Can We Have a Better System than OFDM?

Tongtong Li Jinxian Deng Jian Ren
Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824, USA
Email: {tongli, dengjinx, renjian}@msu.edu.

2023 International Conference on Computing, Networking and Communications (ICNC) | 978-1-6654-5719-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICNC57223.2023.10074195

***Abstract*—Due to its high spectral efficiency and simple transceiver design, OFDM is one of the most popular modulation techniques in wireless communications. However, 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 user's signal is deliberately interfered by the adversary, leading to communication failures. An interesting question is: can we have a better system than OFDM? In this paper, first, we reintroduce the IFFT-Relocated OFDM (IR-OFDM), which is essentially a single-carrier system with frequency domain equalization. By relocating the 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 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 the proposed approach are demonstrated through simulation examples. 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 IoT networks.**

***Index Terms*—OFDM, peak-to-average power ratio, IFFT-Relocated OFDM, jamming, secure precoding**

I. Introduction

Orthogonal Frequency Division Multiplexing (OFDM) has become a key modulation technique for reliable high-speed wireless communication, optical fiber transmission and underwater communication, 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) [1], 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 12dB. 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 inter-carrier interference, both resulting in performance losses and higher hardware design complexity in OFDM systems and raising serious challenges for resource limited IoT devices [2], [3].

In literature, there has been a continuous effort to reduce the PAPR of OFDM. Representative techniques include clipping and filtering [4], low-PAPR oriented block coding [5], selective subcarrier mapping [6], tone reservation approach [7], and active constellation extension [8], and DFT-precoded OFDM [9]. With the techniques discussed above, the PAPR can be reduced to approximately 8dB $\sim$10dB, subject to the constellation used and the cost on computational complexity and performance losses.

In this paper, we will reintroduce the IFFT-Relocated OFDM (IR-OFDM), which is essentially a single-carrier system with frequency domain equalization [10]–[12]. 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, IFFT-Relocated 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 literature [13], 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 [14], recent studies indicate that disguised jamming [13], [15], [16], where the jamming is highly correlated with the signal, can be much more destructive than noise jamming. Due to its high similarity with authorized signal, disguised jamming can mislead the receiver and reduce the system capacity to zero even when the jamming power equals the signal power [13], [17].

Motivated by the observations above and our previous research on anti-jamming system design [13], [16], in this paper, we further design the securely precoded IR-OFDM. The basic idea is to randomize the phases of transmitted symbols using the secure pseudo-random sequences generated

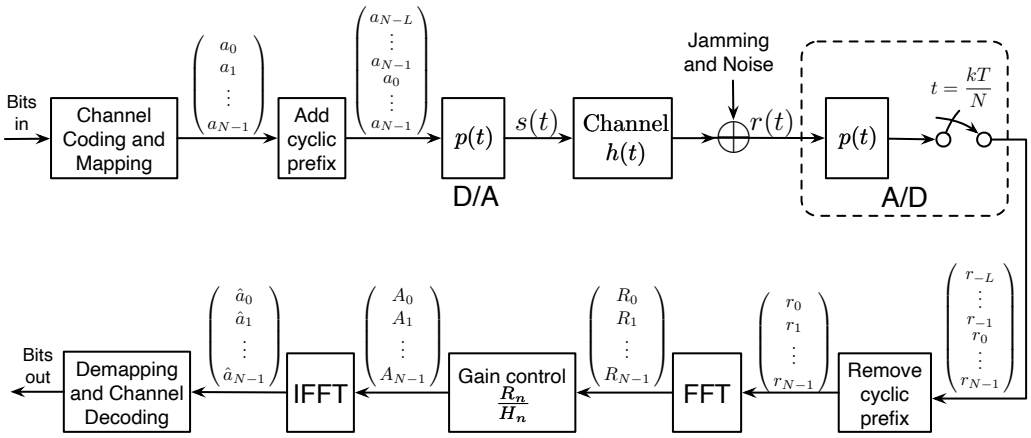

Fig. 1. Block diagram of IFFT-Relocated OFDM.

