Secure Orthogonal Transform Division Multiplexing (OTDM) Waveform for 5G and Beyond

Jehad M. Hamamreh and Huseyin Arslan, *Fellow, IEEE*

***Abstract*— In this letter, a secure waveform design for future 5G wireless system is proposed. The developed waveform referred to as secure orthogonal transform division multiplexing (OTDM) waveform, is designed to diagonalize the multi-path channel matrix of only the legitimate receiver (Bob), while degrading eavesdropper's reception. In particular, instead of using fixed exponential basis functions, generated by IFFT and FFT as in OFDM, orthogonal transform basis functions, which are extracted from the Bob's channel, are utilized to modulate and demodulate the data symbols securely. The simulation results prove that the proposed design provides a significant practical security gap between the Bob's and Eve's performance. The design is shown to be robust against channel imperfection, and it neither sacrifices communication resources nor considers any knowledge on the eavesdropper's channel. Besides security, the scheme results in a higher SNR, leading to a 3-5-dB gain over OFDM at BER $= 10^{-3}$.**

***Index Terms*— Channel-based transforms, orthogonal transform division multiplexing (OTDM), physical layer security, secure 5G waveforms.**

I. Introduction

DUE to the inherent vulnerability of wireless systems to eavesdropping, designing practical physical layer security techniques is of extreme importance in order to provide confidential communication, especially for 5G and beyond systems [1]. The current encryption-based techniques are not sufficient considering the increasing computational power of future devices. Furthermore, the implementation, management, and distribution of keys are not easy tasks especially in de-centralized networks [2]. To address these problems, channel-based security approaches have emerged as a promising solution. Practical security based on signal processing methods can be provided by exploiting the spatial degree of freedom that exists in systems like MIMO, CoMP, relay, etc. However, there has recently been an interest in designing schemes that can provide security even when there is no spatial degree of freedom. Among the ways to meet this is developing techniques tailored to common waveforms like OFDM or designing (from scratch) new inherently secure waveforms [3].

The physical layer security of OFDM was studied from an information-theoretic point of view in [4]. Based on the theoretical study, various OFDM security techniques have been proposed. These techniques can be classified from a high-level perspective into four main enabling approaches. First, adaptive transmission-based approaches, in which the transmission is adjusted to just meet the QoS requirements of the legitimate receiver. Among these approaches are optimal power allocation and pre-equalization [5], adaptive modulation and coding with adaptive automatic repeat request (ARQ) [6], and fading-based sub-carriers activation techniques [7]. Second, artificial noise (AN)-based schemes [8], in which the AN is designed based on the channel of the legitimate receiver and accumulated in the cyclic prefix at the receiver, resulting in an interference free reception of the OFDM symbol. Third, secret key-based schemes, where secret random sequences are extracted from the channel and then used to either encrypt the data bits on the application layer [9] or encrypt the data symbols on the physical layer such as constellation rotation and dynamic coordinate interleaving schemes [10]. Fourth, signal feature suppression techniques such as cyclic prefix (CP) periodicity concealment [11].

As noticed, most of the aforementioned security techniques are tailored to OFDM-based systems. However, with the emersion of 5G and the possibility to use new waveforms (UFMC, GFDM, OTFS, etc.) that meet some specific requirements, it is also of significant importance to devise new waveforms that are inherently secure.

In this work, we propose a novel scheme that replaces the Inverse Fast Fourier Transform (IFFT) and Fast Fourier Transform (FFT) blocks, which are responsible for mapping symbols to sub-carriers in OFDM-based waveforms, by new blocks that can perform the modulation function in an inherently secure manner. Particularly, instead of using the fixed complex exponential transform bases (produced by IFFT and FFT) as information-bearing carriers, new orthogonal bases are extracted from the channel of the legitimate user and then used to carry and extract data at the transmitter and receiver sides, respectively. The presented design not only provides security, but also enhances power efficiency, robustness against channel impairments, and reliability. Particularly, better BER performance is obtained for the legitimate user as a result of increasing the accumulated SNR. These merits could make the proposed waveform a strong candidate for future secure 5G and beyond systems.

