OFDM-Subcarrier Index Selection with Artificially Interfering Signals for Improving the Physical Layer Security of IoT-5G Systems

Jehad M. Hamamreh

***Abstract*—Ensuring the security of the Internet of Things (IoT) is deemed as one of the most critical challenges and needs that have to be addressed in order to guarantee the successful deployment of IoT in emerging technologies like 5G. In an effort to address this challenge, in this work, an improved, flexible physical layer security technique, referred to as orthogonal frequency division multiplexing-subcarrier index selection with artificially interfering signals (OFDM-SIS-AIS), is developed for protecting the transmission of OFDM-based waveforms against eavesdropping in 5G and beyond wireless networks. In this technique, the frequency response of correlated subchannels is first converted into a completely randomized and independent response by means of interleaving. Then, the whole OFDM block is divided into small sub-blocks, each containing a set of subcarriers, from which a subset of these subcarriers, which are corresponding to high subchannel gains, are selected and used for data transmission, while the remaining ones, which are corresponding to low subchannel gains, are used for sending artificially interfering signals. The selected subcarriers are determined through an optimization problem that can effectively maximize the signal-to-noise ratio (SNR) at only the legitimate receiver. The obtained results demonstrate a significant improvement in the secrecy gap performance without considering the knowledge on the eavesdropper channel nor sharing any keys, while maintaining low complexity and high reliability at the legitimate user.**

***Index Terms*—OFDM-based waveforms, sub-carrier index selection (OFDM-SIS), optimal/adaptive subcarrier selection, physical layer security, eavesdropping, artificially interfering signals.**

I. Introduction

SECURITY is becoming not only a necessary and critical requirement in communication networks but also a powerful mean to maintain the sustainability and usefulness of the digital world we are living in. It has recently become very obvious that the super benefits in terms of new services and applications that future 5G and beyond wireless networks are expected to provide cannot be practically realized without ensuring security and having it as a high priority [1].

Providing confidentiality is a challenging task to achieve in wireless systems mainly because of the broadcast nature of the wireless transmission, where the transmitted signals can be captured and recorded by malicious users in the networks in order to intercept the undergoing communication between the legitimate parties, resulting not only in eavesdropping their data, but also in using this eavesdropped data to lunch more attacks such as identity-based attack, denial of service (DoS), man-in-the-middle, data modification, session hijacking, spoofing (impersonation), and sniffing. These critical vulnerabilities could significantly affect the authenticity, confidentiality, integrity, and availability of the communication link between legitimate users. This necessitates providing security defense against eavesdropping, which is considered to be one of the most critical attacks that is needed as a prerequisite to lunch any kind of attacks in the network.

Traditionally, confidentiality against eavesdropping has been tackled using cryptography and encryption-based approaches. However, the tremendous technological advances in future wireless networks (e.g., 5G and beyond networks) substantiate the need fo new alternative security methods that can meet and address new challenges that didn't exist before, making the classically used cryptographic techniques unsuitable, ineffective, and even impractical in future wireless networks due to many hindrances, among which, we mention the key distribution and management processes for the legitimate parties. These are extremely difficult tasks, especially in large-scale, dense, and heterogeneous wireless networks, where a massive amount of smart devices are simultaneously connected to the network, causing excessive complexity, high overhead, and costly computational processes. Besides, the management and control frames exchanged between communication entities are usually not protected.

To address this, physical layer security based on key-less approach has emerged as a new concept and strong alternative that can supplement and may even replace encryption-based approaches [2] [3]. The basic idea is to exploit channel characteristics such as noise, fading, dispersion, and interference; in order to provide secrecy against eavesdropping [2], [4].

Due to that fact that OFDM is the most commonly used waveform in currently existing systems and is expected to keep its dominance in future systems like 5G, securing OFDM waveform has drawn the attention of many researchers. 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 [5], [6].

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

J. M. Hamamreh is with the department of Electrical-Electronics Engineering, Antalya International (Bilim) University, Antalya, Turkey (email: jehad.hamamreh@gmail.com, jehad.hamamreh@antalya.edu.tr).

transmitted data on either the application layer [7] or the physical layer such as dynamic coordinate interleaving and constellation rotation schemes [8]. Second, adaptive transmission-based schemes, in which the transmission parameters are adjusted to just meet the QoS requirements of only the legitimate receiver. Among these techniques are optimal power allocation [9], adaptive modulation with hybrid-automatic-repeat-request (HARQ) [10], adaptive precoding and interleaving [11], fading-based subcarrier deactivation schemes [12], and channel shortening [13]. Third, artificial noise (AN)-based schemes [14], 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 [15] or conceal some key features in the OFDM signal to provide secrecy [16].

Among the aforementioned techniques, OFDM-SIS (sub-carrier index selection) [17], is a recently proposed flexible and adaptive technique that not only provides secrecy but also improves the reliability performance with minimal complexity, making it a very attractive technique for future secure and flexible systems. However, although the optimal sub-carrier index selection technique (OFDM-SIS) can provide a relatively good secrecy performance, its secrecy gap is limited and may not be sufficient in specific scenarios, where it is highly desirable to increase and ensure secrecy even when Eve's average SNR is much higher than that of Bob.

Therefore, this work comes to address the aforementioned limitation of OFDM-SIS by enhancing its secrecy further and maintaining a good secrecy gap over all SNR ranges. In the proposed scheme, named as OFDM-SIS with artificially interfering signals (OFDM-SIS-AIS), the whole OFDM block is divided into sub-blocks, each containing good and bad subcarriers. The good subcarriers, corresponding to high sub-channel gains, are used for data transmission in order to maximize the signal-to-noise ratio (SNR) at only the legitimate receiver, while the rest (the bad ones) are injected with AIS that can only degrade Eve's reception, while not affecting Bob's performance whatsoever. The provided results prove the effectiveness of the proposed design in enhancing the secrecy gap considerably over all SNR regimes, while keeping the BER performance of the legitimate receiver as that achieved by OFDM-SIS.