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 reliable performance of securely precoded IR-OFDM (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. 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, under benign and hostile environments, respectively, especially for resource-constrained Internet of Things (IoT) systems.

II. 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.

In the following, it will be shown 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.

Let $\mathbf{a} = [a_1, a_2, \cdots, a_N]^T$ represent the block of input symbols, generally QAM or PSK symbols, here $(\cdot)^T$ 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.

In fact, at the transmitter, we can define

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

where

$$p(t) = \sqrt{\frac{T}{N}} \frac{\sin(\pi N t/T)}{\pi t} = \sqrt{\frac{N}{T}} \operatorname{sinc}\left(\frac{\pi N t}{T}\right) \tag{2}$$

is the ideal reconstruction filter for a sample rate of $\frac{N}{T}$. Let $\{h_0, h_1, \cdots, h_L\}$ denote the equivalent discrete-time channel impulse response, the received samples r_n can now be represented as

$$r_n = a_n * h_n = \sum_{l=0}^{L} h_l a_{n-l}. \tag{3}$$

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

$$R_n = H_n A_n, \quad n = 0, 1, \cdots, N-1. \tag{4}$$

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.1, and we name this scheme as IFFT-Relocated OFDM (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 1. IR-OFDM requires no precoding, selective mapping, tone reservation or constellation 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.

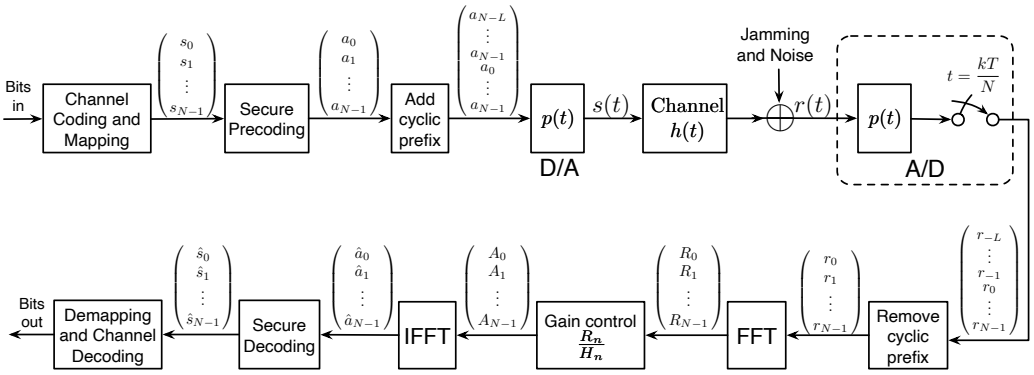

Fig. 2. Block diagram of securely precoded and IFFT-relocated OFDM.

TABLE I
PAPR WITH IFFT-RELOCATED OFDM

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

III. 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. The Disguised Jamming model

In literature [18], 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:

$$r = s + J + w, \tag{5}$$

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

$$C = B\log(1 + \frac{P_s}{P_w + P_J}), \tag{6}$$

where P_s is the signal power, P_w the noise power and P_J the jamming power. From equation (6), 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 [13], [15], [16], 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 [13], [17]. 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 [13]. 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. The 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. 2. In this system, s_k, $k = 0, \cdots, N-1$ denote the original symbols, and a_k, $k = 0, \cdots, N-1$ denote the output of the secure precoder. Consider one symbol block at a time, and define $\mathbf{s} = [s_0, s_1, \cdots, s_{N-1}]^T$ and $\mathbf{a} = [a_0, a_1, \cdots, a_{N-1}]^T$, then the secure precoding process is characterized by

$$\mathbf{a} = \mathbf{P}\mathbf{s}. \tag{7}$$

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

$$\mathbf{P} = \begin{bmatrix} e^{-j\theta_0} & & & \\ & e^{-j\theta_1} & & \\ & & \ddots & \\ & & & e^{-j\theta_{N-1}} \end{bmatrix}. \tag{8}$$

where $\theta_0, \theta_1, \cdots, \theta_{N-1}$ are generated using the AES-based secure pseudorandom phase generator shown in Fig. 3.

