Security and Energy Efficiency: Breaking the Barriers of High Peak-to-Average Power Ratio and Disguised Jamming in NextG IoT System Design

Tongtong Li, *Senior Member, IEEE*, Jinxian Deng, and Jian Ren, *Senior Member, IEEE*

***Abstract*—As a popular modulation technique in wireless communications, orthogonal frequency-division multiplexing (OFDM) has two major disadvantages—one is its high peak-to-average power ratio (PAPR), which causes nonlinear distortion, lower power efficiency, and performance losses; the other is its fragility under hostile jamming attacks, where the authorized users signal is deliberately interfered by the adversary, leading to communication failures. In this article, first, we reintroduce the IFFT-relocated OFDM (IR-OFDM), which is essentially a single-carrier system with frequency-domain equalization. By relocating the inverse fast Fourier transform (IFFT) block in OFDM from the transmitter to receiver, IR-OFDM can completely liberate OFDM from the barriers of high PAPR while achieving the same spectral efficiency. Second, to combat hostile jamming, especially disguised jamming, where the jamming is highly correlated with the authorized signal, we propose a securely precoded IR-OFDM (SP-IR-OFDM). By integrating the advanced encryption standard (AES) into IR-OFDM transceiver design, we obtain a random (or dynamic) constellation. The shared secure randomness introduced by AES breaks the symmetry between the authorized signal and the jamming interference and, hence, ensures reliable performance of the system under disguised jamming. The efficiency and robustness of IR-OFDM and SP-IR-OFDM are demonstrated through simulation examples. It is shown that IR-OFDM can deliver comparable or better performances than OFDM under multipath propagation, and SP-IR-OFDM can achieve strong resistance under disguised jamming while enjoying low PAPR and relatively high spectral efficiency. Our result indicates that, potentially, SP-IR-OFDM can serve as a promising modulation candidate for next-generation secure and energy-efficient high-speed communications, especially for the resource-constrained Internet of Things (IoT) networks.**

***Index Terms*—Inverse fast Fourier transform (IFFT)-relocated OFDM (IR-OFDM), jamming, orthogonal frequency-division multiplexing (OFDM), peak-to-average power ratio (PAPR), secure precoding.**

I. Introduction

ORTHOGONAL frequency-division multiplexing (OFDM) has become a key modulation technique for reliable high-speed wireless communication [1], [2], [3], optical fiber transmission [4], and underwater communication [5], mainly due to its high spectral efficiency and simple receiver design under multipath propagation. In practical systems, there are two major concerns with OFDM—one is its high peak-to-average power ratio (PAPR) [6], [7], [8], another is its fragility under hostile jamming attacks.

High PAPRs occur when the input quadrature amplitude modulation (QAM) or phase-shift keying (PSK) symbols line up constructively in the inverse fast Fourier transform (IFFT) operation at the OFDM transmitter and form peaks in the time-domain signal. In long-term evolution (LTE) systems, for example, OFDM signal PAPR is approximately 12 dB. High PAPR causes nonlinear distortion and lower power efficiency in the power amplifier. Lower power efficiency leads to lower average transmission power, and nonlinear distortion leads to out-of-band frequency dispersion and intercarrier interference, both resulting in performance losses and higher hardware design complexity in OFDM systems and raising serious challenges for resource-limited Internet of Things (IoT) devices [9], [10], [11].

In the literature, there has been a continuous effort to reduce the PAPR of OFDM. A simple technique is clipping and filtering, where the signal amplitude is clipped to a prespecified value [12]. While clipping can reduce PAPR, it also causes signal distortion and undesired high-frequency items. The latter can be filtered out, but filtering may result in some peak regrowth. Block coding is another technique for PAPR reduction [13]. The basic idea is that for each data block, the codeword with the lowest PAPR is selected through exhaustive search. With this approach, both the transmitter and receiver need to store a large lookup code table whose size increases exponentially with the block size. Along the line of preventing the input symbols being combined constructively in the IFFT operation, interleaving, selective subcarrier mapping, and tone reservations have all been attempted to reduce the PAPR. In [14], the input symbol sequence is passed through different random interleavers and each permuted sequence is fed to an IFFT operator. The PAPR corresponding to the permuted sequences and the original input are then calculated, and the sequence with the lowest PAPR is chosen for transmission. The side information on which interleaver to use is sent to the receiver. Similarly, in selective mapping techniques [15], the transmitter uses different phase sets to change the phase of the original signal, and the phase manipulated or precoded signal that results in the lowest PAPR is selected for transmission. In both interleaving and selected mapping-based approaches, lower PAPR is achieved with the cost of increased

Manuscript received 27 May 2022; revised 26 September 2022; accepted 9 October 2022. Date of publication 12 October 2022; date of current version 24 January 2023. This work was supported in part by the National Science Foundation under Award 1919154. *(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: tongli@msu.edu; dengjinx@msu.edu; renjian@msu.edu).

Digital Object Identifier 10.1109/JIOT.2022.3214125

2327-4662 © 2022 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

computational complexity and the transmission of extra overhead or side information. In the tone reservation approach [16], a selected set of subcarriers is reserved as control tones (i.e., not used for signal transmission) to reduce the PAPR. The cost, in turn, is the reduced bandwidth efficiency.

In [17], PAPR reduction is achieved through active constellation extension. More specifically, outer constellation points in active (data-carrying) subcarriers are dynamically extended such that the resulting signal has a lower PAPR. In this approach, addition transmit power is required to reduce the PAPR. In [18], [19], and [20], discrete Fourier transform (DFT)-precoded OFDM—also known as DFT-spread OFDM—was proposed for PAPR reduction. The idea is to divide the whole OFDM band into several subbands, then precode the data carried by the subcarriers on each subband with a DFT matrix before feeding the data to the IFFT block. DFT-spread OFDM has been adopted in LTE uplink transmission.

With the techniques discussed above, the PAPR can be reduced to approximately 8–10 dB, subject to the constellation used and the cost on computational complexity and performance losses. A natural question is: can the PAPR in OFDM be further reduced? Fortunately, the answer is *yes*. In this article, we will reintroduce the IFFT-relocated OFDM (IR-OFDM), which is essentially a single-carrier system with frequency-domain equalization [21], [22], [23]. It can achieve exactly the same low PAPR as the input symbol sequence. In particular, for constant modulus modulations, the PAPR can be reduced to 0 dB. At the same time, IR-OFDM enjoys simple transceiver design and utilizes only one FFT/IFFT pair and has the same spectral efficiency as traditional OFDM. Moreover, since IR-OFDM is essentially a single-carrier system, it is more robust to frequency and phase offsets than traditional OFDM, where intercarrier interference due to frequency and phase offsets is a significant challenge. It is worth to note that in IR-OFDM, both FFT and IFFT are implemented at the receiver end, resulting in extremely simple and efficient transmitter design. This makes IR-OFDM a particularly attractive candidate for resource-limited 5G/6G IoT systems, where one of the major tasks is information collection.

