On the Performance of Index Modulation in OFDM Systems under Jamming Attacks

Jaewon Yun and Yo-Seb Jeon
Department of Electrical Engineering, POSTECH, Pohang, Gyeongbuk 37673, Republic of Korea
Email: {jaewon.yun, yoseb.jeon}@postech.ac.kr

Abstract—**Index modulation (IM) is one of the potential options for enhancing system resilience against jamming attacks in orthogonal frequency division multiplexing (OFDM) systems. In this paper, to shed light on its capacity for secure wireless communication, we evaluate the resistance of the OFDM-IM system against jamming attacks, compared to the traditional OFDM system. Specifically, our investigation delves into a practical resource mapping scenario, considered in 5G cellular standards. Our finding is that the advantage of the OFDM-IM system over the conventional OFDM system diminishes as the jamming power increases, but the OFDM-IM system still exhibits its robustness against jamming attacks when the influence of the jamming signals is confined to a small number of subcarriers.**

I. Introduction

In wireless communications, jamming attacks pose a significant threat to system reliability and security [1]. These attacks involve serious interference with the transmission of signals, disturbing communication channels and causing potential service outages. Jamming attacks can take various forms, such as barrage jamming, partial band jamming, tone jamming, sweep jamming, and arbitrary jamming [2], [3]. These attacks target specific subcarriers, time slots, or frequency bands, aiming to degrade signal quality and disrupt operation [4].

Traditional countermeasures against jamming attacks often rely on cryptographic techniques and error-correcting codes [5]. While these methods provide certain levels of protection, they may not be sufficient in scenarios where adversaries have advanced capabilities and knowledge of encryption protocols. Physical-layer security (PLS) techniques offer an additional layer of defense by exploiting the unique properties of the physical channel to enhance security.

Recently, index modulation (IM) [6] has been investigated as a possible PLS technique for orthogonal frequency division multiplexing (OFDM) systems under jamming attacks. OFDM-IM's inherent ability to convey index bits in the presence of noise and interference makes it feasible solution for improving system resilience against the jamming attacks [7]. By leveraging the sparse nature of IM, OFDM-IM provides an effective means of transmitting information even when subcarriers are targeted by jammers. This capability makes OFDM-IM an interesting choice for future wireless communication systems, where security and reliability are paramount.

Our study aims to investigate the performance of OFDM-IM in jamming scenarios, shedding light on its potential as a robust solution for secure wireless communication. In particular, we evaluate the resistance of the OFDM-IM system against jamming attacks for a practical resource mapping scenario, in which modulated signals are allocated to a designated resource block, as done in 5G cellular standards. Our simulations demonstrate that the performance gain of the OFDM-IM system over the conventional OFDM system decreases as the jamming power increases, but the OFDM-IM system still exhibits its robustness against jamming attacks when the number of subcarriers affected by jamming signals is small.

II. System Model

In this section, we present a communication system for both OFDM and OFDM-IM in the presence of jamming. We also introduce the jamming attack types based on the pattern of jamming signals in the frequency domain.

A. Communication System under Jamming Attack

We consider a multi-carrier communication system with L subcarriers. At the transmitter, m information bits are modulated to generate a frequency domain sequence represented as $\boldsymbol{x} = [x(1), x(2), \cdots, x(L)]^{\mathsf{T}}$ such that $\mathbb{E}[|x(\ell)|^2] = E_b$ for all $\ell \in \{1, \dots, L\}$. Let $\boldsymbol{W}_L$ be the $L \times L$ discrete Fourier transform (DFT) matrix, satisfying $\boldsymbol{W}_L^{\mathsf{H}}\boldsymbol{W}_L = L\mathbf{I}_L$, where $\mathbf{I}_L$ denotes the $L \times L$ identity matrix. Then, the L-point inverse DFT (IDFT) is applied to $\boldsymbol{x}$, in order to generate a time domain sequence represented as $\boldsymbol{x}_T = \frac{1}{\sqrt{L}}\boldsymbol{W}_L^{\mathsf{H}}\boldsymbol{x} = [X(1), X(2), \cdots, X(L)]^{\mathsf{T}}$. After the IDFT operation, a cyclic prefix (CP) of length $L_{\text{CP}} \geq L_{\text{CIR}} - 1$ is appended to the beginning of the time domain signal, where L_{CIR} denotes the number of channel impulse response (CIR) taps. Finally, the CP-appended time domain signal is transmitted to the receiver.