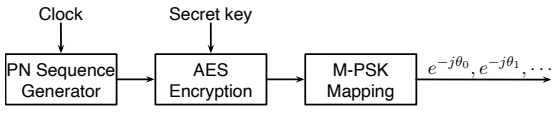

Fig. 3. Secure precoding matrix generator.

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 [19]. Note that the secure phase generation is not limited to any particular cryptographic algorithm, but its 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 additive white Gaussian noise, when M is sufficiently large, the random phase shifts in the secure precoding can be approximated as 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 re-initialization, 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 re-initialization, 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. As will be illustrated in Section IV, 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.

IV. Simulation Results

In this section, we first demonstrate through simulation examples that—while enjoying extremely low PAPR, IFFT-Relocated OFDM (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 securely precoded IR-OFDM (denoted as SP-IR-OFDM) under disguised jamming.

a) Example 1: Performance comparison of IR-OFDM versus traditional OFDM: the performance of IFFT-Relocated OFDM is demonstrated under Rayleigh fading channels with additive white Gaussian noise, 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 bit-error-rate (BER) is averaged overall 2000 Monto Carlo runs. No channel coding is involved. The simulation results are shown in Fig.4.

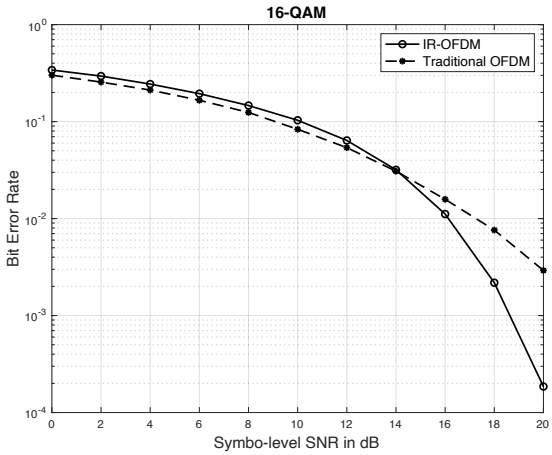

Fig. 4. Performance of IFFT-Relocated OFDM (IR-OFDM) versus traditional OFDM under Rayleigh channels (no channel coding): 16-QAM

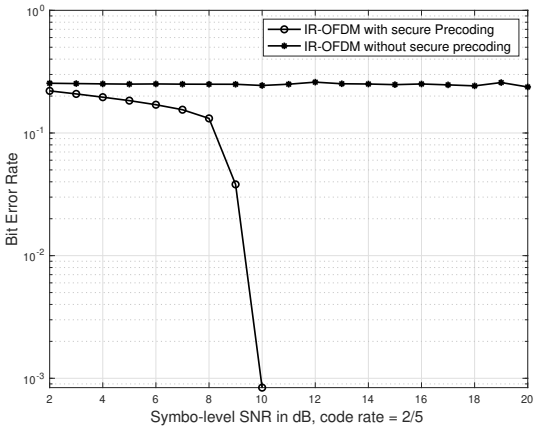

Fig. 5. BER versus symbol-level SNR: IFFT-Relocated OFDM (IR-OFDM) with and without secure precoding under disguised jamming over AWGN channels, signal to jamming power ratio SJR = 0dB, LDPC code rate = 2/5.

