Flexible Physical Layer Security for Joint Data and Pilots in Future Wireless Networks

Salah Eddine Zegrar, Haji M. Furqan, and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*— In this work, novel physical layer security (PLS) schemes are proposed for orthogonal frequency-division multiplexing (OFDM) to secure both data and pilots in multiple-input multiple-output (MIMO) systems. The majority of previous studies focus on only securing the data without considering the security of the pilots used for channel estimation. However, the leakage of channel state information (CSI) from a legitimate node to an eavesdropper allows the latter to acquire knowledge about the channel of the legitimate nodes. To this end, we propose adaptive and flexible PLS algorithms which can 1) secure data, 2) secure pilots, and 3) jointly secure both data and pilots. Particularly, minimum-phase all-pass channel decomposition is exploited, where the proposed algorithms use the all-pass component to provide security without harming the performance of the legitimate user. In the analysis for data security, we evaluate the secrecy under correlated and uncorrelated eavesdropping channels via closed-form bit error rate (BER) formulas. For pilot security, we analyze the estimated channel's normalized mean squared error (NMSE) performance. The simulation results and theoretical analysis demonstrate that the proposed algorithms can effectively enhance the communication secrecy of the overall system.**

***Index Terms*— Data security, pilot security, PHY security, minimum-phase all-pass decomposition, MIMO-OFDM.**

I. Introduction

WHILE an enormous amount of novel and efficient wireless technologies have been proposed in order to fulfill the demands of fifth-generation (5G) and beyond in terms of reliability, throughput, and latency, the security has become a sensitive issue [1]. This is due to the fact that the open and broadcast nature of wireless transmission makes the physical transmitted signal, bearing the communication data and sensitive information, vulnerable to eavesdropping [2]. In order to overcome the security threats, upper-layer encryption-based algorithms are exploited conventionally. Such techniques, however, may not be feasible for future wireless networks because of the difficulties in terms of key management and sharing in these heterogeneous wireless networks. Physical layer security (PLS) has emerged as an interesting and powerful solution that can complement conventional security techniques and improve the overall security of wireless communication networks [3]. Particularly, PLS observes and exploits the dynamic characteristics of the signal, radio, and channel for ensuring the security of features and contents at the physical layer [4].

A. PLS Literature Review

Physical layer security (PLS) techniques have two primary goals, i.e., to secure the data communication and to protect the estimated channel information. The former aims to degrade the data decoding capability of the illegitimate nodes compared to the legitimate ones by exploiting the various properties of the wireless channel. For the latter, the channel estimation of the attacker/eavesdropper is targeted, which will eventually lead to degraded signal recovery for the attacker [5]–[7].

1) PLS for Data: Among the top areas in PLS, securing orthogonal frequency division multiplexing (OFDM) has drawn enormous attention recently since OFDM is the most commonly employed waveform in the current and next-generation systems [8]. In line with this vision, different security techniques have been proposed in the literature. These techniques include key generation-based approaches [9]–[11], adaptive communication-based approaches [12], and artificial noise (AN)-based techniques [13], [14].

Key generation-based techniques are based on the exploitation of channel reciprocity property between legitimate nodes as a common source of randomness. For example, amplitude and phase related to received signal strength (RSS), channel impulse response (CIR), channel frequency response (CFR), and other feedback can be used for key generation [9], [15]. These techniques are interesting in the sense that they can solve key management problems faced by encryption algorithms. However, they are very sensitive to channel estimation error, especially at low signal-to-noise ratio (SNR) [7]. In adaptive transmission-based techniques, the parameters are adjusted/adapted based on the location, channel conditions, and quality-of-service (QoS) requirements of the legitimate receiver only. For example, precoding [12] and channel shortening filter-based [16] techniques provide security at the cost of high peak to average power ratio (PAPR) [17].

Manuscript received September 9, 2021; revised December 27, 2021 and January 24, 2022; accepted February 5, 2022. Date of publication February 14, 2022; date of current version April 18, 2022. The work of Hüseyin Arslan was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 120C142 and the work of Haji M. Furqan was supported by the HISAR Lab at TUBITAK BILGEM, Gebze, Turkey. The associate editor coordinating the review of this article and approving it for publication was Y. Wu. *(Corresponding author: Salah Eddine Zegrar.)*

Salah Eddine Zegrar and Haji M. Furqan are with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey (e-mail: salah.zegrar@std.medipol.edu.tr; furqan_ahmed89@hotmail.com).

Hüseyin Arslan is with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, 34810 Istanbul, Turkey, and also with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: huseyinarslan@medipol.edu.tr).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCOMM.2022.3151341.

Digital Object Identifier 10.1109/TCOMM.2022.3151341

Similarly, subcarrier selection-based techniques [8] provide security at the cost of spectral efficiency degradation. AN-based techniques are also very effective for ensuring secure communication. In these techniques, an interference signal is added by the trusted node to degrade the performance of an illegitimate node without affecting the performance of the legitimate receiver. However, the interference signal may cause an increment in PAPR and slight performance degradation due to the sacrifice of the power resources for noise generation [13], [18].

2) PLS for Pilots: Due to the wireless channel decorrelation property, the attacker cannot decode the data even if it knows the algorithm and tries to apply it based on its channel. However, the work in [19] claimed that under certain assumptions the attacker can acquire the channel state information (CSI) between the legitimate nodes, which puts channel-based PLS techniques at high risk of failure. For instance, the attacker can reverse engineer the beamforming matrix to acquire the CSI between legitimate nodes. The beamforming matrix can be estimated under the assumption that the attacker possesses the CSI between the legitimate transmitter and itself, and that it is equipped with the same number of antennas as that of a legitimate transmitter. After estimating CSI corresponding to legitimate nodes, it can compromise channel-dependent PLS techniques like AN as well as key generation-based techniques [2]. The security can still be ensured in such cases by enforcing poor channel estimation quality at the attacker for the CSI between the legitimate transmitter and the attacker, which motivates the need for pilot security. Securing the pilots protects the propagation environment properties from being extracted at the attacker side. Additionally, pilot security plays a critical role in physical layer authentication techniques.

From the pilot security perspective, few techniques are proposed in the literature. In [20], the phases of pilots subcarriers are rotated based on the previously estimated CSI. However, the channel is assumed to be known at both communicating nodes before the start of the algorithm. Moreover, the phase is manipulated for a single value which makes it easy to attack such a technique. In [21], [22], the security of downlink pilots is provided based on CSI at the transmitter via uplink training. Particularly, AN is added in the null space of the channel to degrade the channel estimation capability at the attacker, though it may increase the PAPR of the signal. On top of that, power allocation between pilot and noise signal needs to be done intelligently in order to enhance security performance. Similarly, in [23], anti-eavesdropping pilots are designed such that the channel can be estimated at legitimate nodes only. However, the proposed algorithm requires full-duplex communication. In [24], the legitimate parties employ secret pilots for channel estimation. In the first step, the first node transmits the secret pilot to another node. Afterwards, the receiving node sends the received signal to the transmitting node using amplify and forward strategy. The second node follows the same procedure as that of the first node. This approach requires extra overhead to share feedback. Although authors in [25] exploit the uniqueness of channel responses between different nodes in order to degrade the channel estimation at the attacker node and showed the effect in terms of bit error rate (BER), they did not consider the sign ambiguity issue when taking the square root of the channel, which in the practical case leads to huge BER due to the erroneous channel estimation.

B. Our Contributions

In order to address the above-mentioned challenges, we propose novel schemes that can provide security for data, pilots, or joint data and pilots. The design of the proposed schemes is based on the all-pass and minimum-phase decomposition of the channel and exploiting the property of the decomposed components to provide security. The proposed schemes are the first work that enables flexible adaptive security based on security needs. Specifically, the security of data, pilot, or both can be adaptively selected based on the security requirements of the applications. Additionally, the proposed novel security scheme is robust against spatially correlated eavesdroppers located near legitimate nodes. The main contributions of the proposed work are as follows:

- We propose two novel minimum-phase all-pass channel decomposition-based PLS schemes for multiple-input multiple-output (MIMO)-OFDM system in rich scattering environments, where the first method secures the data and the latter secures the pilots. The proposed data security algorithm ensures strong security compared to conventional schemes without compromising on or degrading the communication performance of the legitimate user. On top of that, the proposed pilot security algorithm degrades the ability of the eavesdropper in estimating its channel; thus, protecting CSI, sensing, and radio environment mapping information.
- Our novel security methods, focusing on both data and pilot security, exploit the all-pass component of the channel which has unit power property. Therefore, we provide security without any power constraint, particularly PAPR. Whereas, the conventional PLS techniques such as AN, zero forcing, and channel shortening provide security at the cost of changing the power distribution of the transmitted signal. These changes create high power peaks in time (i.e., PAPR) and frequency (exceeding spectrum mask limits).
- The secrecy of the proposed data security algorithm is evaluated under correlated and uncorrelated eavesdropping channels via closed-form expressions for achievable BER. Whereas for pilot security, we analyzed the normalized mean squared error (NMSE) performance of the estimated channel. The simulations agree with the analytical formulas emphasizing the effectiveness of the proposed algorithms.

C. Organization and Notation

The rest of this paper is organized as follows. Section II depicts the system model and discusses OFDM preliminaries. Section III firstly explains the channel decomposition and then presents the proposed data and pilot security algorithms. The numerical analysis of the proposed schemes is given in

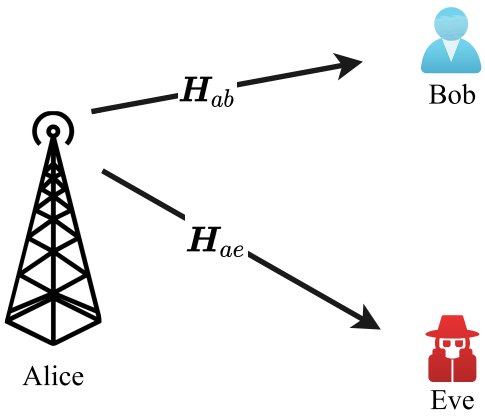


Fig. 1. System model where Alice and Bob are communicating over rich scattering channel with the existence of Eve.

