IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 30, 2017, accepted October 27, 2017, date of publication November 1, 2017, date of current version December 5, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2768558

OFDM-Subcarrier Index Selection for Enhancing Security and Reliability of 5G URLLC Services

JEHAD M. HAMAMREH[1], ERTUGRUL BASAR[2], (Senior Member, IEEE), AND HUSEYIN ARSLAN[1,3], (Fellow, IEEE)

[1]School of Engineering and Natural Sciences, Istanbul Medipol University, 34810 Istanbul, Turkey
[2]Faculty of Electrical and Electronics Engineering, Istanbul Technical University, 34469 Istanbul, Turkey
[3]Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA

Corresponding author: Jehad M. Hamamreh (jmhamamreh@st.medipol.edu.tr)

This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 114E244.

ABSTRACT An efficient physical layer security technique, referred to as OFDM with subcarrier index selection (OFDM-SIS), is proposed for safeguarding the transmission of OFDM-based waveforms against eavesdropping in 5G and beyond wireless networks. This is achieved by developing a joint optimal subcarrier index selection (SIS) and adaptive interleaving (AI) design, which enables providing two levels (sources) of security in time division duplexing (TDD) mode: one is generated by the optimal selection of the subcarrier indices that can maximize the signal-to-noise ratio at only the legitimate receiver, while the other is produced by the AI performed based on the legitimate user's channel that is different from that of the eavesdropper. The proposed scheme not only provides a remarkable secrecy gap, but also enhances the reliability performance of the legitimate user compared with the standard OFDM scheme. Particularly, a gain of 5–10 dB is observed at a bit error rate value of 10^{-3} compared with standard OFDM as a result of using the adaptive channel-based subcarrier selection mechanism. Moreover, the proposed technique saves power, considers no knowledge of the eavesdropper's channel, and provides secrecy even in the worst security scenario, where the eavesdropper can know the channel of the legitimate link when an explicit channel feedback is used as is the case in frequency division duplexing systems. This is achieved while maintaining low complexity and high reliability at the legitimate user, making the proposed scheme a harmonious candidate technique for secure 5G ultra reliable and low latency communications (URLLC) services.

INDEX TERMS OFDM with subcarrier index selection (OFDM-SIS), physical layer security, eavesdropping, interleaving, 5G, adaptive subcarrier selection, URLLC, FDD, TDD.

I. INTRODUCTION

The broadcast nature of communication systems makes wireless transmission susceptible to passive eavesdropping, endangering the secrecy of data-carrying signals. Traditionally, data confidentiality has been tackled using encryption and cryptography-based approaches. However, due to the huge advancement in future 5G and beyond wireless networks, featured by the ability to serve massive amount of devices with diverse requirements and applications, cryptography-based approaches may no longer remain an adequate way to provide security [1]. This is due to the fact that encryption entails key generation, distribution, and management processes, which are extremely challenging tasks especially in dynamic, multi-heterogeneous networks with massive device connections.

To cope with this, key-less physical layer security (PLS) has emerged as a new concept and powerful alternative that can complement and may even replace encryption-based approaches [2], [3]. The basic idea is to exploit channel characteristics alongside well-designed transmission schemes in order to ensure the ability of the intended user to perform successful data decoding, while preventing eavesdroppers from doing so [2], [4]. In the literature, practical signal processing-based security techniques are shown to be among the effective ways in providing secrecy. This can be performed, for-instance, by utilizing the degree of freedom that exists in the space domain like MIMO, coordinated multi-point (CoMP), relay, etc. However, when there is no spatial degree of freedom, exploiting the time and frequency degrees of freedom of the transmit waveforms becomes of significant importance to safeguard wireless transmission against eavesdropping. Moreover, since OFDM is the most commonly used waveform in currently existing systems and is expected to keep its dominance with various numerologies in future

5G systems [5], securing OFDM waveform has drawn the attention of many researchers in recent times. It is worth mentioning that besides developing techniques tailored to common transmit waveforms like OFDM, there have recently been some efforts to design new inherently secure waveforms as in [6] and [7].

In the literature, several OFDM-based security techniques have been proposed. These techniques can be categorized from a high-level viewpoint into four main enabling schemes. First, secret key-based schemes, in which secret random sequences are generated from the channel and then used to encrypt the transmitted data on either the application layer [8] or the physical layer such as dynamic coordinate interleaving and constellation rotation schemes [9]. Second, adaptive transmission-based schemes, in which the transmission parameters are adjusted to just meet the quality-of-service (QoS) requirements of only the legitimate receiver. Among these techniques are optimal power allocation [10], adaptive modulation with hybrid-automatic-repeat-request (HARQ) [11], adaptive precoding and interleaving [12], fading-based subcarrier deactivation schemes [13], channel shortening [14], etc. Third, artificial noise (AN)-based schemes [15], in which AN is designed based on the legitimate receiver's channel so that it only harms the eavesdropper's reception, while maintaining an interference-free reception at the legitimate user. Fourth, schemes that can exploit OFDM transceiver impairments [16] or conceal some key features in the OFDM signal to provide secrecy [17].

As inferred, most of the aforementioned OFDM-tailored PLS designs were introduced without having the special requirements of 5G services in mind. Particularly, ultra-reliable and low-latency communication (URLLC) [18], which is expected to be a critical service in 5G networks, imposes new requirements when the PLS design is considered. For URLLC services, physical layer secrecy is desirable to be achieved, while providing better reliability and power efficiency with minimal complexity and low latency. Besides, the security technique has to work in practical scenarios where a reliable channel state information (CSI) feedback may be required to be publicly sent to the transmitter, allowing the eavesdropper to access it and thus causing CSI leakage [19], [20], which is the case in frequency division duplexing (FDD) systems. These new requirements make many of the OFDM-based security techniques unsuitable for 5G URLLC scenario; mainly because of the needed complexity and significant changes in the transceiver design without providing any extra benefits in terms of: 1) reliability, 2) power efficiency, 3) certain robustness to the legitimate CSI leakage, and/or 4) eliminating the need for the knowledge of the eavesdropper's channel at the transmitter.

To address the above challenges, in this paper, inspired by OFDM with index modulation (OFDM-IM) [21]–[23], where the whole OFDM block is divided into sub-blocks and only a subset of the available subcarriers is used for transmission in each block, we first propose an effective physical layer security scheme called OFDM with subcarrier index selection (OFDM-SIS) by exploiting the principle of subcarrier selection in a different manner to enhance the confidentiality performance and guarantee a good level of secrecy gap even in the FDD mode. In the proposed scheme, the frequency response of correlated subchannels is first converted into a completely uncorrelated effective response by means of adaptive channel-based interleaving. Then, only the subcarriers corresponding to high sub-channel gains in each sub-block are used for data transmission in order to maximize the signal-to-noise ratio (SNR) at only the legitimate receiver, while the rest are nulled and not used for data transmission. Interestingly, the presented design is found out to not only provide secrecy in the worst security scenario, but also to enhance the bit error rate (BER) performance of the legitimate receiver, where a significant gain is obtained while saving the transmit power.

Next, we investigate the enhancement in the secrecy performance that can be achieved by the proposed scheme when time division duplexing (TDD) mode is considered. This is achieved by introducing two levels of security, which are obtained by the joint and hybrid design of subcarrier index selection alongside adaptive interleaving based on the channel of the legitimate user. This scheme is named as OFDM-SIS with adaptive interleaving (OFMD-SIS-AI).

Moreover, to facilitate the BER and outage secrecy performance analysis of the proposed OFDM-SIS scheme, the probability distribution functions (PDFs) of the effective instantaneous power and amplitude of the faded subchannels are numerically calculated using fitting methods Based on these, new mathematical expressions for the BER of both the legitimate receiver and the eavesdropper as well as the secrecy outage probability are derived. The provided results prove the effectiveness of the proposed design in achieving practical secrecy alongside remarkable enhancement in the BER performance of the legitimate receiver with respect to the conventional and index modulation-based OFDM designs.

The rest of the paper is organized as follows. The system model and its preliminaries are described in Section II. The details of the developed secure OFDM-SIS scheme are revealed in Section III. The analytical analysis is presented in Section IV. Computer simulation results are exhibited and discussed in Section V. Finally, the paper is concluded in Section VI.[1]

II. SYSTEM MODEL AND PRELIMINARIES

A single-input single-output (SISO) OFDM system is considered. Specifically, the system is composed of a transmitter (Tx), called Alice, aims at communicating confidentially with a legitimate receiver (Rx), called Bob, whereas an eavesdropper, called Eve, is trying to intercept the data

[1] *Notations*: Vectors are denoted by bold-small letters, matrices are denoted by bold-capital letters, and $\mathbf{I}$ is the identity matrix. The transpose, Hermitian, and inverse are symbolized by $(\cdot)^{\mathrm{T}}$, $(\cdot)^{\mathrm{H}}$ and $(\cdot)^{-1}$, respectively.

