Physical Communication 55 (2022) 101909

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Reactive jammer detection in OFDM with index modulation ☆

Ufuk Altun [a,d,*], Ahmet Kaplan [a], Gunes Karabulut Kurt [a,b], Ibrahim Altunbas [a], Defne Kucukyavuz [c], Mustafa Kesal [c], Ertugrul Basar [d]

[a] Istanbul Technical University, Department of Electronics and Communication Engineering, Istanbul, Turkey
[b] Poly-Grames Research Center, Department of Electrical Engineering, Polytechnique Montréal, Montréal, Canada
[c] ASELSAN Inc., Ankara, Turkey
[d] Koc University, Department of Electrical and Electronics Engineering, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 25 May 2022
Received in revised form 26 August 2022
Accepted 26 September 2022
Available online 6 October 2022

Keywords:
Jammer detection
OFDM
OFDM-IM
Reactive jammer

ABSTRACT

Detection of jamming attacks is an important tool to improve the resource efficiency of jammer resilient communication networks. Detecting reactive jammers is especially difficult since the attacker is cognitive and focuses only on the used channels. Orthogonal frequency division multiplexing with index modulation (OFDM-IM) consists of active and passive subcarriers. Only active subcarriers carry modulated signals while passive subcarriers are left unused. In OFDM-IM systems, information bits are also dynamically embedded in the indices of these active subcarriers. As a result, remaining passive subcarriers cause instantaneously changing and unused holes in the spectrum that a reactive jammer cannot escape from attacking. In this paper, we propose an OFDM-IM-based detection scheme to improve the detection performance against reactive jammers. The proposed method exploits the dynamically changing empty OFDM-IM subcarriers to improve detection performance. A detection mechanism that is based on the variance of received signals is considered to identify the jammed subcarriers reliably and with low complexity. We assumed a destructive and elusive reactive jammer model that applies a zero-mean Gaussian jamming signal to the occupied channels. The performance of the variance detector is investigated analytically for OFDM-IM and OFDM-based systems under the given jammer model. The results showed that passive subcarriers of OFDM-IM inherently provide a better detection performance compared to the classical OFDM. Lastly, the analytical results are verified via simulations against both full-band and partial-band reactive jammers. Also, the effect of noise and the jamming power on the detection performance is investigated via extensive simulations.

1. Introduction

Multiple access and broadcast nature of wireless channels enable the mobility of communication networks. On the other hand, the same nature presents a high vulnerability to attacks on the physical layer such as eavesdropping or jamming [1]. Providing security against these attacks is a major design challenge and requires additional network resources. A common approach against passive attacks, e.g. eavesdropping, is not based on hiding the transmitted signals at the physical layer. Instead, the information is secured with encryption techniques at the upper layers. The jamming attacks are, however, extremely hard to deal with in the upper layers and effective countermeasures are usually based on avoiding the attacker at the physical layer.

Designing a jamming strategy and the corresponding countermeasure are the two sides of the same paradigm and require a good understanding of both sides. The success of an attack or defense mechanism heavily depends on the opposite side's characteristics. For example, an anti-jamming method can provide resilience against a low-complexity jammer by increasing its signal power and surpassing the jamming signal. However, a cognitive jammer that concentrates its jamming power at a crucial point of legitimate communication cannot be avoided with this countermeasure. Here, avoiding the jammer at its cognition stage can be more efficient, although this approach can require additional complexity and bandwidth. Eventually, each countermeasure-jammer pair presents a different balance between the design complexity, resource consumption, and communication quality.

Detecting jammers and identifying their nature is essential for an anti-jamming method to adjust itself against various types of jammers [2,3]. Especially, the resource consumption can be highly reduced by activating the countermeasures only in the presence of a detected jammer. A straightforward method to detect jamming attacks is to measure the packet delivery ratio (PDR) at the

☆ This work was supported by ASELSAN Inc..
* Corresponding author at: Istanbul Technical University, Department of Electronics and Communication Engineering, Istanbul, Turkey.
E-mail address: altunu@itu.edu.tr (U. Altun).

https://doi.org/10.1016/j.phycom.2022.101909
1874-4907/

upper layers [4]. However, PDR does not give any information on the jammer's type. On the other hand, physical layer properties (e.g. signal strength) can be beneficial to identifying the jammer's characteristics [5,6]. Joint usage of signal strength and PDR methods are considered in [5] to improve detection performance. Han et al. [7] propose a jamming detection algorithm which is based on the maximum and minimum variances of the pilot subcarriers of OFDM symbols. The authors of [8] analyze anti-jamming communication using prospect theory (PT) to investigate end-user subjectivity. The objective of both a smart jammer and a secondary user is to increase their signal-to-interference-plus-noise ratio (SINR) based on their PT-based utility functions in a fading channel. Recently, [9] proposed an IM-based frequency hopping (FH) scheme to avoid jamming attacks. The study exploits the traditional FH mechanism to avoid jammers. However, it proposes to carry additional information on the used FH pattern. In other words, the model selects an FH pattern from a pool based on information bits and uses an energy detector at the receiver to obtain the information. In [10], the authors propose a deception strategy by backscattering jamming signals. The study is based on luring the reactive jammer to send jamming signals and then backscattering the received jamming signals to the legitimate receiver. The results of [10] show that communication throughput can be increased when the jamming power increases. The study uses a deep learning-based jamming detection algorithm as a part of a multi-stage framework. Compared to the proposed approach, the detection algorithm of [10] is extremely complex since it requires a training process.

OFDM-IM is an emerging technique that combines traditional OFDM with index modulation (IM) to achieve better performance [11]. An index modulation scheme carries extra information by embedding additional information bits into the indices of a domain. This notion gained popularity with the development of spatial modulation (SM) which uses active antenna indices as a domain (refer to [12] for detailed information). Similar to SM schemes, an OFDM-IM scheme uses active subcarrier indices as a domain and carries extra information by embedding information bits into active subcarrier indices.

OFDM-IM has been pioneered by Basar et al. starting with [11]. Afterwards, various new adaptations of OFDM-IM have been proposed in the literature to improve its performance. In [13], the authors propose layered OFDM-IM, which can increase the number of carried IM bits compared to the traditional OFDM-IM. The main idea behind [13] comes from dividing the subcarrier set into multiple layers in which all layers use a unique constellation. Another interesting idea focuses on eliminating the disadvantages of null subcarriers of OFDM-IM. The authors of [14,15] propose multiple-mode OFDM-IM which eliminates null subcarriers by modulating them with distinct constellations. Moreover, an interleaved grouping method is proposed in [16] which achieves better information rates than traditional OFDM-IM. In [17,18], the authors consider dynamically changing the number of active subcarriers which is fixed in classical OFDM-IM. The performance of OFDM under jamming attack is investigated in [19,20] and it has been shown in [21] that OFDM-IM is more resilient to jammers than the conventional OFDM systems.

Advanced detection schemes exist in the literature for OFDM-IM as in [22,23]. However, these schemes have practical challenges and have never been tested against jamming attacks. On the other hand, energy/variance-based detectors are well known for OFDM-IM systems and jamming scenarios. The presence of the jammer detection algorithms regarding OFDM or OFDM-IM techniques is quite limited in the literature (to our knowledge, only Kaplan et al. [21] considers the performance of OFDM-IM under jamming attacks). However, a more general form of the jammer detection problem that we are interested in can be found in signal detection algorithms of OFDM-based systems. Cognitive radio networks use energy detection to identify available frequency channels. Energy detector designs of OFDM-based cognitive radios [24–26] present a similar detection problem. The authors of [27] also proposed a similar detection mechanism to distinguish between OFDM frames under narrow-band interference.

In this paper, we propose a novel jamming detection method that exploits the sparsity of OFDM-IM symbols. We first focus on the jamming detection capabilities of OFDM-IM systems and demonstrate that the detection of highly complex reactive jammers is possible with OFDM-IM-based communications. The motivation behind this study is to exploit the vacant subcarriers that are unique to OFDM-IM to improve detection performance. OFDM-IM presents empty subcarriers that are spread in each symbol, i.e. holes in the spectrum. Since the location of empty subcarriers change in each symbol according to the information bits, even reactive jammers that observe the spectrum cannot avoid attacking the empty subcarriers. These holes present an opportunity to obtain clean observations for the hypothesis test. Our contributions can be listed as follows.

- *The proposed OFDM-IM-based detection scheme outperforms traditional methods on detecting reactive jammers:* A novel detection mechanism that is based on OFDM-IM and sample variance is proposed against reactive jammers. It is shown that empty subcarriers of the OFDM-IM scheme present better detection performance than the filled subcarriers. Traditional schemes such as OFDM carry modulated signals at each subcarrier. As a result, they require additional methods such as frequency hopping to obtain empty subcarriers and reach the same performance as OFDM-IM. However, OFDM-IM possesses empty subcarriers in its nature without needing an additional method and sacrificing additional bandwidth. Since the task is identifying active/passive/jammed subcarriers, variance/energy detectors provide a low complexity and reliable solution.
- *Detection performance of the proposed method is analytically investigated and compared with OFDM scheme:* The detection and false alarm probabilities are derived in closed form expressions and used in order to prove the performances of OFDM and OFDM-IM.
- *OFDM and OFDM-IM schemes are compared with extensive simulations and the analytical results are verified:* Numerical results show that OFDM-IM-based scheme outperforms OFDM on the detection performance under both full-band and partial-band reactive jammers.

The paper is organized as follows. Section 2 is dedicated to the system model and preliminary information on OFDM-IM and jamming attacks. In Section 3, the jamming detection capability of the OFDM-IM is investigated and the theoretical results are presented. Numerical results are given in Section 4. The paper is concluded in Section 5.

2. Preliminaries

We consider a wireless communication network where two users aim to communicate with each other in the presence of a jammer. Our objective is to obtain information on the jamming attack to determine an effective countermeasure. Our model requires an explanation of three aspects; the jammer model, the communication model and the detection basics (e.g. performance metrics). In this section, we give the related definitions and preliminaries. Throughout the paper, expected value and variance operators are denoted by $E[\cdot]$ and $\mathrm{v}(\cdot)$, respectively.

2.1. Jammer model

A jammer is fundamentally a malicious node that introduces its signal to the channel with the purpose of sabotaging the communication of legitimate users. Jammers can be categorized according to their signal type, their cognitive capabilities or the amount of the jammed frequency band.