Section IV followed by performance and simulation analysis in Section V. Finally, Section VI concludes the paper.

Bold uppercase $\mathbf{A}$, underlined letters ($\underline{\mathrm{a}}, \underline{\mathrm{A}}$), and unbold letters A, a are used to denote matrices, column vectors, and scalar values, respectively. $(\cdot)^H$, $(\cdot)^T$, and $(\cdot)^{-1}$ denote the Hermitian, transpose, and inverse. $|\cdot|$ denotes the Euclidean norm, E[·], var(·), Cov(·), diag(·), and Tr(·) denote the expectation, variance, covariance, diagonal, and trace operators, respectively. $\mathbb{C}^{M\times N}$ denotes the space of $M \times N$ complex-valued matrices. Symbol j represents the imaginary unit of complex numbers with $j^2 = -1$.

II. System Model and Preliminaries

As demonstrated in Fig. 1, a MIMO-OFDM system is considered that consists of a legitimate transmitter (Alice, {a}), legitimate receiver (Bob, {b}), and passive eavesdropper (Eve, {e}) that is trying to intercept the transmission between Alice and Bob, where each node is equipped with M_a, N_b, and N_e antennas, respectively. OFDM system is adopted for the communication, where during the i-th OFDM symbol N complex data symbols in frequency domain $\underline{\mathrm{X}}_i = \left[X_i(0)\ X_i(1)\ \ldots\ X_i(N-1)\right]^{\mathrm{T}}$ are converted to time-domain $\underline{\mathrm{x}}_i = \left[x_i(0)\ x_i(1)\ \ldots\ x_i(N-1)\right]^{\mathrm{T}}$ using inverse fast Fourier transform (IFFT) to form one OFDM symbol as

$$x_i(\nu) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_i(k) e^{j2\pi\nu k/N}. \tag{1}$$

To combat the inter-symbol interference (ISI), a cyclic prefix (CP) is appended to $\underline{\mathrm{x}}_i$ before transmission. Finally, the signal is transmitted through the wireless channel and reaches the Bob and Eve.

For the n-th receive antenna, the CIR $\underline{\mathrm{h}}_i^{(n,m)}$ associated with the m-th transmit antenna (where $m = 1, \ldots, M_a$, and $n = 1, \ldots, N_b$) can be denoted by [26]

$$\underline{\mathrm{h}}_i^{(n,m)}(t,\tau) = \sum_{l=0}^{L-1} h_{i,l}^{(n,m)}(t)\delta(\tau - \tau_l), \tag{2}$$

where $h_{i,l}^{(n,m)}(t)$ and τ_l are the complex channel gain and the delay of the l-th path at time t, respectively. $h_{i,l}^{(n,m)}(t)$ is assumed to have Gaussian distribution with zero-mean. L is the maximum number of effective channel taps and $\delta(\cdot)$ is the Kronecker delta function. The CFR is then expressed as

$$H_i^{(n,m)}(t,f) = \int_{-\infty}^{+\infty} h_i^{(n,m)}(t,\tau) e^{-j2\pi f\tau} d\tau. \tag{3}$$

Assuming that the channel is time-invariant during one OFDM symbol period T_s, and that the frequency spacing is Δf_c, the CIR and the CFR can be respectively represented as [27]

$$\begin{aligned} h_i^{(n,m)}(\nu) &= h_i^{(n,m)}(\nu T_s, \tau),\ H_i^{(n,m)}(k) \\ &= H_i^{(n,m)}(\nu T_s, k\Delta f_c). \end{aligned} \tag{4}$$

Given the system description above, we can represent the MIMO-OFDM channel in another form such as

$$\mathbf{G}(\nu) = \sum_{l=0}^{L-1} \mathbf{G}_l \delta(\nu - l) \tag{5}$$

where $\mathbf{G}$ is the MIMO CIR, and $\mathbf{G}_l$ is a complex matrix describing the MIMO channel coefficients at delay l. Then, the $N_b \times M_a$ MIMO channel seen at the k-th subcarrier is given by [28]

$$\mathbf{H}(k) = \frac{1}{\sqrt{N}} \sum_{l=0}^{L-1} \mathbf{G}_l e^{(-j\frac{2\pi kl}{N})}. \tag{6}$$

At the receiver, the CP is discarded first, and then the fast Fourier transform (FFT) process is applied. The received signal $Y_i(k)$ on the k-th subcarrier is found as

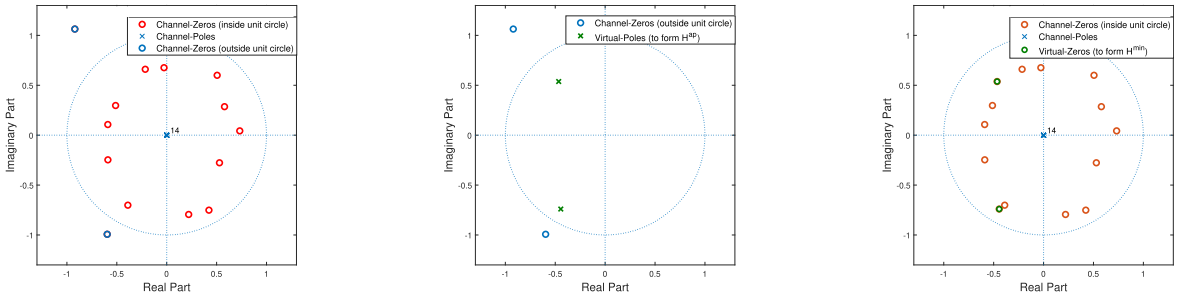
$$Y_i^{(n)}(k) = H_i(k) X_i^{(n)}(k) + W_i^{(n)}(k), \tag{7}$$

where $W_i^{(n)}(k)$ is the zero-mean additive white Gaussian noise (AWGN) vector with variance σ^2 at the k-th subcarrier. It is assumed that the sampling rate satisfies the Nyquist criteria.

As the time-frequency information in every OFDM symbol will be exploited by every transmit-receive antenna pairs adopting the identical processing, the transmit-receive antenna indices will be omitted from now on. Furthermore, the channels observed at Alice $\underline{\mathrm{h}}_{ba} \in \mathbb{C}^{L\times 1} \sim \mathcal{CN}(0, \sigma_b)$, Bob $\underline{\mathrm{h}}_{ab} \in \mathbb{C}^{L\times 1} \sim \mathcal{CN}(0, \sigma_a)$, and Eve $\underline{\mathrm{h}}_{ae} \in \mathbb{C}^{L\times 1} \sim \mathcal{CN}(0, \sigma_e)$ are considered as multi-path slowly varying channels following complex Gaussian distribution. Moreover, due to the channel reciprocity assumption, the channel between Alice-Bob $\underline{\mathrm{h}}_{ab}$ can be estimated from the channel between Bob-Alice $\underline{\mathrm{h}}_{ba}$, where $\underline{\mathrm{h}}_{ab} = \underline{\mathrm{h}}_{ba}^T$ [29]. In addition, due to rich scattering environment with enough distance separation between the nodes, the channel experienced by Bob and Eve is assumed to be independent unless stated otherwise. Furthermore, it is also assumed that Alice has no information about the channel of Eve because of its passive operation.

III. Proposed Algorithm

The increase in the number of wireless communication-based applications with varying requirements motivates the need for adaptive and flexible security designs [5]. Inspired by that, in this section, we firstly present the channel decomposition concept, and then we propose novel algorithms that



(a) Overall Channel. (b) All-pass channel. (c) Minimum-phase channel.

Fig. 2. The zero-pole diagram of the minimum-phase all-pass decomposition of a wireless channel.

are capable of providing adaptive and flexible security. Particularly, we start by providing a data security mechanism followed by a method for securing the pilots. Afterwards, the high security case is considered where both data and pilots need to be secured.

A. Minimum-Phase All-Pass Channel Decomposition

Wireless channel systems are causal because they are real-time systems, where the samples belong only to the present or past. Additionally, the CIR of a wireless channel can be represented by a finite impulse response (FIR) filter, and thus it is stable [30]. Consequently, a stable and causal system with system function $H_\Lambda(z)$ would have all poles at the origin inside its unit circle where $\Lambda = \{ab, ae\}$; however, the zeros are free to wander outside. Let $H^1_\Lambda(z)$ be the system function with all zeros and poles inside the unit circle, and let the zeros outside be at $1/p_k$. This implies that we can decompose such a system into two components as

$$H_\Lambda(z) = \underbrace{\left(H^1_\Lambda(z)\prod_{k=1}^{q}\left(1-p_k^* z^{-1}\right)\right)}_{H^{\min}_\Lambda(z)} \overbrace{\prod_{k=1}^{q}\left(\frac{z^{-1}-p_k}{1-p_k^* z^{-1}}\right)}^{H^{\mathrm{ap}}_\Lambda(z)}, \tag{8}$$

where $H^{\min}_\Lambda(z)$ and $H^{\mathrm{ap}}_\Lambda(z)$ are defined as the minimum-phase and all-pass components of $H_\Lambda(z)$, respectively. For instance, Fig. 2 illustrates the zero-pole diagram of the minimum-phase all-pass decomposition of a random channel. As seen in Fig. 2(a), the overall channel contains zeros inside and outside the unit circle where the poles are centered at the origin. As shown in Fig. 2(b), for the all-pass channel only the zeros outside the unit circle are considered along with virtual poles added at the inverse of the zeros' location to cancel out the attenuation effect, thus passing all frequencies as the name stands. To compensate the effect of these virtual poles, zeros are added on top of them having a system with all zeros inside the unit circle (i.e., minimum-phase system) as illustrated in Fig. 2(c).

The resulting components have various properties; for instance, in terms of the magnitude response $|H(e^{j\omega})|$, the factorization in (8) implies that $|H_{\min}(e^{j\omega})| = |H(e^{j\omega})|$ and $|H_{ap}(e^{j\omega})| = 1$. These properties of the decomposed channel will be exploited to provide security for both data and pilots.