The rest of the paper is organized as follows. The system model and its preliminaries are described in Section II. The details of the proposed OFDM-SIS-AIS scheme are revealed in Section III. Computer simulation results are exhibited and discussed in Section IV. Finally, a concise conclusion is drawn in Section V.[1]

II. PRELIMINARIES AND SYSTEM MODEL

A single-input single-output (SISO) OFDM system is adopted, where a transmitting node (Alice), tries to communicate confidentially with a legitimate receiving node (Bob),

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

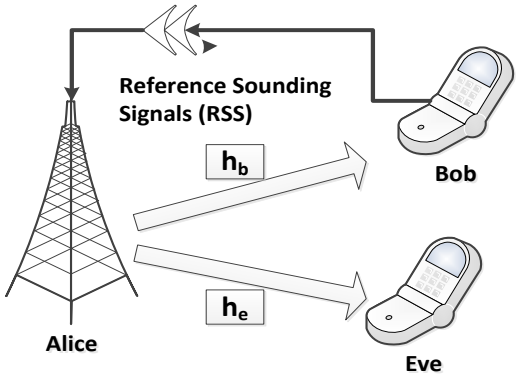

Fig. 1. A simplified system model of the considered PHY security scenario.

whereas an eavesdropping node (Eve) attempts to intercept the communication link between the two legitimate nodes (Alice and Bob) as shown in Fig. 1. The channels of both Bob and Eve, denoted by $\mathbf{h_b} \in \mathbb{C}^{[1\times L]}$ and $\mathbf{h_e} \in \mathbb{C}^{[1\times L]}$, respectively, are assumed to experience multi-path slowly varying channels with L exponentially decaying taps, each with Rayleigh fading distribution. Moreover, as Eve is a passive node in practice, Alice is assumed to have no knowledge of Eve's channel. Also, both Bob and Eve are assumed to experience uncorrelated channels as the channel varies according to the positions of communicating nodes [6]. In addition, time division duplexing (TDD) system is adopted, where Alice and Bob estimate the channel state information (CSI) of their common link by sending sounding reference signals (SRS). This will prevent Eve from accessing or having the knowledge of the CSI of the legitimate link [6] as there is no explicit CSI feedback.

At Alice, N number of frequency-domain complex data symbols is transmitted. Thus, the frequency-domain OFDM symbol can be represented as $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & \dots & s_{N-1} \end{bmatrix}^{\mathrm{T}} \in \mathbb{C}^{[N\times 1]}$. The OFDM symbol is then interleaved in order to eliminate the correlation between the subchannels and make the effective channel response look random and completely independent as shown in Fig. 2. This is performed so that 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 [11]. We select CSI-based adaptive interleaving as it is known to be the best in terms of mitigating burst errors (or consecutive deep-faded subchannels) and make them uniformly distributed over the whole OFDM block when the CSI is available at Tx [18]. It is worth mentioning that the interleaver design devised in [11] was perceived as a kind of precoder due to the fact that $\mathbf{R}$ was extracted by applying SVD on the diagonal matrix of the channel amplitude frequency response, and then take the right unitary matrix, resulting from the decomposition, as the interleaver. For more details on this, we refer the readers to [11], [18]. It should be mentioned that we do not consider in our performance evaluation the secrecy level

that can be obtained by the channel-based adaptive interleaver design as it has already been investigated in the literature [11]. Rather, we focus on the secrecy level obtained by the optimal subcarrier index selection along with artificially interfering signals injection.

Similar to OFDM-IM [19], where the whole OFDM block is split into sub-blocks and only a subset of the available sub-carriers in each sub-block is utilized for data transmission, here we adopt a similar structure; however, in our technique, the sub-carriers are selected based on the channel of the legitimate receiver to improve secrecy. 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-AIS security technique will be explained in the next section. The interleaved block ($\mathbf{Rs}$) 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 preclude 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 (before considering the proposed design) can be represented as

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

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 $\mathbf{D} \in \mathbb{R}^{[N\times(N+L)]}$ and then perform an FFT process using the matrix $\mathbf{F} \in \mathbb{C}^{[N\times N]}$ 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

$$\begin{aligned} \mathbf{y_b} &= \mathbf{FD}\left(\mathbf{H_b CF}^{\mathrm{H}}\mathbf{Rs} + \mathbf{z_b}\right) && (2)\\ &= \mathbf{H_b^f Rs} + \hat{\mathbf{z}}_\mathbf{b}. && (3) \end{aligned}$$

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

$$\begin{aligned} \mathbf{y_e} &= \mathbf{FD}\left(\mathbf{H_e CF}^{\mathrm{H}}\mathbf{Rs} + \mathbf{z_e}\right) && (4)\\ &= \mathbf{H_e^f Rs} + \hat{\mathbf{z}}_\mathbf{e}. && (5) \end{aligned}$$

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 $\hat{\mathbf{z}}_\mathbf{b}$ and $\hat{\mathbf{z}}_\mathbf{e}$ are the Fourier transformed versions of the noise vectors at Bob and Eve, respectively.