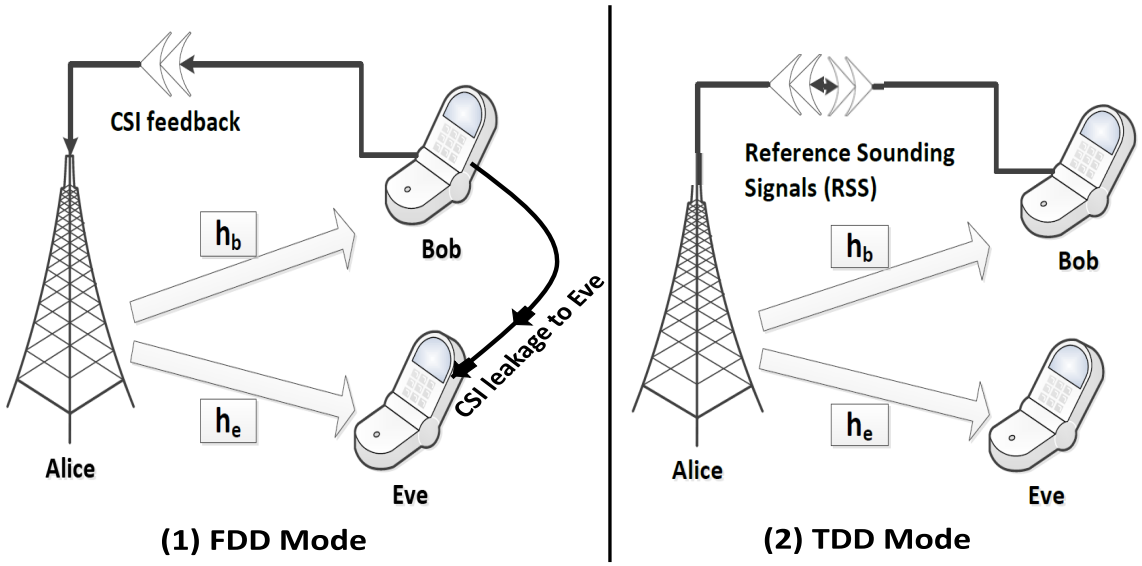

FIGURE 1. A simplified generic system model for the considered two physical layer security scenarios: 1) FDD mode, where the CSI of Bob is sent publicly to Alice, enabling Eve to access it. 2) TDD mode, where the CSI of Bob is estimated by using channel sounding, preventing Eve from accessing it.

TABLE 1. The two operational modes considered in the system model.

	(1) **FDD mode**	(2) **TDD mode**
Scenario description	The CSI of Bob is sent publicly to Alice, enabling Eve to access it (CSI leakage to Eve).	The CSI of Bob is estimated by using channel sounding reference signals, preventing Eve from accessing it (no CSI leakage).
Enabling security technique	Optimal subcarrier index selection in each sub-block to maximize the SNR at Bob only. The technique is named as OFDM-SIS.	Joint optimal subcarrier index selection and adaptive interleaving based on the channel of Bob, resulting in two levels of security. The technique is renamed as OFDM-SIS-AI.
Evesdropper status	Since Eve knows the channel of the legitimate user from the explicit feedback, she is assumed to know the selected subcarriers as well as the used interleaver.	Since Eve does not have the knowledge of the legitimate user's channel as there is no explicit feedback (i.e., channel sounding is used to estimate the channel by exploiting channel reciprocity), she has no knowledge of the used interleaver.

communication link between the two legitimate parties (Alice and Bob) as shown in Fig. 1, where two operational modes (FDD and TDD) are considered for the proposed scheme. The channels experienced by both Bob $\mathbf{h_b} \in \mathbb{C}^{[1\times L]}$ and Eve $\mathbf{h_e} \in \mathbb{C}^{[1\times L]}$ are assumed to be multi-path slowly varying channels of L exponentially decaying taps with Rayleigh fading distribution. Moreover, since Eve is a passive node, the realistic assumption, where Alice has no knowledge of Eve's channel, is adopted. Moreover, both Bob and Eve are assumed to experience independent channels as the wireless channel changes according to the locations of Tx and Rx as well as the environment [7]. In addition, we assume two operational division duplexing modes, whose scenario descriptions, proposed enabling security techniques, and Eve's status for each mode are summarized in Table 1.

At Tx, the number of frequency-domain complex data symbols to be transmitted is N, which also represents the total number of utilized subcarriers. Thus, we represent the frequency-domain OFDM symbol as $\mathbf{s} = \left[s_0\ s_1\ \ldots\ s_{N-1}\right]^{\mathrm{T}} \in \mathbb{C}^{[N\times 1]}$. The OFDM symbol is then interleaved in order to eliminate the correlation between the subchannels and make them look completely random and independent as shown in Fig. 2. This is performed so that

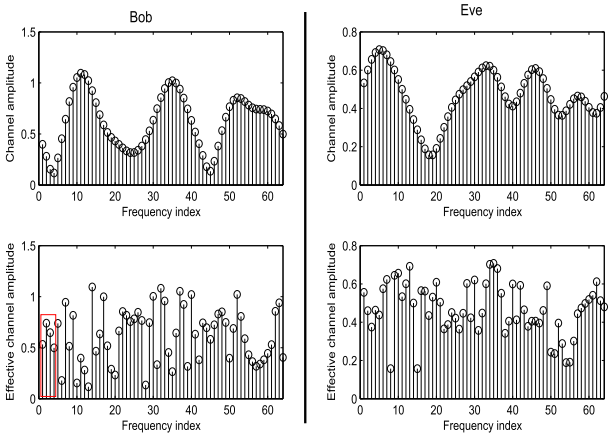

FIGURE 2. Bob's and Eve's channel frequency responses alongside their effective interleaved channels i.e., $\mathbf{H_b^f R}$ and $\mathbf{H_e^f R}$ (shown in lower part of the figure).

we can ensure distributing the deep-faded subchannels uniformly over the whole OFDM symbol, and thus guarantee to experience a few deep-faded subchannels in each subblock. In this work, we consider using an adaptive CSI-dependent interleaver, denoted by a unitary matrix $\mathbf{R}$ of size $N \times N$,

where the entries of each column are all zeros except a single entry of value equals to one at the position of the subcarrier to be permutated [12]. We select CSI-based interleaving for two reasons: 1) it is proven to be the best in terms of eliminating burst errors (or consecutive deep-faded subchannels) and make them uniformly distributed over the whole OFDM block when the CSI is available at Tx [24]; 2) it can be utilized to provide a second level of security in TDD mode beside the level obtained by the optimal subcarrier index selection process [12]. It is worth mentioning that the interleaver design that we have recently devised in [12] was perceived as a kind of precoder due to the fact that $\mathbf{R}$ was extracted by applying singular value decomposition on the diagonal matrix of the channel amplitude frequency response, and then taking the right unitary matrix, resulting from the decomposition, as the interleaving matrix. For more details on the design of this type of interleavers and how it can be made robust to channel reciprocity mismatch, we refer the readers to [12] and [24]. Another important detail to mention here is the fact that Eve is assumed to perfectly know $\mathbf{R}$ in FDD mode as the CSI is publicly sent from Bob to Alice, and thus, Eve can use this CSI to derive the used interleaver $\mathbf{R}$. Similar to OFDM-IM [21], where the whole OFDM block is divided into sub-blocks and only a subset of the available sub-carriers in each sub-block is used for data transmission, here we follow a similar procedure; however, in our technique, the subcarrier indices are not used to convey information, but rather selected adaptively based on the channel of the legitimate receiver to provide secrecy and enhance reliability. This is different from OFDM-IM, where the sub-carriers are selected based on the incoming data to convey information by the sub-carrier indices so that better reliability can be achieved at the expense of a minor spectral efficiency loss. The details of the proposed OFDM-SIS security technique along with its physical structure will be explained in the next section. The resulting interleaved block ($\mathbf{g} = \mathbf{Rs}$) is then passed through an IFFT process $\mathbf{F}^{\mathrm{H}} \in \mathbb{C}^{[N\times N]}$, which basically maps the data points to orthogonal sub-carriers, where $\mathbf{F}$ is the discrete Fourier transform matrix. To avert the inter-symbol-interference, a cyclic prefix (CP) of length L is inserted by using the CP appending matrix $\mathbf{C} \in \mathbb{R}^{[(N+L)\times N]}$. Thus, the transmitted baseband signal by Alice can be represented as

$$\mathbf{x} = \mathbf{CF}^{\mathrm{H}}\mathbf{Rs} = \mathbf{CF}^{\mathrm{H}}\mathbf{g} \in \mathbb{C}^{[(N+L)\times 1]}. \tag{1}$$

After the signal $\mathbf{x}$ passes through the channel and reaches both Bob and Eve, each one of them will first discard the CP part of the signal using the matrix of $\mathbf{D} \in \mathbb{R}^{[N\times(N+L)]}$ and then perform an FFT process using the matrix of $\mathbf{F} \in \mathbb{C}^{[N\times N]}$ to transform the signal into the frequency domain. Thus, the net received signal vector with dimensions $N \times 1$ at Bob after performing the aforementioned operations can be given in a linear matrix representation form as follows

$$\mathbf{y_b} = \mathbf{FD}\left(\mathbf{H_b CF}^{\mathrm{H}}\mathbf{Rs} + \mathbf{z_b}\right) \tag{2}$$

$$= \mathbf{H_b^f Rs} + \hat{\mathbf{z}}_b. \tag{3}$$

On the other hand, at Eve, the captured signal after the FFT process can be formulated as

$$\mathbf{y_e} = \mathbf{FD}\left(\mathbf{H_e CF}^{\mathrm{H}}\mathbf{Rs} + \mathbf{z_e}\right) \tag{4}$$

$$= \mathbf{H_e^f Rs} + \hat{\mathbf{z}}_e. \tag{5}$$

In this model, $\mathbf{H_b} \in \mathbb{C}^{[(N+L)\times(N+L)]}$ and $\mathbf{H_e} \in \mathbb{C}^{[(N+L)\times(N+L)]}$ are the Toeplitz matrices corresponding to the channel impulse responses of both Bob and Eve, whereas $\mathbf{H_b^f} = \mathbf{FDH_bCF}^{\mathrm{H}} = \mathrm{diag}[H_{b_1}, \cdots, H_{b_N}] \in \mathbb{C}^{[N\times N]}$, and $\mathbf{H_e^f} = \mathbf{FDH_eCF}^{\mathrm{H}} = \mathrm{diag}[H_{e_1}, \cdots, H_{e_N}] \in \mathbb{C}^{[N\times N]}$ are the diagonal matrices corresponding to the channel frequency responses of Bob and Eve, respectively. Note that H_{b_i} and H_{e_i} for $1 \le i \le N$ denote the sub-channel frequency response of the i^{th} sub-carrier with respect to Bob and Eve, respectively. The vectors $\mathbf{z_b}$ and $\mathbf{z_e}$ are formed by the samples of the zero-mean complex additive white Gaussian noise (AWGN) with variances of σ_b^2 and σ_e^2 at Bob and Eve respectively, whilst $\hat{\mathbf{z}}_b$ and $\hat{\mathbf{z}}_e$ are the Fourier transformed versions of the noise vectors at Bob and Eve, respectively.