B. Proposed Precoder/Combiner Design

The designed algorithm is based on a novel precoder that exploits the components of the channel separately, instead of using the full channel as in conventional security algorithms [31]. The proposed method uses only the all-pass component of the channel for precoding as explained in Subsection III-A; therefore, the PAPR will not be affected [6]. Additionally, it provides an effective solution to ensure secure communication against eavesdropping. Algorithm 1 summarizes the precoder/combiner design.

Algorithm 1 The Proposed Precoder Design

Input: $\mathbf{H}_{ba}$
Output: $\mathbf{Q}_D$ and $\mathbf{Q}_P$

1 **Bob** sends orthogonal pilot signals $\mathbf{P}$ to Alice to estimate the MIMO channel $\mathbf{H}_{ba} \in \mathbb{C}^{N_b \times M_a \times N}$ [32], where due to channel reciprocity we assume that uplink and downlink CSI are available at Alice.

2 **Alice** decomposes the CFR $\underline{\mathrm{H}}_{ba}$ into all-pass $\underline{\mathrm{H}}^{\mathrm{ap}}_{ab}$ and minimum-phase $\underline{\mathrm{H}}^{\min}_{ab}$ components for each (n, m) antenna pair, as explained in Subsection III-A.

3 **Alice** reconstructs the MIMO all-pass and minimum-phase channels $\mathbf{H}^{\mathrm{ap}}_{ab} \in \mathbb{C}^{N_b \times M_a \times N}$ and $\mathbf{H}^{\min}_{ab} \in \mathbb{C}^{N_b \times M_a \times N}$, respectively, where $\mathbf{H}_{ab} = \mathbf{H}^{\min}_{ab} \circ \mathbf{H}^{\mathrm{ap}}_{ab}$, and $\circ$ denotes the element-wise product.

4 **Alice** designs the precoder $\mathbf{Q}_D(k) \in \mathbb{C}^{M_a \times M_a}$ and $\mathbf{Q}_P(k) \in \mathbb{C}^{M_a \times M_a}$ for data and pilots security for each subcarrier k, respectively, as follows

$$\mathbf{Q}_D(k) = \mathrm{diag}\left(\frac{1}{M_a \times N_b}\sum_{l=m}^{M_a}\sum_{n=1}^{N_b} H^{\mathrm{ap}}_{ab}(k,n,m)\right)^H, \tag{9}$$

and

$$\mathbf{Q}_P(k) = \mathrm{diag}\left(H^{\mathrm{ap}}_{ab}(k,n',m')\right), \tag{10}$$

where $H^{\mathrm{ap}}_{ab}(k,n',m')$ is the (n',m')-th element of $H^{\mathrm{ap}}_{ab}(k)$ which can be set by default to $(n',m') = (1,1)$.

Algorithm 2 The Proposed Data Security Scheme

1 Alice precodes the data subcarriers $\underline{\mathrm{X}}(k_d)$ at indices k_d with $\mathbf{Q}_D(k)$, while the pilots $\underline{\mathrm{X}}(k_p)$ at k_p indices are intact. Then, the transmitted signal by Alice can be expressed as

$$\underline{\mathrm{X}}(k) = \begin{cases} \mathbf{Q}_D(k)\underline{\mathrm{D}}(k) & k \in k_d \\ \underline{\mathrm{P}}(k) & k \in k_p. \end{cases} \tag{11}$$

2 The received signal at Bob can be given as:

$$\underline{\mathrm{Y}}_{ab}(k) = \begin{cases} \mathbf{H}_{ab}(k)\mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ab}(k) & k \in k_d \\ \mathbf{H}_{ab}(k)\underline{\mathrm{P}}(k) + \underline{\mathrm{W}}_{ab}(k) & k \in k_p. \end{cases} \tag{12}$$

Using the pilots $\underline{\mathrm{P}}(k)$ at k_p, the CFR $\tilde{\mathbf{H}}_{ab}$ is estimated.

3 Applying channel decomposition to the estimated channel as in Subsection III-A, Bob obtains $\tilde{\mathbf{H}}_{ab}^{\min}(k)$ and $\tilde{\mathbf{H}}_{ab}^{\mathrm{ap}}(k)$ which will be exploited to design the combiner as in (9). The combined data of the received signal by Bob is given as

$$\begin{aligned} \underline{\mathrm{Y}}_{ab}(k) &= \tilde{\mathbf{Q}}_D^H(k)\mathbf{H}_{ab}(k)\mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \tilde{\mathbf{Q}}_D^H(k)\underline{\mathrm{W}}_{ab}(k) \\ &= \mathbf{H}_{ab}(k)\underline{\mathrm{D}}(k) + \mathbf{Q}_D^H(k)\underline{\mathrm{W}}_{ab}(k)\ k \in k_d, \end{aligned} \tag{13}$$

wherein case of perfect channel estimation $\tilde{\mathbf{Q}}_D(k) = \mathbf{Q}_D(k)$.

4 Using the results of step 3, Bob equalizes $\mathbf{H}_{ab}$ using zero-forcing [33] to decode the data as

$$\begin{aligned} \hat{\underline{\mathrm{X}}}_{Bob}(k) &= \mathbf{Q}_{ZF}(k)\underline{\mathrm{Y}}_{ab}(k) \\ &= \underline{\mathrm{D}}(k) + \tilde{\underline{\mathrm{W}}}_{ab}(k) \quad k \in k_d, \end{aligned} \tag{14}$$

where $\mathbf{Q}_{ZF}(k) = \left(\mathbf{H}_{ab}^H(k)\mathbf{H}_{ab}(k)\right)^{-1}\mathbf{H}_{ab}^H(k)$, $\tilde{\underline{\mathrm{W}}}_{ab}(k) = \mathbf{Q}_{ZF}(k)\mathbf{Q}_D^H(k)\underline{\mathrm{W}}_{ab}(k)$.

Note that $|\mathbf{H}_{ab}(k)\mathbf{Q}_D(k)| = |\mathbf{H}_{ab}(k)\mathbf{Q}_P(k)| = |\mathbf{H}_{ab}(k)|$, thus the proposed precoder indeed does not affect the PAPR.

C. Proposed Data Security Method

This subsection presents the details of the proposed algorithm for providing data security. The proposed algorithm exploits a component of channel for precoding that is capable of providing security without degrading the BER performance. The basic steps are described in Algorithm 2.

On the other hand, the received signal at Eve can be given by

$$\underline{\mathrm{Y}}_{ae}(k) = \begin{cases} \mathbf{H}_{ae}(k)\mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ae}(k) & k \in k_d \\ \mathbf{H}_{ae}(k)\underline{\mathrm{P}}(k) + \underline{\mathrm{W}}_{ae}(k) & k \in k_p. \end{cases} \tag{15}$$

Applying zero-forcing at Eve, the processed signal at Eve can be given as

$$\hat{\underline{\mathrm{X}}}_{Eve}(k) = \mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \tilde{\underline{\mathrm{W}}}_{ae}(k) \quad k \in k_d, \tag{16}$$

where $\tilde{\underline{\mathrm{W}}}_{ae}(k) = \mathbf{Q}_{ZF}(k)\underline{\mathrm{W}}_{ae}(k)$, $\mathbf{Q}_{ZF}(k) = \left(\mathbf{H}_{ae}^H(k)\mathbf{H}_{ae}(k)\right)^{-1}\mathbf{H}_{ae}^H(k)$.

Algorithm 3 The Proposed Pilot Security Scheme

1 Alice precodes the pilots subcarriers $\underline{\mathrm{X}}(k_p)$ at indices k_p with $\mathbf{Q}_P(k)$, while the data subcarriers $\underline{\mathrm{X}}(k_d)$ at k_d indices are intact. Then, the transmitted signal by Alice can be expressed as

$$\underline{\mathrm{X}}(k) = \begin{cases} \underline{\mathrm{D}}(k) & k \in k_d \\ \mathbf{Q}_P(k)\underline{\mathrm{P}}(k) & k \in k_p. \end{cases} \tag{17}$$

2 The received signal at Bob can be given as

$$\underline{\mathrm{Y}}_{ab}(k) = \begin{cases} \mathbf{H}_{ab}(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ab}(k) & k \in k_d \\ \mathbf{H}_{ab}(k)\mathbf{Q}_P(k)\underline{\mathrm{P}}(k) + \underline{\mathrm{W}}_{ab}(k) & k \in k_p. \end{cases} \tag{18}$$

Using the pilots, the precoded CFR corresponding to the (n', m')-th antenna pair $\underline{\tilde{\mathrm{H}}}_{ab}^{(n',m')} = \underline{\mathrm{H}}_{ab}^{(n',m')} \circ \underline{\mathrm{H}}_{ab}^{\mathrm{ap}}(n', m')$ is estimated.

3 In order to find $\underline{\mathrm{H}}_{ab}^{\mathrm{ap}}(n', m')$ from the estimated $\underline{\tilde{\mathrm{H}}}_{ab}^{(n',m')}$, channel decomposition is applied to the estimated precoded channel as explained in Subsection III-A as follows: $\underline{\tilde{\mathrm{H}}}_{ab}^{(n',m')} = \underline{\tilde{\mathrm{H}}}_{ab}^{\min}(n', m') \circ \left(\underline{\tilde{\mathrm{H}}}_{ab}^{\mathrm{ap}}(n', m')\right)^2$, where $\underline{\tilde{\mathrm{H}}}_{ab}^{\min}(n', m')$ is minimum-phase component while $\left(\underline{\tilde{\mathrm{H}}}_{ab}^{\mathrm{ap}}(n', m')\right)^2$ is all-pass component of $\underline{\tilde{\mathrm{H}}}_{ab}^{(n',m')}$.