However, IR-OFDM is as fragile as traditional OFDM under hostile jamming, in which the authorized user's signal is deliberately interfered by the adversary. In wireless systems, jamming is one of the most commonly used techniques for limiting the effectiveness of an opponent's communication. 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 and IoT systems as well.

In the literature [24], [25], [26], jamming has widely been modeled as Gaussian noise. Based on the noise jamming model and Shannon's channel capacity formula, it has long been believed that jamming is really harmful only when the jamming power is much higher than the signal power. However, this is only partially true. Based on the arbitrarily varying channel model [27], [28], [29], recent studies indicate that disguised jamming [30], [31], [32], where the jamming is highly correlated with the signal, can be much more destructive than noise jamming. Due to its high similarity with the authorized signal, disguised jamming can mislead the receiver and reduce the system capacity to zero even when the jamming power equals the signal power [32], [33].

Existing study reveals that the worst problem brought by disguised jamming is the symmetry between the authorized signal and the jamming interference. To design the corresponding anti-jamming system, the main task, therefore, is to break the symmetry between the authorized signal and jamming. For this purpose, encryption or channel coding at the bit level will not really help, since the symmetry appears at the symbol level. That is, instead of using a fixed symbol constellation, we need 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.

Motivated by the observations above and our previous research on anti-jamming system design [31], [32], [34], in this article, we further design the securely precoded IR-OFDM (SP-IR-OFDM). The basic idea is to randomize the phases of transmitted symbols using the secure pseudorandom 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. By integrating AES into IR-OFDM transceiver design, we actually obtain a dynamic constellation. The shared secure randomness introduced by AES breaks the symmetry between the authorized signal and the jamming interference and, hence, ensures a reliable performance of SP-IR-OFDM under disguised jamming. A remarkable feature of the proposed SP-IR-OFDM scheme is that it can achieve strong resistance to disguised jamming while keeping relatively high spectral efficiency. Moreover, the change to physical-layer transceivers is minimal, feasible and affordable.

The efficiency and robustness of IR-OFDM with and without secure precoding are demonstrated through simulation examples. The numerical results indicate the following.

1) IR-OFDM can deliver comparable or better performances—in terms of bit-error rate (BER)—than traditional OFDM under multipath propagation. As can be seen, the IR-OFDM scheme completely liberates OFDM from the barriers of high PAPR without any additional complexity, storage requirement, or performance losses.
2) IR-OFDM and SP-IR-OFDM have a similar performance under Gaussian noise jamming. The BER of both systems can be improved under Gaussian jamming through strong channel coding, such as low-rate low-density parity-check (LDPC) coding.
3) IR-OFDM is fragile under disguised jamming and the BER cannot be improved through channel coding. On the other hand, SP-IR-OFDM is robust under disguised jamming, and can achieve satisfying BER with the assistance of channel coding.

Our result implies that, potentially, IR-OFDM and SP-IR-OFDM can serve as promising modulation candidates for next-generation energy-efficient high-speed communications,

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

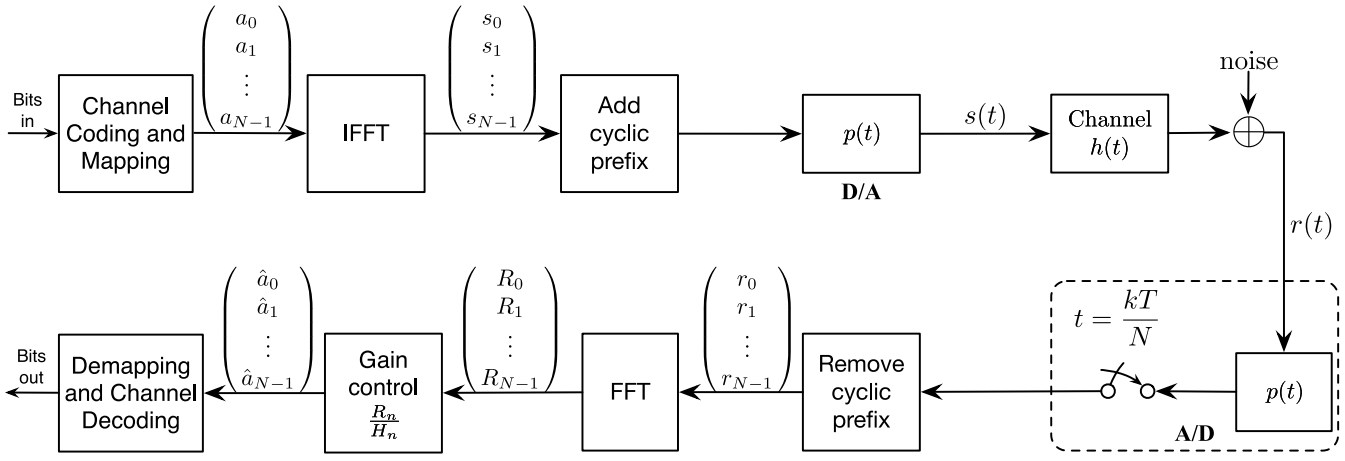


Fig. 1. Block Diagram of traditional OFDM.

under benign and hostile environments, respectively, especially for resource-constrained IoT systems.

The remainder of this article is organized as follows. In Section II, we briefly revisit the design and practical implementation of traditional OFDM; in Section III, we reintroduce the proposed IR-OFDM scheme; in Section IV, we present the proposed SP-IR-OFDM; simulation results are provided in Section V; and we conclude in Section VI.