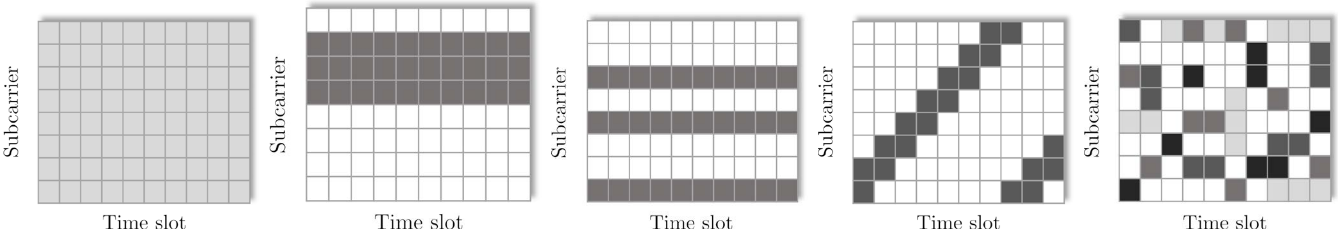
At the receiver, after removing the CP, the L-point DFT is applied to the time domain received signal. Assuming perfect synchronization, the resulting frequency domain received signal is expressed as

$$y(\ell) = h(\ell)x(\ell) + w(\ell) + c(\ell)j(\ell), \tag{1}$$

where $h(\ell)$ is the channel frequency response at subcarrier ℓ, $w(\ell) \sim \mathcal{CN}(0, N_W)$ is additive white Gaussian noise with

This work was supported in part by Korea Research Institute for defense Technology planning and advancement(KRIT) - Grant funded by the Defense Acquisition Program Administration(DAPA) (KRIT-CT-22-078) and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2022R1C1C1010074).

979-8-3503-1327-7/23/$31.00 ©2023 IEEE



(a) Barrage jamming (BJ) (b) Partial band jamming (PBJ) (c) Tone jamming (TJ) (d) Sweep jamming (SJ) (e) Arbitrary jamming (AJ)

Fig. 1. Illustration of jamming patterns in the time-frequency domain according to jamming attack type.

variance N_W, $c(\ell) \geq 0$ is a jamming power coefficient that represents the power of the jamming signal at subcarrier ℓ, and $j(\ell) \sim \mathcal{CN}(0, N_J)$ [7].

B. Jamming Attack Types

In this subsection, we introduce five types of the jamming attack, each of which has a different jamming pattern in the time-frequency domain. We denote the ratio of a jamming bandwidth to a signal bandwidth by $\rho = n_c/L$, where n_c is the number of non-zero jamming signals across L subcarriers (i.e., $n_c = \|\boldsymbol{c}\|_0$). To satisfy the power constraint, the total power of the jamming signals within each time slot is set as $\|\boldsymbol{c}\|^2 = L\rho$, where $0 < \rho \leq 1$.

- Barrage jamming (BJ): In BJ, the jamming power is uniformly spread over all subcarriers, as illustrated in Fig. 1(a). Therefore, we have $\rho = 1$ and $c(\ell) = 1$, $\forall \ell \in \{1, \dots, L\}$.
- Partial band jamming (PBJ): PBJ involves attacking only a partial band of subcarriers with equal power, as shown in Fig. 1(b). The jammer targets n_c consecutive subcarriers, leading to $0 < \rho < 1$.
- Tone jamming (TJ): In TJ, the jammer targets specific subcarriers with uniform power, as shown in Fig. 1(c). TJ focuses on attacking a set of n_c randomly chosen subcarriers, leading to $0 < \rho < 1$.
- Sweep jamming (SJ): SJ entails a jammer that follows a consistent pattern across time slots, targeting particular subcarriers for attack, as seen in Fig. 1(d). SJ attacks n_c consecutive subcarriers within each time slot, leading to $0 < \rho < 1$.
- Arbitrary jamming (AJ) [7]: In AJ, the jammer attacks random subcarriers during each time slot, and these attacks involve variations not only in power but also in the number of targeted subcarriers, as shown in Fig. 1(e).

III. Transmission and Reception Schemes

In this section, we present the transmission techniques for both OFDM and OFDM-IM systems, along with the corresponding maximum likelihood (ML) detection method for the receiver.