4 The estimated combiner at Bob can be calculated as: $\tilde{\mathbf{Q}}_P(k) = \mathrm{diag}\left(\sqrt{\underline{\tilde{\mathrm{H}}}_{ab}^{\mathrm{ap}}(n', m')^2}\right)$. The combined pilots of the received signal by Bob is given as

$$\begin{aligned} \underline{\mathrm{Y}}_{ab}(k) &= \tilde{\mathbf{Q}}_P^H(k)\mathbf{H}_{ab}(k)\mathbf{Q}_P(k)\underline{\mathrm{P}}(k) + \tilde{\mathbf{Q}}_P^H(k)\underline{\mathrm{W}}_{ab}(k) \\ &= \mathbf{H}_{ab}(k)\underline{\mathrm{P}}(k) + \mathbf{Q}_P^H(k)\underline{\mathrm{W}}_{ab}(k) \quad k \in k_p. \end{aligned} \tag{19}$$

where in case of perfect channel estimation $\tilde{\mathbf{Q}}_P(k) = \mathbf{Q}_P(k)$. Therefore the channel can be securely estimated and equalized.

As seen from (16), Eve will not be able to decode the data even if it perfectly estimates its channel. This is due to the unknown randomness caused by the term $\mathbf{Q}_D(k)$ which is uncorrelated with its channel.[1]

D. Proposed Pilot Security Method

This subsection presents the details of the proposed algorithm for providing pilot security. Similar to data security, the proposed pilot security algorithm exploits the components of the channel separately. It ensures that only a legitimate receiver will be able to estimate the channel while Eve will not able to learn the channel or environment without affecting PAPR as in [21]. Additionally, the proposed algorithm is also suitable for the security of feedbacks, hardware impairments, and hardware-based authentication. Furthermore, the eavesdropper will not be able to extract information of precoder

[1]Note that due to channel decorrelation in rich scattering environment between $\mathbf{H}_{ab}$ and $\mathbf{H}_{ae}$, Eve will not be able to estimate and remove the effect of $\mathbf{Q}_D$.

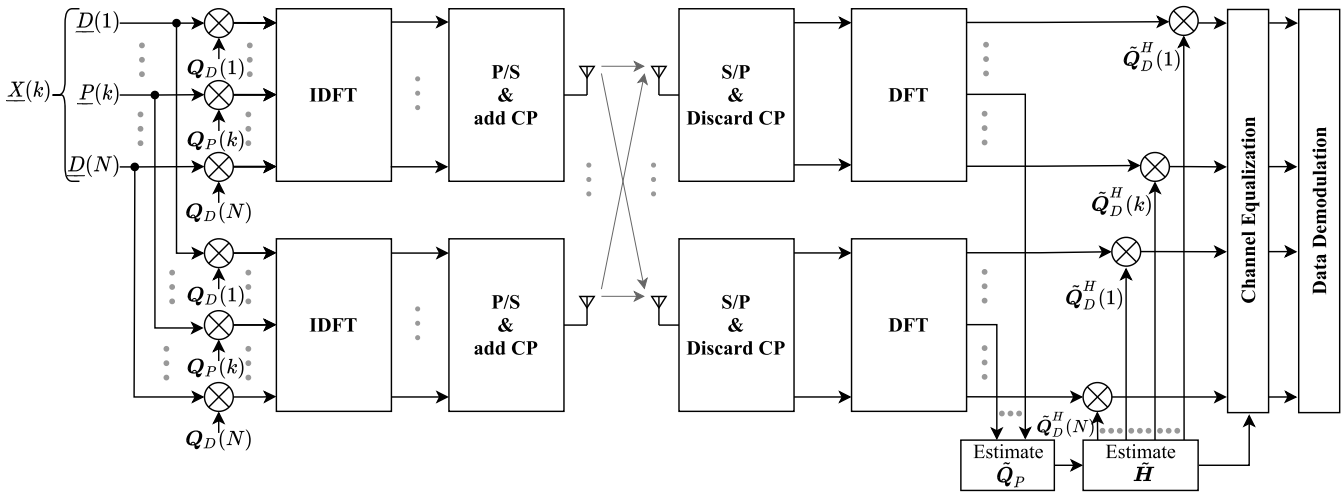


Fig. 3. The block diagram showing the main steps of the proposed joint data and pilot security algorithm.

corresponding to the channel of legitimate nodes from the received signal and thus will not be able to launch attacks to learn CSI corresponding to legitimate node [19]. The basic steps are described in Algorithm 3.

Whereas, at Eve's side, the received signal is given by

$$\underline{\mathrm{Y}}_{ae}(k) = \begin{cases} \mathbf{H}_{ae}(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ae}(k) & k \in k_d \\ \mathbf{H}_{ae}(k)\mathbf{Q}_P(k)\underline{\mathrm{P}}(k) + \underline{\mathrm{W}}_{ae}(k) & k \in k_p. \end{cases} \quad (20)$$

As seen from (20), eavesdropper will not be able to correctly estimate the channel because of the randomness caused by all-pass component $\mathbf{Q}_P(k)$ of the legitimate channel in (20). Hence, it can neither estimate the channel nor learn the environment.

E. Joint Pilot & Data Security

This subsection presents the details of the proposed algorithm for providing joint data and pilot security. Particularly, in case of a very high-security risk, there is a need of securing both pilot and data to provide a very high level of security. Thus, the attacker will not able to learn the channel, environment, and data. Here, the idea is to exploit the proposed algorithm presented in Subsections III-C and III-D to ensure both pilot and data security. The transmitted signal by Alice after applying both data and pilot security can be expressed as

$$\underline{\mathrm{X}}(k) = \begin{cases} \mathbf{Q}_D(k)\underline{\mathrm{D}}(k) & k \in k_d \\ \mathbf{Q}_P(k)\underline{\mathrm{P}}(k) & k \in k_p. \end{cases} \quad (21)$$

In this case, Bob will first estimate the channel using the pilots as described in Subsection III-D, and then he will use the estimated channel to extract the data as shown in Subsection III-C. Figure 3 illustrates the block diagram of the proposed joint data and pilot security algorithm in MIMO-OFDM systems. On the other hand, the received signal at Eve can be given as:

$$\underline{\mathrm{Y}}_{ae}(k) = \begin{cases} \mathbf{H}_{ae}(k)\mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ae}(k) & k \in k_d \\ \mathbf{H}_{ae}(k)\mathbf{Q}_P(k)\underline{\mathrm{P}}(k) + \underline{\mathrm{W}}_{ae}(k) & k \in k_p. \end{cases} \quad (22)$$

It should be noted from (22) that Eve will neither be able to estimate its channel nor the data due to the randomness caused by $\mathbf{Q}_P(k)\underline{\mathrm{P}}(k)$ and $\mathbf{Q}_D(k)\underline{\mathrm{D}}(k)$, respectively. Thus, providing two-level security that is suitable for critical applications.

IV. Numerical Analysis

In this section, we provide the theoretical analysis for both data and pilot security for the proposed methods. For the former, we analyze the BER performance for Bob and Eve under correlated and uncorrelated eavesdropping channels. For the latter, we derive the minimum mean squared error minimum mean squared error (MMSE) of the estimated channel.

A. Data Security: BER-Based Secrecy Gap

In this subsection, we analyze the bit error probability (BEP) under correlated and uncorrelated eavesdropping channels and use it to compare the BER performance gap between Bob and Eve.

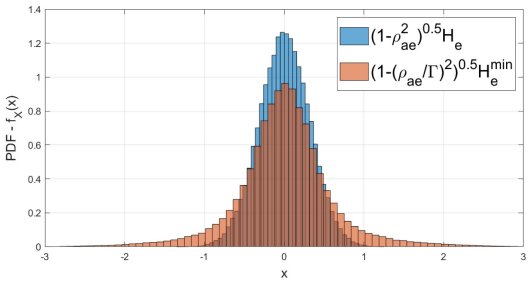
1) Uncorrelated Bob-Eve Channel: One elaborate method to suppress the effect of $\underline{\mathrm{W}}(k)$ when estimating the channel is the MMSE estimation [34]. After estimating the channel $\tilde{\mathbf{H}}_{ab}$, the received signal at the data subcarriers k_d is given in (12) and expressed by

$$\underline{\mathrm{Y}}_{ab}(k) = \mathbf{H}_{ab}(k)\mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ab}(k) \quad k \in k_d. \quad (23)$$

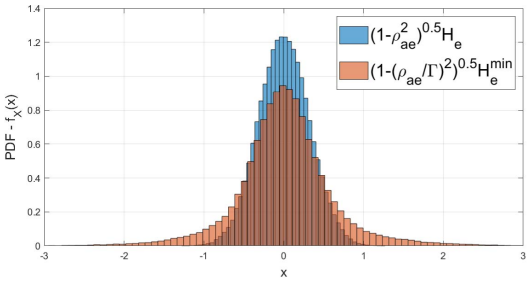
The receiver applies zero-forcing equalization. In case of perfect channel estimation, $\mathrm{E}[|\mathbf{H}_{ab} - \tilde{\mathbf{H}}_{ab}|^2] = 0$, and the correlation coefficients between the actual and the estimated channel responses are respectively found as $\rho_{ab}^1 = 1$ and $\rho_{ab}^2 = 0$. The BEP performance will become the lower bound performance of (43), and it is given as

$$P_{ab}(e) = \frac{1}{N_b}\sum_{n=1}^{N_b}\frac{1}{2}\left[1 - \frac{1}{\sqrt{1+\frac{1}{\gamma_{ab}^{(n)}}}}\right]. \quad (24)$$

where $\gamma_{ab}^{(n)}$ denotes the SNR of the received signal at the k-th subcarrier and n-th receive antenna. Please refer to Appendix A. ■



(a) Real part.



(b) Imaginary part.

Fig. 4. The distribution of uncorrelated part of Eve's channel for $\rho_{ae} = 0.9$.