III. PROPOSED SECURE OFDM-SUBCARRIER INDEX SELECTION (OFDM-SIS) WITH ADAPTIVE INTERLEAVING

The key difference between the use of the proposed technique in FDD and TDD modes is the fact that the adaptive interleaver is known to Eve in FDD mode, resulting in one security level, which is provided by the use of optimal subcarrier index selection (SIS). Thus, the proposed scheme is named in FDD mode as OFDM-SIS. However, in TDD mode, the adaptive interleaver will not be known to Eve, resulting in two security levels which are obtained by both optimal subcarrier index selection and adaptive interleaving (AI). Thus, the scheme is named in TDD mode as OFDM-SIS-AI.

The focus of this section will be on explaining OFDM-SIS, which is introduced for providing secrecy and enhancing reliability. Here, the transmitted OFDM block, i.e., $\mathbf{s}$ of length N, is first divided and partitioned into a set of smaller sub-blocks, each containing K sub-carriers. Recall that interleaving is performed in order to distribute the deep fades of the sub-channels and make them look uncorrelated, random, and uniformly distributed over the whole OFDM block to ensure experiencing a few deep-faded subchannels in each subblock. Also, block partitioning is performed in order to reduce the complexity of the optimization algorithm that will be explained later. The basic idea of the proposed scheme is to enlarge the gap between Bob's and Eve's capacities by making the effective SNR at Bob higher than that at Eve for a given channel frequency response. This is achieved by selecting in each sub-block only the sub-carriers corresponding to the highest sub-channel gains with respect to the legitimate receiver only. Particularly, for each sub-block, a set of M out of K sub-carriers is optimally selected to maximize the SNR at Bob. Note that the SNR of Bob over each sub-carrier can be given by $SNR_{b_i} = \gamma_b = \frac{P\|H_{b_i}\|^2}{\sigma_b^2}$, where P is the

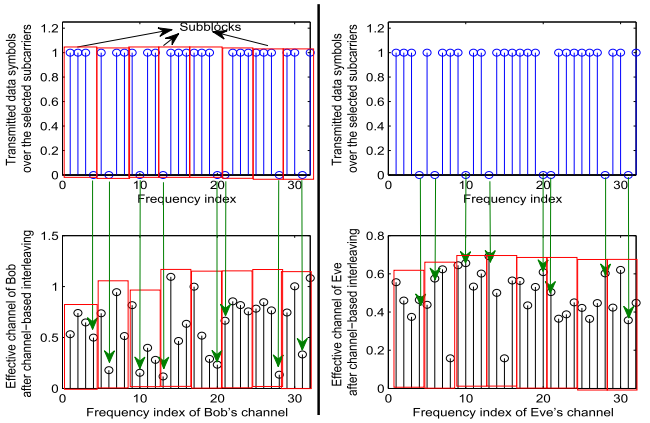

FIGURE 3. Subcarrier structure of the designed secure OFDM-SIS scheme with $\zeta = 3/4$: In each sub-block, surrounded by red rectangle, the sub-carriers experiencing good sub-channel gains with respect to Bob are used for data transmission, while the rest are nulled. Note that with respect to Eve, the nulled sub-carriers do not usually correspond to the weak (bad) sub-channels.

power allocated to each sub-carrier, whereas $\|H_{b_i}\|$ is the subchannel's magnitude. Now, the problem of the optimal selection of indices of M sub-carriers corresponds to solving the below optimization problem for all possible sub-carrier combinations, given as

$$\{c_1^{opt}, \cdots, c_M^{opt}\} = \arg \max_{\{c_1,\cdots,c_M\}\in\mathcal{A}_M} SNR_{b_{[c_1,\cdots,c_M]}}, \quad (6)$$

where $\mathcal{A}_M$ denotes the set of all possible subcarrier combinations with M selected out of K sub-carriers, and $SNR_{b_{[c_1,\cdots,c_M]}}$ is the sum of SNRs of the M selected subcarriers in each subblock. In this scheme, we define $\zeta = M/K$ as the sub-carrier activation ratio of the number of selected sub-carriers to the number of available sub-carriers in each sub-block. Now, since uniform power allocation is used for all sub-carriers, the aforementioned problem boils down to selecting the sub-carriers corresponding to the best sub-channel gains. This can be given as below

$$\{c_1^{opt}, c_2^{opt}, \cdots, c_M^{opt}\} = \arg \max_{\{c_1,\cdots,c_M\}\in\mathcal{A}_M} \|H\|_{b_{[c_1,\cdots,c_M]}}, \quad (7)$$

where $\|H\|_{b_{[c_1,\cdots,c_M]}}$ is the sum of the magnitudes of the sub-channels corresponding to the selected subcarriers. Note that searching all possible subcarrier combinations, i.e., $\binom{K}{M} = \frac{K!}{M!(K-M)!}$, may dictate considerable complexity, especially when the block size is very large. Therefore, it is important to significantly reduce the complexity of solving the above problem. This is achievable when the whole OFDM block is split into smaller parts to reduce the size of the search space.

Moreover, we also want to make sure that, in each sub-block, the sub-carriers have to experience independent as well as different high and low sub-channel gains so that the high ones with respect to Bob can be used for data transmission, while the low ones can be nulled as visualized in Fig. 3. It is obvious from Fig. 3 that, with respect to Bob, the transmitted data points correspond to high subchannel gains, while the nulled ones correspond to deep-faded sub-channels; on the other hand, the selected subcarriers will correspond to random subchannels with respect to Eve.

To further reduce the complexity of the optimization problem, Alice can select M ($1 \leq M \leq K$) out of K subcarriers that maximizes the effective instantaneous SNR at Bob in each sub-block by first ranking the sub-carriers based on their instantaneous channel gains in a descending order, i.e., $\{\|H_{b1}\|^2 \geq \|H_{b2}\|^2 \geq \cdots \geq \|H_{bK}\|^2\}$. Then, Alice selects the first M indices of the sub-carriers corresponding to the sorted sub-channel gains. It should be noted that this scheme has some similarities with the optimal antenna selection techniques in the spatial domain of MIMO systems [25], [26], but here the selection is performed in the spectral domain of the transmit OFDM waveform and different data symbols are sent over different orthogonal sub-channels.

It is manifest from the aforementioned discussion that two different subcarrier selection procedures are introduced, namely, the combination-based and sorting-based selection schemes. Although we can use any one of them as both are optimal in terms of maximizing the SNR at the legitimate receiver; however, we adopt the sorting-based selection scheme for the rest of the paper due to its low-complexity and low-delay features compared to that of combination-based selection. These features are also very favorable and desirable for URLLC services as well as for compact, battery-limited 5G-IoT devices.

At Bob's side, the captured signal can be given as

$$\mathbf{y_b} = \mathbf{H_b^f R P} \begin{bmatrix} \mathbf{s}_d \\ \mathbf{s}_z \end{bmatrix} + \hat{\mathbf{z}_b} \in \mathbb{C}^{[N\times 1]}, \quad (8)$$

where $\mathbf{s}_d = [s_{(1)}\ s_{(2)}\ \cdots\ s_{(N-N_z)}]^{\mathrm{T}}$ is a vector of $N_d = N - N_z = \zeta N$ frequency data symbols, and $\mathbf{s}_z = [s_{(1)}\ s_{(2)}\ \cdots\ s_{(N_z)}]^{\mathrm{T}}$ is a vector of $N_z = (1-\zeta)N$ nulled sub-carriers. $\mathbf{P}$ is the permutation matrix, which determines the positions (or indices) of the used and nulled sub-carriers in each OFDM block. After discarding the unused nulled sub-carriers, $\mathbf{y_b}$ will have the size of $(\zeta N) \times 1$. Bob then employs the low-complexity zero-forcing frequency domain equalization, followed by deinterleaving, to detect the transmitted data symbols.

