) = s(t - t_0)e^{j(\omega_0 t + \phi_0)} + x(t) + n(t), \quad (7)$$

where t_0, ω_0 and ϕ_0 denote the time, frequency and phase offsets between the transmitter and receiver, respectively. Without loss of generality, we can assume that $t_0 \in [0, T_b)$.

As in the traditional OFDM system, the synchronization module of SP-OFDM consists of two stages: a *pre-FFT synchronization*, which makes use of the correlation between the secure CP and the OFDM body tail to roughly estimate the offsets, and a *post-FFT synchronization*, which makes use of the pilot symbols inserted to certain sub-carriers to obtain a fine estimation. The phase shift offset k_0 is also estimated in the pre-FFT stage. The detailed algorithm and analysis on the synchronization of SP-OFDM will be presented in Section III.

The demodulation module at the receiver will crop the CP to obtain the body of each OFDM block, and apply FFT to obtain the frequency component at each sub-carrier. Under perfect synchronization, the received signal of the k-th OFDM block body can be expressed as

$$r_k(t) = s_k(t) + x_k(t) + n_k(t), \quad t \in [0, T_s), \quad (8)$$

where $x_k(t)$ and $n_k(t)$ are the jamming interference and noise overlaid on the k-th OFDM block, respectively. The frequency

components of jamming and noise can be calculated as

$$J_{k,i} = \sum_{m=0}^{N_c-1} x_k(\frac{mT_s}{N_c})e^{-j\frac{2\pi i}{N_c}m}, \quad i = 0, 1, \cdots, N_c - 1, \tag{9}$$

$$\bar{N}_{k,i} = \sum_{m=0}^{N_c-1} n_k(\frac{mT_s}{N_c})e^{-j\frac{2\pi i}{N_c}m}, \quad i = 0, 1, \cdots, N_c - 1, \tag{10}$$

where $\frac{T_s}{N_c}$ is the sampling interval. For an AWGN channel, $\bar{N}_{k,i}$'s are i.i.d. circularly symmetric complex Gaussian random variables with variance σ^2. After applying 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,

$$\tilde{\boldsymbol{R}}_k = \boldsymbol{P}_k \boldsymbol{S}_k + \boldsymbol{J}_k + \bar{\boldsymbol{N}}_k. \tag{11}$$

where

$$\boldsymbol{J}_k = [J_{k,0}, J_{k,1}, \cdots, J_{k,N_c-1}]^T, \tag{12}$$

and

$$\bar{\boldsymbol{N}}_k = [\bar{N}_{k,0}, \bar{N}_{k,1}, \cdots, \bar{N}_{k,N_c-1}]^T. \tag{13}$$

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

$$\boldsymbol{R}_k = \boldsymbol{S}_k + \boldsymbol{P}_k^{-1}\boldsymbol{J}_k + \boldsymbol{P}_k^{-1}\bar{\boldsymbol{N}}_k, \tag{14}$$

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

$$R_{k,i} = S_{k,i} + e^{j\Theta_{k,i}}J_{k,i} + N_{k,i}, \tag{15}$$

where $N_{k,i} = e^{j\Theta_{k,i}}\bar{N}_{k,i}$, and $\Theta_{k,i}$ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, \cdots, M-1\}$. Note that for any circularly symmetric Gaussian random variable N, $e^{j\theta}N$ and N have the same distribution for any angle θ [32, p66]; that is, $N_{k,i}$ is still a circular symmetric complex Gaussian random variable of zero-mean and variance σ^2.

Attacker model: In this paper, we have the following assumptions on the jammer:

- The jammer is fully aware of the transmission protocol and transceiver structures of the legitimate users. The jammer is capable of generating an interference with the same format as the legitimate signal, but the secret key shared between the transmitter and receiver is unavailable to the jammer.
- The jamming has a finite power constraint.
- The delay for the jammer to extract the received authorized CP phase shift C_k and then transmit a disguised CP is greater than the maximum offset of the global time clocks between the transmitter and receiver. In addition, it is impossible for the jammer to extract symbol sequence $\{\tilde{S}_{k,i}\}$, then transmit the opposite signal $\{-\tilde{S}_{k,i}\}$ in perfect synchronization with the authorized sequence $\{\tilde{S}_{k,i}\}$, such that $\{\tilde{S}_{k,i}\}$ is nullified or canceled completely. This is a reasonable assumption due to the existence of transmission and processing delays in the communication systems.

In the theoretical analysis of this paper, we make no assumptions on the form of jamming interference except certain power constraints; so the results apply to general jamming attacks. In the numerical results of this paper, the disguised jamming interference is generated with the same transmitter and transmission power as the legitimate user, except with a different secret key from the legitimate one.

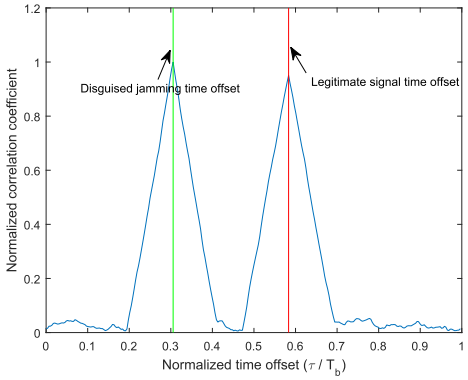

Fig. 5. Correlation coefficients of the original OFDM under disguised jamming.

III. Synchronization in SP-OFDM Under Disguised Jamming

In this section, first, we show the vulnerability of the synchronization process in tradition OFDM under disguised jamming attacks; then we propose the synchronization algorithm of SP-OFDM and prove its effectiveness under hostile jamming.

In modern OFDM systems, there are generally two kinds of approaches to achieve signal synchronization: (i) making use of the correlation between the CP and the tail of each OFDM block [31]; or (ii) inserting certain training symbols in every OFDM frame [33]. However, neither of these two approaches is robust under malicious jamming, especially disguised jamming, where the jammer modulates the interference with OFDM and deceive the receiver into synchronizing with the disguised jamming instead of the legitimate signal. For the training sequence based synchronization approach, even if the training sequence is not public, there is still a chance for the jammer to eavesdrop on the training sequence, and then generate the OFDM modulated disguised jamming with the true training sequence.

Synchronization of traditional OFDM under disguised jamming: To demonstrate the damage of disguised jamming, we calculate the CP based correlation coefficients of the traditional OFDM signal at different time offsets in the AWGN channel under an OFDM modulated disguised jamming. We average the correlation coefficients over multiple OFDM blocks, and the result is shown in Fig. 5. *Without proper encryption applied to the signal, the legitimate signal and the jamming interference are completely symmetric; we can observe peaks of the correlation coefficients at two different time offsets, one corresponding to that of the legitimate signal and the other corresponding to that of the disguised jamming.* If the jamming power is the same as the signal power, then the probability that the receiver chooses to synchronize with jamming is 50%. Obviously, a complete communication failure occurs when the receiver chooses to synchronize with the

disguised jamming instead of the legitimate signal. Such a phenomenon was also observed in [21].

To address this problem, in the synchronization algorithm of SP-OFDM, we apply encrypted phase shifts to the subcarriers and CP. For the ease of analysis, in the following, we consider an AWGN channel model; the effectiveness of the proposed algorithm in multi-path fading channels will be verified through numerical analysis in Section V. Even though our goal is to guarantee the robustness of SP-OFDM under disguised jamming, in the following analysis, we do not assume any specific form on the jamming interference $x(t)$, that is, we prove the robustness of our algorithm under any form of jamming attacks. Without loss of generality, we denote the combined term of jamming and noise as $z(t) = x(t)+n(t)$, and the received signal can be expressed as

$$r(t) = s(t - t_0)e^{j(\omega_0 t+\phi_0)} + z(t). \tag{16}$$

A. Pre-FFT Synchronization

In the pre-FFT stage, we estimate the encrypted phase shift sequence offset k_0, time offset t_0 and the fractional part of $w_0T_s/2\pi$ for frequency offset w_0. Since the phase shift sequence C_k is generated from the global time clock, the receiver has rough bounds on k_0 relative to the arrival time of the signal. We denote the finite candidate set of offset k_0 by $\mathcal{K}$.