2) Correlated Bob-Eve Channel: To further evaluate the performance of the proposed scheme and emphasize its reliability, we consider the effects of the Eve location with respect to the Bob. For that, we consider a correlated eavesdropping channel scenario, where it is assumed that Eve is located near Bob. For a fair comparison with [25], we assume single-input single-output (SISO) system where $\mathbf{Q}_D(k) = (\underline{\mathrm{H}}_{ab}^{\mathrm{ap}}(k))^H$. Note that the results can be extended to MIMO as we did in Subsection IV-B. We model the correlation between channel coefficients [35] as

$$\underline{\mathrm{H}}_{ae} = \rho_{ae}\underline{\mathrm{H}}_{ab} + \sqrt{1-\rho_{ae}^2}\underline{\mathrm{H}}_e, \tag{25}$$

where $\underline{\mathrm{H}}_e$ is i.i.d. $\sim \mathcal{CN}(0, \sigma_a)$ and ρ_{ae} is the correlation function of the legitimate channel gain with the eavesdropping channel given as

$$\rho_{ae} = \frac{\mathrm{Cov}[\underline{\mathrm{H}}_{ab}, \underline{\mathrm{H}}_{ae}^H]}{\sqrt{\mathrm{var}(\underline{\mathrm{H}}_{ab})\,\mathrm{var}(\underline{\mathrm{H}}_{ae}^H)}} = \frac{\mathrm{E}[\underline{\mathrm{H}}_{ab}\underline{\mathrm{H}}_{ae}^H]}{\sigma_a\sigma_e}. \tag{26}$$

Please refer to Appendix B. ■

In the proposed algorithm, the overall channel is not used, and instead, only one component (i.e., all-pass channel) is exploited. Therefore, even if Eve estimates the channel with high correlation, still it will suffer from the error raised due to the decomposition of its channel. This leads to lower eavesdropping channel correlation and enhanced security performance. Fig. 4 shows the distribution of the real and imaginary parts of the uncorrelated part of the channel $\underline{\mathrm{H}}_e$. It is clearly seen that the variance of the uncorrelated term, given blue color, increases after performing the channel decomposition as shown by the orange distribution in Fig. 4. Assuming the same channel model as in (25) we have

$$\underline{\mathrm{H}}_{ae} = \rho_{ae}\underline{\mathrm{H}}_{ab}^{\min}\underline{\mathrm{H}}_{ab}^{\mathrm{ap}} + \sqrt{1-\rho_{ae}^2}\underline{\mathrm{H}}_e. \tag{27}$$

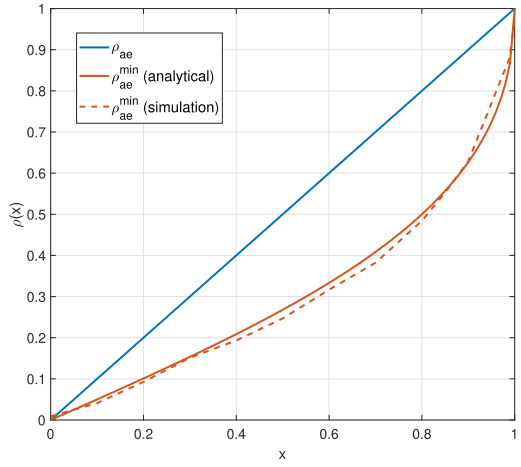


Fig. 5. The channel correlation relationship between the conventional and proposed schemes.

For the channel equalization, only the minimum-phase component of the channel is needed. So, after performing the channel decomposition and normalization, Eve finds

$$\begin{aligned}\underline{\mathrm{H}}_{ae}^{\min} &= \rho_{ae}^{\min}\underline{\mathrm{H}}_{ab}^{\min} + \sqrt{1-(\rho_{ae}^{\min})^2}\underline{\mathrm{H}}_e^{\min} \\ &= \frac{\rho_{ae}}{\Gamma}\underline{\mathrm{H}}_{ab}^{\min} + \sqrt{1-\left(\frac{\rho_{ae}}{\Gamma}\right)^2}\underline{\mathrm{H}}_e^{\min},\end{aligned} \tag{28}$$

where Γ is the correlation attenuation factor. Note that Γ satisfies the following constraints

$$\Gamma \sim \sqrt{1-\rho_{ae}^2} \tag{29a}$$
$$\Gamma \geq 1 \quad \forall \rho_{ae} \tag{29b}$$
$$\Gamma = 1, \quad \text{for } \rho_{ae} = 1 \tag{29c}$$
$$0 \leq \frac{\rho_{ae}}{\Gamma} \leq 1, \quad \forall \rho_{ae}, \tag{29d}$$

where the symbol $\sim$ denotes the proportionality. Taking all the constraints given in (29), we find that

$$\Gamma = 1 + \sqrt{1-\rho_{ae}^2}. \tag{30}$$

Please refer to Appendix C. ■

Fig. 5 shows the relationship between the correlation of the overall channel of Eve and Alice and the correlation of the minimum-phase component of their channels. As observed from Fig. 5, the correlation factor decreases after performing the channel decomposition causing degradation in the data decoding capability at Eve.

Therefore, the correlation function becomes $\rho_{ae}^{\min} = \rho_{ae}/(1+\sqrt{1-\rho_{ae}^2}) < \rho_{ae}$. This result shows another advantage of using the proposed scheme in case of correlated eavesdropping channels. Please refer to Appendix D. ■

To evaluate the results above, the BER performance is analyzed. we adopt the same BER expression given by (24) by including the spatial correlation factor ρ [25]. Then, the BER at both Bob and Eve can be found using (43) as

$$P_\Lambda(e) = \frac{1}{2N_b}\sum_{n=1}^{N_b}\left[1 - \frac{\rho_\Lambda}{\sqrt{1+\frac{1}{\gamma_{ab}^{(n)}}}}\right], \tag{31}$$

and $\Lambda = \{ab, ae\}$.

TABLE I
COMPLEXITY OF THE PROPOSED SECURITY ALGORITHM

	Complexity (MIMO)
Z-transform	$\mathcal{O}(M_a N_b L \log L \log(bL))$
$H^{\min}(z)$ estimation	$\mathcal{O}(M_a N_b N)$
$H^{\mathrm{ap}}(z)$ estimation	$\mathcal{O}(M_a N_b 2NL)$
Precoding/Combining	$\mathcal{O}(M_a N_b N)$
Total transmitter	$\mathcal{O}\left(M_a N_b \left(2N(L+1) + L \log L \log(bL)\right)\right)$
Total receiver	$\mathcal{O}\left(M_a N_b \left(2N(L+1) + L \log L \log(bL)\right)\right)$
Total complexity	$\mathcal{O}\left(2M_a N_b \left(2N(L+1) + L \log L \log(bL)\right)\right)$

TABLE II
SIMULATION PARAMETERS

Parameters	Specifications
FFT Size N	256
Pilot Rate	$1/4$
(M_a, N_b, N_e)	$(4, 4, 4)$
Guard Interval (CP)	64
Signal Constellation	QPSK
Channel Model	IEEE 802.11 channel model PDP [33]
Max channel taps L	11

B. Pilot Security: Channel NMSE

For the MIMO-OFDM channel estimation, frequency domain estimation is used by transmitting orthogonal pilots, which converts the channel estimation in MIMO systems to that in SISO systems. By using the pilot scheme as adopted in Subsection III-D, the MMSE channel estimation for the MIMO-OFDM system between the m'-th transmitter and n'-th receiver can be obtained as [34]

$$\tilde{\mathbf{H}}_{ab}^{\mathrm{MMSE}(n',m')} = \mathbf{F}\mathbf{R}_{h_{ab}Y_{ab}}\mathbf{R}_{Y_{ab}Y_{ab}}^{-1}\mathbf{Y}_{ab}^{(n')}, \tag{32}$$

where

$$\begin{aligned}\mathbf{R}_{h_{ab}Y_{ab}} &= \mathbf{R}_{h_{ab}h_{ab}}^{(n',m')}\mathbf{F}^H(\mathbf{P}^{(n')})^H \\ \mathbf{R}_{Y_{ab}Y_{ab}} &= \mathbf{P}^{(n')}\mathbf{F}\mathbf{R}_{h_{ab}h_{ab}}^{(n',m')}\mathbf{F}^H(\mathbf{P}^{(n')})^H + \sigma^2\mathbf{I}_N,\end{aligned} \tag{33}$$

where $\mathbf{R}_{h_{ab}h_{ab}}$ is the channel autocorrelation matrix, $\mathbf{F}$ is the discrete Fourier transform (DFT) matrix, and $\mathbf{I}_N$ is the identity matrix. Substituting (33) in (32) we find

$$\begin{aligned}&\tilde{\mathbf{H}}_{ab}^{\mathrm{MMSE}(n',m')} \\ &= \mathbf{F}\mathbf{R}_{h_{ab}h_{ab}}^{(n',m')}\mathbf{F}^H(\mathbf{P}^{(n')})^H \\ &\quad\times\left(\mathbf{P}^{(n')}\mathbf{F}\mathbf{R}_{h_{ab}h_{ab}}^{(n',m')}\mathbf{F}^H(\mathbf{P}^{(n')})^H + \sigma^2\mathbf{I}_N\right)^{-1}\mathbf{Y}_{ab}^{(n')}.\end{aligned} \tag{34}$$

Decomposing the estimated channel $\tilde{\mathbf{H}}_{ab}^{\mathrm{MMSE}(n',m')}$ would result in

$$\underline{\tilde{\mathrm{H}}}_{ab}^{\mathrm{MMSE}} = \underline{\tilde{\mathrm{H}}}_{ab}^{\min}\left(\underline{\tilde{\mathrm{H}}}_{ab}^{\mathrm{ap}}\right)^2. \tag{35}$$