II. Revisit to the Design and Practical Implementation of OFDM

In this section, we revisit the design of OFDM and its practical implementation. The whole system design is illustrated in Fig. 1. OFDM is a special kind of orthogonal pulse amplitude modulation (OPAM). Let $\mathbf{a} = [a_1, a_2, \ldots, a_N]^{\mathrm{T}}$ represent the block of input symbols, generally, QAM or PSK symbols; here, $(\cdot)^{\mathrm{T}}$ denotes the transpose of a matrix, and N is the block size which is generally a power of 2. Let T stand for the symbol interval. For $n = 0, 1, \ldots, N-1$, let

$$g_n(t) = \frac{1}{\sqrt{T}} e^{\frac{j2\pi nt}{T}} w(t) \tag{1}$$

where $w(t) = u(t) - u(t-T)$—with $u(t)$ being the unit step function—is a rectangular window over the interval $[0, T)$. These N pulses, $\{g_n(t)\}$, are orthonormal and with frequency separation $1/T$ Hz. The corresponding OPAM signal in one symbol interval can be represented as

$$s(t) = \sum_{n=0}^{N-1} a_n g_n(t) = \frac{1}{\sqrt{T}} \sum_{n=0}^{N-1} a_n e^{\frac{j2\pi nt}{T}} w(t). \tag{2}$$

As $s(t)$ consists of superimposed finite-length signals modulated on different carriers, it is also a special case of multicarrier modulation. Note that $\{g_n(t)\}$ are not bandlimited, for low-complexity practical implementation, they are replaced with another set of similar pulses $\{\tilde{g}_n(t)\}$ through the back-to-back cascade of an ideal A/D and D/A convert pair [35], as shown in Fig. 2.

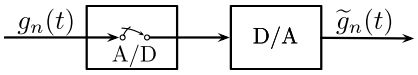


Fig. 2. Generation of the practical pulses in OFDM.

That is, for $n = 0, 1, \ldots, N-1$

$$\tilde{g}_n(t) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{j2\pi nk}{N}} p\left(t - \frac{kT}{N}\right) \tag{3}$$

where

$$p(t) = \sqrt{\frac{T}{N}} \frac{\sin(\pi Nt/T)}{\pi t} = \sqrt{\frac{N}{T}} \mathrm{sinc}\left(\frac{\pi Nt}{T}\right) \tag{4}$$

is the ideal reconstruction filter for a sample rate of (N/T).

With the new pulses $\{\tilde{g}_n(t)\}$, the corresponding OPAM signal in one symbol interval can be represented as

$$s(t) = \sum_{n=0}^{N-1} a_n \tilde{g}_n(t) \tag{5}$$

$$= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} a_n e^{\frac{j2\pi nk}{N}} p\left(t - \frac{kT}{N}\right) \tag{6}$$

$$= \sum_{k=0}^{N-1} \left[\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} a_n e^{\frac{j2\pi nk}{N}} \right] p\left(t - \frac{kT}{N}\right). \tag{7}$$

For $k = 0, 1, \ldots, N-1$, let

$$s_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} a_n e^{\frac{j2\pi nk}{N}} \tag{8}$$

that is, samples s_k are obtained from symbols a_n through IFFT. Note that $\sqrt{N}$ is used in the IFFT instead of N such that $E\{|s_k|^2\} = E\{|a_n|^2\}$; here, $E\{\cdot\}$ stands for the expectation value of the corresponding random variable. We then have

$$s(t) = \sum_{k=0}^{N-1} s_k \, p\left(t - \frac{kT}{N}\right). \tag{9}$$

This is the OFDM modulation, also known as discrete multitone modulation.

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

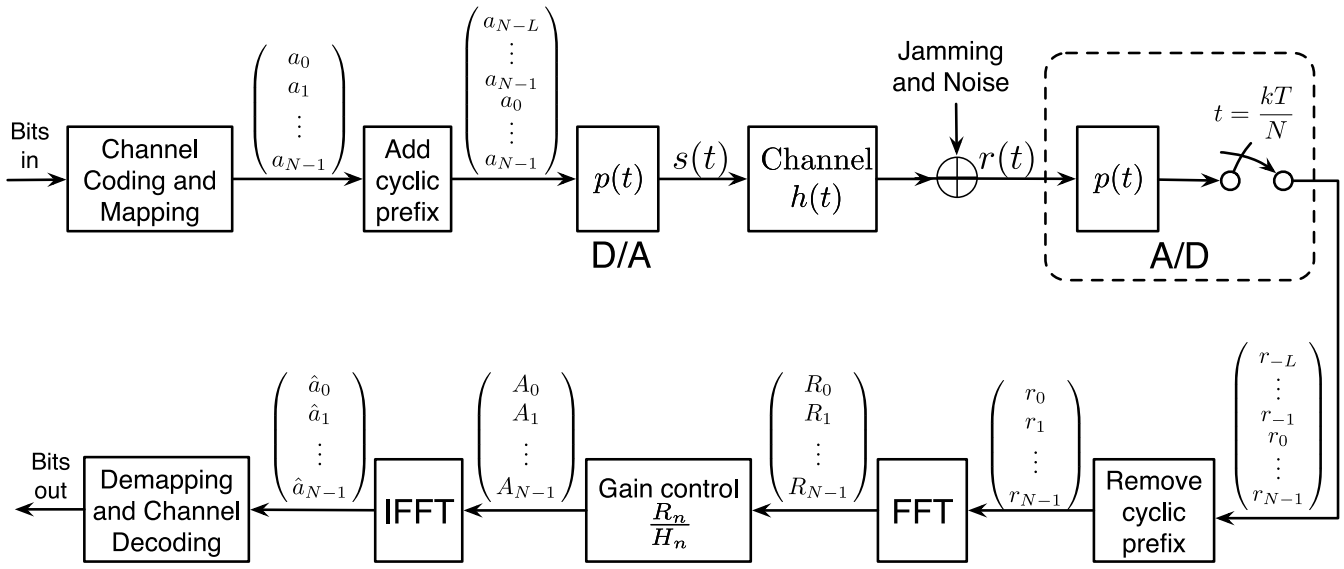


Fig. 3. Block diagram of IR-OFDM.

TABLE I
PAPR WITH IR-OFDM (CONST. STANDS FOR CONSTELLATION)

Const.	PSK	16-QAM	64-QAM	256-QAM	1024-QAM
PAPR	0dB	2.5527dB	3.6798 dB	4.2276 dB	4.4997dB

Note that although s_k and a_n have the same average power, s_k is more like a Gaussian random variable rather than a uniformly distributed random variable. Comparing with a_n, s_k has a much higher peak power and, hence, a much higher PAPR.