In the traditional OFDM system, the CP correlation based synchronization algorithm is derived from the maximum-likelihood (ML) rule [31], [34]. However, since the jamming distribution is unspecified in our case, the ML rule is not applicable. Instead, we prove the robustness of the synchronization algorithm of SP-OFDM using the Chebychev inequality [35, Theorem 5.11].

In the pre-FFT stage, the receiver calculates the following correlation coefficient

$$Y_k(\tau, d) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} r(t)r^*(t + T_s)\tilde{C}^*_{k+d}\mathrm{d}t, \quad k \in \mathbb{Z}^*, \tag{17}$$

for $\tau \in [0, T_b), d \in \mathcal{K}$. We have the following proposition on $Y_k(\tau, d)$, whose proof is given in the appendix.

Proposition 1: If the fourth moment of $z(t)$ is bounded for any time instant t, i.e., $\mathbb{E}\{|z(t)|^4\} < \infty, \forall t \in \mathbb{R}$, then as $K \to +\infty$, we have

$$\frac{1}{K}\sum_{k=0}^{K-1} Y_k(\tau, d) = \begin{cases} \frac{P_S}{N_c}\upsilon(\tau + T_b - t_0)e^{-j\omega_0 T_s}, & d = k_0 - 1, \\ \frac{P_S}{N_c}\upsilon(\tau - t_0)e^{-j\omega_0 T_s}, & d = k_0, \\ \frac{P_S}{N_c}\upsilon(\tau - T_b - t_0)e^{-j\omega_0 T_s}, & d = k_0 + 1, \\ 0, & otherwise, \end{cases} \tag{18}$$

almost surely (a.s.), where

$$\upsilon(\tau) \triangleq \begin{cases} \tau + T_{CP,1}, & -T_{CP,1} \le \tau < 0, \\ T_{CP,1} - \tau, & 0 \le \tau < T_{CP,1}, \\ 0, & otherwise, \end{cases} \tag{19}$$

and P_S is the average symbol power of constellation Φ.

Basing on Proposition 1, to estimate t_0 and k_0, we search for τ and d which can maximize $|\frac{1}{K}\sum_{k=0}^{K-1} Y_k(\tau, d)|$ for some K. Meanwhile, after we obtain t_0 and k_0, the phase of the average correlation coefficient $\frac{1}{K}\sum_{k=0}^{K-1} Y_k(t_0, k_0)$ is

$$-w_0T_s \mod 2\pi, \tag{20}$$

where we can estimate the fractional part of $w_0T_s/2\pi$ as well. In practice, the jamming interference should be peak power bounded considering the constraints in RF, so we can ensure that the fourth moment of $z(t)$ is bounded. The selection of K depends on the power and the form of the jamming interference. In Section V, we will show that under a disguised jamming, SP-OFDM is able to obtain relatively accurate estimation results with 25 to 30 OFDM blocks.

As in the traditional OFDM, the CP based synchronization is only able to provide a coarse estimation of time offset t_0, especially under multi-path fading, and it requires a fine estimation on the time offset at the post-FFT stage. In addition, from (21), it can be seen that even for a very minor estimation error on the carrier frequency, there still may be an essential phase offset. As long as the range of the time estimation error is smaller than the duration of CP2, without loss of generality, we can model the signal after pre-FFT synchronization as

$$r'(t) = s(t - t'_0)e^{j(\frac{2\pi(n_0+\zeta_0)}{T_s}t+\phi_0)} + z'(t), \tag{21}$$

where $z'(t)$ is the jamming interference after pre-FFT synchronization, $t'_0 \in [0, T_{CP,2})$ the remaining time offset, $2\pi(n_0 + \zeta_0)/T_s$ the remaining frequency offset, n_0 an integer and $|\zeta_0| \ll 1$.

B. Post-FFT Synchronization

In this stage, we first estimate $n_0 + \zeta_0$ after demodulating the synchronized signal $r'(t)$ in (21) using FFT. Suppose n_0 satisfies

$$N_l \le n_0 \le N_u, \tag{22}$$

where integers N_l and N_u are determined by the maximum frequency offset between the transmitter and receiver. Basing on (21), to demodulate the k-th OFDM block, the receiver applies FFT to signal $r'(t)$ within interval $[kT_b, kT_b+T_s)$. The received signal of k-th OFDM block after alignment can be expressed as

$$r'_k(t) = s_k(t - t'_0)e^{j(\frac{2\pi(n_0+\zeta_0)}{T_s}t+\phi_k)} + z'_k(t), \quad t \in [0, T_s), \tag{23}$$

where

$$\phi_k = \phi_0 + \frac{2\pi(n_0 + \zeta_0)T_b}{T_s}k, \tag{24}$$

and

$$z'_k(t) = z'(t + kT_b). \tag{25}$$

Considering the frequency offset n_0, the receiver samples the received signal with a sampling frequency $\frac{N_c+N_u-N_l}{T_s}$. Let

$N_c' \triangleq N_c + N_u - N_l$. For $0 \le i < N_c'$, the FFT applied to $r_k'(t)$ can be expressed as

$$R_k(i) = \sum_{m=0}^{N_c'-1} r_k'(\frac{mT_s}{N_c'}) e^{-j\frac{2\pi i}{N_c'}m} = \frac{e^{j\phi_k}}{N_c} \sum_{i'=0}^{N_c'-1} \tilde{S}_{k,i'} \frac{e^{-j\frac{2\pi t_0'}{T_s}i'}(1-e^{j2\pi\zeta_0})}{1-e^{j\frac{2\pi(n_0+\zeta_0+i'-i)}{N_c'}}} + Z_k'(i), \quad (26)$$

where

$$Z_k'(i) = \sum_{m=0}^{N_c'-1} z_k'(\frac{mT_s}{N_c'}) e^{-j\frac{2\pi i}{N_c'}m}. \quad (27)$$

Since we assume $|\zeta_0| \ll 1$, for $0 \le i < N_c'$, we can neglect the ICI in (26) and approximate $R_k(i)$ as

$$R_k(i) = \frac{N_c'}{N_c} e^{j\phi_k} e^{-j\frac{2\pi t_0'}{T_s}[(i-n_0) \mod N_c']} \tilde{S}_{k,i-n_0}' + Z_k'(i), \quad (28)$$

where

$$\tilde{S}_{k,i}' = \begin{cases} \tilde{S}_{k,\ (i \mod N_c')}, & 0 \le i \mod N_c' < N_c, \\ 0, & \text{otherwise.} \end{cases} \quad (29)$$

The post-FFT synchronization generally utilizes the pilot symbols inserted at certain sub-carriers. For the ease of analysis, we assume a pilot symbol $\boldsymbol{p}$ is placed at sub-carrier i_p of each OFDM block. Note that, as the precoding matrix sequence is synchronized with the CP phase shift sequence, the precoding matrix sequence is synchronized at the receiver after pre-FFT synchronization. We calculate the following correlation coefficients for each OFDM block k:

$$\Gamma_k(i) \triangleq R_k(i) R_{k+1}^*(i) e^{j(\Theta_{k,i_p} - \Theta_{k+1,i_p})}. \quad (30)$$

We have the following proposition on $\Gamma_k(i)$.