III. Review of OFDM-Subcarrier Index Selection (OFDM-SIS)

In the OFDM-SIS scheme [17], the transmitted OFDM block, i.e., $\mathbf{s}$, is first divided and partitioned into a set of smaller sub-blocks, each containing K number of sub-carriers. The basic idea of the proposed scheme is to enlarge the gap between Bob 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 dividing the K sub-carriers in each sub-block into two subsets: the first, which includes the sub-carriers corresponding to the highest subchannel gains, is used for data transmission (to maximize the effective SNR at Bob); whereas the second, which includes the sub-carriers

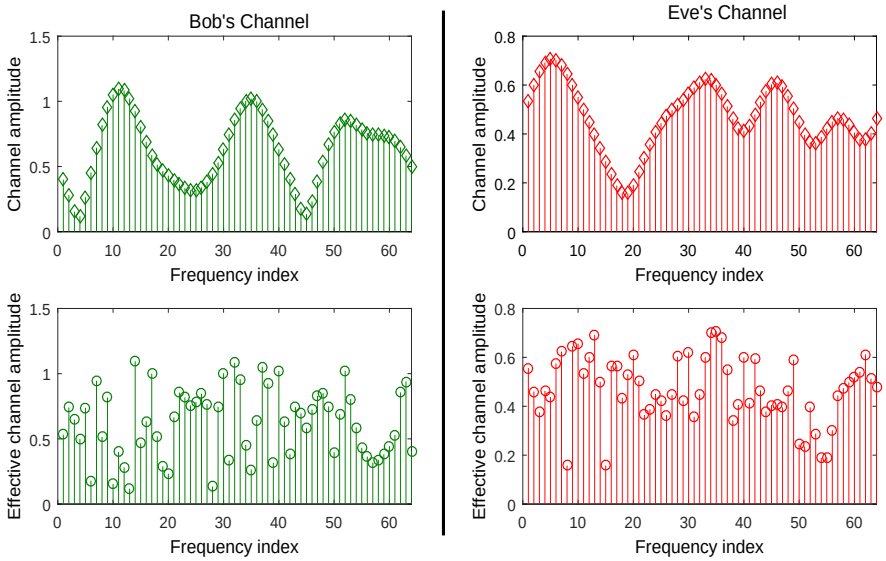

Fig. 2. Bob's and Eve's channel frequency responses alongside their effective channels after interleaving i.e., $\mathbf{H_b^f R}$ and $\mathbf{H_e^f R}$ (shown in the lower part of the figure).

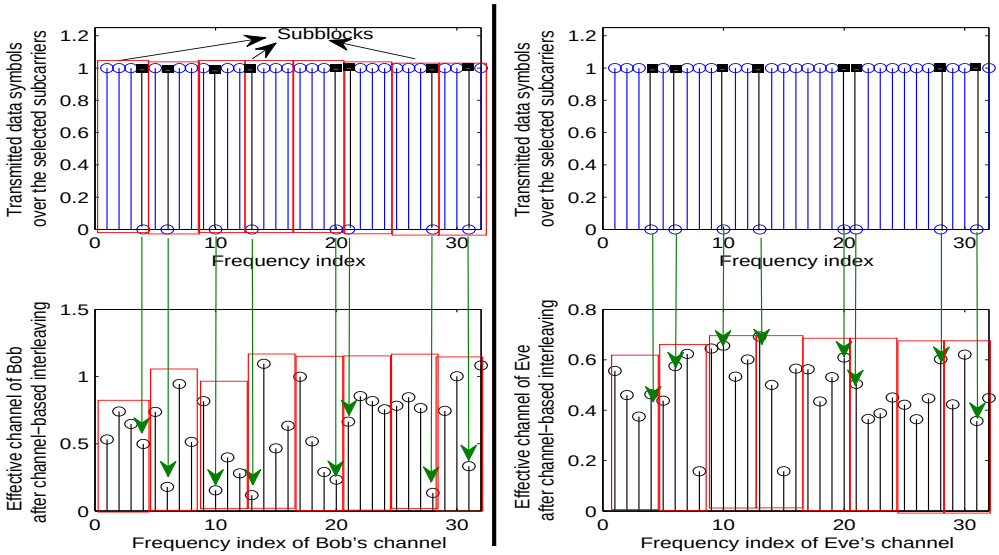

Fig. 3. Subcarrier structure of the designed secure OFDM-SIS-AIS scheme with $\zeta = 3/4$: In each sub-block, surrounded by red rectangle, the sub-carriers (blue-colored) experiencing good sub-channel gains with respect to Bob are used for data transmission, while the rest (black-colored) are injected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

corresponding to the lowest channel gains, is suppressed and nulled (i.e., not used for data transmission).

Particularly, for each sub-block, a set of M out of K sub-carriers is optimally selected to maximize the SNR at Bob, while the remaining $K - M$, which are not used for data transmission, are filled with zeros. Here, $\zeta = M/K$ is defined as the sub-carrier activation ratio of the number of selected sub-carriers to the number of available sub-carriers in each sub-block. 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 power allocated to each sub-carrier. Now, the problem of the optimal selection of the 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. Since uniform power allocation is used for all sub-carriers, the aforementioned problem boils down to selecting the sub-carriers corresponding to the best subchannel gains. This can be given as below

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

That is, finding all possible subcarrier combinations, i.e. $\binom{K}{M} = \frac{K!}{M!(K-M)!}$, may cause huge complexity, especially when the block size is very large. Therefore, it is important to considerably reduce the complexity of solving the above problem. This is possible when the whole OFDM block is divided into smaller parts to decrease the size of the search space. Moreover, it is also required to guarantee that, in each sub-block, the sub-carriers have to experience independent and 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 are suppressed (i.e., filled with zeros).

Now, to further minimize 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.