Let h_k denote the equivalent discrete-time channel impulse response between the transmitted samples s_k and received samples r_k. Assuming the channel order is L, in the noise-free case, we have

$$r_k = s_k * h_k = \sum_{l=0}^{L} h_l s_{k-l}. \tag{10}$$

By adding the cyclic prefix $\{s_{N-L}, \ldots, s_{N-1}\}$ before the N samples $\{s_0, s_1, \ldots, s_{N-1}\}$, we can convert the ordinary convolution to circular convolution. In this case, let $\{H_n\}$ denote the N-point DFT of the channel impulse response $\{h_l\}, l = 0, 1, \ldots, L$, and let $\{R_n\}$ denote the N-point DFT of $\{r_0, r_1, \ldots, r_{N-1}\}$, then we have

$$R_n = H_n a_n, \quad n = 0, 1, \ldots, N-1 \tag{11}$$

since $\{a_n\}$ is the DFT of $\{s_0, s_1, \ldots, s_{N-1}\}$. As a result, for $n = 0, 1, \ldots, N-1$, a_n can be recovered from R_n through the simple gain control $a_n = R_n/H_n$. As can be seen, OFDM has very simple receiver design under multipath propagation.

III. IFFT-RELOCATED OFDM: SINGLE CARRIER SYSTEM WITH FREQUENCY-DOMAIN EQUALIZATION

It is well known that high PAPR occurs when the input symbols line up constructively in the IFFT operation at the OFDM transmitter and form peaks in the time-domain signal. From Section II, we can see that IFFT and FFT are the core parts in OFDM transceiver design. The IFFT-FFT pair makes it possible to recover the original input symbols through a simple scaling operation. For this reason, in all the previous work on PAPR reduction, the IFFT block in the OFDM transmitter remain untouched, even though it is the cause of the high PAPR.

However, a closer observation to the OFDM system design indicates that IFFT at the OFDM transmitter can be relocated to the receiver, and we can still recover the original input symbols through a simple scaling operation. In fact, at the transmitter, we can define

$$s(t) = \sum_{n=0}^{N-1} a_n \, p\left(t - \frac{nT}{N}\right). \tag{12}$$

Still, let $\{h_0, h_1, \ldots, h_L\}$ denote the equivalent discrete-time channel impulse response, the received samples r_n can now be represented as

$$r_n = a_n * h_n = \sum_{l=0}^{L} h_l a_{n-l}. \tag{13}$$

Add cyclic prefix $\{a_{N-L}, \ldots, a_{N-1}\}$ before the N samples $\{a_0, a_1, \ldots, a_{N-1}\}$, again, we convert the ordinary convolution to the circular convolution. Let $\{A_n\}$ denote the N-point DFT of $\{a_0, a_1, \ldots, a_{N-1}\}$, and $\{H_n\}$ the N-point DFT of $\{h_0, h_1, \ldots, h_L\}$, and $\{R_n\}$ the N-point DFT of $\{r_0, r_1, \ldots, r_{N-1}\}$, in the noise-free case, we have

$$R_n = H_n A_n, \quad n = 0, 1, \ldots, N-1. \tag{14}$$

We can then recover A_n from R_n through $A_n = R_n/H_n$, and recover a_n from A_n through the inverse DFT.

The whole process is illustrated in Fig. 3, and we name this scheme IR-OFDM. As can be seen, with IR-OFDM, we completely resolve the PAPR problem of OFDM and, now, the PAPR of the system is exactly the same as that of the original input sequence, as shown in Table I. IR-OFDM requires no precoding, selective mapping, tone reservation, or constellation

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

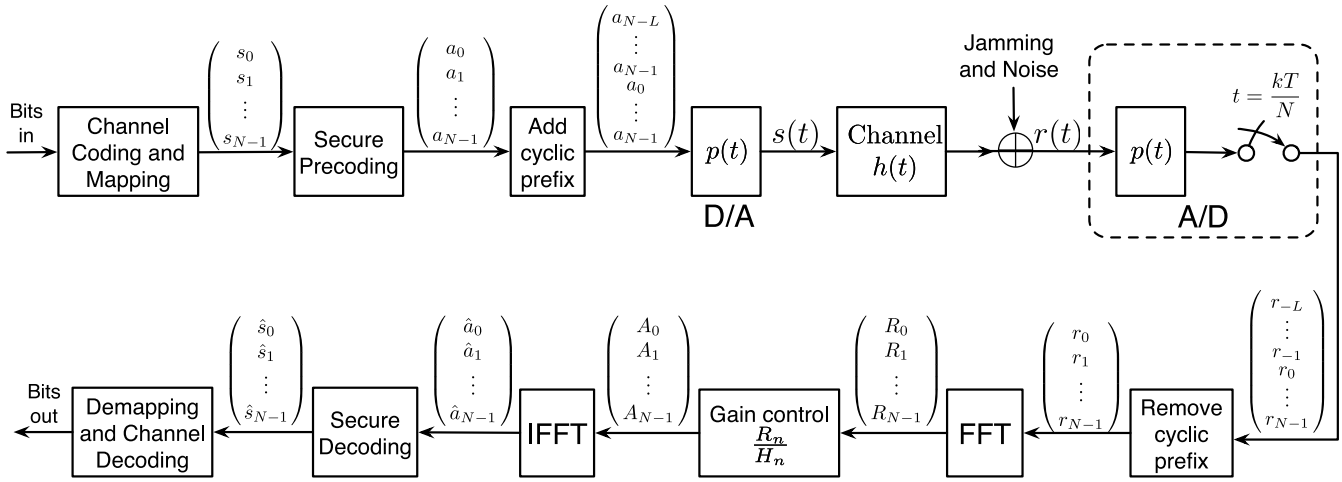


Fig. 4. Block diagram of SP-IR-OFDM and IR-OFDM.

extension, and can achieve exactly the same high spectral efficiency as OFDM. In addition, IR-OFDM improves the power efficiency of traditional OFDM significantly. It also avoids the nonlinear distortion in the power amplifier and, hence, reduce hardware design complexity.

Moreover, we would also like to point out that since IR-OFDM is essentially a single-carrier system, it is less sensitive to frequency and phase offsets than the traditional OFDM, where intercarrier interference due to frequency and phase offsets is a significant challenge.

In short, IR-OFDM is simple, yet effective. The underlying argument is that in the traditional OFDM, the time-domain input signal is treated or twisted as a frequency-domain signal so that FFT can be used at the receiver to convert convolution to multiplication. In IR-OFDM, we just treat the input signal as a time-domain signal as it is, and show that FFT can still be used at the receiver end as in traditional OFDM even if there is no IFFT block at the transmitter.

IV. Anti-Jamming IFFT-Relocated OFDM With Secure Precoding and Decoding

To this point, we have been focused on reliable and efficient data transmission under normal channel conditions, subject to multipath fading and additional noise. However, both OFDM and IR-OFDM are fragile under hostile attacks, especially active attacks like hostile jamming.