2.1.1. Signal type

Jamming signals can be *random* (i.e. noise) or *meaningful* (i.e. interference) or even *correlated* with the legitimate transmission [28]. Noise jammers fundamentally generate a random signal (most commonly Gaussian distributed) at the target frequency. In the interference attacks, the jammer transmits modulated signals at the target frequency in order to distort the legitimate signal. The jammers can also transmit signals that are correlated with the legitimate transmission to inflict the most damage to vulnerable portions of legitimate communication. However, correlated signals require highly complex jammer designs while the generation of noise signals is straightforward. We consider the existence of a noise jammer for the performance evaluations as the detection of correlated signals requires measures beyond our scope.

2.1.2. Cognitive capabilities

The complexity of a jammer design allows jammers to generate more energy-efficient, intense and elusive attacks. In the simplest form, *constant jammers* insert its signal to the channel continuously which is energy inefficient and easily detectable. *Random jammers* use random schedules where they give breaks on their attacks to improve energy efficiency. *Reactive jammers*, on the other hand, emit their signals only when they detect a communication over the channel instead of using a random schedule [29,30]. These cognitive capabilities make reactive jammers highly elusive and energy-efficient in exchange for complexity. In our model, we consider reactive jammers and improve the network's robustness against them.

2.1.3. The amount of jammed frequency band

Jammers can cover the full-band or a partial-band of the used channel. The coverage of the spectrum presents an energy distribution problem for the jammer. A *full-band* jammer (*barrage* jammer, BJ) distributes its energy equally to whole spectrum while the *partial-band* jammers (PBJ) attack only a portion of it. Partial-band jammers can dedicate its total energy to a single subchannel (*single-tone* PBJ) or multiple subchannels (*multi-tone* PBJ). The energy distribution problem of jammers is recently considered in [21] and an *arbitrary* jammer model that considers nonuniform energy distributions to subchannels is proposed.

In this paper, for analytical simplicity, we consider a zero-mean Gaussian noise multi-tone reactive jammer, and this approach is commonly used in the literature [31]. The jammer is assumed to have cognitive capabilities such that it can observe the spectrum for a period of time and makes an estimation on the occupied subchannels with its observation. When the jammer's detection algorithm detects an occupied frequency band, it inserts a zero-mean Gaussian distributed jamming signal targeting the occupied band. We model the interaction of the jammer and the communication system in accordance with the literature as [7,20,28],

$$y = xh + j + w \tag{1}$$

where y, x, h, j and w are the received signal, transmitted signal, channel gain, jamming signal and additive noise in the frequency domain, respectively.

Table 1
An example of OFDM-IM look-up table for $(n; k) = (4; 2)$.

Bits	Indices	OFDM-IM subblocks
[0 0]	{1, 2}	[s_1, s_2, 0, 0]
[0 1]	{2, 3}	[0, s_1, s_2, 0]
[1 0]	{3, 4}	[0, 0, s_1, s_2]
[1 1]	{1, 4}	[s_1, 0, 0, s_2]

2.2. OFDM-IM

OFDM-IM joins traditional OFDM with index modulation and exploits the frequency selectivity of the wireless channel to obtain a better error performance. OFDM-IM is similar to the traditional OFDM on its multiplexing and modulation principles as it uses N orthogonal subcarriers and IFFT-FFT modulation–demodulation. In addition to OFDM, information bits are also carried at the indices of the OFDM-IM subcarriers [11]. Carrying information on the indices of a parameter is a well-known paradigm in the literature and referred as index modulation [32,33]. The novelty of the OFDM-IM scheme comes from using the OFDM subcarriers as a parameter for index modulation.

Example 1. The working mechanism of an OFDM-IM scheme can be illustrated with an example as given in Fig. 1. For this example, consider a traditional OFDM scheme with N subcarriers, where each subcarrier carries a modulated signal denoted by $s \in S$, and S is the set of M-ary signal constellation symbols. OFDM-IM divides these N subcarriers into g subblocks that each subblock contains $n = N/g$ subcarriers and conveys $p = p_1 + p_2$ bits. In each subblock, k subcarriers are selected as active to carry modulated signals according to first $p_1 = \lfloor \log_2 C(n; k) \rfloor$ bits of p bits whereas $n - k$ subcarriers are left empty, i.e. passive, where $C(n; k)$ is the binomial coefficient and $\lfloor \cdot \rfloor$ is the floor function. The modulated signals that are determined by remaining $p_2 = k \log_2 M$ bits are transmitted using active subcarriers and are expressed as $s \in S, \quad = 1; 2; \dots; k$ in each subblock. The total number of transmitted bits and active subcarriers in each OFDM-IM symbol are given by $m = pg$ and $K = gk$, respectively. In our example, each $n = 4$ subcarriers forms a subblock and $k = 2$ subcarriers contain modulated signals s_1 and s_2 in each subblock.

OFDM-IM nodes use a look-up table to assign information bits to the subcarrier indices and then reconstruct the information bits from the indices. The look-up table of an $(n; k) = (4; 2)$ system is given in Table 1. As illustrated in the Table, the transmitter can gain 2 bits of information from 4 possible index sequences. On the other hand, information bits are also carried in the modulated signals and the number of signal-bearing subcarriers is intentionally reduced in OFDM-IM (passive subcarriers). The selection of $(n; k)$ pairs and their effect on the system performance is investigated in [11]. The parameters $(n; k) = (4; 2)$ are shown to outperform OFDM on BER performance and are usually considered as a benchmark.

2.3. Detection basics

The objective of a detection problem is to successfully classify an observation among two distinguishable options. In a jamming detection problem, these two options become the existence and the absence of the jammer in the wireless medium. Solving the detection problem starts with defining the expected observations for these options as the hypotheses of the problem. We define the hypotheses of the jamming detection problem with the observations of OFDM-IM symbols. These hypotheses can be given as

$$\begin{aligned} H_0 &: \quad y_i = x_i h_i + j_i + w_i; \\ H_1 &: \quad y_i = x_i h_i + w_i; \end{aligned} \tag{2}$$

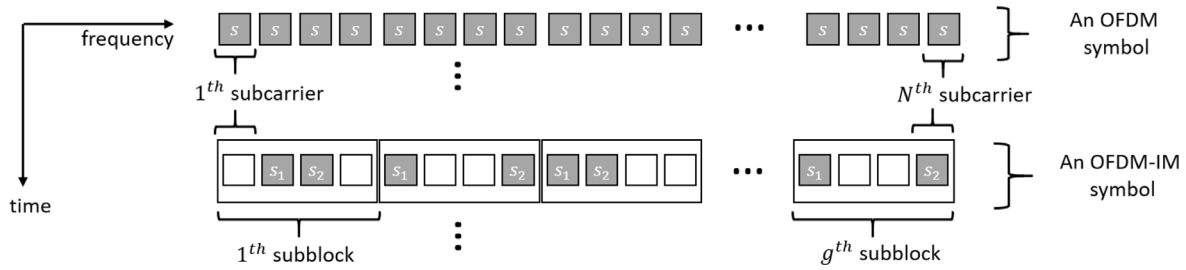


Fig. 1. An illustration of OFDM and (4; 2) OFDM-IM subcarriers. Each square represents a subcarrier. Each subcarrier of an OFDM symbol carries a modulated signal that is denoted by s. In a (4; 2) OFDM-IM, a symbol is divided into subblocks that consist of 4 subcarriers. Each subblock carries information on modulated signals $s_1; s_2$ as well as on the indices of the active subcarriers.

in the frequency domain after the FFT operation (see [11] for detailed information on the block diagram of OFDM-IM). H_0 is the null hypothesis that indicates the existence of a jammer. H_1 hypothesis is the jammer-free scenario. The observation of the ith subcarrier is represented with $y_i;\ i = \{1; 2; \dots; N\}$. The additive noise, the fading coefficient and the jamming signal on the ith subcarrier are denoted with $w_i \sim \mathcal{CN}(0; N_w)$, $h_i \sim \mathcal{CN}(0; 1)$ and $j_i \sim \mathcal{CN}(0; N_j)$, respectively, where $\mathcal{CN}$ is the circularly symmetric complex Gaussian distribution.

It should be noted that N_w is the variance of the noise signal in the frequency domain, which is related by the noise variance in the time domain, denoted as $N_{w;t}$, by $N_w = \frac{k}{n} N_{w;t}$. Also, the variance of jamming signal in frequency domain, N_j, is related with the jamming variance in time domain, denoted as $N_{j;t}$, via $N_j = \frac{k}{n} N_{j;t}$, where is the ratio of jammed frequency bandwidth to signal bandwidth. Here, can be defined as $= \frac{d}{N}$ where d is the number of subcarriers under jamming attack and N is the total number of subcarriers in an OFDM-IM symbol and $0 < \leq 1$ [21]. Transmitted signal of the ith subcarrier is denoted with x_i, where $x_i = 0$ for passive (empty) subcarriers and selected from a signal constellation ($x_i \neq 0$) for active (filled) subcarriers depending on the information bits and the look-up table. The constellation is assumed to be zero-mean and the symbol energies, E_s, are normalized. Here we define the signal-to-noise ratio (SNR) and the signal-to-jamming ratio (SJR) of a symbol by [11],

$$\text{SNR} = \frac{E_s}{N_{w;t}} = \frac{E_s k}{N_w n}; \qquad \text{SJR} = \frac{E_s}{N_{j;t}} = \frac{E_s k}{N_j n}: \tag{3}$$

In a detection mechanism, test statistics ($T(\cdot)$) are compared with a threshold ( ) to make a decision. An observation is decided as H_0 or H_1 when $T(\cdot) >$ or $T(\cdot) \leq$, respectively. Test statistics fundamentally indicate the rules that are used to classify an observation. The efficiency of the test statistics relies on the characteristics of the hypotheses.

The performance of the detection mechanism is measured with the probability of detection (P_d) and the probability of false alarm (P_{fa}) as follows:

$$\begin{aligned} P_d &= P(T(\cdot) > \ ; H_0); \\ P_{fa} &= P(T(\cdot) > \ ; H_1): \end{aligned} \tag{4}$$

Here, various threshold values result in different P_d and P_{fa} characteristics. Investigation of the threshold values reveals a trade-off between P_d and P_{fa}. This trade-off is illustrated through receiver operating characteristic (ROC) curves, where the P_d is depicted as a function of P_{fa}. A detection application usually requires a minimum P_d or a maximum P_{fa} condition in their designs. ROC curves illustrate the expected success or false alarm performance of these conditions according to the used test statistics.