The rest of the letter is organized as follows. The system preliminaries are described in Section II. The details of the developed secure orthogonal transform division multiplexing (OTDM) waveform are revealed in Section III. Section IV gives some insights on OTDM. Simulation results are discussed in Section V, followed by a conclusion in Section VI.

Notations: Vectors are denoted by bold-small letters, whereas matrices are denoted by bold-large letters. $\mathbf{I}$ is the

Manuscript received December 30, 2016; accepted January 9, 2017. Date of publication January 9, 2017; date of current version May 6, 2017. This material is based upon work supported by The Scientific and Technological Research Council of Turkey (TUBITAK) under grant No. 114E244. The associate editor coordinating the review of this letter and approving it for publication was T. Q. Duong.

J. M. Hamamreh is with the School of Engineering and Natural Sciences, Istanbul Medipol University, 34810 Istanbul, Turkey (e-mail: jmhamamreh@st.medipol.edu.tr).

H. Arslan is with the School of Engineering and Natural Sciences, Istanbul Medipol University, 34810 Istanbul, Turkey, and also with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: arslan@usf.edu).

Digital Object Identifier 10.1109/LCOMM.2017.2651801

$N \times N$ identity matrix. The convolution operator is indicated by $(*)$. The transpose, hermitian (conjugate transpose) and inverse are symbolized by $(\cdot)^T$, $(\cdot)^H$ and $(\cdot)^{-1}$, respectively.

II. Preliminaries and Assumptions

A single-input single-output (SISO) system is considered. In particular, a transmitter (Tx), called Alice, needs to confidentially communicate with a legitimate receiver (Rx), called Bob, under the presence of an eavesdropper, called Eve. All received signals exhibit multi-path slowly varying Rayleigh fading channels. Also, the channel reciprocity property is adopted in our design, where the downlink channel (Alice to Bob) can be estimated from the uplink one (Bob to Alice), in a time division duplex (TDD) or hybrid systems (TDD with FDD). Moreover, since Eve is a passive node, the realistic assumption, where Alice has no knowledge of Eve's channel $\mathbf{H_e}$, is adopted. As a final notice, since the wireless channel is unique to the positions of the Tx and Rx, both Bob and Eve are assumed to experience independent channels.

III. Proposed Secure OTDM Waveform

The proposed secure waveform design is illustrated in Fig. 1. At the Tx, the total number of data symbols to be sent is N, where each transmission block is represented as $\mathbf{s} = \begin{bmatrix} s_0 & s_1 & \dots & s_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$. Each one of the complex baseband modulated symbols, s_i, is mapped to or carried by a channel-based orthogonal transform basis $\mathbf{v} \in \mathbb{C}^{[N\times 1]}$, where the mapping process is basically implemented via a simple multiplication operation between each data symbol and the orthogonal basis vector. For the N data symbols to be transmitted, we need N carrying orthogonal bases, which can be taken from the column vectors of $\mathbf{V}$, given by $\mathbf{V} = \begin{bmatrix} \mathbf{v}_0 & \mathbf{v}_1 & \dots & \mathbf{v}_{N-1} \end{bmatrix} \in \mathbb{C}^{[N\times N]}$, where $\mathbf{V}$ is a transformation matrix, extracted from the legitimate user's channel. Also, each ith column vector (transform basis) in $\mathbf{V}$ can be expressed as $\mathbf{v_i} = \begin{bmatrix} v_0 & v_1 & \dots & v_{N-1} \end{bmatrix}^T \in \mathbb{C}^{[N\times 1]}$.

Now, the key idea behind the proposed design is stemmed from the fact that the convolution process between a channel impulse response of L taps, $\mathbf{h} = [h_0, \cdots, h_{(L-1)}]$, and a transmitted data block $\mathbf{x}$ of length N can be represented by the linear multiplication of the Toeplitz matrix $\mathbf{H_b} \in \mathbb{C}^{[(N+L-1)\times N]}$ with $\mathbf{x}$. Since $\mathbf{H_b}$ represents a matrix, whose size is equal to the length of the transmitted data block added to the channel taps (i.e., $(N+L-1)$) times the length of only the transmitted data block (i.e., N), Alice and Bob can extract channel-based sub-carriers (basis functions) by decomposing (performing orthogonal factorization on) $\mathbf{H_b}$.