A. Disguised Jamming Model

In the literature [24], [25], [26], hostile jamming has widely been modeled as Gaussian noise in light of the central limit theorem. Consider the additive white Gaussian noise (AWGN) channel under hostile jamming

$$r = s + J + w \tag{15}$$

where s is the authorized signal and J is the jamming interference. w is the noise independent of J and s, and r is the received signal. Based on the noise jamming model and Shannon's capacity formula, the channel capacity is given by

$$C = B\log\left(1 + \frac{P_s}{P_w + P_J}\right) \tag{16}$$

where P_s is the signal power, P_w is the noise power, and P_J is the jamming power. From (16), we can see that under Gaussian jamming, the channel capacity is always positive, and an intuitive impression is that jamming is harmful only when the jamming power is much higher than the signal power.

However, this is only partially true. Recent studies have found that disguised jamming [30], [31], [32], 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 noise jamming. In fact, 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 complete communication failure [32], [33]. More specifically, for AWGN channels under disguised jamming, due to the symmetry between the authorized signal and jamming interference, the channel capacity is reduced to $C = 0$. The strict proof of this result can be found in [32]. As can be seen, while IF-OFDM can resolve the PAPR problem suffered by the traditional OFDM, it is as fragile as OFDM under disguised jamming.

B. Securely Precoded IF-OFDM System

To combat disguised jamming, we propose a securely precoded IF-OFDM system, which breaks the symmetry between the authorized signal and hostile jamming interference by integrating advanced crytopgraphic techniques into physical-layer transceiver design.

The block diagram of the proposed system is shown in Fig. 4. In this system, s_k, $k = 0, \ldots, N-1$ denote the original symbols, and a_k, $k = 0, \ldots, N-1$ denote the output of the secure precoder. Consider one symbol block at a time, and define $\mathbf{s} = [s_0, s_1, \ldots, s_{N-1}]^{\mathrm{T}}$ and $\mathbf{a} = [a_0, a_1, \ldots, a_{N-1}]^{\mathrm{T}}$,

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

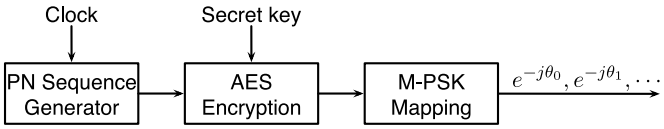


Fig. 5. Secure precoding matrix generator.

then the secure precoding process is characterized by

$$\mathbf{a} = \mathbf{P}\mathbf{s}. \tag{17}$$

Here, the precoding matrix $\mathbf{P}$ is defined as a diagonal matrix

$$\mathbf{P} = \begin{bmatrix} e^{-j\theta_0} & & & \\ & e^{-j\theta_1} & & \\ & & \ddots & \\ & & & e^{-j\theta_{N-1}} \end{bmatrix} \tag{18}$$

where $\theta_0, \theta_1, \ldots, \theta_{N-1}$ are generated using the AES-based secure pseudorandom phase generator shown in Fig. 5.

The PN sequence generator generates a pseudo-random sequence, which is then encrypted with AES. AES is chosen because of its simplicity of design, variable block and key sizes, feasibility in both hardware and software, and resistance against all known attacks [36]. Note that the secure phase generation is not limited to any particular cryptographic algorithm, but it is highly recommended that only thoroughly analyzed cryptographic algorithms are applied.

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. Note that the larger the M, the higher the uncertainty introduced by the secure precoder. Under AWGN, when M is sufficiently large, the random phase shifts in the secure precoding can be approximated as independent and identically distributed (i.i.d.) random variables that are uniformly distributed over $[0, 2\pi)$.

To facilitate the synchronization process between the transmitter and receiver, 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 inaccessible to the jammer.

In the secure precoding process, a random phase shift is applied to each transmitted symbol. In this way, we actually design a random constellation by introducing shared secure randomness between the transmitter and receiver, which breaks the symmetry between the authorized signal and the jamming interference and, hence, can achieve positive channel capacity and ensure reliable performance under disguised jamming. This is demonstrated through simulation examples in the next section. Moreover, it should be noted that if the input symbols sequences are generated from encrypted binary bit streams and the signal-to-jamming-and-noise ratio is reasonably high, then the proposed SP-IR-OFDM will be secure and robust under both eavesdropping (or unauthorized interception) and hostile jamming.

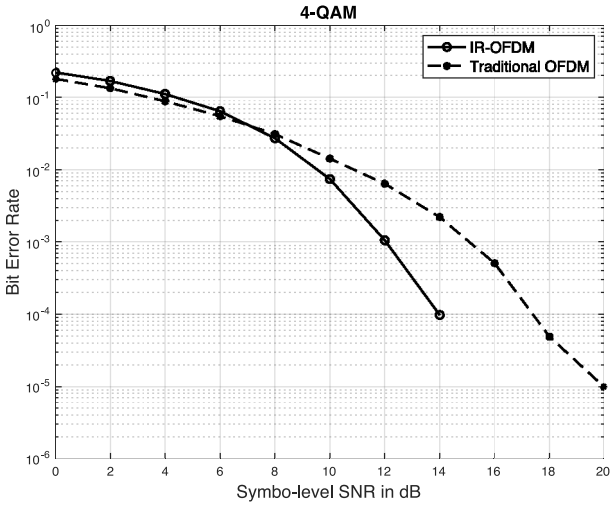


Fig. 6. IR-OFDM versus traditional OFDM under Rayleigh channels (no channel coding): 4-QAM.

Recall that key management for secure precoding is generally performed through the control channel instead of the data channel, the secure precoding process, therefore, does not introduce redundancy into the information stream, and, hence, SP-IR-OFDM has the same spectral efficiency as IR-OFDM and OFDM in the jamming-free case. As will be illustrated in Section V, when hostile jamming exists, low-rate channel coding needs to be used jointly with secure precoding for reliable communication under hostile jamming, especially disguised jamming.

V. Simulation Results

In this section, we first demonstrate through simulation examples that—while enjoying extremely low PAPR—IR-OFDM can achieve comparable BER performance under the same spectral efficiency with that of traditional OFDM. We will then compare the performance of IR-OFDM with that of SP-IR-OFDM under Gaussian noise jamming and disguised jamming.

Example 1 (Performance Comparison of IR-OFDM Versus Traditional OFDM): The performance of IR-OFDM is demonstrated under Rayleigh fading channels with AWGN and is compared with that of the traditional OFDM. The size of the FFT is chosen to be $N = 512$. The input symbols are generated randomly and the results for the BER is averaged overall 2000 Monto Carlo runs. No channel coding is involved. The simulation results are shown in Figs. 6 and 7.