In this scheme, the transmitted base-band signal by Alice can be reformulated as

$$\mathbf{x} = \mathbf{C}\mathbf{F}^{\mathbf{H}}\mathbf{R}\mathbf{P}\begin{bmatrix}\mathbf{s}_d \\ \mathbf{s}_z\end{bmatrix} \in \mathbb{C}^{[(N+L)\times 1]}, \quad (8)$$

where $\mathbf{s}_d = [s_{(1)}, s_{(2)}, \ldots, s_{(N-N_r)}]^{\mathrm{T}}$ is the vector of $N_d = N - N_r = \zeta N$ frequency data symbols, and $\mathbf{s}_z = [s_{(1)}, s_{(2)}, \ldots, s_{(N_r)}]^T$ is the zero vector of $N_r = (1-\zeta)N$ frequency points (i.e., nulled subcarriers). $\mathbf{P}$ is the permutation matrix, which determines the positions of the data and the nulled subcarriers within the subblocks of each OFDM symbol.

IV. Proposed OFDM-Subcarrier Index Selection with Artificially Interfering Signals (OFDM-SIS-AIS)

Although the OFDM-SIS technique discussed in the previous section can provide a relatively good secrecy performance as demonstrated in [17], its secrecy gap may not be sufficient enough in specific scenarios, where it is highly desirable to increase the secrecy gap even when Eve's average SNR is higher than that of Bob. In addition, despite the fact that

OFDM-SIS technique is motivated (besides its low-complexity and better-reliability) by its capability to work in the worst security scenario, where the CSI of the legitimate link can be accessed by Eve due to using explicit feedback as is the case in FDD systems, the technique adheres and maintains its applicability in TDD systems as well and can be modified in such a way to boost the achievable secrecy performance (especially in scenarios where Eve's SNR is higher than that of Bob). This is possible in TDD systems by utilizing the fact that Eve has no knowledge on the CSI between the legitimate parties due to using channel reciprocity-dependent sounding techniques for CSI acquisition instead of sending public channel feedback [3]. This will make Eve ignorant to the indices of the subcarriers used for data transmission.

Motivated by these facts, secrecy performance of the proposed design can be enhanced when TDD is adopted by utilizing the remaining nulled sub-carriers, which are not used for data transmission. Particularly, these nulled sub-carriers can be injected and filled by well-designed artificially interfering signals (AIS) that can only degrade Eve's reception as visualized in Fig. 3, while not affecting Bob's performance whatsoever.

It is obvious from Fig. 3 that, with respect to Bob, the transmitted data points correspond to high sub-channel gains, while the AIS-injected subcarriers correspond to deep-faded sub-channels; on the other hand, it is not the same with respect to Eve, whose channel looks random with respect to the optimally selected subcarriers at Alice. We call this secure transmission scheme enhanced OFDM sub-carrier index selection with artificially interfering signals (OFDM-SIS-AIS) injection. In this scheme, the transmitted base-band signal by Alice can be formulated as

$$\mathbf{x} = \mathbf{C}\mathbf{F}^{\mathbf{H}}\mathbf{R}\mathbf{P}\begin{bmatrix}\mathbf{s}_d\\ \mathbf{s}_r\end{bmatrix} \in \mathbb{C}^{[(N+L)\times 1]}, \tag{9}$$

where $\mathbf{s}_d = [s_{(1)}, s_{(2)}, \ldots, s_{(N-N_r)}]^T$ is a vector of $N_d = N - N_r$ frequency data symbols, and $\mathbf{s}_r = [s_{(1)}, s_{(2)}, \ldots, s_{(N_r)}]^T$ is a vector of N_r artificially interfering symbols within each OFDM block.

In the proposed design, $\mathbf{s}_r$ is judiciously designed to have a distribution and power level similar to that of the data modulated symbols. This is made as so in order to preclude and prohibit Eve from distinguishing the samples of AIS vector ($\mathbf{s}_d$) from that of the data vector itself ($\mathbf{s}_r$). For instance, in the case when QPSK modulation is used, $\mathbf{s}_r$ can be designed according to the below formula

$$\mathbf{s}_r = \sqrt{\frac{1}{2}}\left((2\mathbf{u}-1) + j(2\mathbf{q}-1)\right), \tag{10}$$

where the samples of $\mathbf{u}$ and $\mathbf{q}$ vectors are chosen to be Bernoulli-distributed random variables with values of ones and zeros. Note that the positions of the AIS are channel-dependent and thus, cannot be known by Eve when TDD system is used [6]. For Bob, the positions (indices) of these AIS can be obtained from the previous optimization algorithm as the complement of the indices that maximize the SNR at Bob.

Accordingly, the captured frequency domain signal at Bob's side can be given as

$$\mathbf{y_b} = \mathbf{H_b^f}\mathbf{R}\mathbf{P}\begin{bmatrix}\mathbf{s}_d\\ \mathbf{s}_r\end{bmatrix} + \hat{\mathbf{z}}_\mathbf{b} \in \mathbb{C}^{[N\times 1]}. \tag{11}$$

After discarding the sub-carriers injected with AIS, $\mathbf{y_b}$ will have the size of $(\zeta N) \times 1$. Bob then employs the low-complexity zero-forcing frequency domain equalization and deinterleaving to detect the transmitted data symbols.

At Eve's side, its captured signal can be given by

$$\mathbf{y_e} = \mathbf{H_e^f}\mathbf{R}\mathbf{P}\begin{bmatrix}\mathbf{s}_d\\ \mathbf{s}_r\end{bmatrix} + \hat{\mathbf{z}}_\mathbf{e} \in \mathbb{C}^{[N\times 1]}. \tag{12}$$

Note that Eve cannot avoid the effect of the added AIS in the deep fades of the legitimate channel, which is different from her channel, and thus Eve can only make random guesses. Without loss of generality, for Eve to detect the transmitted symbols, she equalizes its received data symbols vector by its corresponding effective channel frequency response. 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 set selection of transmit sub-carriers with respect to Eve.