3. Jamming detection with OFDM-IM

OFDM-IM exploits the traditional OFDM subcarriers for index modulation. As depicted in Fig. 1, an OFDM-IM symbol consists of subblocks in which certain subcarriers are left passive (unused). OFDM-IM compensates this lost information of passive subcarriers by carrying information on the indices of active subcarriers. Passive subcarriers are also the main components of the detection mechanism.

The jammer is modeled with zero-mean distribution to deceive simple detection mechanisms such as mean detection ($T(y_i) = E[y_i] > $). An efficient solution against zero-mean distributed jamming attacks is using variance detectors, which is a well-known technique in the literature. The following proposition presents the unique interaction of the passive subcarriers and the variance detector.

Proposition 1. *Let the channel model and the hypotheses of the detection problem be as in (2) and the performance metrics P_d and P_{fa} be as in (4), where $T(y_i) = \mathrm{v}(y_i)$ and $\mathrm{v}(\cdot)$ is the variance operator.*

For any $P_{fa} \in (0; 1)$, following inequality holds,

$$P_{d;\ passive} > P_{d;\ OFDM} > P_{d;\ active}; \tag{5}$$

such that $P_d = P(\mathrm{v}(y_i) > \ ; H_0)$, where is the threshold. $P_{d;\ passive}$, $P_{d;\ active}$ and $P_{d;\ OFDM}$ represents the detection probabilities of passive OFDM-IM, active OFDM-IM and OFDM subcarriers, respectively.

Proof. The variance of a subcarrier can be estimated as

$$\mathrm{v}(y_i) = \frac{1}{Z-1} \sum_{z=1}^{Z} |y_{i;z} - \overline{y_i}|^2 \tag{6}$$

where Z is the number of observations, y_i is the observation of the ith subcarrier and $\overline{y_i} = \frac{1}{Z} \sum_{z=1}^{Z} y_{i;z}$.

The authors of [34] state the following three statements in Theorem 5.3.1 that applies to the variance estimator in (6), where $y_{i;z} \sim N(\ ;\ ^2)$.

1. $\mathrm{v}(y_i)$ and $\overline{y_i}$ are independent random variables.
2. $\overline{y_i}$ has a $N(\ ;\ ^2{=}Z)$ distribution.
3. $(Z-1)\mathrm{v}(y_i){=}\ ^2$ has a chi squared distribution with $Z-1$ degrees of freedom.

Since h, x, j and w are *i.i.d.* and as given in (2), y_i is $\mathcal{CN}(0;\ ^2)$ distributed under both hypotheses, where

$$y_i = \Re(y_i) + j\Im(y_i); \tag{7}$$

and

$$\begin{aligned} \Re(y_i) &\sim N(0;\ ^2{=}2); \\ \Im(y_i) &\sim N(0;\ ^2{=}2): \end{aligned} \tag{8}$$

Also, it should be noted that the variance operation can be distributed as,

$$\mathrm{v}(y_i) = \mathrm{v}(\Re(y_i) + j\Im(y_i)) = \mathrm{v}(\Re(y_i)) + \mathrm{v}(\Im(y_i)): \tag{9}$$

From the third statement of Theorem 5.3.1 [34] and the summation property of chi-square distribution,

$$\frac{Z-1}{^2=2}\cdot v(\Re(y_i)) + v(\Im(y_i))/ \sim X^2(2(Z-1)): \tag{10}$$

The expression above can be given as Gamma distribution and can be rearranged with the scaling property,

$$\begin{aligned} &\frac{Z-1}{^2=2} v(y_i) \sim \quad (Z-1;2); \\ &v(y_i) \sim \quad (Z-1; \frac{^2}{Z-1}): \end{aligned} \tag{11}$$

P_d (probability of detection) and P_{fa} (probability of false alarm) of the detection problem eventually seek the probability that test statistics takes on a value larger than the threshold. Notice that a cumulative distribution function (CDF) seeks exactly the complement of these metrics by seeking the probability that a random variable takes on a value less than or equal to a threshold. With this knowledge, P_d and P_{fa} of the detection problem now can be expressed with the CDF of Gamma distribution as,

$$P(v(y_i) > \quad) = 1 - F_v(\quad) = 1 - \frac{Z-1;\ \frac{(Z-1)}{2}}{(Z-2)!}; \tag{12}$$

where $F_v(\quad)$ is the CDF of the test statistics, $(Z-1;\ \frac{(Z-1)}{2}) = \int_0^{\frac{(Z-1)}{2}} t^{Z-2}e^{-t}dt$ is the lower incomplete Gamma function and is the threshold. The probability of detection is,

$$P_d = P(v(y_i) > \quad ; H_0) = 1 - \frac{Z-1;\ \frac{(Z-1)}{\frac{2}{d}}}{(Z-2)!}; \tag{13}$$

where $\frac{2}{d}$ denotes the variance of the received samples under H_0 and can be given as,

$$\frac{2}{d} = \begin{cases} N_j + N_w & \text{for passive subcarriers,} \\ 1 + N_j + N_w & \text{for active subcarriers,} \\ 1 + (n=k)N_j + (n=k)N_w & \text{for OFDM subcarriers.} \end{cases} \tag{14}$$

We note that n and k terms appear in $\frac{2}{d}$ parameter of OFDM subcarriers. A careful reader can ask why OFDM-IM-specific terms appear for OFDM subcarriers. The reason comes from the normalization. Identical SNR and SJR conditions are assumed for OFDM-IM and OFDM schemes. Assume that an arbitrary transmit power is provided for both schemes. It can be seen that OFDM subcarriers are exposed to $n=k$ times the noise and jamming of OFDM-IM scenario when transmit powers are normalized. The probability of false alarm can be given as,

$$P_{fa} = P(v(y_i) > \quad ; H_1) = 1 - \frac{Z-1;\ \frac{(Z-1)}{\frac{2}{fa}}}{(Z-2)!}; \tag{15}$$

where $\frac{2}{fa}$ denotes the variance of the received samples under H_1 as,

$$\frac{2}{fa} = \begin{cases} N_w & \text{for passive subcarriers,} \\ 1 + N_w & \text{for active subcarriers,} \\ 1 + (n=k)N_w & \text{for OFDM subcarriers.} \end{cases} \tag{16}$$

Assuming fixed Z and P_{fa} values, the following equality can be extracted from (15).

$$\frac{\text{passive}}{N_w} = \frac{\text{active}}{1+N_w} = \frac{\text{OFDM}}{1+\frac{n}{k}N_w}. \tag{17}$$

Then, detection probabilities over OFDM-IM and OFDM subcarriers for a fixed Z and P_{fa} become,

$$\begin{aligned} P_{d;\text{passive}} &= 1 - \frac{1}{(Z-2)!}\ (Z-1;\ \underbrace{\frac{(Z-1)\ \text{passive}}{N_j+N_w}}); \\ P_{d;\text{active}} &= 1 - \frac{1}{(Z-2)!}\ (Z-1;\ \frac{(Z-1)\ \text{active}}{1+N_j+N_w}); \\ &= 1 - \frac{1}{(Z-2)!}\ (Z-1;\ \underbrace{\frac{(Z-1)\ \text{passive}}{N_j+N_w}}_{c_1}\ \underbrace{\frac{1+\frac{1}{N_w}}{1+\frac{1}{N_j+N_w}}}); \\ P_{d;\text{OFDM}} &= 1 - \frac{1}{(Z-2)!}\ (Z-1;\ \frac{(Z-1)\ \text{OFDM}}{1+\frac{n}{k}(N_j+N_w)}); \\ &= 1 - \frac{1}{(Z-2)!}\ (Z-1;\ \underbrace{\frac{(Z-1)\ \text{passive}}{N_j+N_w}}_{c_2}\ \underbrace{\frac{\frac{n}{k}+\frac{1}{N_w}}{\frac{n}{k}+\frac{1}{N_j+N_w}}}): \end{aligned} \tag{18}$$

It can be seen from the above expressions that $c_1 > c_2 > 1$ when $N_j > 0$ and $n=k > 1$. Since $(k;\ )$ function increases with larger ,

$$(Z-1;\ ) < \ (Z-1;\ c_2) < \ (Z-1;\ c_1); \tag{19}$$

and since P_d decrease with larger $(k;\ )$ values, the following inequality holds.

$$P_{d;\text{ passive}} > P_{d;\text{ OFDM}} > P_{d;\text{ active}}: \ \square \tag{20}$$

Proposition 1 states the efficiency of passive subcarriers on the detection problem. The main result of Proposition 1 is that passive subcarriers show a better detection performance than OFDM subcarriers. It is obvious that any unused frequency band would show the same characteristics as the passive subcarriers. However, reactive jammers especially target the occupied frequency bands by using its own energy detection system. Traditionally, avoiding reactive jammers require spread spectrum techniques that reduce the bandwidth efficiency of the system throughout the communication. On the other hand, OFDM-IM possesses a supplementary spread spectrum mechanism on its own without reducing bandwidth efficiency.

Remark 1. The probability of false alarm expression given in (15) and (16) does not depend on N_j. As a result, the receiver can decide on a threshold without any information on the jamming power. With the knowledge of SNR, the receiver can select a suitable threshold to satisfy any P_{fa} requirements. Also, as given in (12), (14) and (16), detection performance over passive subcarriers rely only on threshold, noise variance and jamming variance. The number of passive subcarriers in a subblock $(n-k)$ does not affect the detection performance. However, the selection of $n; k$ parameters directly affects the symbol energy, hence it would change the detection performance over active subcarriers.

The proof and the results of Proposition 1 is illustrated in Fig. 2. The variance detector essentially estimates the test statistics $(T(y_i))$ from a finite set. As a result, $T(y_i)$ can be modeled using a probability distribution. The proof states the relationship between the P_{fa} and P_d by using the distributions of $T(y_i)$ for H_0 and H_1 hypotheses. When a is chosen as the threshold, the observations above is considered as a jamming detection. Hence, the area of distributions above gives the P_{fa} and P_d performance metrics.