From the simulation results, it can be seen that for both 4-QAM and 16-QAM, the performance of IR-OFDM is comparable to traditional OFDM when SNR is low, and IR-OFDM outperforms traditional OFDM when the SNR is reasonably high. The underlying argument may be that in traditional OFDM, the IFFT operation at the transmitter generates a

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

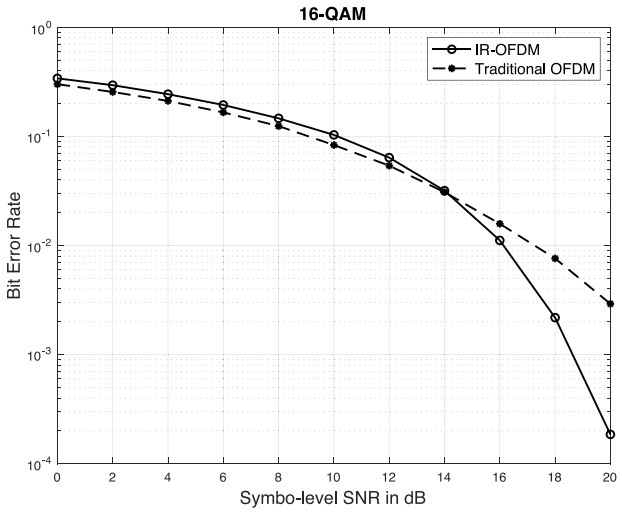


Fig. 7. Performance of IR-OFDM versus traditional OFDM under Rayleigh channels (no channel coding): 16-QAM.

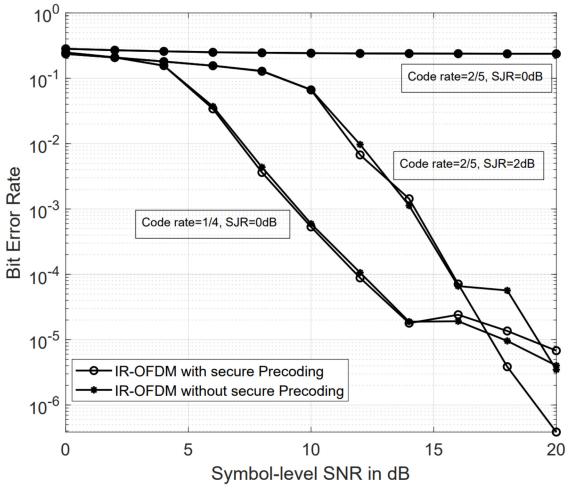


Fig. 8. BER versus symbol-level SNR: IR-OFDM with and without secure precoding under Gaussian jamming over Rayleigh channels, with LDPC coding.

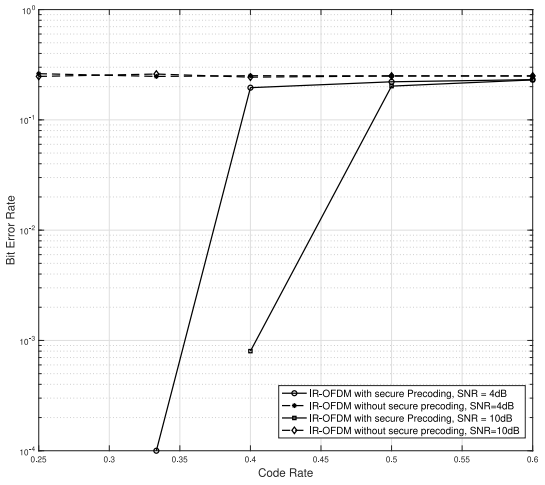


Fig. 9. BER under different code rates and SNR levels: IR-OFDM with and without secure precoding under disguised jamming over AWGN channels (with LDPC coding): signal to jamming power ratio SJR = 0 dB.

Gaussian-like constellation and reduces the minimum distance among the neighboring symbols.

Example 2 (Performance Comparison of IR-OFDM and Securely Precoded IR-OFDM Under Gaussian Jamming): In this example, we analyze the BER of IR-OFDM and SP-IR-OFDM under Gaussian noise jamming over Rayleigh channels. Perfect synchronization is assumed and we use the LDPC codes for channel coding, adopting the parity check matrices from the DVB-S.2 standard [37]. The signal-to-jamming ratio (SJR) is set to be 0 and 2 dB. Following (16), we can see that under Gaussian jamming, the channel capacity is always positive, though could be very low when the noise and/or jamming power is high. In particular, when SJR $= 0$ dB and SNR $= 0$ dB, the channel capacity is $C = 0.2925$ bit/symbol; when SJR $= 0$ dB and SNR $=10$ dB, $C = 0.4664$ bit/symbol; and $C \to 0.5$ bit/symbol as SNR$\to \infty$. This implies that under noise jamming, with strong channel coding, successful transmission is still possible even when SJR $=0$ dB. The theoretical analysis is demonstrated through numerical examples, as shown in Fig. 8. It is also shown that when the SJR is increased from 0 to 2 dB, a higher code-rate can be used to achieve satisfying BER. Overall, from Fig. 8, it can be seen that under Gaussian noise jamming, IR-OFDM with and without secure precoding have a comparable performance over Rayleigh channels.

Example 3 (Performance Comparison of IR-OFDM and Securely Precoded IR-OFDM Under Disguised Jamming): In this example, we analyze the BER of IR-OFDM and SP-IR-OFDM under disguised jamming in both AWGN and Rayleigh channels. As in Example 2, perfect synchronization is assumed, and we use the LDPC codes for channel coding, following the DVB-S.2 standard [37]. The SJR is set to be 0 dB. The BER of the two systems under disguised jamming is calculated versus different SNR levels, and the result is shown in Figs. 9–11. It can be observed that: 1) under disguised jamming, in the IR-OFDM system, the BER cannot be reduced by decreasing the code rate or the noise power, which indicates that without appropriate anti-jamming procedures, IR-OFDM cannot achieve reliable communications under disguised jamming and 2) with the SP-IR-OFDM scheme, BER can be significantly reduced when the code rate is sufficiently low. This demonstrates that the proposed SP-IR-OFDM system can achieve a positive deterministic channel coding capacity under disguised jamming.