This is made possible by applying any of the linear decomposition methods (SVD, GMD, UCD, etc.). For familiarity, SVD, a tool commonly used in MIMO systems [12]), is chosen as the underlying method. Thus, $\mathbf{H_b}$ can equivalently be expressed in-terms of three new matrices as follows:

$$\mathbf{H_b} = \underbrace{\mathbf{U}}_{\in \mathbb{C}^{[(N+L-1)\times N]}} \underbrace{\mathbf{E}}_{\in \mathbb{C}^{[N\times N]}} \underbrace{\mathbf{V}^H}_{\in \mathbb{C}^{[N\times N]}}, \tag{1}$$

where $\mathbf{U}$ and $\mathbf{V}^H$ are orthonormal matrices and $\mathbf{E}$ is a diagonal matrix with real entires. It should be noted that the number of orthogonal bases at the Tx depends on the columns' number of $\mathbf{V}$, which is equal to the transmitted data block length (N). When the transmitted block gets convolved with the channel, then the number of orthogonal bases at the Rx depends on the columns' number of $\mathbf{U}^H$, which is equal to the number of data symbols plus the channel taps ($N + L - 1$). From (1), Alice can take the hermitian of $\mathbf{V}^H$ to get $\mathbf{V}$. Since the column vectors of $\mathbf{V}$ are orthogonal to each other, Alice can use them as basis functions (sub-carriers) to transmit symbols without interference. Alice maps each symbol to its corresponding basis function via simple multiplication, and then multiplex all the resulting multiplications as they are orthogonal to each other. This results in a block of samples, $\mathbf{x}$, referred to as one OTDM symbol. This process can mathematically be given as

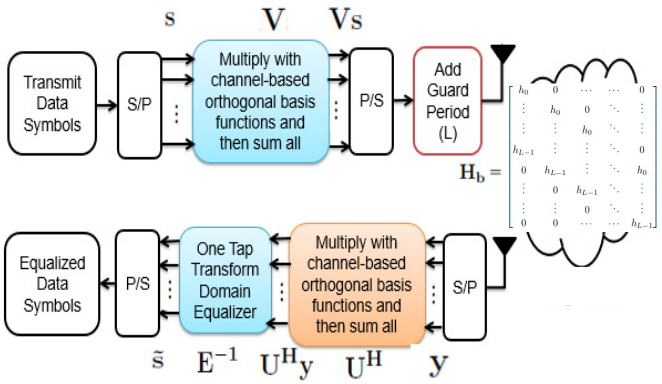

Fig. 1. Structure of the designed baseband secure OTDM waveform.

$$\mathbf{x} = \sum_{i=0}^{N-1} s_i \mathbf{v}_i \in \mathbb{C}^{[N\times 1]}, \tag{2}$$

which can further be simplified into a matrix form as

$$\mathbf{x} = \mathbf{V}\mathbf{s} \in \mathbb{C}^{[N\times 1]}. \tag{3}$$

From a signal processing point of view, this is somehow similar to transmit pre-coding process in spatial multiplexing MIMO systems [12], but here it is in the temporal domain of a SISO system. Furthermore, what looks like precoding is interestingly similar to the IFFT transform matrix in OFDM, and since $\mathbf{V}$ satisfies the transform properties, $\mathbf{V}$ can be seen as a transform matrix too, but extracted from the channel rather than being fixed as in OFDM.