Proposition 2: If the fourth moment of $z(t)$ is bounded for any time t, then as $K \to +\infty$, we have

$$\frac{1}{K}\sum_{k=0}^{K-1} \Gamma_k(i) = \begin{cases} \left(\frac{N_c'}{N_c}\right)^2 e^{j\frac{2\pi(n_0+\zeta_0)T_b}{T_s}} |\boldsymbol{p}|^2, & i = n_0 + i_p \mod N_c', \\ 0, & \textit{otherwise}, \end{cases} \ a.s.. \quad (31)$$

Proof: Note that $\Gamma_k(i)$ can be derived as

$$\Gamma_k(i) = [(N_c'/N_c)^2 e^{j\frac{2\pi(n_0+\zeta_0)T_b}{T_s}} \tilde{S}_{k,i-n_0}' \tilde{S}_{k+1,i-n_0}'^* + \frac{N_c'}{N_c} e^{j\phi_k} \tilde{S}_{k,i-n_0}' Z_{k+1}'^*(i) + \frac{N_c'}{N_c} e^{j\phi_{k+1}} \tilde{S}_{k+1,i-n_0}'^* Z_k'(i) + Z_k'(i) Z_{k+1}'^*(i)] e^{j(\Theta_{k,i_p} - \Theta_{k+1,i_p})}. \quad (32)$$

Since the phase shifts $\Theta_{k,i}$'s are independent across the sub-carriers, following the approach in the pre-FFT analysis, we have

$$\mathbb{E}\{\Gamma_k(i)\} = \begin{cases} \left(\frac{N_c'}{N_c}\right)^2 e^{j\frac{2\pi(n_0+\zeta_0)T_b}{T_s}} |\boldsymbol{p}|^2, & i = n_0 + i_p \mod N_c', \\ 0, & \text{otherwise.} \end{cases} \quad (33)$$

while the variance of $\frac{1}{K}\sum_{k=0}^{K-1} \Gamma_k(i)$ converges to 0 as $K \to +\infty$. Therefore (31) is obtained accordingly. We skip the details here for brevity. □

Following Proposition 2, n_0 can be estimated by finding the i which maximizes $\frac{1}{K}\sum_{k=0}^{K-1} \Gamma_k(i)$. With the n_0 obtained, we can further estimate the frequency estimation error ζ_0 in the pre-FFT stage by evaluating the phase of $\frac{1}{K}\sum_{k=0}^{K-1} \Gamma_k((n_0 + i_p) \mod N_c')$.

After n_0 is estimated, without loss of generality, we can assume $n_0 = 0$ in the following derivation. In terms of the time offset t_0', given two pilot symbols $\boldsymbol{p}_1$ and $\boldsymbol{p}_2$ located at sub-carriers i_{p_1} and i_{p_2}, respectively, we evaluate the following correlation coefficient for each OFDM block k:

$$\Upsilon_k(i_{p_1}, i_{p_2}) = R_k(i_{p_1}) R_k^*(i_{p_2}) \boldsymbol{p}_1^* \boldsymbol{p}_2 e^{j(\Theta_{k,i_{p_1}} - \Theta_{k,i_{p_2}})}, \quad (34)$$

and we have the following proposition.

Proposition 3: If the fourth moment of $z(t)$ is bounded for any time t, then as $K \to +\infty$, we have

$$\frac{1}{K}\sum_{k=0}^{K-1} \Upsilon_k(i_{p_1}, i_{p_2}) = \left(\frac{N_c'}{N_c}\right)^2 e^{-j\frac{2\pi t_0'}{T_s}(i_{p_1} - i_{p_2})} |\boldsymbol{p}_1|^2 |\boldsymbol{p}_2|^2, \ a.s. \quad (35)$$

The proof of Proposition 3 follows a similar approach as Proposition 1, and we skip it for brevity. Note that $t_0' \in [0, T_{CP,2})$, so t_0' can be estimated from the phase of $\frac{1}{K}\sum_{k=0}^{K-1} \Upsilon_k(i_{p_1}, i_{p_2})$. Likewise, the phase offset ϕ_0 can be estimated by averaging $R_k(i_p) e^{j\Theta_{k,i_p}}$ after compensating for the frequency offset.

Discussions: Note that under disguised jamming, the estimator averages multiple OFDM blocks to make use of the encrypted signal for an accurate synchronization. In practice, estimation errors always exist in synchronization, so the receiver has to keep track of all the offsets, which can be implemented by the moving average approach.

The pre-FFT synchronization exploits the correlation between secure CP and the OFDM body tail. The data-aided synchronization approach, i.e., inserting independent training sequence in each OFDM frame, is still an option under disguised jamming if encryption is applied to the training sequence. However, the CP based approach experiences less delay in synchronization. By inserting secure CP for each OFDM block, it is easier to keep track of the time offset continuously.

In the post-FFT stage, inserting more pilots can accelerate the synchronization process; meanwhile, under fading channels, the channel estimation process necessitates pilot symbols over different sub-carrier locations. Channel estimation can be implemented by averaging the received pilot symbols at each sub-carrier location following the approach in synchronization. However, an important point here is that for time varying channels, the duration of the OFDM blocks used for averaging should be shorter than the channel coherence time so that the channel does not change significantly during each estimation. This is guaranteed in practical systems where the whole OFDM frame duration is shorter than the channel coherence time [33].

IV. Symmetricity and Capacity Analysis Using the AVC Model

In this section, we analyze the symmetricity and capacity of the proposed SP-OFDM system using the arbitrarily varying channel (AVC) model. Recall that from Section II, under perfect synchronization, the equivalent channel model of SP-OFDM can be expressed as

$$R = S + e^{j\Theta} J + N, \tag{36}$$

where $S \in \Phi, J \in \mathbb{C}$, $N \sim \mathcal{CN}(0, \sigma^2 I)$, Θ is uniformly distributed over $\{\frac{2\pi i}{M} \mid i = 0, 1, \ldots, M-1\}$, and $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{\Sigma})$ denotes a circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and variance $\boldsymbol{\Sigma}$. For generality, in this section, we do not assume any *a priori* information on the jamming J, except a finite average power constraint of P_J, i.e., $\mathbb{E}\{|J|^2\} \leq P_J$. We will show that the AVC corresponding to SP-OFDM is nonsymmetrizable, and hence the AVC capacity of SP-OFDM is positive under disguised jamming.

A. AVC Symmetricity Analysis

The arbitrarily varying channel (AVC) model, first introduced in [29], characterizes the communication channels with unknown states which may vary in arbitrary manners across time. For the jamming channel (36) 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 [36]. 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 ([36], [37]): 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 (36) is symmetrizable iff for some auxiliary channel $\pi : \Phi \to \mathbb{C}$, $\forall \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C}$, we have

$$\int_{\mathbb{C}} W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{x}) dF_\pi(\boldsymbol{x}|\boldsymbol{s}') = \int_{\mathbb{C}} W(\boldsymbol{r} \mid \boldsymbol{s}', \boldsymbol{x}) dF_\pi(\boldsymbol{x}|\boldsymbol{s}), \tag{37}$$

where $F_\pi(\cdot|\cdot)$ is the probability measure of the output of channel π given the input, i.e., the conditional CDF

$$F_\pi(\boldsymbol{x}|\boldsymbol{s}) = \Pr\{Re(\pi(\boldsymbol{s})) \leq Re(\boldsymbol{x}), Im(\pi(\boldsymbol{s})) \leq Im(\boldsymbol{x})\}, \tag{38}$$

for $\boldsymbol{x} \in \mathbb{C}, \boldsymbol{s} \in \Phi$, 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 (36) by Π, that is,

$$\Pi = \left\{\pi \mid \text{ Eq. (37) is satisfied w.r.t. } \pi \ \forall \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C}\right\}. \tag{39}$$

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

Definition 2 ([37]): The AVC channel (36) is called l-symmetrizable under average jamming power constraint iff there exists a $\pi \in \Pi$ such that

$$\int_{\mathbb{C}} |\boldsymbol{x}|^2 dF_\pi(\boldsymbol{x}|\boldsymbol{s}) < \infty, \quad \forall \boldsymbol{s} \in \Phi. \tag{40}$$

In [37], it was shown that reliable communication can be achieved as long as the AVC channel is not l-symmetrizable.