At Eve's side, and by assuming that Eve has a sophisticated receiver with full knowledge of the transmission technique and the CSI of the legitimate channel, enabling her to know the indices of the sub-carriers used for data transmission, its captured signal can be given by

$$\mathbf{y_e} = \mathbf{H_e^f R P} \begin{bmatrix} \mathbf{s}_d \\ \mathbf{s}_z \end{bmatrix} + \hat{\mathbf{z}_b} \in \mathbb{C}^{[N\times 1]}. \quad (9)$$

After discarding the unused nulled sub-carriers, $\mathbf{y_e}$ will have the size of $(\zeta N) \times 1$. For Eve to detect the transmitted symbols, she equalizes its received data symbols vector by its corresponding channel frequency response, and then deinterleaves using $\mathbf{R}$ to detect the transmitted symbols. Note that Eve will not have the same performance as that of the

legitimate receiver due to the fact that her channel is different from Bob's one. In other words, since the selected sub-carriers at Alice are independent of Eve's channel, the M strongest, selected transmit sub-carriers for Bob corresponds to a random transmit sub-carriers selection with respect to Eve. According to this design, the proposed OFDM-SIS scheme not only provides secrecy, enhances reliability, and saves power, but also enjoys low-complexity receiver structure compared to the sophisticated ML-based receivers in OFDM-IM.

It is worth mentioning that the proposed scheme results in a controllable spectral efficiency loss due to not using all subcarriers (specifically, the ones with low subchannel gains) for data transmission. However, the adjustable spectral efficiency loss turns into a significant gain in terms of providing better reliability and secrecy with less transmit power and minimal processing and modification at Rx side, making it suitable for URLLC service [18]. Moreover, the extra degree of freedom formed by the OFDM-SIS technique due to subcarrier selection process can provide flexibility in the OFDM design in the sense that it can be exploited to not only enhance secrecy with minimal capacity reduction, but also to perform other useful functionalities. More precisely, unlike OFDM-IM, where the nulled subcarriers cannot be exploited to provide other advantages besides conveying information, in OFDM-SIS, the inactive nulled subcarriers can intelligently be utilized through filling them with specially designed signals to reduce out-of-band emission (OOBE), peak-to-average power ratio (PAPR), and/or adjacent channel interference (ACI) in multiuser scenario as is the case in unique-word OFDM waveform [27]. These kind of designs are beyond the scope of this paper, but can be considered as future works on the proposed technique from the perspective of waveform design.

IV. PERFORMANCE ANALYSIS

Since two levels of security (one by optimal subcarrier index selection and the other by adaptive interleaving) are provided by the proposed security design in the TDD mode, whereas only one security level (optimal subcarrier index selection) is provided in the FDD mode, it is important to quantify the performance obtained by each level individually and then jointly. Thus, in this section, we first analyze the performance obtained by OFDM-SIS (FDD mode), and then by OFDM-SIS-AI (TDD mode).

In order to evaluate the secrecy performance of the proposed OFDM-SIS technique, we need to calculate the statistics of the effective instantaneous SNR at both Bob and Eve, given by $\gamma_b = \frac{\|H_{b_i}\|^2 P}{\sigma_b^2}$ and $\gamma_e = \frac{\|H_{e_i}\|^2 P}{\sigma_e^2}$, respectively. Since both Bob's and Eve's SNRs are functions of the instantaneous amplitude (or power) of their effective corresponding channels, we require to calculate the distributions associated with these quantities so that we can use them to determine the distributions of γ_b and γ_e and then quantify the obtained secrecy and reliability performance.

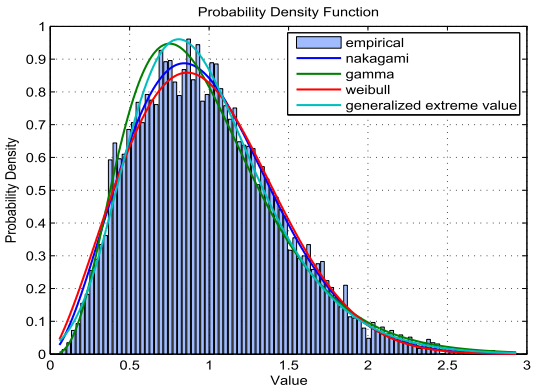

FIGURE 4. The amplitude distribution of the effective subchannels for Bob using the proposed technique with $\zeta = 3/4$. As shown, it follows Nakagami distribution with shape and scale parameters given by $u = 1.297$ and $w = 1.156$, respectively. Note that Nakagami fits the best with the aforementioned parameters that are obtained by fitting methods after applying the proposed OFMD-SIS scheme.

A. STATISTICS OF Bob's EFFECTIVE SNR

The proposed OFDM-SIS results in changing the effective fading distribution over the transmit sub-carriers with respect to Bob. This is due to the fact that a certain percentage of the most deep-faded subchannels are excluded from being used for data transmission, and thus, the fading depth is reduced. The proposed transmission scheme will intuitively lead to an enhancement in the BER performance of the legitimate receiver compared to the standard OFDM transmission as will be demonstrated by computer simulations in Section VI. In order to obtain the distributions of the amplitude and power of the faded subchannels, we use numerical data fitting methods. Particularly, the distributions are obtained by simulating 10000 realizations generated from a standard Rayleigh fading distribution with power delay profile as that explained in the simualtion result section. Then, the proposed OFDM-SIS scheme is applied for selecting the optimal set of sub-carriers, to be used for data transmission. Last, fitting tools are utilized to find the best matching distribution for the fading amplitude and power of the actual used sub-channels.

It is observed from the fitting results that the effective sub-channel fading amplitude distribution over each sub-carrier under the effect of the proposed technique with $\zeta = 3/4$ turns out to follow Nakagami distribution with shape and scale parameters given by $u = 1.297$ and $w = 1.156$, respectively, as shown in Fig. 4. This is different from the conventional OFDM, in which the fading distribution does not change and remains Rayleigh as it is assumed in the system model. Moreover, the effective sub-channel power distribution over each sub-carrier changes from being exponential as is in OFDM to become Gamma with shape and scale parameters given by $u' = 1.297$ and $w' = 0.891$, respectively, as shown in Fig. 5. The resulting PDF of the effective sub-channel fading amplitude, i.e., $\alpha = \|H_{b_i}\|$, corresponding to each transmit sub-carrier, can mathematically be given as

$$P_\alpha(\alpha) = 2\left(\frac{u}{w}\right)^u \frac{1}{\Gamma(u)} \alpha^{2u-1} \exp\left(-\frac{u}{w}\alpha^2\right), \qquad (10)$$

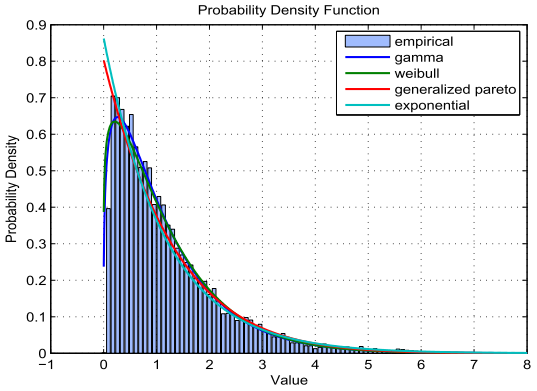

FIGURE 5. The power distribution of the effective subchannels for Bob using the proposed technique with $\zeta = 3/4$. As shown, it follows Gamma distribution with shape and scale parameters given by $u' = 1.297$ and $w' = 0.891$, respectively. Note that Gamma fits the best with the aforementioned parameters.

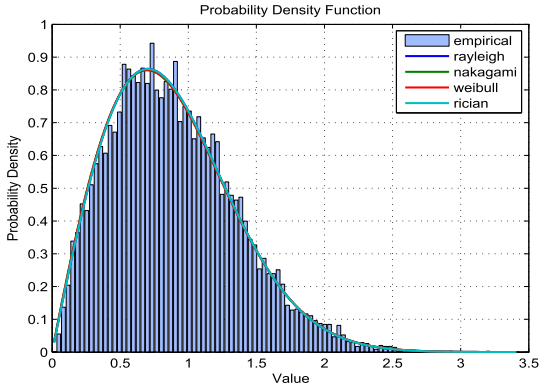

FIGURE 6. The amplitude distribution of the effective subchannels for Eve using the proposed technique with $\zeta = 3/4$. As shown, it is Rayleigh distribution with scale parameter $\beta = 0.704$. Note that the other distributions with their own corresponding parameters that make them equivalent to the fitted subchannel power values can also be used in the analysis.

where u and w are respectively the shape and scale parameters of the obtained Nakagami distribution. Also, we define Ω as the mean square of the sub-channel fading amplitude of α, i.e., $\Omega = E\{\alpha^2\}$. It should be emphasized that the fading distribution of the effective subchannel depends solely on the selection ratio ζ of the proposed scheme. For the two selection ratios we investigate in this paper, i.e., $\zeta = 2/4$ and $\zeta = 3/4$, we have the following Nakagami distribution related parameters:

$$\zeta = 2/4 \Rightarrow u = 1.48, \quad w = 1.31, \ \Omega = 1.3534 \tag{11}$$

$$\zeta = 3/4 \Rightarrow u = 1.297, \quad w = 1.156, \ \Omega = 1.1565. \tag{12}$$

Note that for different values of ζ, different fitting parameters of the Nakagami distribution will be obtained. These are the parameters of the distribution that best fit the effective subchannel amplitude after employing the proposed ODFM-SIS scheme with a certain selection ratio.