The noise level increases the scale parameter of the $T(y_i)$ distributions as given in Fig. 2. Note that OFDM is a special version of OFDM-IM where all subcarriers are active. The jamming signal increases the scale parameter of H_0 curves for active, passive and OFDM subcarriers. However, the modulated signal only increases

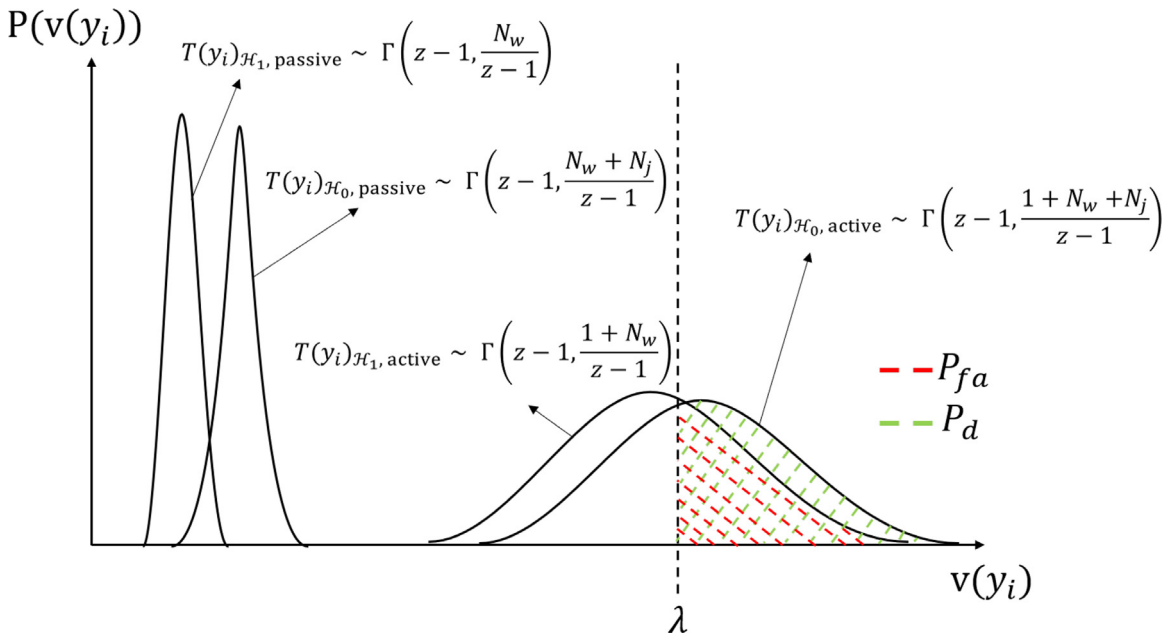


Fig. 2. An illustration of Proposition 1 and the detection performance. As the scale parameter increases, the Gamma distribution spreads.

the scale parameter of active subcarriers of OFDM-IM and OFDM. Since increasing scale parameters spreads the Gamma distribution for active OFDM-IM and OFDM subcarriers, the curves of hypotheses H_0 and H_1 overlap with each other on a bigger area. As a result, equal P_{fa} conditions give smaller successful detection performance for these subcarriers. In other words, distinguishing between H_0 and H_1 becomes more difficult and the detection mechanism has a greater chance to flag a false alarm.

3.1. Threshold selection

A discussion on selection of the detector threshold is presented in this subsection. The performance of the proposed scheme depends on the threshold as appears in both (13) and (15). As a result, the threshold can be selected to satisfy a minimum detection probability or a maximum false alarm probability. As Proposition 1 proves the superiority of OFDM-IM scheme in jammer detection, we are interested in finding a suitable threshold for passive subcarriers. From (13) and (14), a threshold that provides a certain P_d level over passive subcarriers can be obtained as,

$$= \frac{^{-1}(Z-1;\,1-P_d(Z-2)!)}{(Z-1)=(N_j+N_w)}; \tag{21}$$

where $^{-1}(Z-1;\,1-P_d(Z-2)!)$ is the inverse of the lower incomplete Gamma function such that $1-P_d(Z-2)! = Z-1;\ (Z-1)=(N_j+N_w)$. The main observation from (21) is that achieving a certain P_d level requires the knowledge of jamming power (N_j), which is an idealistic assumption. However, a minimum N_j value which endangers the communication system can be selected arbitrarily. If the detection system faces a stronger jamming signal, the detection probability would be higher than the targeted P_d level as in (13). On the other hand, weaker jamming signals would reduce the detection probability, however they would be less harmful to the legitimate communication.

Another important parameter in threshold selection is the maximum false alarm level. Using (15) and (16), a threshold that attains a certain P_{fa} level can be selected as,

$$= \frac{^{-1}(Z-1;\,1-P_{fa}(Z-2)!)}{(Z-1)=N_w}. \tag{22}$$

P_{fa} based threshold selection only requires the noise power (N_w) knowledge. It should be noted that a threshold that satisfies both P_d and P_{fa} conditions may not exist. Eventually, detection mechanism presents a trade-off between P_d and P_{fa}. As will be illustrated in the following sections, possible P_d and P_{fa} pairs can be obtained for various thresholds and N_j, N_w values. Depending on the application, designers can obtain the threshold for the desired $(P_d; P_{fa})$ pair using (21) and (22).

3.2. Relation between P_{fa} and P_d

The probability of detection and false alarm metrics can be given explicitly by using (13) and (15) as,

$$\begin{aligned} P_{fa} &= 1-\frac{1}{(Z-2)!}\int_{Z^0-}^{Z} t^{Z-2}e^{-t}\mathrm{d}t; \\ P_d &= 1-\frac{1}{(Z-2)!}\int_{0}^{} t^{Z-2}e^{-t}\mathrm{d}t: \end{aligned} \tag{23}$$

where,

$$-= \frac{(Z-1)}{\frac{2}{fa}} \quad \frac{\frac{2}{fa}}{\frac{2}{d}}.$$

Since $\frac{\frac{2}{fa}}{\frac{2}{d}} < 1$ and $^{-} <$, the relation between P_d and P_{fa} can be obtained as follows:

$$P_d = P_{fa} + \frac{1}{(Z-2)!}\int_{-}^{Z} t^{Z-2}e^{-t}\mathrm{d}t: \tag{24}$$

3.3. Asymptotic analysis of P_{fa} and P_d

In this section, the effect of SNR and SJR on the detection performance is investigated. Using (24), the asymptotic behavior of the performance metrics for OFDM-IM and OFDM subcarriers are given as follows.

3.3.1. OFDM-IM (passive) subcarriers

The relation between $\bar{}$ and is $\bar{} = \frac{N_w}{N_w+N_j}$. As $N_w \to \infty$, $\bar{} =$ and P_d approaches to P_{fa}. As $N_w \to 0$, $\bar{}$ approaches to zero and from (23), $P_d \to 1$.

When $N_j \to \infty$, $\bar{} \to 0$ and P_d becomes 1. As $N_j \to 0$, $\bar{} =$ and P_d approaches to P_{fa}.

3.3.2. OFDM subcarriers

For OFDM subcarriers, $\bar{} = \frac{1+\frac{n}{k}N_w}{1+\frac{n}{k}N_w+\frac{n}{k}N_j}$. When $N_w \to \infty$ or $N_j \to 0$, P_d approaches to P_{fa}. Also, as $N_j \to \infty$, P_d approaches to 1. When $N_w \to 0$, P_d can be given as a function of P_{fa} and N_j as follows:

$$P_d = P_{fa} + \frac{1}{(Z-2)!} \int_{(\frac{1}{1+\frac{n}{k}N_j})}^{Z} t^{Z-2}e^{-t}\mathrm{d}t: \tag{25}$$

3.4. Acquisition of OFDM-IM (passive) subcarrier indices

One of the largest drawbacks of the proposed scheme is the lack of indices information of passive subcarriers. An OFDM-IM receiver decides upon the passive subcarrier indices at the demodulation stage. However, the traditional demodulation process becomes unreliable under a jamming attack. For this reason, we utilize a sorting algorithm to obtain the passive subcarrier indices at the receiver.

The algorithm sorts the test statistics for each subblock. Passive subcarriers are expected to present less energy since they do not contain modulated signal. Depending on $(n; k)$ parameters, k subcarriers with the smallest $T(y_i)$ value is considered as passive at each subblock. The detection over these subcarriers is expected to present a better performance than the classical OFDM subcarriers.

The order statistics is an important probability theory tool that can present the theoretical basis of a sorting operation. The order statistics state that the sorted sample values also constitute random variables which distributions can be derived from the initial distribution [35]. Specifically, we are interested in the resulting test statistics after the sorting operation. It can be seen in (12) that the test statistics can be expressed in the form of cumulative distribution functions before the sorting operation. The order statistics proves that the CDF of the maximum and minimum distribution of a sorted sample set can be presented as,

$$P(\max\{X_1; \dots; X_r\} \le x) = [F_X(x)]^r$$
$$P(\min\{X_1; \dots; X_r\} \le x) = 1 - [1 - F_X(x)]^r$$

where $F_X(x)$ is the CDF of the random variable X before sorting. When we apply this property in our scenario, we can obtain the test statistics and $P_{fa}; P_d$ performance metrics of the sorted $T(y_i)$ distributions. The original test statistics given in (12) becomes,

$$[1 - F_v(\ )]^r = \left[1 - \frac{\int_{\frac{(Z-1)}{2}}^{Z} t^{Z-1;}e^{-t}\mathrm{d}t}{(Z-2)!}\right]^r; \tag{26}$$

for the subcarrier with the maximum observation variance where ^{2} is as given in (14) for P_d and as given in (16) for P_{fa}. Here, r denotes the number of random variables (subcarrier variances) that are sorted in each subblock which is $r = n - k$ for passive subcarriers and $r = k$ for active subcarriers. Similarly, the performance metrics of the subcarrier with the minimum observation variance can be given as,

$$1 - [1 - .1 - F_v(\ )/]^r = 1 - \left[\frac{\int_{\frac{(Z-1)}{2}}^{Z} t^{Z-1;}e^{-t}\mathrm{d}t}{(Z-2)!}\right]^r \tag{27}$$

where ^{2} is as given in (14) for P_d and as given in (16) for P_{fa}.

3.5. The overall algorithm

The proposed detection system is given in Algorithm 1. In a realistic case, only OFDM-IM parameters such as $N; n; k$ are known at the receiver. Since the indices of passive subcarriers are decoded at the receiver, this information is unreliable under a jamming attack. For this reason, the receiver calculates the test statistics for all subcarriers in the 3rd line of the algorithm. In the 6th line, calculated test statistics are sorted in each subblock to find passive subcarriers. Since passive subcarriers do not contain information bearing signals, the smallest test statistics is expected to belong to a passive subcarrier. Note that previously, we exploited order statistics to obtain the theoretical basis for this sorting operation. Specifically, presented P_{fa} and P_d performance metrics for the subcarrier with the maximum variance in (26) and for the subcarrier with the minimum variance in (27). These equations later will be theoretical benchmarks in the numerical analysis of Algorithm 1.