Now, to avoid the interference between consecutive blocks, known as inter block interference (IBI), zero-padding (ZP), as a guard period interval with length equal to the channel delay spread L, is appended to the end of each block. This results in saving power resources compared to CP-OFDM, since no energy is sent in the ZP period. The baseband received OTDM symbol at Bob after S/P conversion can be given as

$$\mathbf{y} = \mathbf{h_b} * \mathbf{x} + \mathbf{z_b} \in \mathbb{C}^{[(N+L-1)\times 1]}, \tag{4}$$

where $\mathbf{y} = \begin{bmatrix} y_0 & y_1 & \dots & y_{N+L-1} \end{bmatrix}^T$, in which $y_i = \sum_{l=0}^{L-1} h_l x_{(i-l)} + z_{b(i)}$, and $\mathbf{z_b} \in \mathbb{C}^{[(N+L-1)\times 1]}$ is the zero-mean complex additive white Gaussian noise (AWGN) at Bob. The convolution form can be written in a matrix form as

$$\mathbf{y} = \mathbf{H_b}\mathbf{x} + \mathbf{z_b} = \mathbf{H_b}\mathbf{V}\mathbf{s} + \mathbf{z_b}. \tag{5}$$

At the receiver side, Bob applies SVD on the Toeplitz matrix of its available channel response, and then takes the hermitian of $\mathbf{U}$ to get $\mathbf{U}^H$. Since the column vectors of $\mathbf{U}^H = \left[\mathbf{u}_0^* \ \mathbf{u}_1^* \ \dots \ \mathbf{u}_{L+N-1}^*\right]$ are orthogonal to each others, Bob can use them as inverse basis functions to optimally extract the data symbols from the received OTDM block without causing any interference. This can be implemented as follows:

$$\hat{\hat{\mathbf{s}}} = \sum_{i=0}^{N+L-1} y_i \mathbf{u}_i^* \in \mathbb{C}^{[N\times 1]}. \tag{6}$$

After that, Bob uses $\mathbf{E} = diag\left[e_0 \ e_1 \ \dots \ e_{N-1}\right]$ to perform simple one tap zero-forcing equalization process for $\hat{\hat{\mathbf{s}}}$ to get the final equalized data symbols block $\hat{\mathbf{s}}$. The reception processes (channel-based transformation and equalization) can further be simplified into a matrix form as

$$\hat{\mathbf{s}} = \mathbf{E^{-1}}\hat{\hat{\mathbf{s}}} = \mathbf{E^{-1}U^H y} = \mathbf{E^{-1}U^H}\left(\mathbf{H_b V s} + \mathbf{z}\right) \tag{7}$$

$$= \mathbf{E^{-1}U^H}(\mathbf{UEV^H V s} + \mathbf{z}) = \mathbf{s} + \mathbf{E}^{-1}\mathbf{U}^H\mathbf{z}. \tag{8}$$

The previous process clearly shows that the transformation performed on $\mathbf{y}$ using matrix $\mathbf{U^H}$, which consists of multiple orthogonal basis functions extracted from the channel, diagonalizes the channel response. This process is then followed by equalization, in the transform domain, using the diagonal matrix $\mathbf{E}$. Also, it is evident how the transformation matrix $\mathbf{V}$ used at the Tx cancels the effect of the right part $\mathbf{V}^H$ of the decomposed channel since their multiplication results in an identity matrix ($\mathbf{I}$). Similarly, $\mathbf{U^H}$ used at the Rx cancels the effect of the left part $\mathbf{U}$ of the decomposed channel. It should be noticed that the basis functions at Bob are longer than those at Alice due to channel spreading, allowing the receiver to optimally collect the spread energy in the guard period. However after the transformation process, the length of the received block becomes as that of the transmitter. This is different from OFDM, where the exponential basis functions of IFFT and FFT have the same length, resulting in a small energy loss since the spread part of the signal in the CP is usually discarded before FFT process. The exact gain due to this process will be shown in the simulation results section.

On the eavesdropper side, the captured signal is given by

$$\mathbf{y_e} = \mathbf{H_e x} + \mathbf{z_e} = \mathbf{H_e V s} + \mathbf{z_e}, \tag{9}$$