Now, the PDF of the effective instantaneous SNR at Bob γ_b can be determined by using a change of variables in the expression for the fading distribution $P_\alpha(\alpha)$ of α [28], giving

$$P_{\gamma_b}(\gamma_b) = \frac{P_\alpha\left(\sqrt{\frac{\Omega\gamma_b}{\bar{\gamma}_b}}\right)}{2\sqrt{\frac{\bar{\gamma}_b\gamma_b}{\Omega}}}. \tag{13}$$

By considering the special case of $\zeta = 2/4$ as an example and approximating the scale parameter u and make it equal to 1.5, $P_\gamma(\gamma)$ can be given as below[2]

$$P_{\gamma_b}(\gamma_b) \approx \left(\frac{u}{w}\right)^u \frac{1}{\Gamma(u)} \frac{\Omega^{\frac{3}{2}}\sqrt{\gamma_b}}{\bar{\gamma_b}^{\frac{3}{2}}} \exp\left(-\frac{u}{w}\frac{\Omega\gamma_b}{\bar{\gamma}_b}\right). \tag{14}$$

The above formula represents a Gamma distribution with parameters associated with $\zeta = 2/4$.

[2]The approximation is made in order to be able to integrate the BER formula (to appear in subsection C) and get an *approximated* closed-form expression. Due to this approximation a slight deviation from computer simulation will occur (as it will be shown in Section VI).

B. STATISTICS OF Eve's EFFECTIVE SNR

To find the probability distribution of the instantaneous SNR at Eve under the effect of the proposed technique, we perform fitting for the effective subchannel fading amplitude experienced by each transmit sub-carrier similar to the case of Bob's channel. Since selecting the optimal set of subcarriers, corresponding to the strongest set of subchannels for Bob, corresponds to a random subchannels set with respect to Eve, the distribution is intuitively anticipated to be similar to the original assumed fading distribution, i.e., Rayleigh. Our obtained results confirm this intuition and demonstrate that the effective distribution of the subchannel amplitude is approximately Rayleigh distributed (same as the original one) with scale factor β as shown in Fig. 6. Also, the effective distribution of the subchannel power is exponential with mean factor ψ as shown in Fig. 7. Mathematically, the amplitude subchannel distribution can be given as below:

$$P_{\alpha_e}(\alpha_e) = \frac{\alpha_e}{\beta^2}\exp\left(-\frac{\alpha_e^2}{2\beta^2}\right), \tag{15}$$

where β is the scale parameter of the obtained Rayleigh distribution. Also, Ω_e is the mean square variable of α_e i.e., $\Omega_e = E\{\alpha_e^2\}$, which is also equal to ψ obtained by fitting methods. For the selection ratios we adopt in this paper, we have the following approximated distribution parameters

$$\zeta = 2/4 \Rightarrow \beta = 0.706, \quad \Omega_e \approx 1 \tag{16}$$

$$\zeta = 3/4 \Rightarrow \beta = 0.704, \quad \Omega_e \approx 1 \tag{17}$$

The PDF of γ_e can be determined by using a change of variables in the expression for the fading distribution $P_{\alpha_e}(\alpha_e)$ of α_e, yielding

$$P_{\gamma_e}(\gamma_e) = \frac{P_\alpha\left(\sqrt{\frac{\Omega_e\gamma_e}{\bar{\gamma}_e}}\right)}{2\sqrt{\frac{\bar{\gamma}_e\gamma_e}{\Omega_e}}}. \tag{18}$$

By taking the special case of the scheme with $\zeta = 2/4$ as an example, the approximated PDF of the effective Eve's SNR,

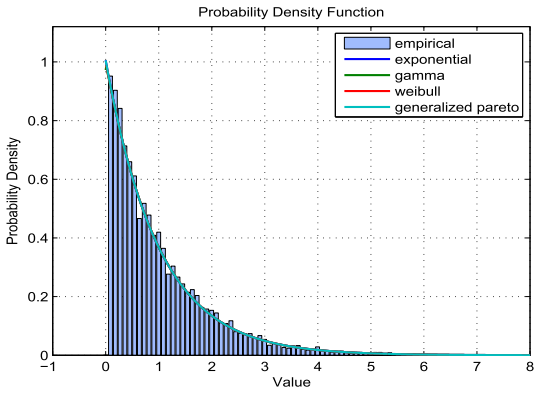

FIGURE 7. The power distribution of the effective subchannels for Eve using the proposed technique with $\zeta = 3/4$. As shown, it is exponential distribution with mean parameter $\psi \approx 1$ (which is equal to Ω_e as well). Note that there are four distribution models that match and coincide with each others when considering their own specific fitting parameters.

$P_{\gamma_e}(\gamma_e)$, can be given in an exponential distribution form as

$$P_{\gamma_e}(\gamma_e) = \left(\frac{1}{\bar{\gamma}_e}\right) \exp\left(\frac{\gamma_e}{\bar{\gamma}_e}\right). \tag{19}$$

Using the above calculated distribution functions, we can now evaluate the BER performance of both Bob and Eve. Moreover, since we now have the SNR statistics of both Bob and Eve, evaluating and analyzing the secrecy performance analytically becomes feasible and convenient, enabling us to examine the advantages of the proposed scheme.

C. Bob's AVERAGE BER

Having formulated the PDF of the instantaneous SNR of Bob, we can analytically evaluate the BER performance of Bob under the effect of the proposed OFDM-SIS scheme. For BPSK/QPSK modulation, the BER of Bob can be given as

$$BER_b = \frac{1}{2}\int_0^\infty \text{erfc}(\sqrt{\gamma_b}) P_{\gamma_b}(\gamma_b)\, d\gamma_b, \tag{20}$$

where erfc(·) is the complementary error function. By substituting the PDF of the effective instantaneous SNR of Bob into (20), we get the following integration formula

$$BER_b = \frac{1}{2}\left(\frac{u}{w}\right)^u \frac{1}{\Gamma(u)} \frac{\Omega^{\frac{3}{2}}}{\bar{\gamma}_b^{\frac{3}{2}}} \int_0^\infty \text{erfc}(\sqrt{\gamma_b})\sqrt{\gamma_b} \times \exp\left(-\frac{u}{w}\frac{\Omega\gamma_b}{\bar{\gamma}_b}\right) d\gamma_b. \tag{21}$$

The above integral is solvable [29], and its final solution results in an approximated closed-form expression, which can be given as

$$BER_b \approx \frac{G}{2\sqrt{\pi}}\left(\frac{\arctan(\sqrt{\rho})}{2\rho^{3/2}} - \frac{1}{2\rho(1+\rho)}\right), \tag{22}$$

where $G = \left(\frac{u}{w}\right)^u \frac{1}{\Gamma(u)} \frac{\Omega^{\frac{3}{2}}}{\bar{\gamma}_b^{\frac{3}{2}}}$, $\rho = \frac{u}{w}\frac{\Omega}{\bar{\gamma}_b}$, and arctan(·) is the tangent inverse.

It should be mentioned that the above derived BER of Bob is also applicable to the case of TDD mode as optimal subcarrier index selection is used in both modes. Now, since channel coding is not included in the design, adaptive interleaving does not contribute to the BER performance. However, one can expect further enhancement in the BER when coded design is considered as it will improve the decoding performance [24]. It is also important to mention that Bob's BER obviously does not get affected whether Eve knows the interleaver (FDD mode) or not (TDD mode). However, the secrecy level will remarkably be affected as Eve's BER in TDD mode will not be the same due to not knowing the interleaving matrix as it will be shown in the next subsection.

D. Eve's AVERAGE BER

As we have demonstrated in the previous analysis that the PDF of the instantaneous SNR of Eve does not change and remains Rayleigh as anticipated, one can analytically show that the BER performance of Eve under the effect of the proposed scheme is the same as the conventional OFDM.

For BPSK/QPSK modulation system, the BER of Eve can be given as

$$BER_e = \frac{1}{2}\int_0^\infty \text{erfc}(\sqrt{\gamma_e}) P_{\gamma_e}(\gamma_e)\, d\gamma_e. \tag{23}$$

By substituting the PDF of the effective instantaneous SNR of Eve into (23), we get the following integration formula

$$BER_e = \frac{1}{2}\int_0^\infty \text{erfc}(\sqrt{\gamma_e})\left(\frac{1}{\bar{\gamma}_e}\right) \exp\left(\frac{\gamma_e}{\bar{\gamma}_e}\right) d\gamma_e. \tag{24}$$

The above integral can readily be solved, and its final solution yields an exact closed-form expression for Eve's BER, which can be given as

$$BER_e = \frac{1}{2}\left(1 - \sqrt{\frac{\bar{\gamma}_e}{(1+\bar{\gamma}_e)}}\right). \tag{25}$$

For the case of TDD mode, where the adaptive interleaver cannot be known to Eve due to performing the estimation of the legitimate user's channel by using channel reciprocity-based sounding techniques instead of sending CSI feedback; Eve's BER will not be the same as the above derived formula. Particularly, Eve's BER will severely be affected by her inability to guess the interleaving matrix $\mathbf{R}$.

Since all the subcarrier indices of the OFDM symbol are involved in the interleaving process, there will be $N!$ possible interleaving patterns. Thus, the probability that Eve can guess the extracted interleaver is $P_e = \frac{1}{N!}$. Accordingly, the BER of Eve in TDD mode with unknown interleaving pattern, denoted by BER_e^*, can be given as $BER_e^* \approx P_e \times BER_e + \frac{1}{2}(1 - P_e)$ [9]. It is obvious that the secrecy gap level (i.e., BER difference between Bob and Eve [3]) will significantly be improved as Eve's BER (BER_e^*) will be extremely bad, i.e., Eve's BER will be equal to 0.5, which is the worst random guess any receiver can make.