Lemma 1 ([37, Corollary 2]): The deterministic coding capacity[2] of AVC channel (36) 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

$$C = \max_{\mathcal{P}_S} \min_{F_J} I(S, R), \quad s.t. \int_{\mathbb{C}} |\boldsymbol{x}|^2 dF_J(\boldsymbol{x}) \leq P_J, \tag{41}$$

where $I(S, R)$ denotes the mutual information (MI) between the R and S in (36), $\mathcal{P}_S$ denotes the probability distribution of S over Φ and $F_J(\cdot)$ the CDF of J.

First, we show that the traditional OFDM system is l-symmetrizable under disguised jamming.

Theorem 1: The traditional OFDM system is l-symmetrizable. Therefore, the deterministic coding capacity is zero under the worst disguised jamming with finite average jamming power.

Proof: The AVC model of the traditional OFDM system is

$$R = S + J + N. \tag{42}$$

We will show that when S and J have the same constellation Φ, hence the same finite average power, the AVC channel is l-symmetrizable. It follows from (42) that

$$W(\boldsymbol{r} \mid \boldsymbol{s}, \boldsymbol{s}') = W(\boldsymbol{r} \mid \boldsymbol{s}', \boldsymbol{s}), \quad \forall \boldsymbol{s}, \boldsymbol{s}' \in \Phi, \boldsymbol{r} \in \mathbb{C}. \tag{43}$$

Since Φ has finite average power, the average power constraint (40) is satisfied by disguised jamming. Hence, channel (42) is l-symmetrizable. From Lemma 1, a necessary condition for a positive AVC deterministic coding capacity is that the channel is not l-symmetrizable. So the traditional OFDM system has zero deterministic coding capacity under disguised jamming with finite average jamming power. □

Next, we show that with the proposed secure precoding, it is impossible to l-symmetrize the AVC channel (36) corresponding to the SP-OFDM system.

Theorem 2: The AVC channel corresponding to the proposed SP-OFDM is not l-symmetrizable.

Proof: We prove this result by contradiction. Suppose that there exists a channel $\pi \in \Pi$ such that the AVC channel is l-symmetrizable. Denote the output of channel π given input

[2]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 [38].

$\boldsymbol{x}$ by $\pi(\boldsymbol{x})$, and define the corresponding AVC channel output for inputs $\boldsymbol{s}$ and $\boldsymbol{s}'$ as

$$\hat{R}(\boldsymbol{s}, \boldsymbol{s}') = \boldsymbol{s} + \pi(\boldsymbol{s}')e^{j\Theta} + N, \tag{44}$$

where $\hat{R}(\boldsymbol{s}, \boldsymbol{s}')$ denotes the channel output. Following (37), $\hat{R}(\boldsymbol{s}, \boldsymbol{s}')$ and $\hat{R}(\boldsymbol{s}', \boldsymbol{s})$ have the same distribution. Let $\varphi_X(\omega_1, \omega_2)$ denote the characteristic function (CF) of a complex random variable X. So we have

$$\varphi_{\hat{R}(\boldsymbol{s},\boldsymbol{s}')}(\omega_1, \omega_2) \equiv \varphi_{\hat{R}(\boldsymbol{s}',\boldsymbol{s})}(\omega_1, \omega_2), \tag{45}$$

and

$$\varphi_{\hat{R}(\boldsymbol{s},\boldsymbol{s}')}(\omega_1, \omega_2) = \varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}]}(\omega_1, \omega_2)\ \varphi_N(\omega_1, \omega_2), \tag{46}$$

where, for the complex Gaussian noise N, we have

$$\varphi_N(\omega_1, \omega_2) = e^{-\frac{\sigma^2}{4}(\omega_1^2+\omega_2^2)}, \quad \omega_1, \omega_2 \in (-\infty, +\infty), \tag{47}$$

which is non-zero over $\mathbb{R}^2$. Thus by eliminating the characteristic functions of the Gaussian noises on both sides of equation (45), we have

$$\varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}]}(\omega_1, \omega_2) = \varphi_{[\boldsymbol{s}'+\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2). \tag{48}$$

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

$$\varphi_{[\boldsymbol{s}+\pi(\boldsymbol{s}')e^{j\Theta}]}(\omega_1, \omega_2) = e^{js_1\omega_1 + js_2\omega_2}\varphi_{[\pi(\boldsymbol{s}')e^{j\Theta}]}(\omega_1, \omega_2), \tag{49}$$

and

$$\begin{aligned}\varphi_{[\pi(\boldsymbol{s}')e^{j\Theta}]}(\omega_1, \omega_2) &= \mathbb{E}\{e^{j\omega_1 Re(\pi(\boldsymbol{s}')e^{j\Theta}) + j\omega_2 Im(\pi(\boldsymbol{s}')e^{j\Theta})}\} \\ &= \int_{\mathbb{C}} \mathbb{E}\{e^{j\omega_1 Re(\boldsymbol{x}e^{j\Theta}) + j\omega_2 Im(\boldsymbol{x}e^{j\Theta})}\} \mathrm{d}F_\pi(\boldsymbol{x}|\boldsymbol{s}').\end{aligned} \tag{50}$$

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

$$\begin{aligned}&\mathbb{E}\{e^{j\omega_1 Re(\boldsymbol{x}e^{j\Theta}) + j\omega_2 Im(\boldsymbol{x}e^{j\Theta})}\} \\ &\quad= \frac{1}{M}\sum_{i=0}^{M-1} e^{j\omega_1|\boldsymbol{x}|\cos(\frac{2\pi i}{M}+\arg(\boldsymbol{x})) + j\omega_2|\boldsymbol{x}|\sin(\frac{2\pi i}{M}+\arg(\boldsymbol{x}))} \\ 7 &= \frac{2}{M}\sum_{i=0}^{M/2-1} \cos\{\omega_1|\boldsymbol{x}|\cos[2\pi i/M + \arg(\boldsymbol{x})] \\ &\quad + \omega_2|\boldsymbol{x}|\sin[2\pi i/M + \arg(\boldsymbol{x})]\},\end{aligned} \tag{51}$$

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 real-valued over $\mathbb{R}^2$. For $\boldsymbol{s} \neq \boldsymbol{s}'$ and $\boldsymbol{s}' = s_1' + js_2'$, $e^{j[(s_1-s_1')\omega_1 + (s_2-s_2')\omega_2]}$ 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 (48), (49) and (51), for $\omega_1 + \frac{s_2-s_2'}{s_1-s_1'}\omega_2 \neq \frac{n\pi}{s_1-s_1'}, \forall n \in \mathbb{Z}$, we have

$$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2) = 0. \tag{52}$$

On the other hand, the characteristic function of an RV should be uniformly continuous in the real domain [35, Theorem 15.21]. So for any fixed $\omega_2 \in (-\infty, \infty)$, we should have

$$\begin{aligned}&\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}\left(\frac{n\pi - (s_2 - s_2')\omega_2}{s_1 - s_1'}, \omega_2\right) \\ &\quad= \lim_{\omega_1 \to \frac{n\pi-(s_2-s_2')\omega_2}{s_1-s_1'}} \varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2), \quad \forall n \in \mathbb{Z}.\end{aligned} \tag{53}$$

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

$$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}\left(\frac{n\pi - (s_2 - s_2')\omega_2}{s_1 - s_1'}, \omega_2\right) = 0, \quad \forall n \in \mathbb{Z}. \tag{54}$$

Combining (52) and (54), we have

$$\varphi_{[\pi(\boldsymbol{s})e^{j\Theta}]}(\omega_1, \omega_2) = 0, \quad \forall \omega_1, \omega_2 \in (-\infty, \infty). \tag{55}$$

However, (55) cannot be a valid characteristic function for any RV. Therefore, the auxiliary channel π does not exist, and Π is empty. Hence, the AVC channel is not l-symmerizable. □

Following Lemma 1, the result in Theorem 2 implies that the proposed SP-OFDM will always have positive capacity under any hostile jamming with finite average power constraint. The next subsection is focused on how to calculate the channel capacity of SP-OFDM under hostile jamming.