It is worth noting that in practical scenarios, when the jammer can estimate the channel between the jammer and the authorized user, as well as the channel between the jammer and the receiver, it is then possible for the jammer to launch disguised jamming. In other words, disguised jamming is a genuine and serious threat, and the proposed symbol-level secure precoding is a particularly effective tool to combat it. When secure precoding is combined with IR-OFDM, we obtain a secure and power-efficient communication system for next-generation wireless communications, especially resource-limited IoT systems.

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

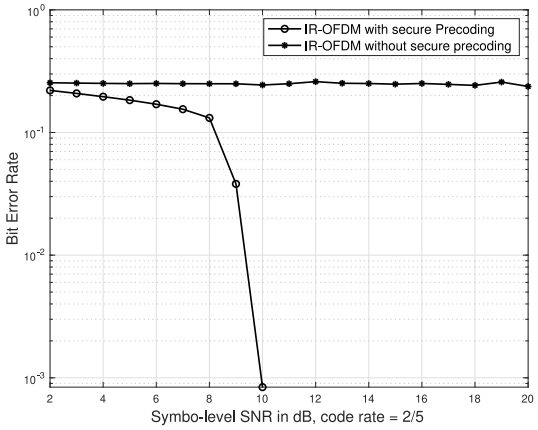


Fig. 10. BER versus symbol-level SNR: IR-OFDM with and without secure precoding under disguised jamming over AWGN channels, signal to jamming power ratio SJR = 0 dB, LDPC code rate = 2/5.

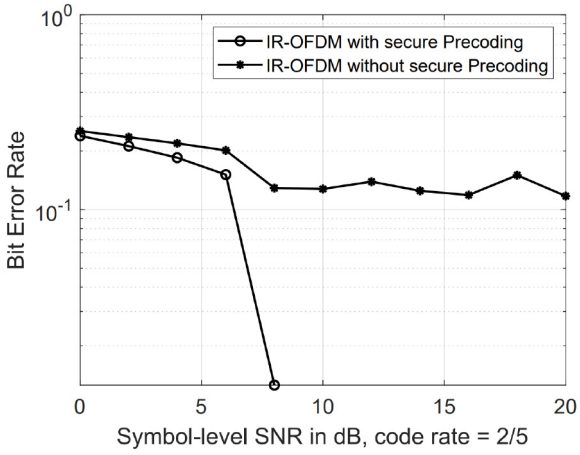


Fig. 11. BER versus symbol-level SNR: IR-OFDM with and without secure precoding under disguised jamming over Rayleigh channels, signal to jamming power ratio SJR = 0 dB, LDPC code rate = 2/5.

VI. Conclusion

In this article, we introduced a new communication scheme, referred to as SP-IR-OFDM, which aimed to break through the barriers of high PAPR in the traditional OFDM and, at the same time, enhance the system security under disguised jamming. This was achieved in two steps. First, by relocating the IFFT block in traditional OFDM from the transmitter to receiver, we obtained IR-OFDM, which is essentially a single-carrier system with frequency-domain equalization. IR-OFDM achieves the same low PAPR with the input symbols. In particular, for constant-modulus input (such as QPSK), the PAPR can be reduced to 0 dB. IR-OFDM has a simple transceiver design and does not require selective mapping, tone reservation, or constellation extension. It only needs one FFT/IFFT pair and has the same spectral efficiency as traditional OFDM. In addition, since IR-OFDM is essentially a single-carrier system, it is more robust to frequency and phase offsets than traditional OFDM, where intercarrier interference due to frequency and phase offsets is a significant challenge. Second, to combat hostile jamming, especially disguised jamming which can reduce the channel capacity to zero, we proposed to add the secure precoder and decoder to IR-OFDM, and obtained the SP-IR-OFDM. Based on the secure randomness introduced by AES, SP-IR-OFDM actually utilizes a dynamic constellation and breaks the symmetry between the authorized signal and the jamming interference and, therefore, ensures a reliable performance under disguised jamming.

The efficiency and robustness of IR-OFDM and SP-IR-OFDM were demonstrated through simulation examples. It is shown that IR-OFDM can deliver comparable or better performances than OFDM under multipath propagation. It liberates OFDM from the bottleneck of high PAPR without any additional computational complexity, storage requirement, or performance losses. Moreover, it achieves higher power efficiency and reduces the hardware design complexity. On the other hand, by integrating advanced cryptographic techniques into IR-OFDM transceiver design, SP-IR-OFDM can achieve strong resistance to disguised jamming while enjoying low PAPR and relatively high spectral efficiency. Note that under disguised jamming, the performance of IR-OFDM cannot be improved through channel coding, resulting in complete communication failure. When the hostile jamming if Gaussian, the performance of SP-IR-OFDM and IR-OFDM are comparable and can both be improved using strong channel coding under reasonable SJR, and the information rate is limited by Shannon's capacity formula.

We would also like to point out that unlike traditional security techniques which mainly rely on higher layer data encryption, SP-IR-OFDM has inherent security which is built into the physical-layer transceiver design and, hence, is also more robust under passive attacks like eavesdropping or unauthorized interception. Overall, our result indicates that, potentially, SP-IR-OFDM can serve as a promising modulation candidate for next-generation secure and energy-efficient high-speed communications, especially for resource-constrained IoT networks.

References

[1] L. Cimini, "Analysis and simulation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE Trans. Commun.*, vol. C-33, no. 7, pp. 665–675, Jul. 1985.

[2] J. Bingham, "Multicarrier modulation for data transmission: An idea whose time has come," *IEEE Commun. Mag.*, vol. 28, no. 5, pp. 5–14, May 1990.

[3] *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*, IEEE Standard 802.11-2020, 2021.

[4] T. J. Xia, S. Gringeri, and M. Tomizawa, "High-capacity optical transport networks," *IEEE Commun. Mag.*, vol. 50, no. 11, pp. 170–178, Nov. 2012.

[5] M. Stojanovic, "Low complexity OFDM detector for underwater acoustic channels," in *Proc. OCEANS*, 2006, pp. 1–6.

[6] Y. Rahmatallah and S. Mohan, "Peak-to-average power ratio reduction in OFDM systems: A survey and taxonomy," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 4, pp. 1567–1592, 4th Quart., 2013.

[7] G. Rojo and M. Stojanovic, "Peak-to-average power ratio (PAR) reduction for acoustic OFDM systems," in *Proc. OCEANS*, 2009, pp. 1–7.

[8] C. Fengjuan, Y. Hui, and G. Yue-Hong, "A new method in PTS to reduce the peak-to-average power ratio in MIMO-OFDM system," in *Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, 2009, pp. 279–282.