From the simulation results, it can be seen that 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.

b) Example 2: Performance comparison of IR-OFDM and Securely Precoded IR-OFDM under disguised jamming: In this example, we analyze the BER of IR-OFDM and securely precoded IR-OFDM under disguised jamming in both AWGN and Rayleigh channels. Here perfect synchronization is assumed, and we use the LDPC codes for channel coding, following the DVB-S.2 standard [20]. The signal-to-jamming ratio (SJR) is set to be 0dB. The BER of the two systems under disguised jamming is calculated versus different SNR levels, and the result is shown in Fig.5 and Fig.6. It can be observed that: (i) under disguised jamming, in the IR-OFDM system, the BER cannot be reduced through channel coding or by reducing the noise power, which indicates that without appropriate anti-jamming procedures, IR-OFDM cannot achieve reliable communications under disguised jamming; (ii)

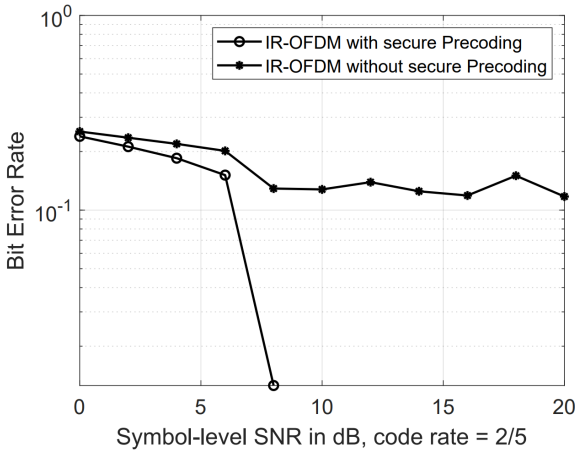

Fig. 6. BER versus symbol-level SNR: IFFT-Relocated OFDM (IR-OFDM) with and without secure precoding under disguised jamming over Rayleigh channels, signal to jamming power ratio SJR = 0dB, LDPC code rate = 2/5.

with the securely precoded IR-OFDM scheme, BER can be significantly reduced when the code rate is sufficiently low. This demonstrates that the proposed securely precoded 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.

V. Conclusions

In this paper, we introduced a new communication scheme, referred to as securely precoded IFFT-Relocated OFDM (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 IFFT-Relocated OFDM (IR-OFDM). 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 securely precoded IR-OFDM (SP-IR-OFDM).

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

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

[3] H. Asplund and D. Astely et al., *Advanced Antenna Systems for 5G Network Deployments: Bridging the Gap Between Theory and Practice*, 1st ed. Academic Press, 2020.

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

[5] T. Wilkinson and A. Jones, "Minimisation of the peak to mean envelope power ratio of multicarrier transmission schemes by block coding," in *1995 IEEE 45th Vehicular Technology Conference. Countdown to the Wireless Twenty-First Century*, vol. 2, 1995, pp. 825–829 vol.2.

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

[7] J. Tellado, *Multicarrier modulation with low PAR: applications to DSL and wireless*. Springer, 2000.

[8] B. Krongold and D. Jones, "PAR reduction in OFDM via active constellation extension," *IEEE Transactions on Broadcasting*, vol. 49, no. 3, pp. 258–268, 2003.

[9] T.-A. Truong, M. Arzel, H. Lin, B. Jahan, and M. Jézéquel, "DFT precoded OFDM—an alternative candidate for next generation PONs," *Journal of Lightwave Technology*, vol. 32, no. 6, pp. 1228–1238, 2014.

[10] Z. Wang and G. B. Giannakis, "Wireless multicarrier communications," *IEEE signal processing magazine*, vol. 17, no. 3, pp. 29–48, 2000.

[11] Z. Wang, X. Ma, and G. Giannakis, "OFDM or single-carrier block transmissions?" *IEEE Transactions on Communications*, vol. 52, no. 3, pp. 380–394, 2004.

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

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

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

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

[16] T. Song, K. Zhou, and T. Li, "CDMA System Design and Capacity Analysis Under Disguised Jamming," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2487–2498, 2016.

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

[18] T. Basar, "The gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

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

[20] A. Morello and V. Mignone, "DVB-S2: The Second Generation Standard for Satellite Broad-Band Services," *Proceedings of the IEEE*, vol. 94, no. 1, pp. 210–227, 2006.