E. SECRECY OUTAGE PERFORMANCE

In this subsection, we use the secrecy outage probability as a metric to analytically evaluate the secrecy performance of the proposed OFDM-SIS scheme in the FDD mode. Secrecy outage is chosen as a suitable metric to quantify the performance because of the fact that the CSI of Eve's channel in a practical passive eavesdropping scenario is neither available to Alice nor to Bob. The secrecy outage probability can be given as [3]

$$P_{\text{sout}} = \Pr\{R_{sec} < R_s\}, \tag{26}$$

where R_{sec} is the instantaneous secrecy rate of the proposed OFDM-SIS technique and is given by $R_{sec} = [R_b - R_e]^+$, in which $[q]^+$ denotes $\max\{0; x\}$, $R_b = \log_2(1+\gamma_b)$ is the instantaneous rate of the Bob's effective channel, and $R_e = \log_2(1+\gamma_e)$ is the instantaneous rate of the Eve's effective channel, whereas $R_s > 0$ is a predefined targeted secrecy rate. The secrecy outage probability can be further defined as [2]

$$\begin{aligned} P_{\text{sout}} &= \Pr[R_{sec} < R_s \mid \gamma_b > \gamma_e]\Pr[\gamma_b > \gamma_e] \\ &\quad + \Pr[R_{sec} < R_s \mid \gamma_b \le \gamma_e]\Pr[\gamma_b \le \gamma_e]. \end{aligned} \tag{27}$$

Since $\Pr[R_{sec} < R_s \mid \gamma_b \le \gamma_e]$ always equals to unity when $\gamma_b \le \gamma_e$, the above formula can be reduced to

$$\begin{aligned} P_{\text{sout}} &= \Pr[R_{sec} < R_s \mid \gamma_b > \gamma_e]\Pr[\gamma_b > \gamma_e] \\ &\quad + \Pr[\gamma_b \le \gamma_e]. \end{aligned} \tag{28}$$

Using probability concepts, we can rewrite the previous formula as

$$P_{\text{sout}} = \int_0^{\infty} F_{\gamma_b}\left(2^{R_s}(1+x)-1\right) f_{\gamma_e}(x)dx, \tag{29}$$

where x stands for the realizations of γ_e due to notational simplicity (i.e., $f_{\gamma_e}(x) = P_{\gamma_e}(\gamma_e)$). $F_{\gamma_b}(.)$ is the CDF of the SNR of Bob. For $\zeta = 2/4$, the CDF of γ_b can be obtained by integrating its PDF given in (14), resulting in the following expression

$$F_{\gamma_b}(x) = G\left(\frac{\sqrt{\pi}\,\text{erf}\left(\sqrt{\rho}\sqrt{x}\right)}{2\rho^{\frac{3}{2}}} - \frac{\sqrt{x}\text{e}^{-\rho x}}{\rho}\right), \tag{30}$$

where erf(.) is the error function [29]. By substituting the CDF and PDF of the effective instantaneous SNR of Bob and Eve, respectively, into (29), we get the following formula for

$$\begin{aligned} &P_{\text{sout}} \\ &= rG\int_0^{\infty}\left(\frac{\sqrt{\pi}\,\text{erf}\left(\sqrt{\rho}\sqrt{\left(2^{R_s}(1+x)-1\right)}\right)}{2\rho^{\frac{3}{2}}}\text{e}^{-rx}dx\right) \\ &\quad - rG\int_0^{\infty}\left(\frac{\sqrt{\left(2^{R_s}(1+x)-1\right)}\text{e}^{-\rho\left(2^{R_s}(1+x)-1\right)}}{\rho}\text{e}^{-rx}\right)dx \end{aligned} \tag{31}$$

where $r = \frac{1}{\gamma_e}$. By integrating the above equation, we obtain the final expression of the secrecy outage probability formula given in (32), which is placed at the top of the next page, where $\Gamma(.,.)$ is the incomplete Gamma function [29].

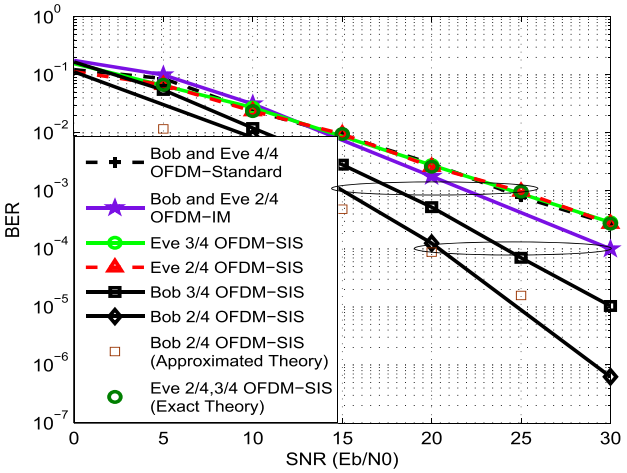

FIGURE 8. BER of both Bob and Eve using the proposed OFDM-SIS in FDD mode compared to OFDM and OFDM-IM. QPSK modulation and different ζ values are used. FDD system is considered, where Eve knows Bob's CSI.

V. SIMULATION RESULTS

In this section, we provide computer simulation results to demonstrate and validate the effectiveness of the proposed security scheme and to also examine the impacts of the selection ratio and the average SNR on the security and reliability performance. First, we quantify the secrecy performance obtained by OFDM-SIS scheme in an FDD mode, then we examine the expected performance gain when OFDM-SIS-AI is used in a TDD mode. We consider a practical uncoded SISO-OFDM system with $N = 64$ sub-carriers adopting quadrature phase shift keying (QPSK) modulation and a guard period of length L. The number of sub-blocks in each OFDM block is considered to be $N/K = 16$, where each sub-block contains $K = 4$ available sub-carriers. Two different values of the activation ratio ζ are considered, i.e., $\zeta = 3/4$ and $\zeta = 2/4$. The channel is modeled as an independent and identically distributed (i.i.d.) block-fading, where channel coefficients are drawn from a Rayleigh fading distribution, and the channel is deemed to be slowly varying. The Rayleigh multi-path fading channels of both Bob and Eve are assumed to have the same length, $L = 9$ samples, with a normalized power delay profile given by $\mathbf{p} = [0.8407,\ 0,\ 0,\ 0.1332,\ 0,\ 0.0168,\ 0.0067,\ 0,\ 0.0027]$ mW [30]. Additionally, we consider an eavesdropper, who perfectly knows the transmission technique used at Alice as well as the CSI of the legitimate receiver in an FDD system during the channel feedback process.

In the performance evaluation, we use both secrecy outage probability metric to quantify the achievable secrecy level, and BER-based secrecy gap metric [7] to not only evaluate the secrecy, but also to quantify the amount of information leakage to Eve and the reliability enhancement with respect to the legitimate receiver.

Fig. 8 shows the BER performance gain of a legitimate Rx, employing the proposed OFDM-SIS in FDD mode with selection ratios $\zeta = 3/4$ and $\zeta = 2/4$ compared to an OFDM-IM scheme with unity and half selection ratios, i.e., $\zeta = 4/4 = 1$ and $\zeta = 2/4 = 0.5$, respectively.

$$
\begin{aligned}
P_{\text{sout}} &= \left[\frac{rG\sqrt{\pi}}{2\rho^{\frac{3}{2}}} \left(\frac{\sqrt{\rho}\cdot 2^{\frac{R_s}{2}} \mathrm{e}^{r-\frac{r}{2^{R_s}}} \operatorname{erf}\left(\frac{\sqrt{\rho\cdot 2^{R_s}+r}\sqrt{2^{R_s}x+2^{R_s}-1}}{2^{\frac{R_s}{2}}} \right)}{r\sqrt{\rho\cdot 2^{R_s}+r}} - \frac{\mathrm{e}^{-rx} \operatorname{erf}\left(\sqrt{\rho}\sqrt{2^{R_s}x+2^{R_s}-1} \right)}{r} \right) \right]_0^{\infty} \\
&\quad + \left[\frac{rG\,\Gamma\left(\frac{3}{2}, \frac{(\rho\cdot 2^{R_s}+r)(2^{R_s}x+2^{R_s}-1)}{2^{R_s}} \right) \rho^{\frac{3}{2}}\cdot 2^{\frac{R_s}{2}+1} \mathrm{e}^{\frac{r\left(2^{R_s}-1\right)}{2^{R_s}}}}{\rho\left(\rho\cdot 2^{R_s}+r\right)^{\frac{3}{2}}} \right]_0^{\infty}. \\
&= \frac{rG\sqrt{\pi}}{2\rho^{\frac{3}{2}}} \left(\frac{\sqrt{\rho}\cdot 2^{\frac{R_s}{2}} \mathrm{e}^{r-\frac{r}{2^{R_s}}}}{r\sqrt{\rho\cdot 2^{R_s}+r}} - \frac{\sqrt{\rho}\cdot 2^{\frac{R_s}{2}} \mathrm{e}^{r-\frac{r}{2^{R_s}}} \operatorname{erf}\left(\frac{\sqrt{\rho\cdot 2^{R_s}+r}\sqrt{2^{R_s}-1}}{2^{\frac{R_s}{2}}} \right)}{r\sqrt{\rho\cdot 2^{R_s}+r}} + \frac{\operatorname{erf}\left(\sqrt{\rho}\sqrt{2^{R_s}-1} \right)}{r} \right) \\
&\quad - \frac{rG\,\Gamma\left(\frac{3}{2}, \frac{(\rho\cdot 2^{R_s}+r)(2^{R_s}-1)}{2^{R_s}} \right) \rho^{\frac{3}{2}}\cdot 2^{\frac{R_s}{2}+1} \mathrm{e}^{\frac{r\left(2^{R_s}-1\right)}{2^{R_s}}}}{\rho\left(\rho\cdot 2^{R_s}+r\right)^{\frac{3}{2}}}.
\end{aligned} \tag{32}
$$

Note that OFDM-IM with unity selection ratio corresponds to standard OFDM. Particularity, it is shown that OFDM-SIS outperforms OFDM at BER $= 10^{-3}$ by more than 5 dB and by around 10 dB for $\zeta = 3/4$ and $\zeta = 2/4$, respectively, and the gain difference gradually grows as the SNR increases. This gain is obtained by utilizing the optimal sub-carrier selection scheme according to the Bob's channel, in such a way that the Bob's SNR is maximized. This causes avoiding the deep-faded sub-channels (which limits the performance) with respect to only Bob, resulting in changing the fading distribution to a less severe fading, and thus, enhancing the BER performance of the fading-limited OFDM-based transmission waveforms.