It is worth mentioning that the extra degree of freedom formed by OFDM-SIS-AIS scheme 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, the AIS can intelligently be redesigned to reduce peak-to-average power ratio (PAPR), out-of-band emission (OOBE), and/or adjacent channel interference (ACI) in multiuser scenario as is the case in unique-word OFDM waveform [20]. These kind of designs are beyond the scope of this paper, but can be considered as a future work on the proposed technique from a waveform design perspective.

V. Performance Analysis

Assuming Eve is fully aware and knowledgeable of the applied PHY security technique (OFDM-SIS-AIS), then she can perform any of following reception procedures: 1) Receive the OFDM symbol, and try to randomly guess the indices used for data from that used for AIS injection. Note that since the structure of the AIS is the same as that of the data, Eve cannot benefit from using intelligent detection technique and thus can never be certain about which subcarrier indices used for what purpose (i.e., data transmission or AIS injection). 2) Receive the OFDM symbol, and try to guess the indices used for data from that used for AIS injection based on Eve's channel quality in a similar manner as Bob does. However, since the channel of Eve is different and independent from that of Bob, Eve will end up making mistakes in the process of selecting and deciding on the subcarrier indices used for

data from that used for AIS injection[2].

Note that since the process of identifying and detecting the subcarriers injected by AIS is fully random in both of the above explained reception procedures, the performance results for both cases will be similar (this will be demonstrated in the numerical evaluation results). Accordingly, the investigation and theoretical analysis of one of the cases is sufficient enough to provide and quantify the detailed performance of the proposed OFDM-SIS-AIS technique.

A. Error Probability Associated with Bob and Eve

Under the proposed OFDM-SIS-AIS design, the BER of Bob is anticipated to be the same as that of OFDM-SIS for any used selection ratio. This is due to the fact that Bob can (by using his channel estimate) simply detect and identify the subcarriers used for data transmission from those used for injecting AIS. Thus Bob can exclude all these subcarriers filled with AIS in his detection process, resulting in an interference-free detection with a BER performance equivalent to that of OFDM-SIS technique that we have recently analyzed in our work in [17].

On the flip side, the BER performance of Eve will not be the same as that of Bob due to injecting AIS as well as selecting the transmit subcarriers based on Bob's channel. Thus, Eve will not be able to avoid the detrimental effect of AIS as her channel is different from that of Bob. Specifically, the error probability (P_e) of the inability of Eve to correctly detect the subcarriers injected with AIS in each subblock is equal to the product of two error probability events. The first error event denoted by ($P_{e1} = 1 - P_{c1}$) represents the probability that the $K - M$ subcarriers injected with AIS are detected wrongly in each subblock composed of K subcarriers, whereas the second error event denoted by ($P_{e2} = 1 - P_{c2}$) represents the probability that the $K - M$ subcarriers injected with AIS are detected wrongly in the shortened subblock composed of the remaining $K-(K-M)$ subcarriers. Mathematically, this can be given as

$$\begin{aligned} P_e &= P_{e1} \times P_{e2} = (1 - P_{c1}) \times (1 - P_{c2}) \\ &= \left(1 - \frac{(K-M)}{K}\right) \times \left(1 - \frac{(K-M)}{K-(K-M)}\right). \end{aligned} \tag{13}$$

Thus, at high SNR regimes, Eve's average BER can be simply formulated as

$$BER_e = \frac{1}{2} \times P_e = \frac{1}{2} \times \frac{M}{K} \times \frac{2M-K}{M}. \tag{14}$$

For the special case when $\zeta = 3/4$, P_e can be given as

$$\begin{aligned} P_e &= \left(1 - \frac{(4-3)}{4}\right) \times \left(1 - \frac{(4-3)}{4-(4-3)}\right) \\ &= \left(\frac{3}{4}\right) \times \left(\frac{2}{3}\right) = \frac{1}{2}. \end{aligned} \tag{15}$$

[2]Remark: If Eve is assumed to be not aware of the used security technique, Eve may think and assume that this is a normal received OFDM signal since the structure of the interference subcarriers is the same as that of the data, i.e., there is no distinctive features between the subcarriers carrying data from that carrying interference at the receiving side with respect to Eve. Hence, Eve will try to decode the whole OFDM symbol as in usual cases without considering the fact that there are subcarriers that are filled with interference. In the this case, the analysis will give worse results compared to the above cases.

In this case when $\zeta = 3/4$, BER_e is given as

$$BER_e = \frac{1}{2} \times P_e = \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}. \tag{16}$$

For the case when $\zeta = 2/4$, $BER_e = \frac{1}{2}$.

B. Secrecy Outage

In this subsection, we use the secrecy outage probability as a metric to analytically evaluate the secrecy performance of the proposed OFDM-SIS-AIS scheme. 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. Before calculating secrecy outage, we need first to determine the effective SNR formulas at both Bob and Eve. Besides, we need to determine the effective channel distribution of both the good subchannel used for data transmission and the bad ones used for injecting AIS.