At the last step, detector compares the test statistics of passive subcarriers with a predefined threshold. If the test statistics is greater than the threshold, the statement of the 8th line alarms a jamming attack at the jth subblock. As Proposition 1 states, detection over passive OFDM-IM subcarriers outperforms traditional schemes.

3.5.1. Complexity analysis

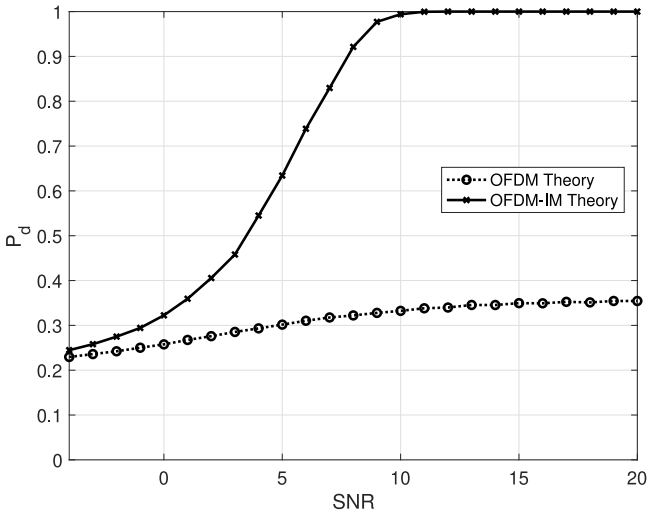
We aim to investigate the complexity and scalability of the proposed algorithm by checking its asymptotic behavior. Big O notation is used to define the asymptotic behavior of the algorithm. Also, we aim to compare the complexity of our algorithm with an OFDM-based energy detector. Algorithm 1 consists of two major steps that define its complexity. In the first step (line 2), the algorithm calculates test statistics for all subcarriers. The calculation of the test statistics scales with $O(NZ)$ where N is the number of subcarriers and Z is the number of samples per variance calculation. In the second major step (line 5), the algorithm sorts the test statistics in each subblock. Assuming a sorting algorithm that scales with the square of its input size, each sorting operation scales with $O(n^2)$ where n is the subblock size. However, we repeat sorting operation for each subblock which requires $O(Nn)$. The overall algorithm scales with $O(N(Z+n))$. An OFDM-based traditional energy detector does not require a sorting step. It only calculates the test statistics for each subcarrier as line 2 of Algorithm 1. Then, compares the test statistics with a threshold. As a result, an OFDM-based energy detector would scale with $O(NZ)$. Although traditional energy detector has less complexity ($O(NZ) < O(N(Z+n))$), this difference is small in practical applications. The reason comes from the fact that n should be much smaller than Z for a practical implementation. In general, n is chosen to be small (e.g. $n = 4$) since high n values lead to impractical active subcarrier combination calculations. On the other hand, Z is chosen to be high (e.g. $Z = 100$) to obtain a good approximation of the variance. In an example scenario where $Z = 100; n = 4$, we expect a 4% increase in the complexity compared to OFDM-based energy detector.

3.6. Theoretical comparison of OFDM-IM (the proposed algorithm) and OFDM

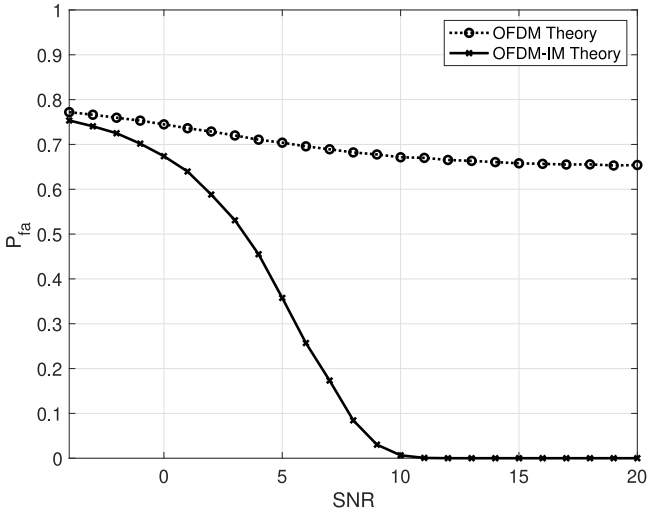
Theoretical comparison of OFDM-IM-based and OFDM-based jamming detection schemes is presented in Fig. 3. The figure illustrates the detection scheme given in Algorithm 1 based on the theoretical result of Eq. (27). Comparison of detection performances is presented in Fig. 3(a). For a false alarm limit of $P_{fa} = 0{:}2$, it can be seen that OFDM-IM outperforms OFDM on the

Algorithm 1 OFDM-IM detection algorithm

Initialize N, n, k, Z and .
for $i = 1 : N$ **do**
  Calculate the test statistics $T(y_i) = \mathrm{v}(y_i)$ using (6).
end for
for $j = 1 : N{=}n$ **do**
  Sort $T(y_{j\times n}); T(y_{j\times n+1}); \cdots ; T(y_{j\times n+n})$ in ascending order and set the minimum value as $T_{\text{passive}}(y)$.
  if $T_{\text{passive}}(y) >$ **then**
    j^{th} subblock is under jamming attack
  else
    j^{th} subblock is not under jamming attack
  end if
end for



(a)



(b)

Fig. 3. Theoretical comparison of OFDM-IM and OFDM for detection and false alarm performances. For $N = 8$ OFDM-IM ($n = 4; k = 2$) and OFDM ($n = 1; k = 1$) systems, the output of Algorithm 1 is presented. (a) Comparison of detection performances where a maximum of $P_{fa} = 0.2$ level is allowed. (b) Comparison of false alarm performances where a minimum of $P_d = 0.8$ level is required.

detection performance, especially on higher SNR levels. Fig. 3(b) shows the comparison of false alarm performances of OFDM-IM and OFDM. The figure shows the possible false alarm rates when a minimum of $P_d = 0.8$ detection rate is required. As seen in the figure, OFDM-based system cannot obtain $P_d = 0.8$ without raising more than 60% false alarm. On the other hand, Algorithm 1 can reach to $P_d = 0.8$ with almost zero percent false alarm above 10 dB SNR.

4. Numerical results

Our observations from Proposition 1 are verified with simulations in this section. OFDM-IM and OFDM-based communication systems are modeled over Rayleigh channel. $(n; k) = (4; 2)$ pair is used with the look-up table given in Table 1 and each active subcarrier is modulated with binary phase-shift keying (BPSK). The parameters, their symbols and their values that are used in the simulations are presented in Table 2. In the simulations, an OFDM system with 8 subcarriers and an OFDM-IM system with 4 active, 4 passive subcarriers are exposed to full-band and partial-band jamming attacks. Both jammers are assumed to uniformly distribute the jamming power to the targeted subcarriers.

The performance of OFDM-IM and OFDM systems are investigated for two cases. In the first case, an ideal scenario is assumed, where the indices of passive subcarriers are available at the receiver. In the second case, a realistic scenario is considered, where the receiver sorts the test statistics to obtain passive subcarrier indices. Firstly, the detection performance against full-band jamming attacks is presented for the two cases. The theoretical results on the effect of SJR and SNR are verified with numerical results. Secondly, the detection performance against partial-band jammers is investigated with simulations.

4.1. Analysis of the receiver operating characteristics under full-band jamming attack

The detection performance of the OFDM and OFDM-IM systems are exhibited with ROC curves in Fig. 4. The ROC curves represent the P_d and P_{fa} characteristics of a detection mechanism with respect to varying values. Fig. 4 includes P_d and P_{fa} of 10^4 different values in each curve. In Fig. 4(a), simulations and theoretical results of (12) are presented for 15 dB SJR, 10 dB SNR and full-band jamming attack. In Fig. 4(b), a sorting algorithm is applied to each subblock. The theoretical results of (26) and (27) are used to verify the maximum and minimum variance passive subcarriers after the sorting operation. It should be noted that the sorting algorithm is noneffective in OFDM system since a subblock contains a single subcarrier in OFDM.

Increasing SJR reduces the jammer energy compared to E_s and diminishes the difference between H_0 and H_1. As a result, detection performance reduces with increasing SJR for both OFDM and OFDM-IM systems. In both cases (ideal and realistic), passive OFDM-IM subcarriers outperform OFDM as stated in Proposition 1.

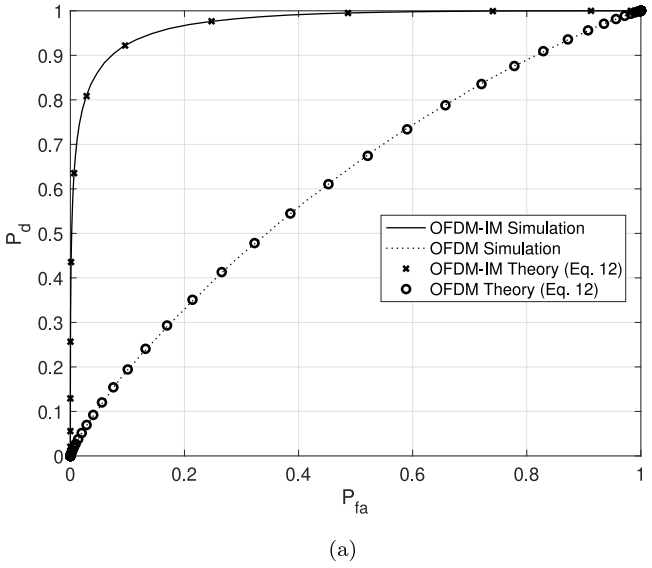
4.2. Analysis of the effect of SJR on the detection performance

The influence of the jamming power on detection performance is examined in Fig. 5 for both ideal and realistic cases. The probability of false alarm is kept constant at $P_{fa} = 0.2$ for each case at 10 dB SNR. In both cases, passive OFDM-IM subcarriers are more robust to high SJR region than OFDM subcarriers. Approximately 10 dB SJR gap exists between passive OFDM-IM subcarriers and OFDM subcarriers at the average SJR region.