A. OFDM System

In the OFDM system, the transmitter employs a symbol constellation set $\mathcal{S}$ with an order of M, containing 2^M symbols. For example, if the BPSK modulation is employed, the symbol constellation set is given by $\mathcal{S} = \{-\sqrt{E_b}, \sqrt{E_b}\}$ with $M = 1$. The transmitter divides the m coded bits into $K = m/M$ groups, with each group containing M bits. Then, each group of M bits is mapped into a symbol from the constellation set based on a predetermined mapping rule. Each symbol is transmitted using a single subcarrier, resulting in $x(\ell) \in \mathcal{S}$ for all $\ell \in \{1, \dots, L\}$. Note that the constellation set is properly determined to satisfy $\mathbb{E}[|x(\ell)|^2] = E_b$ for all $\ell \in \{1, \dots, L\}$.

In the OFDM system, all the transmitted signals in $\{x(\ell)\}$ are independent. Meanwhile, both the noise and jamming signals are circularly symmetric complex Gaussian, as explained in Sec. II-A. Therefore, from (1), the ML detection rule for determining the transmitted signal at subcarrier ℓ is given by

$$\hat{x}(\ell) = \underset{x \in \mathcal{S}}{\operatorname{argmin}} \, |y(\ell) - h(\ell)x|^2, \quad \forall \ell \in \{1, \dots, L\}. \tag{2}$$

B. OFDM-IM System

In the OFDM-IM system, the transmitter splits the m coded bits into $G = m/p$ groups, with each group containing p bits. Then, each group of p bits constructs an OFDM-IM subblock which consists of N frequency domain signals. The fundamental idea behind subblock construction involves activating K signals among the N signals while deactivating the remaining $N - K$ signals. Suppose $p = p_1 + p_2$ with $p_1 > 0$ and $p_2 > 0$. The first p_1 bits out of the p bits are used to represent indicate the indices of the K active signals among the N signals in the subblock. Meanwhile, the remaining p_2 bits determine the K symbols corresponding to the K active signals. The above construction implies that $p_1 \leq \log_2(C(N, K))$ and $p_2 = K \log_2 M$, where $C(N, K)$ is the number of ways to choose K elements out of a set of N elements, and M is the modulation order of the constellation set. For the fairness of the power allocation, the constellation set is properly determined to satisfy $\mathbb{E}[\|\boldsymbol{x}_g\|^2] = NE_b$ for all $g \in \{1, \dots, G\}$, where $\boldsymbol{x}_g$ is the g-th OFDM-IM subblock.

At the receiver, for the ML detection, each OFDM-IM subblock needs to be jointly determined from the corresponding received signals. Let $\boldsymbol{y}_g$ be a received signal vector for the g-th OFDM-IM subblock, which consists of N frequency domain received signals associated with the subcarriers utilized for transmitting $\boldsymbol{x}_g$. Also, let $\mathcal{X}_g$ be a set that consists of all possible candidates for $\boldsymbol{x}_g$. Then, from (1), the ML detection rule for determining $\boldsymbol{x}_g$ is given by [7]

$$\hat{\boldsymbol{x}}_g = \underset{x \in \mathcal{X}_g}{\operatorname{argmin}} \, \|\boldsymbol{y}_g - \boldsymbol{h}_g \odot \boldsymbol{x}_g\|^2, \quad \forall g \in \{1, \dots, G\}, \tag{3}$$

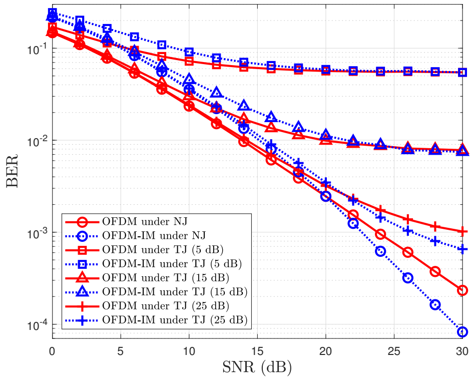


Fig. 2. BER comparison of the OFDM and OFDM-IM systems with and without the jamming attack.

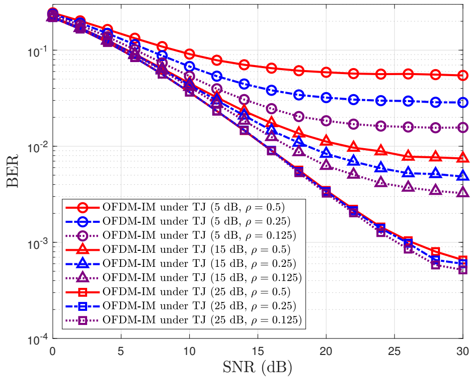


Fig. 3. BER comparison of the OFDM-IM system under the TJ attack with different parameters.

where $\odot$ is the Hadamard product, and $\boldsymbol{h}_g$ consists of N channel frequency responses associated with the subcarriers utilized for transmitting $\boldsymbol{x}_g$.