[9] C. Park and T. S. Rappaport, "Short-range wireless communications for next-generation networks: UWB, 60 GHz millimeter-wave WPAN, and ZigBee," *IEEE Wireless Commun.*, vol. 14, no. 4, pp. 70–78, Aug. 2007.

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.

[10] M. Sun, Q. Song, B. Li, L. Zhao, and C. Zhao, "Nonlinear estimation for 60GHz millimeter-wave radar system based on Bayesian particle filtering," *EURASIP J. Wireless Commun. Netw.*, vol. 33, no. 1, Dec. 2013.

[11] H. Asplund et al., *Advanced Antenna Systems for 5G Network Deployments: Bridging the Gap Between Theory and Practice*, 1st ed. New York, NY, USA: Academic, 2020.

[12] X. Li and L. Cimini, "Effects of clipping and filtering on the performance of OFDM," *IEEE Commun. Lett.*, vol. 2, no. 5, pp. 131–133, May 1998.

[13] T. Wilkinson and A. Jones, "Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding," in *Proc. IEEE 45th Veh. Technol. Conf. Countdown Wireless 21st Century*, vol. 2, 1995, pp. 825–829.

[14] A. Jayalath and C. Tellambura, "Reducing the peak-to-average power ratio of orthogonal frequency division multiplexing signal through bit or symbol interleaving," *Electron. Lett.*, vol. 36, no. 13, pp. 1161–1163, 2000.

[15] R. Bauml, R. Fischer, and J. Huber, "Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping," *Electron. Lett.*, vol. 32, no. 22, pp. 2056–2057, 1996.

[16] J. Tellado, *Multicarrier Modulation With Low PAR: Applications to DSL and Wireless*. New York, NY, USA: Springer, 2000.

[17] B. Krongold and D. Jones, "PAR reduction in OFDM via active constellation extension," *IEEE Trans. Broadcast.*, vol. 49, no. 3, pp. 258–268, Sep. 2003.

[18] Y. Tang, W. Shieh, and B. S. Krongold, "DFT-spread OFDM for fiber nonlinearity mitigation," *IEEE Photon. Technol. Lett.*, vol. 22, no. 16, pp. 1250–1252, Aug. 2010.

[19] W. Shieh and Y. Tang, "Ultrahigh-speed signal transmission over nonlinear and dispersive fiber optic channel: The multicarrier advantage," *IEEE Photon. J.*, vol. 2, no. 3, pp. 276–283, Jun. 2010.

[20] T.-A. Truong, M. Arzel, H. Lin, B. Jahan, and Michel Jézéquel, "DFT precoded OFDM—An alternative candidate for next generation PONs," *J. Lightw. Technol.*, vol. 32, no. 6, pp. 1228–1238, Mar. 2014.

[21] Z. Wang and G. B. Giannakis, "Wireless multicarrier communications," *IEEE Signal Process. Mag.*, vol. 17, no. 3, pp. 29–48, May 2000.

[22] Z. Wang, X. Ma, and G. B. Giannakis, "OFDM or single-carrier block transmissions?" *IEEE Trans. Commun.*, vol. 52, no. 3, pp. 380–394, Mar. 2004.

[23] F. Pancaldi, G. M. Vitetta, R. Kalbasi, N. Al-Dhahir, M. Uysal, and H. Mheidat, "Single-carrier frequency domain equalization," *IEEE Signal Process. Mag.*, vol. 25, no. 5, pp. 37–56, Sep. 2008.

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

[25] J. Lee, R. French, and L. Miller, "Error-correcting codes and nonlinear diversity combining against worst case partial-band noise jamming of frequency-hopping MFSK systems," *IEEE Trans. Commun.*, vol. 36, no. 4, pp. 471–478, Apr. 1988.

[26] C. Geng and S. A. Jafar, "Secure GDoF of K-user Gaussian interference channels: When secrecy incurs no penalty," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1287–1290, Aug. 2015.

[27] 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.

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

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

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

[31] 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.

[32] T. Li, T. Song, and Y. Liang, *Wireless Communications Under Hostile Jamming: Security and Efficiency*. Singapore: Springer, 2018.

[33] A. El Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[34] Y. Liang, J. Ren, and T. Li, "Secure OFDM system design and capacity analysis under disguised jamming," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 738–752, 2020.

[35] J. R. Barry, E. A. Lee, and D. G. Messerschmitt, *Digital Communication*, 3rd ed. New York, NY, USA: Kluwer, 2003.

[36] F. Miller and A. Vandome, *Advanced Encryption Standard*. Orlando, FL, USA: Alpha, 2009.

[37] 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.



Tongtong Li (Senior Member, IEEE) received the first Ph.D. degree in math from Sun Yat-sen University, Guangzhou, China, in 1995, and the second Ph.D. degree in electrical engineering from Auburn University, Auburn, AL, USA, in 2000.

She was with Bell Labs, Denver, CO, USA, from 2000 to 2002, and had been working on the design and implementation of 3G and 4G systems. She has been with Michigan State University, East Lansing, MI, USA, since 2002, where she is a Professor. Her research interests fall into the areas of wireless and wired communications, wireless security, information theory, and statistical signal processing, with applications in neuroscience.

Prof. Li is a recipient of the National Science Foundation 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 the *EURASIP Journal 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.



Jinxian Deng received the B.S. degree in electrical and computer engineering from Michigan State University (MSU), East Lansing, MI, USA, in 2020, where he is currently pursuing the Ph.D. degree.

He is a Research Assistant with the Broadband Access Wireless Communication Laboratory, Department of Electrical and Computer Engineering, MSU. His research interests fall into the areas of wireless and wired communications, wireless security, information theory, and computational neuroscience.



Jian Ren (Senior Member, IEEE) received the B.S. and M.S. degrees in mathematics from Shaanxi Normal University, Xi'an, China, in 1988 and 1991, respectively, and the Ph.D. degree in electrical engineering from Xidian University, Xi'an, in 1994.

He is a Professor with the Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI, USA. His current research interests include cybersecurity, cloud computing security, distributed data sharing and storage, decentralized data management, blockchain-based e-voting and AI security, and Internet of Things.

Prof. Ren is 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 and the General Chair for ICNC'18, and has been serving as the Executive Chair for ICNC since 2019. He currently serves as an Associate Editor for the IEEE TRANSACTIONS ON MOBILE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, and *ACM Transactions on Sensor Networks*, and a Deputy Editor-in-Chief for *IET Communications*.

Authorized licensed use limited to: Michigan State University. Downloaded on August 07,2023 at 18:48:56 UTC from IEEE Xplore. Restrictions apply.