where $\mathbf{H_e} \in \mathbb{C}^{[(N+L-1)\times N]}$ and $\mathbf{z_e} \in \mathbb{C}^{[(N+L-1)\times 1]}$ are the complex Toeplitz channel response matrix and AWGN of Eve, respectively. Although Eve is assumed to have a complex receiver with full knowledge of the transmission technique, she will not be able to decode the data correctly. This is due to the fact that her channel is different from Bob's one, thus when she extracts orthogonal basis functions using SVD, she will have different basis functions from Bob, making her unable to decode. Also, even if Eve is considered to know the same basis functions as Bob, still she will not be able to decode because these functions are not optimized to her channel as the transformation at Alice is extracted from Bob's channel, but not Eve. In this miserable situation to Eve, she will be forced to perform an extremely exhaustive search process, trying to find some transformation matrices that might reduce errors. However, this would be impractical as the matrix size is relatively huge and the possible values are large. Also, since the time variation nature of wireless channels provides frequently updated randomness, the secure waveform design would be updated frequently, which further increases the security robustness. Thus, from a signal processing perspective, it is almost impossible for Eve to decode the data correctly.

IV. OTDM vs OFDM and Some Insights

Compared to OFDM-based systems, there are several important points, which should be emphasized. 1) IFFT processing at the Tx in OFDM is replaced by the pre-transformation matrix $\mathbf{V}$, in OTDM. 2) FFT processing at the Rx in OFDM is replaced by the post-transformation matrix $\mathbf{U^H}$. 3) The Frequency domain equalization in OFDM is substituted in OTDM by a transform domain equalization process, with the same complexity as that of OFDM. 4) The cyclic-prefix in CP-OFDM is replaced by a ZP guard period with the same length as the delay spread of the channel. This means that cyclic convolution in OFDM is not required in OTDM as there is no need to go to the frequency domain to make equalization. 5) The fixed rectangular pulses, with shifted frequencies, in OFDM are replaced by channel-based orthogonal bases, whose length at the Rx is greater than those at the Tx by channel spread length. This allows the Rx to collect the energy in the ZP period, instead of removing it as in OFDM. 6) OTDM has the power efficiency advantage of zero padding (ZP)-OFDM system, since a zero-suffix guard period of length equal to the channel spread is used instead of the CP. 7) Unlike OFDM, in which synchronization can be achieved by either exploiting the CP or by sending a training sequence, in OTDM, only training-based algorithms can be used because there is no CP in OTDM. 8) The channel estimation in OTDM is foreseen to be similar to OFDM as both of them are block-based transmission techniques. Thus, the delay spread and number of taps of the channel can be determined by performing time-based or frequency-based channel sounding techniques. 9) OTDM is specifically designed to work best over frequency selective channels, which is the case in most broadband systems. Therefore, the proposed design needs some modifications to make it applicable for flat fading channels (this can be a subject of future research). 10) Since OTDM updates its bases based on the channel, this requires extra processing than OFDM.

V. Simulation Results

Simulations are performed to investigate the performance of OTDM by choosing BER as a security metric [2], [3]. We consider an OTDM system with $N = 64$ modulated QPSK data symbols and a ZP of length $L = 9$, which is equal to the number of taps in the channel. For the sake of fair comparison, we also consider a standard OFDM system with $N = 64$ active sub-carriers and a CP of length L. In order to focus on the security design concept, we consider for both schemes (OTDM and OFDM) uncoded non-adaptive loaded systems with simple zero-forcing equalization. Thus, the effect of coding, complex equalization and adaptive loading with optimal power allocation is left as a future research. Fig. 2 shows the BER of a legitimate Rx, employing the proposed OTDM

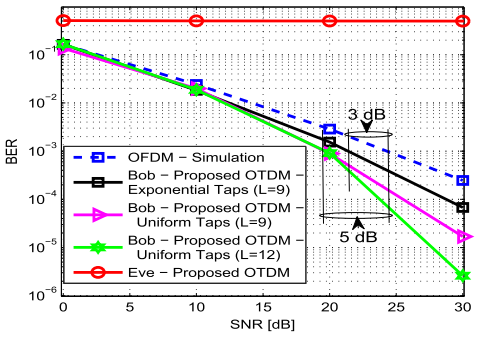

Fig. 2. BER comparison between OFDM and OTDM with QPSK.