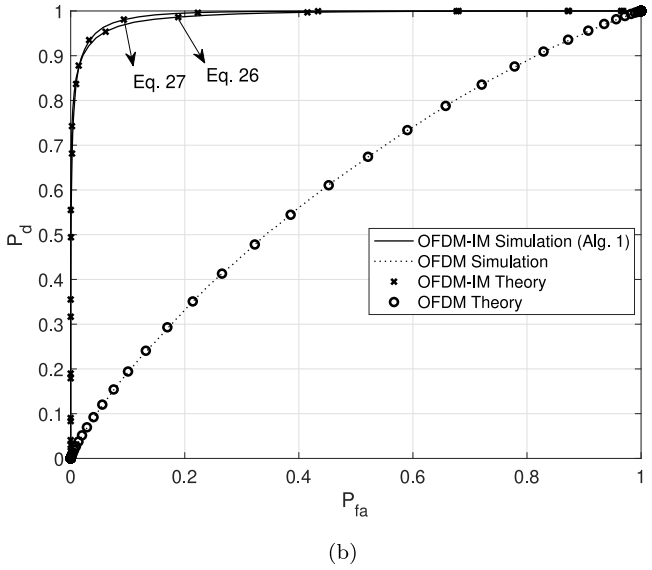
It can be seen that P_d asymptotically approaches to $P_{fa} = 0.2$ with increasing SJR. This result also can be observed from the

Table 2
Simulation parameters and their values.

Description	Value	Description	Value
Number of subcarriers in a subblock	$n = 4$	Number of active subcarriers in a subblock	$k = 2$
Number of subcarriers in a symbol	$N = 8$	Cyclic prefix length	$N_{CP} = 4$
Modulation	BPSK	Variance estimation sample size	$Z = 100$
Monte Carlo size	10^5	Number of channel paths	$L = 3$
Number of subblocks in a symbol	$g = N$=n	Number of active subcarriers in a symbol	K = kg
Number of bits carrier by a symbol	m	Bit energy	$E_s = (N + N_{CP})$=m
SNR	$E_s k$=($N_w n$)	SJR	$E_s k$=($N_j n$)

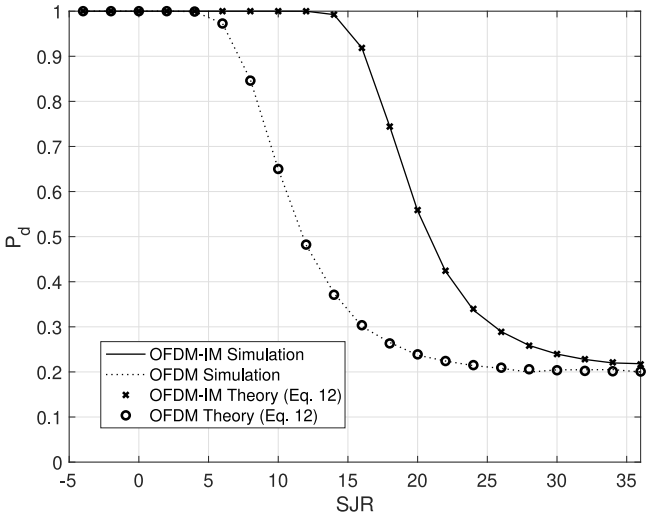


(a)

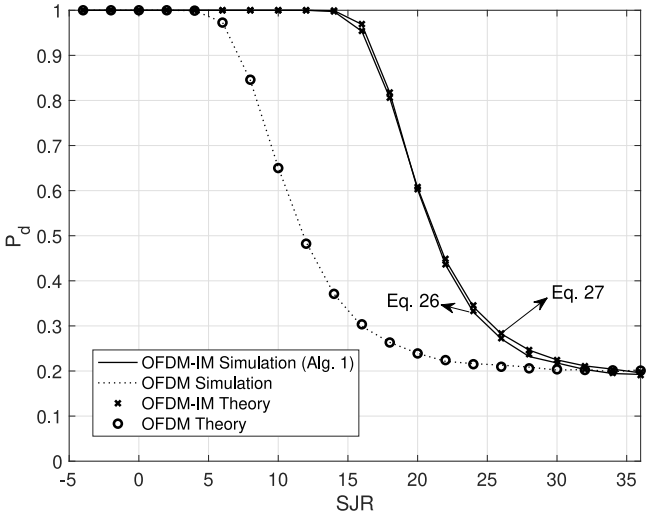


(b)

Fig. 4. ROC curves for full-band jamming detection at 15 dB SJR and 10 dB SNR. For $N = 8$ OFDM-IM and OFDM systems. (a) Ideal case. (b) Realistic case with the proposed sorting algorithm. Test statistics are sorted for each subblock to obtain passive subcarrier test statistics (OFDM-IM subcarriers with maximum (Eq. (26)) and minimum (Eq. (27)) test statistics are presented to verify the impact of sorting).

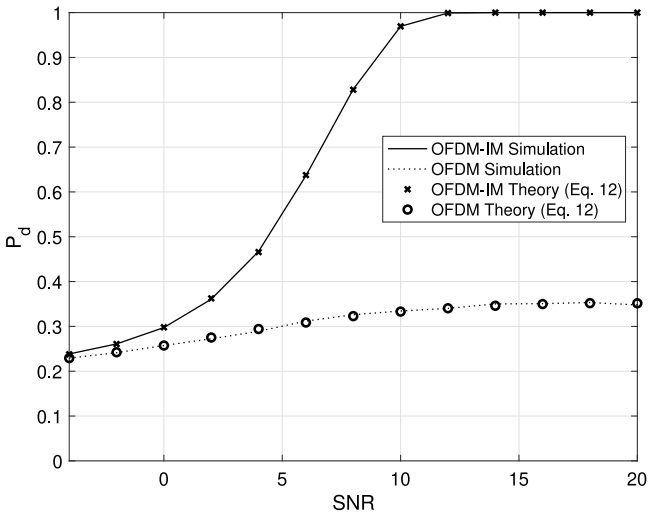


(a)

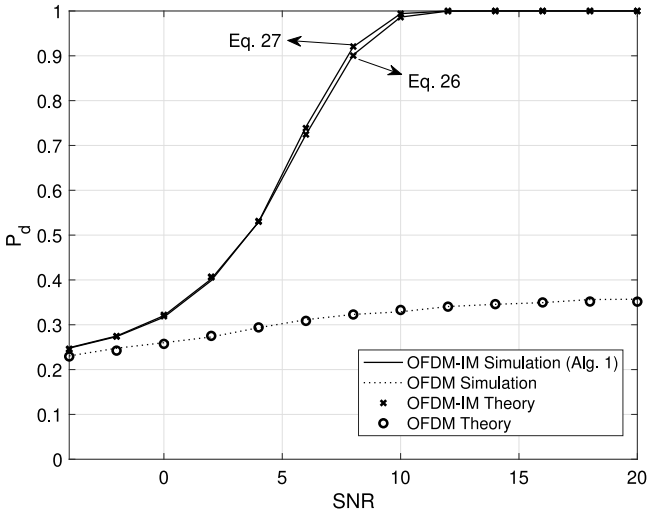


(b)

Fig. 5. The effect of SJR on the detection performance (P_d). A maximum of $P_{fa} = 0.2$ level is allowed in the detection mechanism at 10 dB SNR. (a) Ideal case. (b) Realistic case with the sorting algorithm. Test statistics are sorted for each subblock to obtain passive subcarrier test statistics (OFDM-IM subcarriers with maximum (Eq. (26)) and minimum (Eq. (27)) test statistics are presented to verify the impact of sorting).



(a)



(b)

Fig. 6. The effect of SNR on the detection performance (P_d). A maximum of $P_{fa} = 0.2$ level is allowed in the detection mechanism at 15 dB SJR. (a) Ideal case. (b) Realistic case with the sorting algorithm. Test statistics are sorted for each subblock to obtain passive subcarrier test statistics (OFDM-IM subcarriers with maximum (Eq. (26)) and minimum (Eq. (27)) test statistics are presented to verify the impact of sorting).

distributions of the test statistics that are illustrated in Fig. 2. Since $N_j = 0$ as SJR $\rightarrow \infty$, the distributions of the received test statistics for both H_0 and H_1 hypotheses become identical. When we set a detection threshold (a vertical line in Fig. 2), the green and red areas (P_{fa} and P_d respectively) become identical. Hence we obtain $P_{fa} = P_d$ asymptotically. Also, the probability of detection approaches to 1 as $N_j \rightarrow \infty$ for a constant P_{fa} level.

4.3. Analysis of the effect of SNR on the detection performance

The effect of SNR on P_d is investigated in Fig. 6 at 15 dB SJR under $P_{fa} = 0.2$ restriction for both ideal and realistic cases. The detection performance improves for both OFDM and OFDM-IM systems with increasing SNR. Passive OFDM-IM subcarriers outperform OFDM subcarriers. The figure shows that passive OFDM-IM subcarriers are more robust to noise in both ideal and realistic cases.

The proof of Proposition 1 implies that asymptotically both SNR and SJR limit the detection performance. The figure also shows an example of this observation. The low SNR region introduces more noise to the test statistics and degrades the detection performance. Specifically, a constant P_{fa} results $P_d = P_{fa}$ as $N_w \rightarrow \infty$. The effect of noise decreases at high SNR values and the energy of the jamming signal becomes the only bottleneck of the detection performance. P_d of OFDM subcarriers are related to the P_{fa} constraint as shown in (25), while P_d of passive OFDM-IM subcarriers approaches to 1 as $N_w \rightarrow 0$. The detection performance asymptotically becomes $P_d = 1$ and $P_d = 0.3566$ for passive OFDM-IM and OFDM, respectively as $N_w \rightarrow 0$ and SJR is 15 dB.