Since Bob knows exactly the locations (indices) of the subcarriers filled with interfering signals, he can just discard these subcarriers carrying non-data interfering signals. Thus, Bob's effective SNR will not be affected by interference, and it can be given per each subblock as

$$\gamma_b = \frac{\zeta |H_{b_i}|^2 P}{\sigma_b^2} \tag{17}$$

$$\gamma_e = \frac{\zeta |H_{e_i}|^2 P}{(1-\zeta)|H_{e_i,int}|^2 P_{int} + \sigma_e^2} \tag{18}$$

$$\gamma_e = \frac{\phi_1 \sigma}{\phi_2 \tau + 1}, \tag{19}$$

where $\phi_1 = \frac{\zeta P}{\sigma_e^2}$, $\phi_2 = \frac{(1-\zeta)P_{int}}{\sigma_e^2}$, $\sigma = |H_{e_i}|^2$, and $\tau = |H_{e_i,int}|^2$. Note that both $|H_{e_i}|^2$ and $|H_{e_i,int}|^2$ have exponential power distribution. Consequently, the effective CDF of γ_e can be found as follows.

$$\begin{aligned} F(\gamma_e) &= \int_{\tau=0}^{+\infty} \int_{\sigma=0}^{\gamma_e(\tau+1)} f(\sigma,\tau) d\sigma \, d\tau & (20) \\ &= \int_{\tau=0}^{+\infty} \int_{\sigma=0}^{\gamma_e(\tau+1)} \phi_1 \phi_2 e^{(-\phi_1 \sigma)} e^{(-\phi_2 \tau)} d\sigma \, d\tau & (21) \\ &= \phi_1 \phi_2 \int_{\tau=0}^{+\infty} e^{(-\phi_2 \tau)} \int_{\sigma=0}^{\gamma_e(\tau+1)} e^{(-\phi_1 \sigma)} d\sigma \, d\tau & (22) \\ &= \phi_2 \int_{\tau=0}^{+\infty} e^{(-\phi_2 \tau)} . (1 - e^{(-\phi_1 (1+\tau) . \gamma_e)}) d\tau & (23) \\ &= \phi_2 \left(\frac{1}{\phi_2} - \frac{e^{(-\phi_1 \gamma_e)}}{\phi_2 + \phi_1 . \gamma_e} \right). & (24) \end{aligned}$$

To find the PDF of γ_e, we derive the above CDF with respect to γ_e to obtain

$$\begin{aligned} f_{\gamma_e}(\gamma_e) &= \frac{dF(\gamma_e)}{d\gamma_e} & (25) \\ &= \phi_1 \phi_2 e^{(-\phi_1 \gamma_e)} . \left[\frac{1}{\phi_1 \gamma_e + \phi_2} + \frac{1}{(\phi_1 \gamma_e + \phi_2)^2} \right] & (26) \end{aligned}$$

Now, having obtained the PDF and CDF of the effective instantaneous SNR at Eve as well as Bob, one can analytically find and calculate the secrecy outage probability as follows. The secrecy outage probability can be given as [3]

$$P_{\text{sout}} = \Pr\{R_{sec} < R_s\}, \tag{27}$$

where R_{sec} is the instantaneous secrecy rate of the proposed OFDM-SIS-AIS 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 channel, and $R_e = \log_2(1+\gamma_e)$ is the instantaneous rate of the Eve's channel, whereas $R_s > 0$ is a predefined targeted secrecy rate. The secrecy outage probability can be further defined as [2]

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

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

$$\begin{aligned} P_{\text{sout}} &= \Pr[R_{sec} < R_s \mid \gamma_b > \gamma_e] \Pr[\gamma_b > \gamma_e] \\ &+ \Pr[\gamma_b \leq \gamma_e]. \end{aligned} \tag{29}$$

Using probability concepts, we can rewrite the previous formula as

$$P_{\text{sout}} = \int_0^{\infty} F_{\gamma_b}\left(2^{R_s}(1+x)-1\right) f_{\gamma_e}(x)dx, \tag{30}$$

where $x = \gamma_e$, $f_{\gamma_e}(x) = P_{\gamma_e}(\gamma_e)$, and $F_{\gamma_b}(.)$ is the CDF of Bob. The CDF of γ_b heavily depends on the selection ratio (ζ) as explained in [17]. For the case when $\zeta = 2/4$, Bob's CDF is given as [17]

$$F_{\gamma_b}(x) = G\left(\frac{\sqrt{\pi}\,\text{erf}\left(\sqrt{\rho}\sqrt{x}\right)}{2\rho^{\frac{3}{2}}} - \frac{\sqrt{x}\text{e}^{-\rho x}}{\rho}\right), \tag{31}$$

where erf(.) is the error function [21]. By substituting the CDF and PDF of the effective instantaneous SNR of Bob and Eve, respectively, into (30), one can get the final expression of P_{sout}.

VI. SIMULATION RESULTS

In this section, we provide simulation results to demonstrate and validate the effectiveness of the proposed security schemes and to also examine the impacts of the selection ratio and the average SNRs on the security performance.

We consider a practical SISO-OFDM system with $N = 64$ subcarriers 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 $K = 4$ subcarriers. Two different values for the selection 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 sparse, normalized power delay profile given by $\mathbf{p} = [0.8407,\ 0,\ 0,\ 0.1332,\ 0,\ 0.0168,\ 0.0067,\ 0,\ 0.0027]$ mW. Additionally, we consider that Eve is aware of the transmission technique used by Alice and also knows her CSI, but does not know the channel of the legitimate link. In the performance evaluation, we use BER-based secrecy gap metric [6] to both evaluate the secrecy gap between Bob and Eve, and to quantify the amount of information leakage to Eve.