B. Capacity Analysis

From Lemma 1, the capacity of channel $R = S + e^{j\Theta}J + N$ is given by

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

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 3: 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 (41) under average jamming power constraint P_J and noise power $P_N = \sigma^2$ is given by

$$C = \log\left(1 + \frac{P_S}{P_J + P_N}\right). \tag{56}$$

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

To prove Theorem 3, we need the following lemma [37, Lemma 4].

Lemma 2: Mutual information $I(S, R)$ is concave with respect to the input distribution $F_S(\cdot)$ and convex with respect to the jamming distribution $F_J(\cdot)$.

Proof: [Proof of Theorem 3] First, following Lemma 1 and Theorem 2, we can get that the deterministic coding capacity of SP-OFDM is positive under any hostile jamming.

Second, we will evaluate the channel capacity of SP-OFDM under hostile jamming. When the support of S is $\Phi = \mathbb{C}$, the whole complex plane, following Lemma 1, the channel capacity in (41) equals

$$C = \max_{F_S} \min_{F_J} I(S, R), \tag{57}$$

$$s.t. \int_{\mathbb{C}} |\boldsymbol{x}|^2 \mathrm{d}F_S(\boldsymbol{x}) \le P_S, \tag{58}$$

$$\int_{\mathbb{C}} |\boldsymbol{x}|^2 \mathrm{d}F_J(\boldsymbol{x}) \le P_J, \tag{59}$$

where $F_S(\cdot)$ denotes the CDF function of S defined on $\mathbb{C}$, and (58) and (59) denote the average power constraints on the input and the jamming, respectively.

We denote the $I(S, R)$ w.r.t the input distribution $F_S(\cdot)$ and the jamming distribution $F_J(\cdot)$ by $\phi(F_S, F_J)$. Following Lemma 2, $\phi(F_S, F_J)$ is concave w.r.t. $F_S(\cdot)$ and convex w.r.t. $F_J(\cdot)$. As shown in [39], if we can find the input distribution F_S^* and the jamming distribution F_J^* such that

$$\phi(F_S, F_J^*) \le \phi(F_S^*, F_J^*) \le \phi(F_S^*, F_J), \tag{60}$$

for any F_S and F_J satisfying the average power constraints (58) and (59), respectively, then

$$\phi(F_S^*, F_J^*) = C. \tag{61}$$

That is, the pair (F_S^*, F_J^*) is the saddle point of the max-min problem in equation (57) [40].

Assume the jamming interference is circularly symmetric complex Gaussian with average power P_J, that is, $F_J^* = \mathcal{CN}(0, P_J)$. Note that the phase shift would not change the distribution of a complex Gaussian RV, and the fact that the jamming J and the noise N are independent, hence the jammed channel in this case is equivalent to a complex AWGN channel with noise power $P_J + P_N$, where the capacity achieving input distribution is also a complex Gaussian with power P_S, that is, $F_S^* = \mathcal{CN}(0, P_S)$. It follows that for any input distribution F_S satisfying the power constraint P_S,

$$\phi(F_S, \mathcal{CN}(0, P_J)) \le \phi(\mathcal{CN}(0, P_S), \mathcal{CN}(0, P_J)). \tag{62}$$

On the other hand, when the input distribution is $F_S^* = \mathcal{CN}(0, P_S)$, the worst noise in terms of capacity for Gaussian input is Gaussian [9]. Since $e^{j\Theta}J + N$ is complex Gaussian with power $P_J + P_N$ if $F_J^* = \mathcal{CN}(0, P_J)$, then for any jamming distribution F_J satisfying the power constraint P_J,

$$\phi(\mathcal{CN}(0, P_S), \mathcal{CN}(0, P_J)) \le \phi(\mathcal{CN}(0, P_S), F_J). \tag{63}$$

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

$$C = \log\left(1 + \frac{P_S}{P_J + P_N}\right), \tag{64}$$

which completes the proof. □

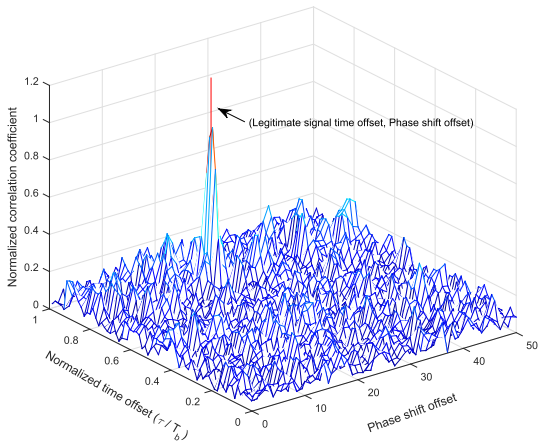

Fig. 6. Correlation coefficients of SP-OFDM at different time and phase shift sequence offsets under disguised jamming.

V. Numerical Results

In this section, we evaluate the synchronization and bit error rate (BER) performances of the proposed SP-OFDM system under disguised jamming attacks through numerical examples. Throughout this section, we consider the case where the malicious user generates disguised jamming using OFDM, with the same format and power level as that of the legitimate signal.

Example 1 (Synchronization Performance Under Disguised Jamming in AWGN Channels): In this example, we verify the robustness of SP-OFDM under disguised jamming in terms of synchronization for AWGN channels. The system parameters are listed in Table I. We first compute the average correlation coefficients at different time offsets and phase shift sequence offsets for the received signal as in (17), and the result is plotted in Fig. 6 for $K = 40$.[3] Here, K denotes the number of OFDM blocks used for estimation. It shows that with the secure precoding scheme, even under disguised jamming, the receiver is able to correctly estimate the time offset as well as the phase shift sequence offset of the legitimate signal. Then we simulate the synchronization accuracy of SP-OFDM by calculating the cumulative distribution functions (CDFs) of the estimation errors with different numbers of OFDM blocks K to average the correlation coefficients. We normalize the time offset by the duration of one OFDM block T_b and the frequency offset by the sub-carrier spacing $1/T_s$, and the results are shown in Fig. 7. It can be observed that under the given setup, with 25 OFDM blocks to compute the correlation coefficients, the synchronization algorithm is robust under disguised jamming, where 99% cases have less than 0.01 *normalized* time offset estimation errors and 98% cases have less than 0.04 *normalized* frequency offset estimation errors.

Example 2 (Synchronization Performance Under Disguised Jamming in Multi-Path Fading Channels): In this example, we simulate the synchronization accuracy of SP-OFDM under disguised jamming in static and time varying multi-

[3]In the 802.11a WLAN [33], 40 OFDM blocks correspond to 1440 data bytes with 64-QAM mapping, while the OFDM frame length can be as large as 2312 bytes.

TABLE I
SP-OFDM PARAMETERS IN NUMERICAL RESULTS (T_s: DURATION OF OFDM BODY)

Carrier number N_c	128	CP1 duration $T_{CP,1}$	$T_s/8$	CP2 duration $T_{CP,2}$	$T_s/16$
Number of candidate phase shift offset $\|\mathcal{K}\|$	50	Signal-to-noise ratio (dB)	15	Phase shift constellation size M	16

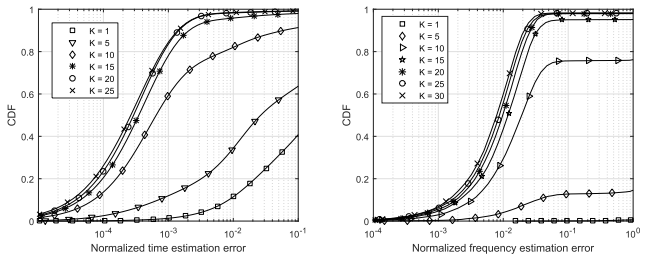

Fig. 7. The synchronization error distribution under AWGN channels with disguised jamming attack.