C. Computational Complexity Analysis

The total system design of the proposed security method includes Z-transform, $H^{\min}(z)$ estimation, $H^{\mathrm{ap}}(z)$ estimation, and precoding at both transmitter and receiver. Accordingly, the computational complexity is calculated considering the number of multiplications. For instance, the Z-transform converts a discrete-time signal, which is a sequence of real or complex numbers, into a complex frequency-domain representation as follows

$$H(z) = \sum_{\nu=-\infty}^{\infty} h(\nu)z^{-\nu}, \tag{36}$$

where n is an integer and z is, in general, a complex number. The wireless channel is a causal finite system with maximum L taps, therefore

$$H(z) = \sum_{\nu=0}^{L-1} h(\nu)z^{-\nu}. \tag{37}$$

After obtaining the Z-transform of the wireless channel, the zeros of the resultant polynomial are computed to calculate the minimum-phase component of the channel. Furthermore, the arithmetic complexity of approximating to all the zeros of a polynomial $H(z)$ is $\mathcal{O}(L \log L \log(bL))$ [36], where b is the bit size. After, computing the zeros of $H(z)$, the zeros outside the unit circle with value $1/p_k$ are selected; then, the all-pass part is computed as follows

$$H^{\mathrm{ap}}(e^{j\omega}) = \prod_{k=1}^{q}\left(\frac{e^{-j\omega} - p_k}{1 - p_k^* e^{-j\omega}}\right), \tag{38}$$

where $1 \leq q \leq L$. The maximum complexity of computing (38) is $\mathcal{O}(2NL)$. The minimum-phase part is found straight forward by using element-wise division as $H^{\min}(e^{j\omega}) = H(e^{j\omega})/H^{\mathrm{ap}}(e^{j\omega})$, which has complexity of $\mathcal{O}(N)$. The precoder applies element-wise multiplication for each subcarrier, thus its complexity is of order $\mathcal{O}(N)$. Then, for single antenna pair (n, m) the total computational complexity is of order $\mathcal{O}\left(2N(L+1) + L \log L \log(bL)\right)$. Considering the total MIMO system the total complexity becomes $\mathcal{O}\left(2M_a N_b \left(2N(L+1) + L \log L \log(bL)\right)\right)$. Table I summarizes the computational complexity of each component.

V. SIMULATION RESULTS

In this section, we demonstrate the performance of channel decomposition-based PLS algorithms proposed for MIMO-OFDM systems. To do so, the BER-based secrecy gap and NMSE-based secrecy gap metrics are used to evaluate the security of data and pilots, respectively. The BER-based secrecy gap will quantify the amount of information leakage to the Eve, evaluate the secrecy, and also shows the effect of the proposed algorithm on the reliability with respect to legitimate nodes [8]. On the other hand, NMSE-based secrecy gap shows the difference between the quality of estimated channel at the legitimate node and illegitimate node. Moreover, the effect of the proposed algorithm on the PAPR is also presented along with the comparison to the conventional algorithms. The simulated MIMO-OFDM system parameters are described in Table II.

Figure 6 shows the BER performance versus SNR of the proposed data security algorithm when $M_a = N_b = N_e = 4$, along with the comparison to the conventional algorithms such as AN-based [13], channel shortening [16], and conventional CP-OFDM [33]. In [13], the transmitted signal is added to a properly designed AN in such a way that AN gets accumulated over the CP part of the signal at Bob only while degrading

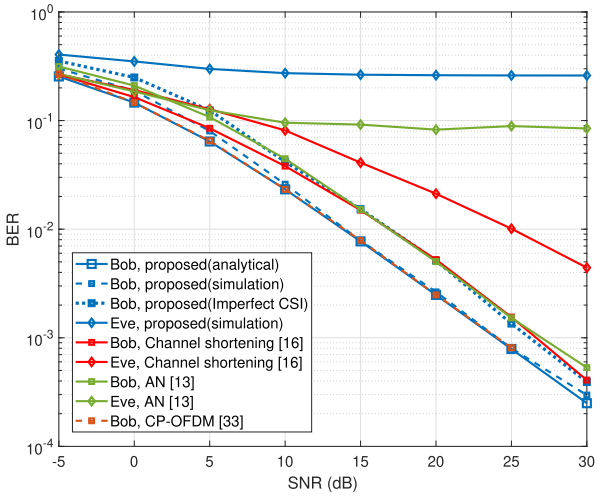


Fig. 6. BER performance of the proposed data security algorithm vs channel shortening [16], AN [13] and conventional CP-OFDM [33].

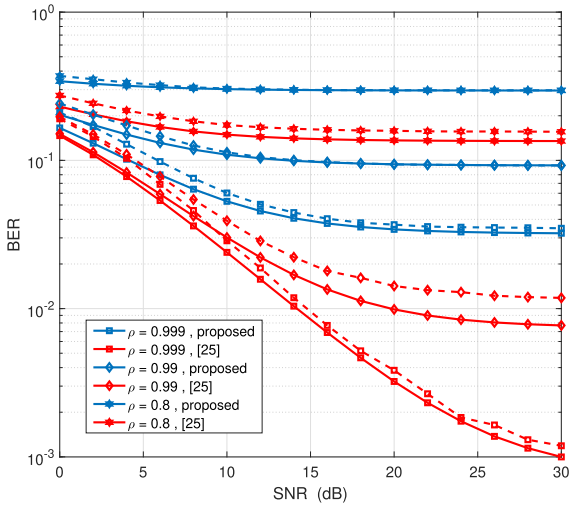


Fig. 7. Performance comparison of the proposed algorithm (blue color) vs. LS [25] (red color) in terms of Eve's BER under correlated eavesdropping channels. The solid and dashed lines stand for the analytical and simulation results, respectively.

the performance of attacker, where equal power is allocated to data and noise. In [16], a channel shortening filter is designed based on the channel of the legitimate user (Bob) in such a way that the length of the effective channel is made equal to or less than the CP at Bob only, while the length of the effective channel at the illegitimate receiver (Eve) is greater than CP. Firstly, it is observed from Fig. 6 that the derived analytical results match well with the simulations except at low SNR regime where a small mismatch is noted. Because, when deriving the BER formula, it is assumed that the channel frequency response is normally distributed. This is because of the assumption in theoretical analysis that channel frequency response (CFR) is normally distributed. However, at very low SNR, after performing the minimum-phase all-pass decomposition to channel, the distribution of the $H^{\min}$ and H^{ap} becomes different from the normal distribution due to the effect of noise decomposition. This effect gets smaller as the SNR increases and the BER finally converges to the derived formula. Also, note that under perfect channel estimation the proposed scheme performs exactly as the CP-OFDM [33], while Eve suffers from high error rates. This implies that the proposed data scheme does not degrade the performance of the legitimate user. Moreover, our novel design exhibits a significant BER gap performance compared to AN and channel shortening by ensuring the lowest BER values at Bob and the highest error rate at Eve. This result emphasizes the effectiveness of the data security algorithm in maintaining high secrecy levels while preserving the performance of the legitimate user. Figure 6 also shows the BER performance of Bob under imperfect channel estimation. It is seen that at low SNR values, Bob has almost the same performance as AN while at high SNR values larger than 20 dB it performed slightly better.

Figure 7 illustrates the analytical as well as the simulated results of Eve's BER performance of the proposed algorithm and link-signature (LS) based algorithm in [25] for the case when Eve's channel is correlated with Bob's. The analytical results agree well with the simulations confirming the model developed in Subsection IV-A. The BER performance is evaluated for the correlation values of $\rho = \{0.999, 0.99, 0.8\}$. It is observed that the performance of Eve improves as the correlation values increase. However, for the same correlation value, we notice a large BER performance gap between the proposed algorithm and LS, where the proposed algorithm clearly outperforms LS method. For instance, when $\rho = 0.999$ the error floor of the proposed scheme settles at 0.03; while if LS is used, the error falls below 0.001. This is due to the fact that the proposed algorithm is using one component of the channel instead of the overall channel, which provides resilience against eavesdroppers near the legitimate nodes as explained in Subsection IV-A.

Thanks to the unit power property of the all-pass channel as explained in Subsection III-A, the proposed precoding would not cause any power issues since it only changes the phase of each OFDM subcarriers. Figure 8 depicts the complementary cumulative distribution function (CCDF) performance of the PAPR of the proposed algorithm compared to CP-OFDM, AN, LS, and channel shortening methods. It is observed that the PAPR performance of the proposed algorithm is similar to that of conventional OFDM while the application of other security schemes causes an increase in PAPR. This result makes the usage of the proposed precoding technique independent of any power constraint.

Figure 9 shows the NMSE versus SNR performance of the estimated channel at the legitimate node and Eve when $M_a = N_b = N_e = 4$. The proposed algorithm is compared to [20], [23], and CP-OFDM [33]. It is observed that there is a significant estimation error gap between Bob and Eve at the cost of some degradation in the estimation quality at very low SNR values compared to conventional channel estimation [33]. This ensures that Eve will neither be able to estimate its channel nor acquire the sensing information from the surrounding environment. It is also observed that the estimation error slightly increases when estimating the minimum-phase

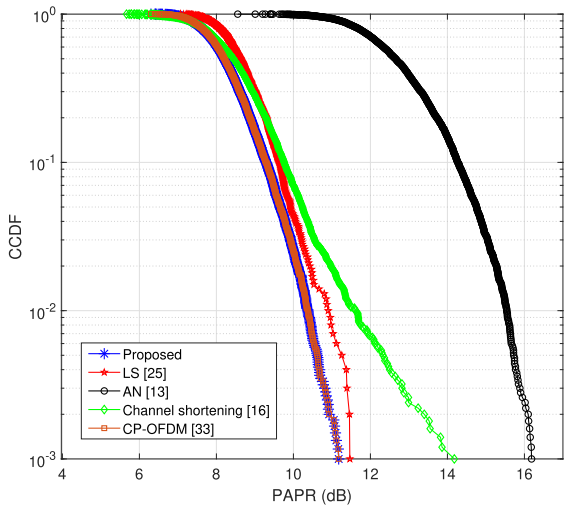


Fig. 8. The CCDF of the PAPR for the proposed algorithm compared to channel shortening [16], AN [13], LS [25], and conventional CP-OFDM [33].