IV. Numerical Results

In this section, we evaluate the bit error rates (BERs) of the OFDM and OFDM-IM systems under the jamming attack, using simulations. We consider the frequency-selective Rayleigh fading channel, in which the i-th CIR tap is distributed as $\mathcal{CN}(0, \sigma_i^2)$. To determine the channel-tap powers in $\{\sigma_i^2\}_{i=1}^{L_{\text{CIR}}}$, we employ the extended typical urban power delay profile (PDP). We assume that $m = 672$ information bits are mapped into a resource block (RB) which consists of $L_{\text{RB}} = 12$ subcarriers and $N_{\text{RB}} = 54$ time slots. By assuming $L = 1024$, each OFDM symbol consists of 85 resource blocks, and a total of $L_{\text{RB}} \times 85 = 1020$ subcarriers are utilized for data transmission. For the OFDM system, we set $M = 2$ (i.e., BPSK modulation). For the OFDM-IM system, we set $N = 4$, $K = 2$, and $M = 2$. The other system parameters are configured as follows: the central frequency is set to $f_c = 3.5$ GHz, the time slot interval is $t_s = 71.35$ μs, and the receiver speed is $v = 3$ km/s. We assume that channel estimation is perfect. The signal-to-noise ratio (SNR) and signal-to-jamming ratio (SJR) are defined as SNR $= \frac{E_b}{N_W}$ and SJR $= \frac{E_b}{N_J}$, respectively.

In Fig. 2, we compare the BERs of the OFDM and OFDM-IM systems with and without the jamming attack, where NJ stands for no jamming. Fig. 2 shows that without the jamming attack, the OFDM-IM system outperforms the OFDM system when the SNR exceeds 20 dB. However, under the jamming attack, the performance gap between the OFDM and OFDM-IM systems decreases as the SJR decreases (i.e., the jamming power increases). This is because, in the OFDM-IM system, if the jamming signal is present on the subcarrier with the active signal, it is challenging not only to detect the correct symbol in that subcarrier, but also to correctly identify the indices of the active signals. On the contrary, in the OFDM system, the jamming signal in a certain subcarrier exclusively corrupts a single modulated symbol transmitted using that subcarrier, without exerting any influence on the other symbols.

In Fig. 3, we compare the BERs of the OFDM-IM system under the TJ attack with different parameters. Fig. 3 shows that for the same total power of the jamming signals, the BER of the OFDM-IM system improves as the signal-to-jamming bandwidth ratio ρ reduces. This is because with a lower value of ρ, the impact of the jamming signals is limited to fewer subcarriers. Notice that only a subset of the subcarriers are active for data transmission in the OFDM-IM system. Therefore, this system is robust in scenarios with a small number of the jammed subcarriers.

V. Conclusion

In this paper, we investigated the resistance of the OFDM-IM system against jamming attacks, compared to the traditional OFDM system. Our key finding is that under a practical resource mapping scenario, the advantage of the OFDM-IM system over the conventional OFDM system diminishes as the jamming power increases. Nevertheless, the OFDM-IM system still exhibits its robustness against jamming attacks when the influence of the jamming signals is confined to a small number of subcarriers.

References

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

[2] R. A. Yost and R. H. Pettit, "Susceptibility of DS/FH,M, binary DPSK to partial and full band barrage jamming," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 17, no. 7, pp. 665–675, Jul. 1985.

[3] C.-L. Chang and T.-M. Tu, "Performance analysis of FFH/BFSK product-combining receiver with partial-band jamming over independent Rician fading channels," *IEEE Trans. Wireless. Commun.*, vol. 4, no. 6, pp. 2629–2635, Nov. 2005.

[4] N. A. White, P. S. Maybeck and S. L. DeVilbiss, "Detection of interference/jamming and spoofing in a DGPS-aided inertial system," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 34, no. 4, pp. 1208-1217, Oct. 1998.

[5] A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 101–114, Jan./Feb. 2012.

[6] E. Basar, Ü. Aygölü, E. Panayirci, and H. V. Poor, "Orthogonal frequency division multiplexing with index modulation," *IEEE Trans. Signal Process.*, vol. 61, no. 22, pp. 5536–5549, Nov. 2013.

[7] A. Kaplan, M. Can, I. Altunbas, G. K. Kurt, and D. Kucukyavuz, "Comparative performance evaluation of LDPC coded OFDM-IM under jamming attack," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 6209–6224, May 2023.