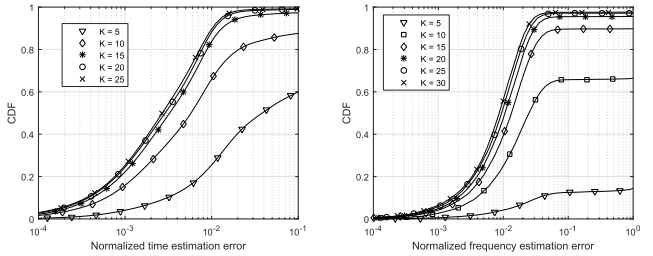

Fig. 8. The synchronization error distribution under static multi-path fading channels with disguised jamming attack.

path fading channels, which are modeled as 4 paths fading channels with a maximum delay spread of $3T_s/256$. Fig. 8 shows the estimation error distribution in the static channel. A slight performance loss is observed compared with the AWGN case, where 98% cases have less than 0.02 *normalized* time offset estimation errors and 96.5% cases have less than 0.04 *normalized* frequency offset estimation errors using 25 OFDM blocks in estimation. To demonstrate the effectiveness of the synchronization algorithm under slow time varying channels, we introduce a Doppler shift to each path with a maximum value of 2% sub-carrier spacing ($0.02/T_s$) in the multi-path fading channel. Fig. 9 shows the estimation error distribution under the time-varying multi-path fading channel, where around 98% cases have less than 0.02 normalized time offset estimation errors and 96.5% cases have less than 0.04 normalized frequency offset estimation errors using 30 OFDM blocks in estimation.

The simulation results illustrate the robustness of SP-OFDM synchronization against disguised jamming attacks under various channel conditions. This is because that: 1) in a static channel, the delay spread of multi-path fading would introduce certain inter-symbol interference (ISI) at the beginning of CP, though, the correlation of the remaining CP with the tail would not be affected by multi-path delay. As long as the duration of CP is much longer than the delay spread, the pre-FFT synchronization is still functional; for the post-FFT synchronization, multi-path fading would incur a channel gain being multiplied to the pilot symbol, which would not void

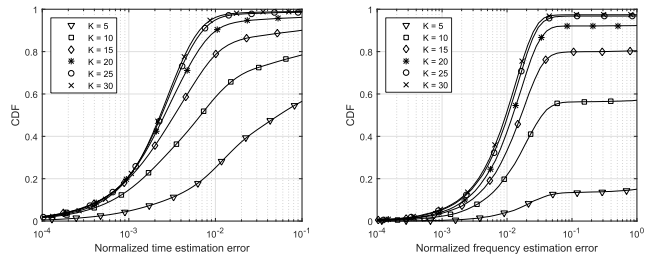

Fig. 9. The synchronization error distribution under time varying multi-path fading channels with disguised jamming attack.

the generality of the synchronization scheme. 2) In a time varying channel, as long as the channel coherence time is much longer than the duration of an OFDM block, i.e., the channel impulse response keeps relatively constant between two successive OFDM blocks, the correlation between CP and tail is still valid in the pre-FFT synchronization; for the post-FFT synchronization, since the correlation coefficient is calculated from the pilot symbols of two successive OFDM blocks, a strong correlation between the channel gains of two successive OFDM blocks would ensure the effectiveness of the synchronization scheme.

Example 3 (BER Performance Under Disguised Jamming in AWGN Channels): In this example, we analyze the bit error rate (BER) of the proposed system under disguised jamming in AWGN channels. Perfect synchronization is assumed. We use the low density parity check (LDPC) codes for channel coding, and adopt the parity check matrices from the DVB-S.2 standard [41]. 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 [42] 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 the disguised jamming, 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 distributions or mapping schemes, customized likelihood functions basing on the jamming distribution will be needed for the optimal performance. Fig. 10 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 dis-

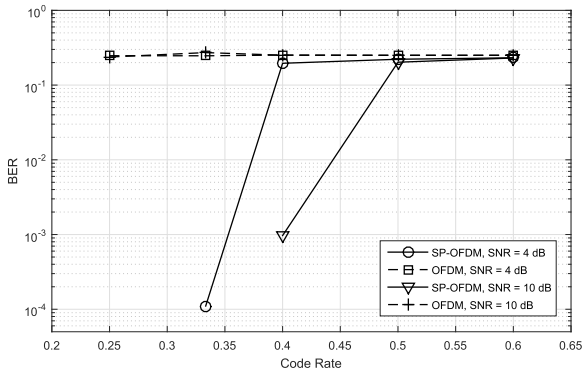

Fig. 10. BER performance comparison under disguised jamming in AWGN channels: SP-OFDM versus the traditional OFDM system, signal to jamming power ratio (SJR) = 0 dB.

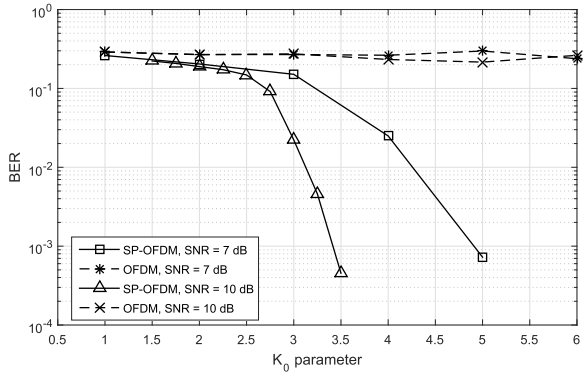

Fig. 11. BER performance comparison under disguised jamming in Rician channels: code rate = 1/3, SJR = 0 dB. Here the K_0 parameter refers to the power ratio between the direct path and the scattered path.

guised 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, the traditional OFDM cannot achieve reliable communications under disguised jamming; (ii) with the proposed SP-OFDM scheme, when the code rates are below certain thresholds, the BER can be significantly reduced with the decrease of code rates using the proposed secure precoding. This demonstrates that the proposed SP-OFDM system can achieve a positive deterministic channel coding capacity under disguised jamming.

Example 4 (BER 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 [43]. 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_0 parameter, which is the ratio between the power of the direct path and that of the scattered path. Fig. 11 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_0 parameter. For a small K_0 parameter, i.e., when the fading is severe, channel estimation and equalization will be needed to guarantee a reliable communication.

VI. Conclusion

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 demonstrated the destructive effect of disguised jamming on the traditional OFDM system, and proved the robustness of SP-OFDM against disguised jamming in terms of synchronization and channel capacity. First, we showed that the traditional OFDM cannot distinguish between the legitimate signal and disguised jamming in the synchronization process, while SP-OFDM, with the secure CP, can achieve accurate synchronization under disguised jamming. Second, we analyzed the channel capacity of the traditional OFDM and the proposed SP-OFDM under hostile jamming using the arbitrarily varying channel (AVC) model. It was shown that the deterministic coding capacity of the traditional OFDM is zero under the worst disguised jamming; on the other hand, 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 capacity under disguised jamming. Both our theoretical and numerical results demonstrated that SP-OFDM is robust under disguised jamming and frequency selective fading. Potentially, SP-OFDM is a promising modulation scheme for high-speed transmission under hostile environments, and the secure precoding scheme proposed in this paper can also be applied to modulation techniques other than OFDM.

Appendix
Proof of Proposition 1

Proof: Note that $r(t)r^*(t+T_s)$ can be calculated as

$$\begin{aligned} r(t)r^*(t+T_s) &= s(t-t_0)s^*(t+T_s-t_0)e^{-j\omega_0 T_s} \\ &\quad + z(t)s^*(t+T_s-t_0)e^{-j(\omega_0 t+\omega_0 T_s+\phi_0)} \\ &\quad + s(t-t_0)e^{j(\omega_0 t+\phi_0)}z^*(t+T_s) \\ &\quad + z(t)z^*(t+T_s). \end{aligned} \tag{65}$$

In the following we analyze the four terms on the right-hand-side (RHS) of (65) respectively.