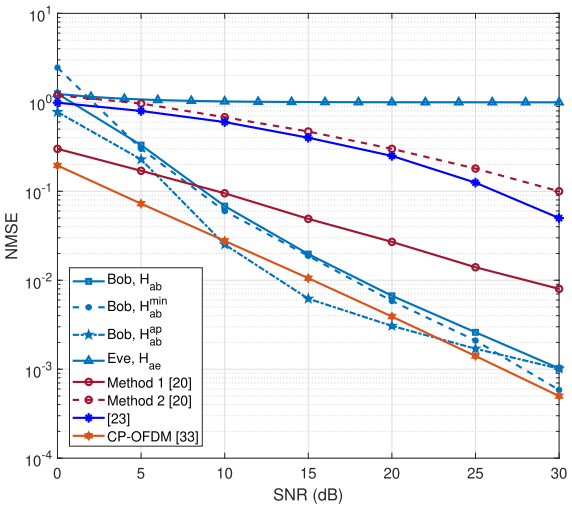


Fig. 9. The channel estimation's NMSE performance vs SNR at Bob and Eve compared to [20], [23], and [33].

or the all-pass channels compared to the effective channel, which justifies the BER performance degradation in Fig. 6. The plots also show that the proposed algorithm outperforms the schemes in [20] and [23] especially at high SNR values.

VI. Conclusion

In this work, we proposed novel security algorithms for providing data and pilot security. Unlike conventional security schemes which use the full channel, the proposed algorithms decompose the channel into its minimum-phase and all-pass components and exploit only the all-pass part. The latter provides enough randomness to secure the communication without causing any power issues such as high PAPR value at the transmitter due to its unit amplitude property. Particularly, the all-pass component and its conjugate are used to secure the pilots and the data, respectively. For data security, we have considered two scenarios of correlated and uncorrelated eavesdropping channels and evaluated the BER gap. Our results reveal that using one component of the channel provides better security than using the total effective channel in both scenarios. Moreover, the results also ensure that the proposed algorithm provides effective security with minimal degradation in the legitimate user's performance compared to conventional algorithms. The results show that the proposed algorithm is capable of providing significant degradation in the estimated channel quality at the eavesdropper. This will ensure not only securing the CSI but also securing radio environment mapping information. Additionally, the proposed algorithm can enable flexibility in terms of providing security to data, pilot, or both depending upon the application requirements.

Appendix A
BER Derivation

The received data at k_d subcarriers is expressed by

$$\underline{\mathrm{Y}}_{ab}(k) = \mathbf{H}_{ab}(k)\mathbf{Q}_D(k)\underline{\mathrm{D}}(k) + \underline{\mathrm{W}}_{ab}(k)\ k \in k_d. \quad (39)$$

Therefore, by enforcing the constraint $\mathrm{E}[\mathrm{Tr}(\underline{\mathrm{D}}(k)\underline{\mathrm{D}}^H(k))] = 1$, the SNR of the received signal at the k-th subcarrier is given by [37]

$$\gamma_{ab} \triangleq \frac{\mathrm{E}\left[\mathrm{Tr}\left(\mathbf{H}_{ab}(k)\mathbf{Q}_D(k)\left(\mathbf{H}_{ab}(k)\mathbf{Q}_D(k)\right)^H\right)\right]}{M_a N_b M\,\mathrm{E}\left[\mathrm{Tr}(\underline{\mathrm{W}}(k)\underline{\mathrm{W}}^H(k))\right]}, \quad (40)$$

where M denotes the number of bits represented by each symbol. As demonstrated in Subsection III-A, the minimum-phase component shares the same power with the overall channel response itself $|\mathbf{H}_{ab}(k)\mathbf{Q}_D(k)|^2 = |\mathbf{H}_{ab}(k)|^2$. Thus, the SNR can be written as

$$\begin{aligned}\gamma_{ab} &\triangleq \frac{\mathrm{E}\left[\mathrm{Tr}\left(\mathbf{H}_{ab}(k)\left(\mathbf{H}_{ab}(k)\right)^H\right)\right]}{M_a N_b M\,\mathrm{E}\left[\mathrm{Tr}(\underline{\mathbf{W}}(k)\underline{\mathbf{W}}^H(k))\right]} \\ &= \frac{\mathrm{E}\left[\sum_{n=1}^{N_b}|H_{ab}^{(n)}(k)|^2\right]}{M_a N_b M\cdot\mathrm{E}\left[\sum_{n=1}^{N_b}|W^{(n)}(k)|^2\right]}. \end{aligned} \quad (41)$$

Using linearity property and assuming that noise samples are i.i.d, (41) becomes

$$\begin{aligned}&= \frac{1}{N_b}\sum_{n=1}^{N_b}\frac{\mathrm{E}\left[|H_{ab}^{(n)}(k)|^2\right]}{M_a M\sigma^2} \\ &= \frac{1}{N_b}\sum_{n=1}^{N_b}\gamma_{ab}^{(n)}. \end{aligned} \quad (42)$$

We conclude from (42) that the BER can be computed by averaging the error at each receive antenna. The average BEP $P_{ab}^{(n)}(e)$ then is given as function of $\gamma_{ab}^{(n)}$ and the correlation coefficients ρ_{ab}^1 and ρ_{ab}^2 between the actual and the estimated channel responses [38] by

$$\begin{aligned}P_{ab}^{(n)}(e) = \frac{1}{2}\Bigg[1 &- \frac{1}{2}\frac{\frac{\left(\rho_{ab}^1+\rho_{ab}^2\right)}{\sqrt{2}}}{\sqrt{1+\frac{1}{2\gamma_{ab}^{(n)}}-\frac{\left(\rho_{ab}^1-\rho_{ab}^2\right)^2}{2}}} \\ &- \frac{1}{2}\frac{\frac{\left(\rho_{ab}^1-\rho_{ab}^2\right)}{\sqrt{2}}}{\sqrt{1+\frac{1}{2\gamma_{ab}^{(n)}}-\frac{\left(\rho_{ab}^1+\rho_{ab}^2\right)^2}{2}}}\Bigg]. \end{aligned} \quad (43)$$

The total BER is then given by

$$P_{ab}(e) = \frac{1}{N_b}\sum_{n=1}^{N_b} P_{ab}^{(n)}. \tag{44}$$

Note that similar step can be followed to compute the BER at Eve.

APPENDIX B
PROOF OF (26)

Assuming the system model in (25)

$$\underline{\mathbf{H}}_{ae} = \hat{\rho}_{ae}\underline{\mathbf{H}}_{ab} + \sqrt{1-\hat{\rho}_{ae}^2}\underline{\mathbf{H}}_{e}. \tag{45}$$

Let the correlation function of the legitimate channel gain with the eavesdropping channel be given as

$$\begin{aligned}\rho_{ae} &= \frac{\mathrm{Cov}(\underline{\mathbf{H}}_{ab}^H, \underline{\mathbf{H}}_{ae})}{\sqrt{\mathrm{var}(\underline{\mathbf{H}}_{ab}^H)\,\mathrm{var}(\underline{\mathbf{H}}_{ae})}} \\ &= \frac{\mathrm{E}[\underline{\mathbf{H}}_{ab}H_{ae}^H] - \mathrm{E}[\underline{\mathbf{H}}_{ab}]\,\mathrm{E}[\underline{\mathbf{H}}_{ae}^H]}{\sigma_a\sigma_e}.\end{aligned} \tag{46}$$

We know that $\mathrm{E}[\underline{\mathbf{H}}_{ab}] = \mathrm{E}[\underline{\mathbf{H}}_{ae}] = 0$. Additionally $\underline{\mathbf{H}}_{ae}$ is given by (25), then

$$\begin{aligned}\rho_{ae} &= \frac{\mathrm{E}[\underline{\mathbf{H}}_{ab}^H \cdot (\hat{\rho}_{ae}\underline{\mathbf{H}}_{ab} + \sqrt{1-\hat{\rho}_{ae}^2}\underline{\mathbf{H}}_{e})]}{\sigma_a\sigma_e} \\ &= \frac{\hat{\rho}_{ae}\,\mathrm{E}[|\underline{\mathbf{H}}_{ab}|^2] + \sqrt{1-\hat{\rho}_{ae}^2}\left(\mathrm{E}[\underline{\mathbf{H}}_{ab}^H]\,\mathrm{E}[\underline{\mathbf{H}}_{e}]\right)}{\sigma_a\sigma_e} \\ &= \frac{\hat{\rho}_{ae}\,\mathrm{E}[|\underline{\mathbf{H}}_{ab}|^2]}{\sigma_a\sigma_e}.\end{aligned} \tag{47}$$

Note that $\sigma_a^2 = \mathrm{var}(\underline{\mathbf{H}}_{ab}) = \mathrm{E}[|\underline{\mathbf{H}}_{ab}|^2] - (\mathrm{E}[\underline{\mathbf{H}}_{ab}])^2 = \mathrm{E}[|\underline{\mathbf{H}}_{ab}|^2]$, and $\sigma_e^2 = \mathrm{var}(\hat{\rho}_{ae}\underline{\mathbf{H}}_{ab} + \sqrt{1-\hat{\rho}_{ae}^2}\underline{\mathbf{H}}_{e}) = \hat{\rho}_{ae}^2\sigma_a^2 + (1-\hat{\rho}_{ae}^2)\sigma_a^2 = \sigma_a^2$. Therefore, we find

$$\rho_{ae} = \frac{\hat{\rho}_{ae}\sigma_a^2}{\sigma_a\sigma_a} = \hat{\rho}_{ae}. \tag{48}$$

Thus, we prove that in the channel model given by (25), $\hat{\rho}_{ae}$ corresponds to the channel correlation between Bob and Eve.

APPENDIX C
PROOF OF (30)

To identify the expression of Γ and instead of using complex probability distributions analysis, we exploit the four constraints given in (29). For instance, from (29a), we know that Γ is proportional to $\sqrt{1-\rho_{ae}^2}$. And if a linear relationship is assumed, we find

$$\Gamma = \alpha + \beta\sqrt{1-\rho_{ae}^2}, \tag{49}$$

where α and β are the linear model's parameters to be defined, and by solving the equation in (29c), i.e., $\rho_{ae}(\Gamma = 1) = 1$, we find the value of the slope as $\alpha = 1$.