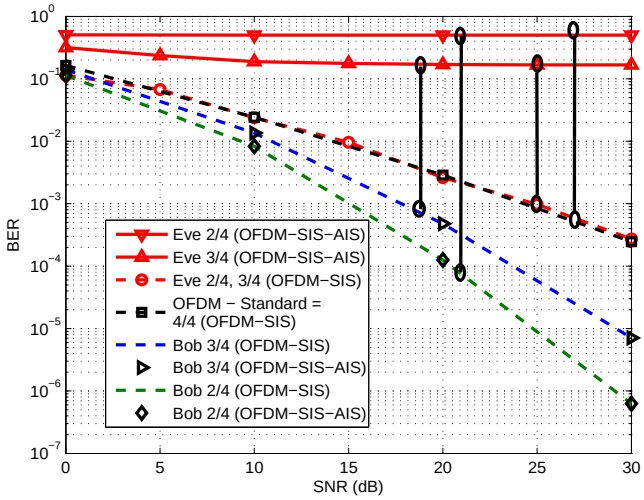

Fig. 4. BER performance comparison between Bob and Eve when OFDM-SIS-AIS is used compared to OFDM-SIS. QPSK modulation alongside $\zeta = 3/4$ and $\zeta = 2/4$ are adopted. TDD mode is considered, where Eve does not know Bob's CSI [6].

Fig. 4 exhibits the BER performance of the benchmark scheme (i.e., OFDM-SIS [17]) for both Bob and Eve. It is assumed that Eve is aware of the used scheme as well as the indices of the nulled sub-carriers (which are not used for data transmission in OFDM-SIS) as these sub-carriers have very low power (ideally zero), making it easy for her to identify and then exclude them from the detection process. It is shown that Eve's performance is the same as that of standard OFDM. 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 side. In contrast, Bob's BER is enhanced as the selection ratio decreases due to sending the data over the subcarriers that are experiencing good subchannels with respect to only Bob. As noticed, the secrecy gap between Bob's and Eve's channel is promising and can be utilized to provide QoS-based secrecy [10].

However, as it can be observed, secrecy cannot be maintained over all SNR values. For instance, for $\zeta = 3/4$ and for the case when Bob's SNR is equal to or less than 18 dB, while Eve's SNR is equal to or greater than 25 dB, Eve will be able to reliably decode a service of BER requirement equals to 10^{-3}, while Bob cannot. Thus, there is a security breach as the secrecy gap in this case will be negative. This problem can be addressed by the proposed OFDM-SIS-AIS scheme, where positive secrecy gap can be ensured at any SNR Bob and Eve may experience.

Fig. 4 presents the BER performance of both Bob and Eve using the proposed OFDM-SIS-AIS scheme with $\zeta = 3/4$ and $\zeta = 2/4$, compared to OFDM-SIS with the same ζ values and standard OFDM (equivalent to OFDM-SIS with $\zeta = 4/4$). It is depicted that the BER performance of Bob using OFDM-SIS-AIS remains the same as that of OFDM-SIS since Bob can just discard the subcarriers not used for data transmission as he knows his CSI, which is assumed in this technique to be estimated using channel sounding techniques in a TDD system. With respect to Eve, a considerable BER degradation is observed over all SNR range due to the artificially injected interfering signals, which cannot be avoided by Eve due to having a channel different than that of Bob. It is observed that the secrecy gap as well as the BER performance of Bob increases as the selection ratio decreases.

Fig. 5 depicts the secrecy outage probability performance versus Bob's average SNR. The performance achieved by the proposed OFDM-SIS-AIS scheme is also compared with conventional OFDM-SIS and standard OFDM schemes when the predefined secrecy rate threshold is set to unity (i.e., $R_s = 1$) and Eve's average SNR ($\bar{\gamma}_e$) is equal to 10 dB , and the selection ratio ζ equals to 2/4 and 3/4. From Fig. 5, we first observe the OFDM-SIS-AIS scheme has superior performance (lower secrecy outage) compared to conventional OFDM-SIS scheme for ζ=3/4 as well as ζ=2/4. In addition, we notice that the decrease of ζ yields a better (lower) secrecy outage performance as the effective SNR at Bob increases, whereas the injection of AIS worsens Eve's SNR, resulting in a larger SNR difference between Bob and Eve.

In Fig. 6, we fix the selection ratio ζ at 3/4 and change Eve's average SNR $\bar{\gamma}_e$ from 10 dB (as it was in the previous setup, whose performance is depicted in Fig.5) to 0 dB and 20 dB. This is set as so in order to investigate the effect of changing $\bar{\gamma}_e$ on the secrecy outage performance of OFDM-SIS-AIS and how it compares to conventional OFDM-SIS scheme. We can see that the outage gets lower when $\bar{\gamma}_e$ decreases as expected. A more interesting observation is that the performance difference between the proposed OFDM-SIS-AIS scheme and the conventional OFDM-SIS gets larger as $\bar{\gamma}_e$ increases, and vice versa (it gets lower as $\bar{\gamma}_e$ decreases). The reason for this behavior is that the injection of AIS becomes less effective in degrading Eve's performance when her SNR is already very bad (like 0 dB). Thus, the performance of OFDM-SIS-AIS boils down (i.e., become comparable) to that obtained by OFDM-SIS when Eve's SNR is extremely very low as demonstrated in Fig. 6.

It is noteworthy to mention here that there is a clear trade-off between secrecy and reliability from one side and throughput from another side (i.e., secrecy increases as ζ decreases). However, the new degree of freedom resulted from the controllable selection process can bring more advantages in terms of providing more flexibility to the OFDM design. More precisely, the subcarriers which are used to send AIS because of their low channel gains (which already limit the performance of both BER and throughput) can be deliberately filled with specially optimized signals that can fulfill other important functionalities (besides secrecy) such as reducing PAPR and OOBE.