First, define

$$Y_{k,1}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} s(t-t_0)s^*(t+T_s-t_0)\mathrm{d}t, \tag{66}$$

for $k \in \mathbb{Z}^*, \tau \in [0, T_b)$. We evaluate the expectation of $Y_{k,1}(\tau)\tilde{C}^*_{k+d}$ for $d \in \mathcal{K}$. Note that for $t \in [\tau - T_{CP} + kT_b, \tau - T_{CP,2} + kT_b]$, where $\tau \in [0, T_b)$, we have

$$s(t-t_0) = \sum_{l=k-1}^{k+1} s_l(t-t_0-lT_b), \tag{67}$$

$$s(t+T_s-t_0) = \sum_{l=k-1}^{k+1} s_l(t+T_s-t_0-lT_b). \tag{68}$$

Note that since the OFDM blocks are zero-mean and independent, for $k_1 \neq k_2$, we have

$$\mathbb{E}\left\{s_{k_1}(t_1)s_{k_2}^*(t_2)\right\} = 0, \quad \forall t_1, t_2 \in \mathbb{R}. \tag{69}$$

So we focus on

$$\begin{aligned}&\int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} \sum_{l=k-1}^{k+1} s_l(t-t_0-lT_b)s_l^*(t+T_s-t_0-lT_b)\ \mathrm{d}t \\ &= \frac{1}{N_c^2}\sum_{l=-1}^{1}\int_{\tau-lT_b-t_0-T_{CP}}^{\tau-lT_b-t_0-T_{CP,2}} \sum_{i_1=0}^{N_c-1} \tilde{S}_{l+k,i_1}e^{j\frac{2\pi i_1}{T_s}t}u_{l+k}(t) \\ &\quad \times \sum_{i_2=0}^{N_c-1} \tilde{S}_{l+k,i_2}^* e^{-j\frac{2\pi i_2}{T_s}t}u_{l+k}^*(t+T_s)\ \mathrm{d}t.\end{aligned} \tag{70}$$

Since for $i_1 \neq i_2$, $\mathbb{E}\{\tilde{S}_{k,i_1}\tilde{S}_{k,i_2}^*\} = 0$, we further focus on

$$\frac{1}{N_c^2}\sum_{l=-1}^{1}\sum_{i=0}^{N_c-1}|\tilde{S}_{l+k,i}|^2\int_{\tau-lT_b-t_0-T_{CP}}^{\tau-lT_b-t_0-T_{CP,2}} u_{l+k}(t)u_{l+k}^*(t+T_s)\ \mathrm{d}t. \tag{71}$$

Define function $\upsilon_k(\tau)$ as

$$\begin{aligned}\upsilon_k(\tau) &\triangleq \int_{\tau-T_{CP}}^{\tau-T_{CP,2}} u_k(t)u_k^*(t+T_s)\mathrm{d}t \\ &= \begin{cases}(\tau+T_{CP,1})C_k, & -T_{CP,1} \leq \tau < 0, \\ \tau+(T_{CP,1}-\tau)C_k, & 0 \leq \tau < T_{CP,2}, \\ T_{CP,2}+(T_{CP,1}-\tau)C_k, & T_{CP,2} \leq \tau < T_{CP,1}, \\ T_{CP}-\tau, & T_{CP,1} \leq \tau < T_{CP}, \\ 0, & otherwise.\end{cases}\end{aligned} \tag{72}$$

So (71) can be expressed as

$$\frac{1}{N_c^2}\sum_{l=-1}^{1}\sum_{i=0}^{N_c-1}|\tilde{S}_{l+k,i}|^2\upsilon_{l+k}(\tau-lT_b-t_0). \tag{73}$$

In addition, since the phase shift symbols are zero-mean and independent, for $\tau \in \mathbb{R}$, we have

$$\mathbb{E}\{\upsilon_{k_1}(\tau)C_{k_2}^*\} = \begin{cases}\upsilon(\tau), & k_1 = k_2, \\ 0, & k_1 \neq k_2.\end{cases} \tag{74}$$

So the expectation of $Y_{k,1}(\tau)\tilde{C}_{k+d}^*$ is

$$\mathbb{E}\{Y_{k,1}(\tau)\tilde{C}_{k+d}^*\} = \begin{cases}\frac{P_S}{N_c}\upsilon(\tau+T_b-t_0), & d = k_0-1, \\ \frac{P_S}{N_c}\upsilon(\tau-t_0), & d = k_0, \\ \frac{P_S}{N_c}\upsilon(\tau-T_b-t_0), & d = k_0+1, \\ 0, & otherwise.\end{cases} \tag{75}$$

whose maximum is achieved at $\tau = t_0$ and $d = k_0$. In addition, since constellation Φ is a finite set, the variance of $Y_{k,1}(\tau)\tilde{C}_{k+d}^*$ is bounded for any possible k, τ and d, while given τ and d,

$$\mathbb{E}\{Y_{k_1,1}(\tau)\tilde{C}_{k_1+d}^*Y_{k_2,1}(\tau)\tilde{C}_{k_2+d}^*\} = 0, \quad \text{for } |k_1-k_2| > 1. \tag{76}$$

So as $K \to \infty$, the variance of $\frac{1}{K}\sum_{k=0}^{K-1}Y_{k,1}(t_0)\tilde{C}_{k+k_0}^*$ converges to 0, and using the Chebychev inequality, we have

$$\frac{1}{K}\sum_{k=0}^{K-1}Y_{k,1}(t_0)\tilde{C}_{k+k_0}^* = \frac{P_S T_{CP,1}}{N_c}, a.s.. \tag{77}$$

Second, define

$$Y_{k,2}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} z(t)s^*(t+T_s-t_0)e^{-j(\omega_0 t+\omega_0 T_s+\phi_0)}\mathrm{d}t, \tag{78}$$

and

$$Z_{k,l}(\omega,\tau,t_0) \triangleq \int_{\tau-T_{CP}}^{\tau-T_{CP,2}} z(t+kT_b)e^{j\omega t}u_l(t-lT_b+T_s-t_0)\mathrm{d}t. \tag{79}$$

It can be derived that

$$Y_{k,2}(\tau) = \sum_{l=-1}^{1}\sum_{i=0}^{N_c-1}\frac{e^{j\frac{2\pi i}{T_s}[-lT_b-t_0]}\tilde{S}_{k+l,i}Z_{k,l}(\frac{2\pi i}{T_s}-\omega_0,\tau,t_0)}{N_c e^{j(k\omega_0 T_b+\omega_0 T_s+\phi_0)}}. \tag{80}$$

Considering the delay in signal processing, we assume the jamming term $Z_{k,l}(\frac{2\pi i}{T_s}-\omega_0,\tau,t_0)$ is independent of the transmitted symbol $\tilde{S}_{k+l,i}$ in (80). Therefore, we have

$$\mathbb{E}\{Y_{k,2}(\tau)\tilde{C}_{k+d}^*\} = 0, \quad \forall k \in \mathbb{Z}^*,\ \tau \in [0,T_b),\ d \in \mathcal{K}. \tag{81}$$

Note that the fourth moment of jamming interference $z(t)$ is bounded, so are the variances of $z(t)$ of $Y_{k,2}(\tau)\tilde{C}_{k+d}^*$. In addition, for $\tau \in [0,T_b), d \in \mathcal{K}$, we have

$$\mathbb{E}\{Y_{k_1,2}(\tau)\tilde{C}_{k_1+d}^*Y_{k_2,2}^*(\tau)\tilde{C}_{k_2+d}\} = 0, \quad \forall |k_1-k_2| > 1. \tag{82}$$

Therefore,

$$\frac{1}{K}\sum_{k=0}^{K-1}Y_{k,2}(\tau)\tilde{C}_{k+d}^* = 0, \quad \forall \tau \in [0,T_b),\ d \in \mathcal{K}, a.s.. \tag{83}$$

Third, define

$$Y_{k,3}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} s(t-t_0)e^{j(\omega_0 t+\phi_0)}z^*(t+T_s)\mathrm{d}t.$$

Following the same argument as in the derivation of (83) on $Y_{k,2}(\tau)$, we have

$$\frac{1}{K}\sum_{k=0}^{K-1}Y_{k,3}(\tau)\tilde{C}_{k+d}^* = 0, \quad \forall \tau \in [0,T_b),\ d \in \mathcal{K}, a.s.. \tag{84}$$

At last, we define

$$Y_{k,4}(\tau) \triangleq \int_{\tau-T_{CP}+kT_b}^{\tau-T_{CP,2}+kT_b} z(t)z^*(t+T_s)\mathrm{d}t.$$

Considering the security of phase shift sequence C_k and the delay in signal processing, we assume that for $t \leq (k+1)T_b + T_s - T_{CP,2}$, the jammer is unable to recover $\tilde{C}_{k+d}, \forall d \in \mathcal{K}$. Since the fourth moment of $z(t)$ is bounded, we can have

$$\frac{1}{K}\sum_{k=0}^{K-1}Y_{k,4}(\tau)\tilde{C}_{k+d}^* = 0, \quad \forall \tau \in [0,T_b),\ d \in \mathcal{K}, a.s.. \tag{85}$$

In conclusion, by averaging the correlation coefficients $Y_k(\tau,d)$ over multiple OFDM blocks, (18) can be obtained. □

REFERENCES

[1] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 152–157, Jan. 1983.