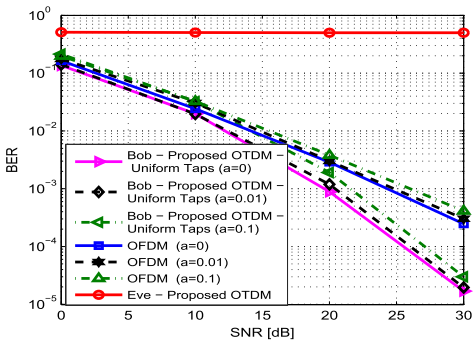

Fig. 3. The effect of imperfect channel estimation on OTDM.

(channel-based transforms), compared to OFDM (Fourier-based transforms). It is shown that at BER=10^{-3}, OTDM outperforms OFDM by at least 3 dB and 5 dB for the cases of exponentially decaying and uniformly distributed power delay profiles with $L = 9$, respectively. Uniform profile gives better BER than exponential due to the fact that the former has equally significant spreading gain over all taps, while the later has an insignificant gain at most of its high ordered taps (i.e., the last $(L-1)$th taps) due to the decaying nature of the channel. Thus, the accumulated energy from the ZP period in the case of uniform profile is higher than that of the exponential profile, resulting in a lower BER. Moreover, Fig. 2 shows that the performance depends on the number of taps. In specific, Bob's BER gets enhanced as the number of taps increases from $L = 9$ to $L = 12$ due to having more signal energy spread in the ZP when the channel length is longer. From another perspective, the way the interference leakage in the guard period is gathered in the presence of noise using $\mathbf{U}^H$ is optimal as less noise is accumulated with the signal energy. This results in a higher SNR, leading to a better BER. This is dissimilar to OFDM, in which the guard period, containing the dispersed signal energy, is discarded before the FTT process.

Additionally, Fig. 2 depicts the degraded BER performance of Eve even though she is assumed to be fully aware of the method and uses the same transform matrix as Bob. This happens due to the use of channel-dependent waveforms over Alice-to-Bob channel, which are different from Alice-to-Eve channel. As a result, the system response will not be diagonalized and a severe inter-symbol interference between data symbols will occur with respect to Eve.

To assess the robustness of our scheme against imperfect channel estimation (ICE), we add intentional errors at both the Tx and Rx ($\Delta\mathbf{h}_{T/R}$) to the true channel ($\mathbf{h}$) in order to obtain new erroneous channels given by $\hat{\mathbf{h}}_{T/R} = \mathbf{h} + \Delta\mathbf{h}_{T/R}$. $\Delta\mathbf{h}$ is modeled as an independent complex Gaussian noise with zero mean and variance $\sigma^2{}_{T/R} = a \times 10^{\frac{-SNR_{dB}}{10}}$. Fig. 3 presents the performance under different estimation qualities with $a = 0$ (perfect estimation), $a = 0.01$ and $a = 0.1$. It is shown that ICE leads to a small degradation due to the error mismatch between the generated transforms $\hat{\mathbf{V}}$ and $\hat{\mathbf{U}}^H$ at the Tx and Rx sides, respectively, and their actual values coming from the true channel. This results in a small ISI between the data symbols as $\hat{\mathbf{V}}$ and $\hat{\mathbf{U}}^H$ extracted from the estimated channel will not perfectly cancel the effect of $\mathbf{V}$ and $\mathbf{U}^H$ coming from the true channel. However, this degradation can be overcome by increasing the length or power of the training sequence or by using channel quantization techniques [12].

VI. Conclusion

This work has proposed a 5G waveform design for providing physical security over dispersive channels. Particularly, orthogonal basis functions are extracted from the legitimate channel and then used as data bearing carriers instead of the exponential functions in OFDM. Thus, channel-based transformations are used instead of Fourier transforms to diagonalize the channel response of only the legitimate receiver. Besides security, the scheme is shown to enhance reliability, power efficiency and robustness against channel impairments.

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] 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.

[4] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug. 2012.

[5] 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.

[6] 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.

[7] E. Güvenkaya 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.

[8] 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.

[9] 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.

[10] 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.

[11] Z. E. Ankaral, M. Karabacak, and H. Arslan, "Cyclic feature concealing CP selection for physical layer security," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, Oct. 2014, pp. 485–489.

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