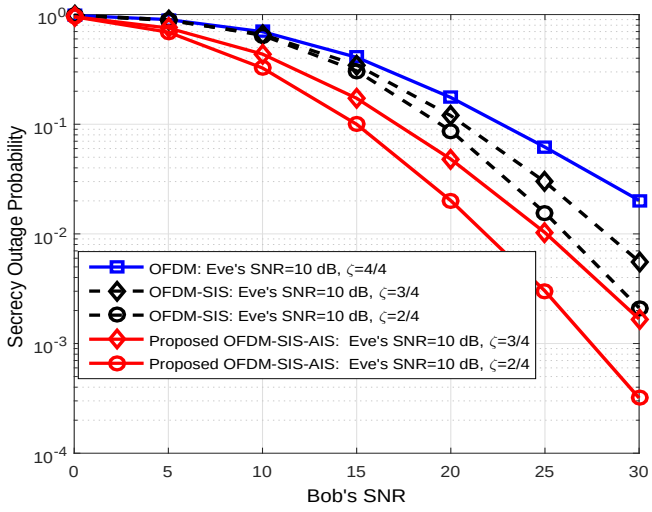

Fig. 5. Secrecy outage probability of the proposed OFDM-SIS-AIS for $\zeta = 1, 3/4, 2/4$, $\bar{\gamma}_e = 10$ dB, and $R_s = 1$ compared to conventional OFDM-SIS.

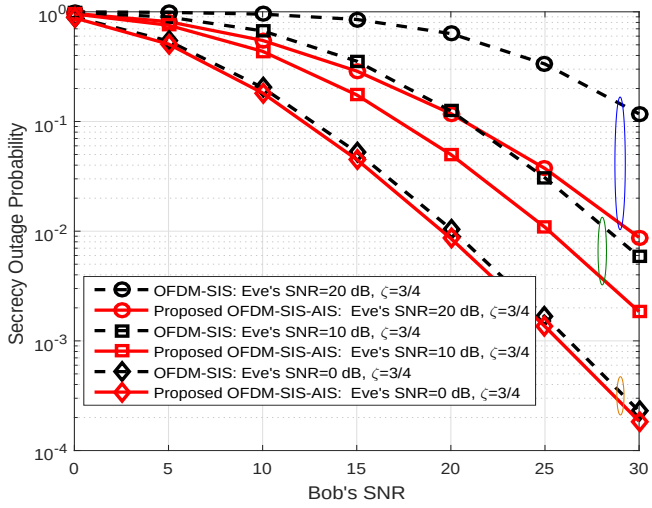

Fig. 6. Secrecy outage probability of the proposed OFDM-SIS-AIS for $\bar{\gamma}_e = 0, 10, 20$ dB, $\zeta = 3/4$ and $R_s = 1$ compared to conventional OFDM-SIS.

Based on the obtained results, we have demonstrated that the performance of the proposed OFDM-SIS-AIS outperforms that of OFDM-SIS in terms of secrecy, while maintaining the same reliability performance as that of OFDM-SIS.

This enhancement is achieved without sharing secret keys, nor knowing Eve's channel, nor even causing any major changes in the receiver design. Given the simplicity of the proposed design, its hardware testbed implementation is very handy to structure, making it very attractive for flexible 5G and beyond systems and low-complexity Internet of Things (IoT) devices.

VII. CONCLUSION

An enhanced physical layer security technique has been proposed for safeguarding OFDM-based transmission against eavesdropping. In this technique, named as OFDM-SIS-AIS,

the secrecy performance of the recently proposed OFDM-SIS technique is boosted by injecting artificiality interfering signals (AIS) in the sub-carriers that are not used for data transmission, resulting in a significant improvement in the secrecy gap when TDD system is used. The presented results have proven the capability of the proposed schemes 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-IoT and Tactile Internet applications. Future work can consider designing and investigating the secrecy performance of different variations of the proposed OFDM-SIS-AIS scheme assuming different subblock sizes and activation ratios.

CONFLICTS OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this article.

REFERENCES

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

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

[3] E. Guvenkaya, J. M. Hamamreh, and H. Arslan, "On physical-layer concepts and metrics in secure signal transmission," *Physical Communication*, vol. 25, pp. 14 – 25, Aug. 2017.

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

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

[6] J. M. Hamamreh and H. Arslan, "Secure orthogonal transform division multiplexing (OTDM) waveform for 5G and beyond," *IEEE Commun. Lett.*, vol. PP, no. 99, pp. 1–1, Jan. 2017.

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

[8] 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.

[9] 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.

[10] 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. 2016 IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2016, pp. 1–7.

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

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

[13] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM-based systems using channel shortening," in *Proc. 2017 IEEE Intern. Symp. Pers., Indoor, Mob. Radio Commun. (PIMRC)*, Oct. 2017, pp. 8–13.

[14] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[15] M. Yusuf and H. Arslan, "Controlled inter-carrier interference for Physical Layer Security in OFDM Systems," in *Proc. IEEE Veh. Tech. Conf. (VTC-Fall)*, Sep. 2016, pp. 1–5.

[16] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic Feature Concealing CP Selection for Physical Layer Security," in *2014 IEEE Military Communications Conference*, Oct 2014, pp. 485–489.

[17] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, to appear, 2017.

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

[19] E. Basar, M. Wen, R. Mesleh, M. D. Renzo, Y. Xiao, and H. Haas, "Index modulation techniques for next-generation wireless networks," *IEEE Access*, vol. 5, no. 1, pp. 16 693–16 746, Sep. 2017.

[20] M. Huemer, C. Hofbauer, and J. B. Huber, "The potential of unique words in OFDM," in *Proc. 15th Int. OFDM-Workshop 2010 (InOWo' 10)*, Sep. 2010, pp. 140–144.

[21] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products P.891 (8.258)*, 7th ed. Academic, 2007.