4.4. Analysis of the receiver operating characteristics under partial-band jamming attack

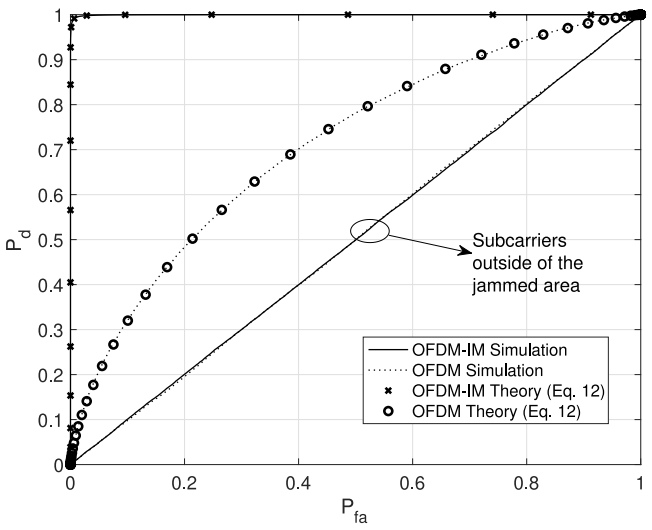
The partial-band jamming attack scenario is also considered for both ideal and realistic cases. The jammer is assumed to attack the first half of the subcarriers ($= 0.5$) with a uniformly distributed jamming power. In Fig. 7, the simulation results of OFDM-IM and OFDM systems are presented for 15 dB SJR and 10 dB SNR conditions. The jammer is assumed to concentrate its energy on the half of the subcarriers. Note that two subcarrier groups (passive OFDM-IM, OFDM) are observed under a full-band jamming attack. In the partial-band jamming scenario, subcarriers are clustered into three groups. This emerges from the existence of subcarriers that are unaffected from the attack. Subcarriers that are outside of the jammed area show $P_d = P_{fa}$ relation for both OFDM and OFDM-IM systems since their distributions on both hypotheses become identical without the jamming signal. On the other hand, passive OFDM-IM subcarriers under the focus of the jammer demonstrate a higher detection performance than OFDM subcarriers.

It should be noted that the subcarriers of both OFDM and OFDM-IM systems present better performance under PBJ compared to the BJ at the same SJR level. The reason comes from the energy distribution of PBJ. At constant SJR condition, BJ distributes its total energy to more subchannels than PBJ and the subcarriers under PBJ are exposed to more jamming energy.

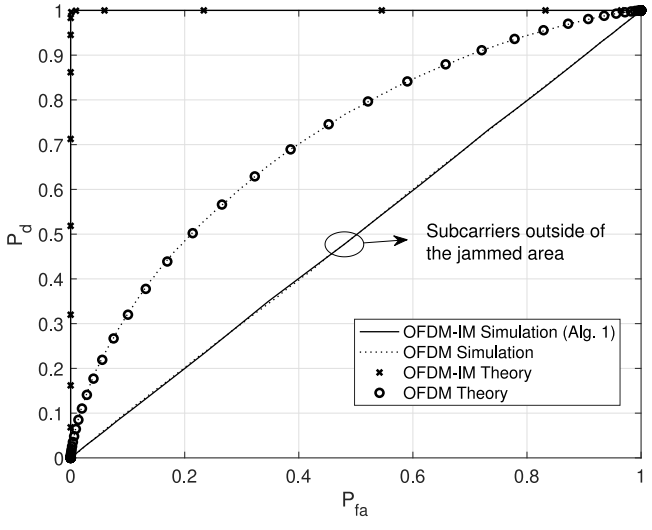
The proposed model performs its detection mechanism on each subcarrier. Since each subblock of an OFDM-IM system contains at least one passive subcarrier, the OFDM-IM system can detect jamming attacks with a high performance at each subblock. As a result, the OFDM-IM system is effective against PBJ attacks that are at least on the subblock level. Single-tone PBJ attacks that target only a single subcarrier of the system can hit the legitimate communication while deceiving the proposed approach. However, it is not feasible in a practical scenario since passive subcarriers in OFDM-IM change dynamically. Even if the single-tone jammer targets only active subcarriers (and keeps other subcarriers idle), the passive subcarriers will be different in the following symbols. Eventually, the target of the single-tone PBJ will match with passive subcarriers which will result in the detection.

5. Conclusion

In this paper, the jamming detection performance of OFDM-IM has been investigated and compared with OFDM under reactive jamming attacks. An elusive reactive jammer model that inserts a zero-mean Gaussian jamming signal to the channel has been assumed. A variance detector has been considered against the proposed jammer model. The passive subcarriers that inherently



(a)



(b)

Fig. 7. ROC curves for partial-band jamming detection at 15 dB SJR and 10 dB SNR. (a) Ideal case. (b) Realistic case with the sorting algorithm. Test statistics are sorted for each subblock to obtain passive subcarrier test statistics (The analyses in Eqs. (26) and (27) are not theoretically valid for partial-band jamming scenario. However, OFDM-IM Theory curve is still given with Eq. (27) for comparison.).

exist in the structure of an OFDM-IM signal are theoretically proven to exhibit better detection performance than the OFDM subcarriers with the given detection mechanism. Moreover, a sorting algorithm-based jamming detection approach has been proposed to cover a realistic scenario, where passive subcarrier indices are unknown to the receiver. The theoretical results have been later verified with simulations under full-band and partial-band jamming attacks. Ideal and realistic cases have been investigated in the simulations. Also, the impact of the SNR and SJR on the detection performance has been investigated. Extensive simulations revealed that taking advantage of the structure of the OFDM-IM signal, the variance detector lends itself as a powerful jammer detector against both full-band and partial-band reactive jammers.

CRediT authorship contribution statement

Ufuk Altun: Conceptualization, Methodology, Investigation, Software, Validation, Writing – original draft. **Ahmet Kaplan:** Data curation, Writing – review & editing, Investigation, Validation. **Gunes Karabulut Kurt:** Conceptualization, Supervision, Writing – review & editing. **Ibrahim Altunbas:** Supervision, Writing – review & editing, Project administration. **Defne Kucukyavuz:** Formal analysis, Supervision, Writing – review & editing, Project administration. **Mustafa Kesal:** Writing – review & editing, Supervision. **Ertugrul Basar:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Ufuk Altun reports financial support was provided by ASELSAN AS. Ufuk Altun has patent pending to Ufuk Altun.

Data availability

The data that has been used is confidential.

References

[1] Y. Liu, H.-H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges, IEEE Commun. Surv. Tutor. 19 (1) (2017) 347–376, http://dx.doi.org/10.1109/COMST.2016.2598968.

[2] A.A. Bodkhe, A.R. Raut, Identifying jammers in wireless sensor network with an approach to defend reactive jammer, in: Int. Conf. on Commun. Systems and Network Technologies, 2014, pp. 89–92, http://dx.doi.org/10.1109/CSNT.2014.26.

[3] K. Grover, A. Lim, Q. Yang, Jamming and anti–jamming techniques in wireless networks: A survey, Int. J. Ad Hoc Ubiquitous Comput. 17 (4) (2014) 197–215, http://dx.doi.org/10.1504/IJAHUC.2014.066419.

[4] J. Thangapoo Nancy, K. VijayaKumar, P. Ganesh Kumar, Detection of jammer in wireless sensor network, in: Int. Conf. on Commun. and Signal Processing, 2014, pp. 1435–1439, http://dx.doi.org/10.1109/ICCSP.2014.6950086.

[5] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Symp. Mobile Ad Hoc Networking and Computing, 2005, pp. 46–57, http://dx.doi.org/10.1145/1062689.1062697.

[6] W. Xu, K. Ma, W. Trappe, Y. Zhang, Jamming sensor networks: Attack and defense strategies, IEEE Netw. 20 (3) (2006) 41–47, http://dx.doi.org/10.1109/MNET.2006.1637931.

[7] M. Han, T. Yu, J. Kim, K. Kwak, S. Lee, S. Han, D. Hong, OFDM channel estimation with jammed pilot detector under narrow-band jamming, IEEE Trans. Veh. Technol. 57 (3) (2008) 1934–1939, http://dx.doi.org/10.1109/TVT.2007.907314.

[8] L. Xiao, J. Liu, Q. Li, N.B. Mandayam, H.V. Poor, User-centric view of jamming games in cognitive radio networks, IEEE Trans. Inf. Forensics Secur. 10 (12) (2015) 2578–2590, http://dx.doi.org/10.1109/TIFS.2015.2467593.

[9] Y. Shi, K. An, Y. Li, Index modulation based frequency hopping: Anti-jamming design and analysis, IEEE Trans. Veh. Technol. 70 (7) (2021) 6930–6942, http://dx.doi.org/10.1109/TVT.2021.3087640.

[10] N. Van Huynh, D.N. Nguyen, D.T. Hoang, T.X. Vu, E. Dutkiewicz, S. Chatzinotas, Defeating super-reactive jammers with deception strategy: Modeling, signal detection, and performance analysis, IEEE Trans. Wirel. Commun. 3 (3) (2022) 1, http://dx.doi.org/10.1109/TWC.2022.3158189.

[11] E. Basar, U. Aygolu, E. Panayirci, H.V. Poor, Orthogonal frequency division multiplexing with index modulation, IEEE Trans. Signal Process. 61 (22) (2013) 5536–5549, http://dx.doi.org/10.1109/TSP.2013.2279771.

[12] M. Wen, B. Zheng, K.J. Kim, M. Di Renzo, T.A. Tsiftsis, K.-C. Chen, N. Al-Dhahir, A survey on spatial modulation in emerging wireless systems: Research progresses and applications, IEEE J. Sel. Areas Commun. 37 (9) (2019) 1949–1972, http://dx.doi.org/10.1109/JSAC.2019.2929453.

[13] J. Li, S. Dang, M. Wen, X.-Q. Jiang, Y. Peng, H. Hai, Layered orthogonal frequency division multiplexing with index modulation, IEEE Syst. J. 13 (4) (2019) 3793–3802, http://dx.doi.org/10.1109/JSYST.2019.2918068.