Generally, it is observed from Fig. 8 that the BER performance enhances as the selection ratio decreases with the price of reduced spectral efficiency. More precisely, an extra gain of 5 dB is achieved at BER$= 10^{-4}$ when the selection ratio reduced from $\zeta = 3/4$ to $\zeta = 2/4$. It should be mentioned that for $\zeta = 2/4$, the slight mismatch between the derived closed form BER expression of Bob and its numerical result is due to two reasons: 1) the necessary approximation we used for the scale parameter u, which appears in the PDF of the effective SNR of Bob, as stated in the footnote of Section IV; 2) the effective subchannel amplitude distributions of Bob over each subcarrier changes according to the considered power-delay profile of the channel. Specifically, it is observed that the channel amplitude fading distribution in OFDM-SIS is not exactly the same for all subchannels as opposed to the case in conventional OFDM.

Furthermore, Fig. 8 exhibits the BER performance of Eve assuming that she is fully aware of the used scheme and also the interleaving matrix as well as the indices of the sub-carriers selected for data transmission as she is considered to know the legitimate CSI link in case of FDD system. Both simulation and analytical results exhibit matching BER performance and prove that Eve's BER under the proposed scheme is the same as that of standard OFDM as expected. This happens due to the use of channel-dependent optimal subcarrier indices selection with respect to Alice-to-Bob channel that is different from Alice-to-Eve channel, for which the selection process looks random (not optimal). Thus, the system response will not be favorable to Eve and no performance gain is delivered to her.

It is also observed that Eve's BER does not change with the variation of selection ratio and the secrecy gap between Bob's and Eve's sides increases as the average SNR grows due to the enhancement in the Bob's BER. The obtained secrecy gap is significant and can be utilized to provide QoS-based secrecy [11], [3]. For instance, at BER$= 10^{-4}$, there is a difference (secrecy gap) of 10-12 dB between Bob and Eve, and thus for a service requiring BER below 10^{-4}, Bob can reliably use the service when his average SNR is equal or greater than 20 dB, while Eve is prevented from using it at comparable SNR values. In fact, Eve needs 10-12 dB more signal power than the average SNR of Bob (i.e., Eve's SNR must be at least 32 dB) to be able to decode the same service reliably. This created gap in BER performances between Bob and Eve results in a good secrecy level that can be effectively utilized to deliver a certain service securely.

Fig. 9 depicts the performance of the secrecy outage probability achieved by the introduced OFDM-SIS scheme in FDD mode when the predefined secrecy rate threshold is set to unity (i.e., $R_s = 1$). Secrecy outage is drawn versus Bob's average SNR when Eve's average SNR ($\bar{\gamma}_e$) is equal to 0 dB and 10 dB, while the selection ratio ζ equals to 2/4, 3/4, and 4/4. From Fig. 9, we see that the decrease of ζ results in a better secrecy outage performance as the effective SNR at Bob increases. This occurs due to avoiding deep fades

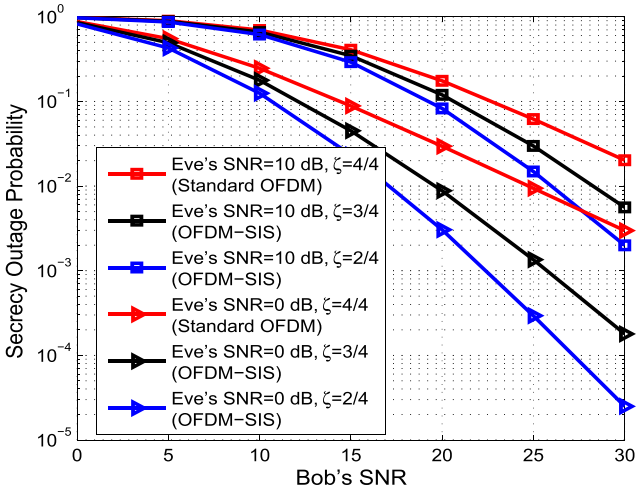

FIGURE 9. Secrecy outage probability of the proposed OFDM-SIS in FDD mode for $\zeta = 1, 0.75, 0.5$; $R_s = 1$; and $\bar{\gamma}_e = 0$ dB and 10 dB.

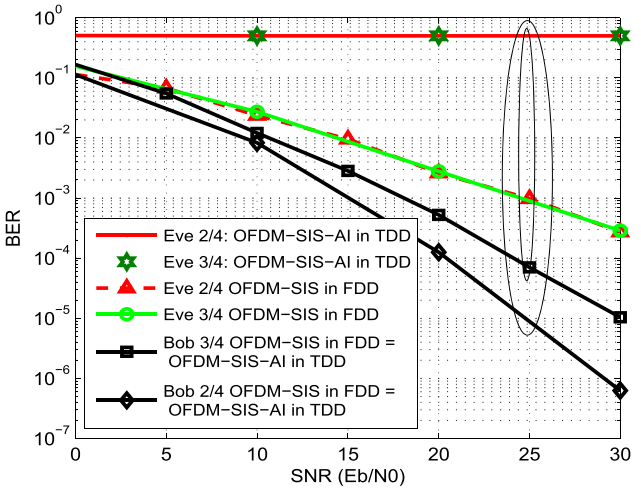

FIGURE 10. BER secrecy gap comparison between the proposed OFDM-SIS in FDD mode and OFDM-SIS-AI in TDD mode. QPSK modulation with different ζ values are used.

and using only the subchannels of highest gain with respect to Bob.

Fig. 10 presents the secrecy gap performance obtained by OFDM-SIS-AI, which is used in TDD mode and provides two security levels: one by the adaptive interleaver and the other by the subcarrier index selection. This figure also provides the comparison of the OFDM-SIS-AI scheme with OFDM-SIS, which is proposed for the FDD mode and also used in TDD mode. Particularly, Fig. 10 shows that the BER performance of Eve using OFDM-SIS-AI remains at 0.5 for both selection ratios $\zeta = 2/4$ and $\zeta = 3/4$ as Eve has no information about the interleaver matrix extracted from Bob's channel. Also, the BER of Bob is the same as that provided by the OFDM-SIS scheme in an uncoded system for the same ζ values. It is important to mention that OFDM-SIS-AI scheme can provide better BER performance to the legitimate user when channel coding is used as it breaks burst errors by mitigating the correlation between subchannels, and thus enhancing the decoding capability. Note that the performance investigation of the proposed scheme with channel coding as well as the effect of practical issues, such as synchronization and estimation errors are beyond the scope of this paper, and left for future research studies.

Based on the obtained results and from both security and reliability perspectives, we have demonstrated that the reliability performance of the proposed OFDM-SIS scheme outperforms both conventional OFDM as well as OFDM-IM. Furthermore, the secrecy performance gain is achieved not only in TDD mode, but also in FDD mode by considering a very challenging scenario where Eve can access the CSI of the legitimate link, and without sharing secret keys, or knowing Eve's channel, or even causing any major changes in the receiver design. Given the simplicity of the proposed design, its hardware testbed implementation is very handy and straightforward to build, making it very appealing for advanced 5G and beyond systems and URLLC services as well as low-complexity Internet of Things (IoT) devices.

It is noteworthy to mention that there is an interesting trade-off between the achievable secrecy and reliability from one side and spectral efficiency from another side (i.e., both secrecy and reliability performance enhances as the spectral efficiency decreases). This trade-off is fully controllable and adjustable via the selection ratio parameter ζ, which can be modified according to the requirements of the user applications and services.

Moreover, the proposed scheme has the advantage of the new degree of freedom created from the selection process, which can provide more flexibility in the OFDM design. More precisely, the subcarriers that are not used for data transmission because of their low subchannel gains, which already limit the performance of both BER and throughput, can be deliberately filled with specially designed signals, that can perform other important functionalities like reducing OOBE and PAPR in each subblock for burst transmission scenarios [5]. In this kind of design, better secrecy and reliability can be achieved while mitigating the effect of challenging problems such as power leakage, PAPR, and interference. Thus, there is almost no loss in the overall system performance, but rather more gains.