[2] M. Medard, "Capacity of correlated jamming channels," in *Proc. Annual Allerton Conf. Commun. Control Comput.*, 1997, pp. 1043–1052.

[3] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[4] T. Song, W. E. Stark, T. Li, and J. K. Tugnait, "Optimal multiband transmission under hostile jamming," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 4013–4027, Sep. 2016.

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

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

[7] L. Zhang and T. Li, "Anti-jamming message-driven frequency hopping—Part II: Capacity analysis under disguised jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 80–88, Jan. 2013.

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

[9] A. El Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge Univ. Press, 2012.

[10] T. Hwang, C. Yang, G. Wu, S. Li, and G. Y. Li, "OFDM and its wireless applications: A survey," *IEEE Trans. Veh. Technol.*, vol. 58, no. 4, pp. 1673–1694, May 2009.

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

[12] L. Jun, J. H. Andrian, and C. Zhou, "Bit error rate analysis of jamming for OFDM systems," in *Proc. Wireless Telecommun. Symp.*, Apr. 2007, pp. 1–8.

[13] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2212–2224, Oct. 2015.

[14] L. Mailaender, "Anti-jam communications using frequency-hopped OFDM and LDPC with erasure decoding ('Minotaur')," in *Proc. IEEE Military Commun. Conf.*, Nov. 2013, pp. 84–88.

[15] T. C. Clancy, "Efficient OFDM denial: Pilot jamming and pilot nulling," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2011, pp. 1–5.

[16] P. Cuccaro and G. Romano, "Non uniform power allocation pilot tone jamming in OFDM systems," in *Proc. 40th Int. Conf. Telecommun. Signal Process. (TSP)*, Jul. 2017, pp. 152–155.

[17] M. J. L. Pan, T. C. Clancy, and R. W. McGwier, "Jamming attacks against OFDM timing synchronization and signal acquisition," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct./Nov. 2010, pp. 1–7.

[18] 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, Mar. 2009, Art. no. 1.

[19] M. Labib, V. Marojevic, J. H. Reed, and A. I. Zaghloul, "How to enhance the immunity of LTE systems against RF spoofing," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Kauai, HI, USA, Feb. 2016, pp. 1–5.

[20] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: Threat assessment and mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, Apr. 2016.

[21] C. Shahriar *et al.*, "PHY-layer resiliency in OFDM communications: A tutorial," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 292–314, 1st Quart., 2015.

[22] A. El-Keyi, O. Üreten, H. Yanikomeroglu, and T. Yensen, "LTE for public safety networks: Synchronization in the presence of jamming," *IEEE Access*, vol. 5, pp. 20800–20813, 2017.

[23] C. Shahriar, R. McGwier, and T. C. Clancy, "Performance impact of pilot tone randomization to mitigate OFDM jamming attacks," in *Proc. IEEE CCNC*, Jan. 2013, pp. 813–816.

[24] D. Xu, P. Ren, Y. Wang, Q. Du, and L. Sun, "ICA-SBDC: A channel estimation and identification mechanism for MISO-OFDM systems under pilot spoofing attack," in *Proc. IEEE ICC*, May 2017, pp. 1–6.

[25] D. Xu, P. Ren, and J. A. Ritcey, "Hierarchical 2-D feature coding for secure pilot authentication in multi-user multi-antenna OFDM systems: A reliability bound contraction perspective," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 592–607, Mar. 2019.

[26] T. Ericson, "The noncooperative binary adder channel," *IEEE Trans. Inf. Theory*, vol. 32, no. 3, pp. 365–374, May 1986.

[27] L. Zhang, H. Wang, and T. Li, "Anti-jamming message-driven frequency hopping—Part I: System design," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 70–79, Jan. 2013.

[28] 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, Jun. 1978.

[29] 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, Sep. 1960.

[30] F. P. Miller, A. F. Vandome, and J. McBrewster, *Advanced Encryption Standard*. Orlando, FL, USA: Alpha Press, 2009.

[31] J.-J. van de Beek, M. Sandell, and P. O. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Trans. Signal Process.*, vol. 45, no. 7, pp. 1800–1805, Jul. 1997.

[32] J. R. Barry, D. G. Messerschmitt, and E. A. Lee, *Digital Communication*, 3rd. ed. Norwell, MA, USA: Kluwer, 2003.

[33] *IEEE Standard for Information Technology–Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Standard IEEE Std 802.11-2012, Mar. 2012.

[34] T. Lv and J. Chen, "ML estimation of timing and frequency offset using multiple OFDM symbols in OFDM systems," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2003, vol. 4, pp. 2280–2284.

[35] A. Klenke, *Probability Theory: A Comprehensive Course*. London, U.K.: Springer, 2008.

[36] I. Csiszar and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, Mar. 1988.

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

[38] T. Ericson, "Exponential error bounds for random codes in the arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 1, pp. 42–48, Jan. 1985.

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

[40] D. Du and P. Pardalos, *Minimax Application*. Washington, DC, USA: Springer, 1995.

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

[42] 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 Trans. Inf. Theory*, vol. 47, no. 2, pp. 657–670, Feb. 2001.

[43] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2001.

Yuan Liang received the B.S. degree in electrical engineering from the Nanjing University of Posts and Telecommunications, China, in 2012, the M.S. degree in electrical engineering from Southeast University, China, in 2015, and the Ph.D. degree in electrical and computer engineering from Michigan State University, in 2019. His research interests include wireless communications and networking, information theory, and computational brain analysis.

Jian Ren (SM'09) received the B.S. and M.S. degrees in mathematics from Shaanxi Normal University, and the Ph.D. degree in electrical engineering from Xidian University, China. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, Michigan State University. His current research interests include network security, cloud computing security, privacy-preserving communications, distributed network storage, and the Internet of Things. He was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award, in 2009. He served as the TPC Chair for IEEE ICNC'17, the General Chair for ICNC'18, and the Executive Chair for ICNC'19 and ICNC'20. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING, *ACM Transactions on Sensor Networks* (TOSN), and a Senior Associate Editor for *IET Communications*.

Tongtong Li received the Ph.D. degree in electrical engineering from Auburn University, in 2000, and the Ph.D. degree in mathematics from Sun Yat-sen University, in 1995. From 2000 to 2002, she was with Bell Labs, where she had been working on the design and implementation of 3G and 4G systems. Since 2002, she has been with Michigan State University, where she is currently an Associate Professor. Her research interests include wireless and wired communications, wireless security, information theory, statistical signal processing, and computational brain analysis. She was a recipient of the National Science Foundation (NSF) CAREER Award in 2008 for her research on efficient and reliable wireless communications. She served as an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS from 2007 to 2009 and an Editorial Board Member for *EURASIP Journal on Wireless Communications and Networking* from 2004 to 2011. She served as an Associate Editor for the IEEE TRANSACTIONS ON SIGNAL PROCESSING from 2012 to 2016.