[14] M. Wen, E. Basar, Q. Li, B. Zheng, M. Zhang, Multiple-mode orthogonal frequency division multiplexing with index modulation, IEEE Trans. Commun. 65 (9) (2017) 3892–3906, http://dx.doi.org/10.1109/TCOMM.2017.2710312.
[15] M. Wen, Q. Li, E. Basar, W. Zhang, Generalized multiple-mode OFDM with index modulation, IEEE Trans. Wirel. Commun. 17 (10) (2018) 6531–6543, http://dx.doi.org/10.1109/TWC.2018.2860954.
[16] M. Wen, X. Cheng, M. Ma, B. Jiao, H.V. Poor, On the achievable rate of OFDM with index modulation, IEEE Trans. Signal Process. 64 (8) (2016) 1919–1932, http://dx.doi.org/10.1109/TSP.2015.2500880.
[17] A.M. Jaradat, J.M. Hamamreh, H. Arslan, OFDM with subcarrier number modulation, IEEE Wirel. Commun. Lett. 7 (6) (2018) 914–917, http://dx.doi.org/10.1109/LWC.2018.2839624.
[18] M. Wen, J. Li, S. Dang, Q. Li, S. Mumtaz, H. Arslan, Joint-mapping orthogonal frequency division multiplexing with subcarrier number modulation, IEEE Trans. Commun. 69 (7) (2021) 4306–4318, http://dx.doi.org/10.1109/TCOMM.2021.3066584.
[19] C. Shan, P. Wang, G. Sun, Performance of OFDM in the presence of multitone jamming, in: IEEE Symp. on Robotics and Applications (ISRA), Vol. 2, 2012, pp. 118–121, http://dx.doi.org/10.1109/ISRA.2012.6219135, 1.
[20] M.A. Soliman, K.H. Moussa, W.M. Saad, S. Shaaban, M.R.M. Rizk, Analysis of jamming attacks on a hopped OFDM communication system, in: IEEE Int. Conf. on Communication Technology (ICCT), 2018, pp. 407–411, http://dx.doi.org/10.1109/ICCT.2018.8599930.
[21] A. Kaplan, I. Altunbas, G.K. Kurt, M. Kesal, D. Kucukyavuz, OFDM-IM performance evaluation under jamming attack, in: Int. Telecommunication Networks and Applications Conference (ITNAC), 2020, pp. 1–6, http://dx.doi.org/10.1109/ITNAC50341.2020.9315104.
[22] T.V. Luong, Y. Ko, N.A. Vien, D.H.N. Nguyen, M. Matthaiou, Deep learning-based detector for OFDM-IM, IEEE Wirel. Commun. Lett. 8 (4) (2019) 1159–1162, http://dx.doi.org/10.1109/LWC.2019.2909893.
[23] H. Qing, H. Yu, M. Wen, F. Chen, F. Ji, A novel detector based on EM algorithm for multiple-mode OFDM with index modulation, EURASIP J. Wireless Commun. Networking 2020 (2020) http://dx.doi.org/10.1186/s13638-020-01676-7.
[24] Z. Sun, Q. Wang, C. Che, Study of cognitive radio spectrum detection in OFDM system, in: 2010 Asia-Pacific Conf. on Wearable Computing Systems, 2010, pp. 235–238, http://dx.doi.org/10.1109/APWCS.2010.66.
[25] Y. Yan, M. Ma, SNR improvement for energy detection of narrow band signal in OFDM system, IEEE Commun. Lett. 18 (11) (2014) 1967–1970, http://dx.doi.org/10.1109/LCOMM.2014.2354363.
[26] N. Armi, C. Wael, Taufiqurrahman, Y. Wijayanto, W. Khan, W. Gharibi, OFDM based signal detection performance in cognitive radio systems, in: Int. Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018, pp. 591–594, http://dx.doi.org/10.1109/ISRITI.2018.8864276.
[27] L. Sanguinetti, M. Morelli, H. Poor, Frame detection and timing acquisition for OFDM transmissions with unknown interference, IEEE Trans. Wirel. Commun. 9 (3) (2010) 1226–1236, http://dx.doi.org/10.1109/TWC.2010.03.091213.
[28] C. Shahriar, M. La Pan, M. Lichtman, T.C. Clancy, R. McGwier, R. Tandon, S. Sodagari, J.H. Reed, PHY-layer resiliency in OFDM communications: A tutorial, IEEE Commun. Surv. Tutor. 17 (1) (2015) 292–314, http://dx.doi.org/10.1109/COMST.2014.2349883.
[29] K. Pelechrinis, M. Iliofotou, S.V. Krishnamurthy, Denial of service attacks in wireless networks: The case of jammers, IEEE Commun. Surv. Tutor. 13 (2) (2011) 245–257, http://dx.doi.org/10.1109/SURV.2011.041110.00022.
[30] T. Hamza, G. Kaddoum, A. Meddeb, G. Matar, A survey on intelligent MAC layer jamming attacks and countermeasures in WSNs, in: Vehicular Technology Conference (VTC-Fall), 2016, pp. 1–5, http://dx.doi.org/10.1109/VTCFall.2016.7880885.
[31] S. Sciancalepore, R. Di Pietro, Bittransfer: Mitigating reactive jamming in electronic warfare scenarios, IEEE Access 7 (2019) 156175–156190, http://dx.doi.org/10.1109/ACCESS.2019.2949716.
[32] T. Mao, Q. Wang, Z. Wang, S. Chen, Novel index modulation techniques: A survey, IEEE Commun. Surv. Tutor. 21 (1) (2019) 315–348, http://dx.doi.org/10.1109/COMST.2018.2858567.
[33] Q. Li, M. Wen, B. Clerckx, S. Mumtaz, A. Al-Dulaimi, R.Q. Hu, Subcarrier index modulation for future wireless networks: Principles, applications, and challenges, IEEE Wireless Commun. 27 (3) (2020) 118–125, http://dx.doi.org/10.1109/MWC.001.1900335.
[34] G. Casella, R.L. Berger, Statistical Inference, second ed., Duxbury Press, 2002, p. 218, http://dx.doi.org/10.1016/B978-0-12-409548-9.10592-5, arXiv:1603.04929.
[35] H. David, H. Nagaraja, Order Statistics, Third Edition, 2005, pp. 367–450, http://dx.doi.org/10.1002/0471722162.refs.

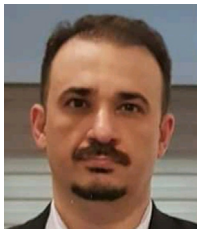
Ufuk Altun was born in Isparta, Turkey, in 1993. He received the B.Sc. and M.Sc. degrees, in electronics and communication engineering, from the Istanbul Technical University, Istanbul, Turkey, in 2017 and 2020, respectively. He is currently a Research Assistant at Trakya University, Edirne, Turkey and a PhD student at Koç University, Istanbul, Turkey. His research interests include layer security (currently focuses its possible interaction with autoencoders, machine learning and deep learning algorithms), reconfigurable intelligence surfaces, OFDM-IM and indoor localization.

Ahmet Kaplan was born in Istanbul, Turkey, in 1994. He received the B.Sc. and M.Sc. degrees (Hons.), in electronics and communication engineering, from the Istanbul Technical University, Istanbul, Turkey, in 2017 and 2020, respectively. From 2017 to 2019, he was a 5G Research Engineer with Turkcell, Istanbul, Turkey. He is currently a Research and Teaching Assistant with the Istanbul Technical University. His research interests include index modulation, physical layer security, and low-density parity-check coding.

Gunes Karabulut Kurt is currently an Associate Professor of Electrical Engineering at Polytechnique Montréal, Montreal, QC, Canada. She received the B.S. degree with high honors in electronics and electrical engineering from the Bogazici University, Istanbul, Turkey, in 2000 and the M.A.Sc. and the Ph.D. degrees in electrical engineering from the University of Ottawa, ON, Canada, in 2002 and 2006, respectively. From 2000 to 2005, she was a Research Assistant at the University of Ottawa. Between 2005 and 2006, Gunes was with TenXc Wireless, Canada. From 2006 to 2008, she was with Edgewater Computer Systems Inc., Canada. From 2008 to 2010, she was with Turkcell Research and Development Applied Research and Technology, Istanbul. Gunes has been with Istanbul Technical University since 2010, where she is currently on a leave of absence. She is a Marie Curie Fellow and has received the Turkish Academy of Sciences Outstanding Young Scientist (TÜBA-GEBIP) Award in 2019. She is an Adjunct Research Professor at Carleton University. She is also currently serving as an Associate Technical Editor (ATE) of the IEEE Communications Magazine and a member of the IEEE WCNC Steering Board.

İbrahim Altunbaş was born in Sütçüler, Isparta, Turkey, in 1967. He received the B.Sc., M.Sc. and Ph.D. degrees, all in electronics and communication engineering, from the Istanbul Technical University, Istanbul, Turkey, in 1988, 1992 and 1999, respectively. From 1992 to 1999, he was a Research Assistant, from 1999 to 2006, he was an Assistant Professor and from 2006 to 2011 he was an Associate Professor at the Istanbul Technical University. He is currently a Professor at the same university. Between January 2001–November 2001, he was a Visiting Researcher at Texas A&M University, USA. Between November 2001 September 2002 and June 2015i–August 2015, he was a Postdoctoral Fellow and a Visiting Researcher, respectively at the University of Ottawa, Canada. His current research interests include spatial modulation, nonorthogonal multiple access, physical layer security, satellite and UAV/drone-integrated wireless communications, reconfigurable intelligence surface-based communication.

Defne Kucukyavuz received her B.S. degree in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey in 1996. She received her M.S. and Ph.D. degrees in Electrical Engineering from The Ohio State University, Columbus, OH in 1998 and 2002, respectively. After working as a Postdoctoral Research Fellow at The Ohio State University and The University of Melbourne, Australia, she was an Assistant Professor at the Department of Electrical and Electronics Engineering, Bilkent University, Ankara, Turkey. Currently, she is working as a design engineer at ASELSAN Inc., Ankara, Turkey. Dr. Aktas is a recipient of the European Union Marie Curie Fellowship (2006–2009) and TUBITAK Career Grant (2008–2010). Her research interests are in the broad area of communication theory, in particular physical layer aspects of wireless communication systems, with emphasis on design of waveforms for broadband networks.



Mustafa Kesal received his B.S. degree in Electrical and Electronics Engineering from Bogazici University, Istanbul, Turkey in 1998. He received his M.S. degree in Electrical and Computer Engineering and M.A. degree in Applied Mathematics and Optimization both from University of Illinois at Urbana Champaign in 2005 and 2006, respectively. During his studies in UIUC, he actively worked for Anti-Piracy and Cryptography group of Microsoft Research Division, Redmond, WA for 2001–2006 period, and later he joined Aware Inc and then Qualcomm with communication engineering roles. Before joining Afiniti Inc, he worked in Aselsan, Ankara, Turkey for ten years as a design engineer for projects ranging from satellite payload design to elliptic curve cryptography implementations on FPGA. His research interests are information theory, in particular side information communication scenarios, and wireless communication theory.

Ertugrul Basar received his Ph.D. degree from Istanbul Technical University in 2013. He is currently an Associate Professor with the Department of Electrical and Electronics Engineering, Koc University, Istanbul, Turkey and the director of Communications Research and Innovation Laboratory (CoreLab). His primary research interests include beyond 5G systems, index modulation, intelligent surfaces, waveform design, and signal processing for communications. Dr. Basar currently serves as a Senior Editor of IEEE Communications Letters and an Editor of IEEE Transactions on Communications and Frontiers in Communications and Networks. He is a Young Member of Turkish Academy of Sciences and a Senior Member of IEEE.