It should also be emphasized that although OFDM-SIS is proposed in this work for a single user scenario, where the subcarriers assigned to a certain user are channel-dependent as well as adaptively distributed over the whole band (with a structure similar to that of OFDM-IM before interleaving) thanks to the use of channel-based adaptive interleavers; OFDM-SIS can also be employed for multi-user scenarios. Specifically, in a multi-user scenario, full subcarrier utilization can be achieved as bad subcarriers with respect to a certain user can be good with respect to another user experiencing a different channel condition. Thus, minimal spectral efficiency reduction of the proposed scheme can be guaranteed by assigning the nulled subcarriers with respect to a certain user to other users in the network to send their data over these subcarriers, which may experience good subchannel gains, resulting in what is called *multi-user diversity*

facilitated by different scheduling and resource allocation techniques.

VI. CONCLUSION

An efficient 5G URLLC-tailored physical layer security technique, which can provide two security levels in TDD mode and one in FDD mode, has been proposed for protecting OFDM-based waveforms against eavesdropping. In this technique, named as OFDM-SIS, the frequency response of correlated subchannels is first converted into a completely uncorrelated effective response by means of adaptive channel-based interleaving. Then, the whole OFDM symbol is divided into small sub-blocks, each containing a set of sub-carriers experiencing uncorrelated random sub-channels, from which we select and use only the ones corresponding to good sub-channels for data transmission, while the remaining ones are suppressed. This transmission mechanism results not only in providing remarkable secrecy gap, but also enhances the reliability performance of the legitimate user compared to the standard OFDM transmission. Moreover, the technique saves power and provides secrecy even in the worst security scenario, where the eavesdropper is assumed to know the channel of the legitimate link due to using some kind of explicit FDD-based feedback. The presented results have proven the capability of the proposed scheme in achieving practical secrecy without increasing the complexity of the OFDM structure or knowing Eve's channel, making it very suitable for low complexity 5G-URLLC services (IoT-based remote control and tactile applications). Future work can consider designing and investigating the secrecy performance of different variations of the proposed OFDM-SIS scheme assuming different block sizes and activation ratios. Moreover, utilizing the degree of freedom created by the proposed scheme for providing larger secrecy gap as well as performing other advantageous functionalities besides secrecy, such as reducing PAPR and mitigating OOB leakage (two main drawbacks of OFDM-based waveforms) are appealing future research directions in order to maximize the overall system performance gain.

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[2] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[3] E. Güvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Phys. Commun.*, vol. 25, pp. 14–25, Dec. 2017.

[4] J. M. Hamamreh, E. Güvenkaya, T. Baykas, and H. Arslan, "A practical physical-layer security method for precoded OSTBC-based systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2016, pp. 1–6.

[5] Z. E. Ankarali, B. Peköz, and H. Arslan, "Flexible radio access beyond 5G: A future projection on waveform, numerology, and frame design principles," *IEEE Access*, vol. 5, pp. 18295–18309, May 2017.

[6] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure SISO transmissions and multicasting," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1864–1874, Sep. 2013.

[7] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1191–1194, May 2017.

[8] Y. El Hajj Shehadeh, O. Alfandi, and D. Hogrefe, "Towards robust key extraction from multipath wireless channels," *J. Commun. Netw.*, vol. 14, no. 4, pp. 385–395, Aug. 2012.

[9] H. Li, X. Wang, and J. Y. Chouinard, "Eavesdropping-resilient OFDM system using sorted subcarrier interleaving," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 1155–1165, Feb. 2015.

[10] D. W. K. Ng, E. S. Lo, and R. Schober, "Energy-efficient resource allocation for secure OFDMA systems," *IEEE Trans. Veh. Technol.*, vol. 61, no. 6, pp. 2572–2585, Jul. 2012.

[11] J. M. Hamamreh, M. Yusuf, T. Baykas, and H. Arslan, "Cross MAC/PHY layer security design using ARQ with MRC and adaptive modulation," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2016, pp. 1–7.

[12] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Secure pre-coding and post-coding for OFDM systems along with hardware implementation," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1338–1343.

[13] E. Guvenkaya and H. Arslan, "Secure communication in frequency selective channels with fade-avoiding subchannel usage," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2014, pp. 813–818.

[14] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM-based systems using channel shortening," in *Proc. IEEE Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017.

[15] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[16] M. Yusuf and H. Arslan, "Controlled inter-carrier interference for physical layer security in OFDM systems," in *Proc. IEEE 84th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–5.

[17] Z. E. Ankaralı, H. Arslan, "Cyclic feature suppression for physical layer security," *Phys. Commun.*, to be published. [Online]. Available: https://doi.org/10.1016/j.phycom.2016.09.003.

[18] C.-P. Li, J. Jiang, W. Chen, T. Ji, and J. Smee, "5G ultra-reliable and low-latency systems design," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2017, pp. 1–5.

[19] T.-Y. Liu, P.-H. Lin, S.-C. Lin, Y.-W. P. Hong, and E. A. Jorswieck, "To avoid or not to avoid CSI leakage in physical layer secret communication systems," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 19–25, Dec. 2015.

[20] M. Yusuf and H. Arslan, "On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels," *Phys. Commun.*, vol. 24, pp. 154–160, Sep. 2017.

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

[22] E. Basar, M. Wen, R. Mesleh, M. Di Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE Access*, vol. 5, no. 1, pp. 16693–16746, Sep. 2017.

[23] E. Basar, "Index modulation techniques for 5G wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 168–175, Jul. 2016.

[24] S.-W. Lei and V. K. N. Lau, "Performance analysis of adaptive interleaving for OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 51, no. 3, pp. 435–444, May 2002.

[25] R. W. Heath, Jr., and A. Paulraj, "Antenna selection for spatial multiplexing systems based on minimum error rate," in *Proc. IEEE Int. Conf. Commun. Conf.*, vol. 7. Jun. 2001, pp. 2276–2280.

[26] C. S. Park and K. B. Lee, "Statistical multimode transmit antenna selection for limited feedback MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4432–4438, Nov. 2008.

[27] M. Huemer, C. Hofbauer, and J. B. Huber, "The potential of unique words in OFDM," in *Proc. 15th Int. OFDM-Workshop (InOWo)*, Sep. 2010, pp. 140–144.

[28] M. K. Simon and M.-S. Alouini, *Fading Channel Characterization and Modeling*. Hoboken, NJ, USA: Wiley, 2002, pp. 15–30.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.

[30] Y. Cho, J. Kim, W. Yang, and C. Kang, *MIMO-OFDM Wireless Communication With MATLAB*. Singapore: Wiley, Nov. 2010.

JEHAD M. HAMAMREH received the B.Sc. degree in electrical and telecommunication engineering from An-Najah University, Nablus, in 2013. He is currently pursuing the Ph.D. degree as a member of the Communications, Signal Processing, and Networking Center with Istanbul Medipol University, Turkey. He was a Trainee Researcher with the Department of Electrical and Computer Engineering, Texas A&M University at Qatar. His current research interests are in wireless physical and MAC layers security including the design of advanced secure waveforms, new modulation techniques, and multiple access schemes for future 5G and beyond wireless systems.

ERTUGRUL BASAR (S'09–M'13–SM'16) received the B.S. degree (Hons.) from Istanbul University, Turkey, in 2007, and the M.S. and Ph.D. degrees from Istanbul Technical University in 2009 and 2013, respectively. He was with the Department of Electrical Engineering, Princeton University, NJ, USA, from 2011 to 2012. He was an Assistant Professor with Istanbul Technical University from 2014 to 2017, where he is currently an Associate Professor of electronics and communication engineering. His primary research interests include MIMO systems, index modulation, cooperative communications, OFDM, and visible light communications. He has invented two pending patents on index modulation schemes.

Dr. Basar was a recipient of the Istanbul Technical University Best Ph.D. Thesis Award in 2014 and has received three Best Paper Awards including one from the IEEE International Conference on Communications 2016. He currently serves as an Associate Editor for the IEEE COMMUNICATIONS LETTERS and the IEEE ACCESS, and an Editor for *Physical Communication* (Elsevier). He is also a regular reviewer for various IEEE journals and has served as a TPC member for several conferences.

HUSEYIN ARSLAN (S'95–M'98–SM'04–F'15) received the B.S. degree from Middle East Technical University, Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University, Dallas, TX, USA, in 1994 and 1998, respectively. From 1998 to 2002, he was with the Research Group, Ericsson Inc., NC, USA, where he was involved in several projects related to 2G and 3G wireless communication systems. Since 2002, he has been with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA. He has also been the Dean of the College of Engineering and Natural Sciences, Istanbul Medipol University, since 2014. He was a part-time Consultant for various companies and institutions, including Anritsu Company, Morgan Hill, CA, USA, and The Scientific and Technological Research Council of Turkey. His research interests are in physical layer security, mm-Wave communications, small cells, multicarrier wireless technologies, co-existence issues on heterogeneous networks, aeronautical (high-altitude platform) communications, *in vivo* channel modeling, and system design.

Dr. Arslan has served as a member of the Editorial Board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, the *Elsevier Physical Communication Journal*, the *Hindawi Journal of Electrical and Computer Engineering*, and the *Wiley Wireless Communication and Mobile Computing Journal*. He is currently a member of the editorial board for the IEEE SURVEYS AND TUTORIALS and the *Sensors Journal*. He has served as the technical program committee chair, a technical program committee member, a session and symposium organizer, and the workshop chair in several IEEE conferences.