Also, by using (29b) and (29d) we find the following

$$0 \le \sqrt{1-\rho_{ae}^2} \le \beta. \tag{50}$$

And since $0 \le \sqrt{1-\rho_{ae}^2} \le 1$, we conclude that $\beta = 1$, therefore

$$\Gamma = 1 + \sqrt{1-\rho_{ae}^2}. \tag{51}$$

This model for Γ agrees very well with the simulation results as shown in Fig. 5.

APPENDIX D
PROOF OF (28)

The correlation function of the legitimate minimum-phase channel component gain with the eavesdropping channel be given as

$$\begin{aligned}&\rho_{ae}^{\min} \\ &= \frac{\mathrm{Cov}(\underline{\mathbf{H}}_{ab}^{\min H}, \underline{\mathbf{H}}_{ae}^{\min})}{\sqrt{\mathrm{var}(\underline{\mathbf{H}}_{ab}^{\min H})\,\mathrm{var}(\underline{\mathbf{H}}_{ae}^{\min})}} \\ &= \frac{\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min H}\cdot\underline{\mathbf{H}}_{ae}^{\min}] - \mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min H}]\,\mathrm{E}[\underline{\mathbf{H}}_{ae}^{\min}]}{\sqrt{\left(\mathrm{E}[|\underline{\mathbf{H}}_{ab}^{\min}|^2] - \left(\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min}]\right)^2\right)\left(\mathrm{E}[|\underline{\mathbf{H}}_{ae}^{\min}|^2] - \left(\mathrm{E}[\underline{\mathbf{H}}_{ae}^{\min}]\right)^2\right)}}.\end{aligned} \tag{52}$$

Note that $\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min}] = \mathrm{E}[\underline{\mathbf{H}}_{ae}^{\min}] = 0$, $\mathrm{E}[|\underline{\mathbf{H}}_{ae}^{\min}|^2] = \mathrm{E}[|\underline{\mathbf{H}}_{ae}|^2] = \sigma_e^2$, and $\mathrm{E}[|\underline{\mathbf{H}}_{ab}^{\min}|^2] = \mathrm{E}[|\underline{\mathbf{H}}_{ab}|^2] = \sigma_a^2$. Please refer to Appendix E. ■

Thus, we find

$$\begin{aligned}&\rho_{ae}^{\min} \\ &= \frac{\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min H}\underline{\mathbf{H}}_{ae}^{\min}]}{\sigma_a\sigma_e} \\ &= \frac{\mathrm{E}\left[\underline{\mathbf{H}}_{ab}^{\min H}\cdot\left(\frac{\rho_{ae}}{1+\sqrt{1-\rho_{ae}^2}}\underline{\mathbf{H}}_{ab}^{\min} + \sqrt{1-\left(\frac{\rho_{ae}}{\Gamma}\right)^2}\underline{\mathbf{H}}_{e}^{\min}\right)\right]}{\sigma_a\sigma_e} \\ &= \frac{\frac{\rho_{ae}}{1+\sqrt{1-\rho_{ae}^2}}\,\mathrm{E}[|\underline{\mathbf{H}}_{ab}^{\min}|^2] + \sqrt{1-\left(\frac{\rho_{ae}}{\Gamma}\right)^2}\left(\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min H}]\,\mathrm{E}[\underline{\mathbf{H}}_{e}^{\min}]\right)}{\sigma_a\sigma_e} \\ &= \frac{\frac{\rho_{ae}}{1+\sqrt{1-\rho_{ae}^2}}\sigma_a^2}{\sigma_a\sigma_e}.\end{aligned} \tag{53}$$

Finally, the correlation is found as

$$\rho_{ae}^{\min} = \frac{\rho_{ae}}{1+\sqrt{1-\rho_{ae}^2}} < \rho_{ae}. \tag{54}$$

APPENDIX E
PROOF OF $\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min}] = \mathrm{E}[\underline{\mathbf{H}}_{ae}^{\min}] = 0$

As explained in Subsection III-A, any FIR causal channel $\underline{\mathbf{H}}_{ab}$ can be decomposed as follows: $\underline{\mathbf{H}}_{ab} = \underline{\mathbf{H}}_{ab}^{\min}\cdot\underline{\mathbf{H}}_{ab}^{\mathrm{ap}}$, where $\underline{\mathbf{H}}_{ab}^{\mathrm{ap}} = e^{jU}$ and $U \sim \mathcal{U}(0, 2\pi)$. Thus, $\underline{\mathbf{H}}_{ab}^{\mathrm{ap}}$ has the following probability density function (PDF): $f_X(x) = \frac{1}{j2\pi x}$.

With reference to the main problem, the expectation of $\underline{\mathbf{H}}_{ab}$ is given as

$$\mathrm{E}[\underline{\mathbf{H}}_{ab}] = \mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min H}\cdot\underline{\mathbf{H}}_{ab}^{\mathrm{ap}}] = 0. \tag{55}$$

Since the minimum-phase and all-pass components are independent, we find

$$\mathrm{E}[\underline{\mathbf{H}}_{ab}] = \mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min}]\,\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\mathrm{ap}}] = 0. \tag{56}$$

As shown in (56), whether $\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min}] = 0$ or $\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\mathrm{ap}}] = 0$. However, $\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\mathrm{ap}}] = \int_{-\infty}^{+\infty}\frac{x}{j2\pi x}dx \neq 0$. Therefore

$$\mathrm{E}[\underline{\mathbf{H}}_{ab}^{\min}] = 0. \tag{57}$$

REFERENCES

[1] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," *ETSI White Paper*, vol. 11, no. 11, pp. 1–16, Jun. 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, Aug. 2014.

[3] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[4] R. L. Rivest, "Cryptography," in *Handbook of Theoretical Computer Science*, vol. A, J. Van Leeuwen and J. Leeuwen, Eds. Amsterdam, The Netherlands: Elsevier, 1990, ch. 13, pp. 718–755.

[5] H. M. Furqan, M. S. J. Solaija, H. Turkmen, and H. Arslan, "Wireless communication, sensing, and REM: A security perspective," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 287–321, 2021.

[6] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, Feb. 2019.

[8] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, 2017.

[9] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.

[10] J. Zhang *et al.*, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[11] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 332–341, 2015.

[12] K. Naito, H. Sakakibara, Y. Mukai, K. Mori, and H. Kobayashi, "Channel state based secure wireless communication," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2016, pp. 828–834.

[13] 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.

[14] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[15] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[16] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Enhancing physical layer security of OFDM systems using channel shortening," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.

[17] Y. Ding, T. N. Davidson, Z.-Q. Luo, and K. M. Wong, "Minimum BER block precoders for zero-forcing equalization," *IEEE Trans. Signal Process.*, vol. 51, no. 9, pp. 2410–2423, Sep. 2003.

[18] 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.

[19] X. Zhang and E. W. Knightly, "$CSI snoop$: Inferring channel state information in multi-user MIMO WLANs," *IEEE/ACM Trans. Netw.*, vol. 27, no. 1, pp. 231–244, Feb. 2019.

[20] M. Soltani, T. Baykas, and H. Arslan, "Achieving secure communication through pilot manipulation," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug. 2015, pp. 527–531.

[21] T.-Y. Liu, S.-C. Lin, and Y.-W. P. Hong, "On the role of artificial noise in training and data transmission for secret communications," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 3, pp. 516–531, Mar. 2017.

[22] T.-H. Chang, Y.-W.-P. Hong, and C.-Y. Chi, "Training signal design for discriminatory channel estimation," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Nov. 2009, pp. 1–6.

[23] Q. Zhu, S. Wu, and Y. Hua, "Optimal pilots for anti-eavesdropping channel estimation," *IEEE Trans. Signal Process.*, vol. 68, pp. 2629–2644, 2020.

[24] Y.-N. Du, S. Han, S. Xu, and C. Li, "Improving secrecy under high correlation via discriminatory channel estimation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[25] A. Albehadili, K. A. A. Shamaileh, A. Y. Javaid, and V. K. Devabhakuni, "Link-signature-based discriminatory channel estimation (LS-DCE) for physical layer security in stationary and mobile OFDM transceivers," *IEEE Trans. Veh. Technol.*, vol. 69, no. 8, pp. 8119–8131, Aug. 2020.

[26] L. Dai, Z. Wang, and Z. Yang, "Spectrally efficient time-frequency training OFDM for mobile large-scale MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 2, pp. 251–263, Feb. 2013.

[27] Y. Liu, Z. Tan, H. Hu, L. J. Cimini, and G. Y. Li, "Channel estimation for OFDM," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1891–1908, May 2014.

[28] A. V. Zelst and T. C. W. Schenk, "Implementation of a MIMO OFDM-based wireless LAN system," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 483–494, Feb. 2004.

[29] D. Mi, M. Dianati, L. Zhang, S. Muhaidat, and R. Tafazolli, "Massive MIMO performance with imperfect channel reciprocity and channel estimation error," *IEEE Trans. Commun.*, vol. 65, no. 9, pp. 3734–3749, Sep. 2017.

[30] A. V. Oppenheim, *Discrete-Time Signal Processing*. London, U.K.: Pearson, 1999.

[31] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[32] D. Hu, L. Yang, Y. Shi, and L. He, "Optimal pilot sequence design for channel estimation in MIMO OFDM systems," *IEEE Commun. Lett.*, vol. 10, no. 1, pp. 1–3, Jan. 2006.

[33] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. Hoboken, NJ, USA: Wiley, 2010.

[34] K. P. Bagadi and P. S. Das, "MIMO-OFDM channel estimation using pilot carries," *Int. J. Comput. Appl.*, vol. 2, no. 3, pp. 81–88, May 2010.

[35] N. S. Ferdinand, D. B. da Costa, A. L. F. de Almeida, and M. Latva-Aho, "Physical layer secrecy performance of TAS wiretap channels with correlated main and eavesdropper channels," *IEEE Wireless Commun. Lett.*, vol. 3, no. 1, pp. 86–89, Feb. 2014.

[36] V. Pan, "Sequential and parallel complexity of approximate evaluation of polynomial zeros," *Comput. Math. Appl.*, vol. 14, no. 8, pp. 591–622, 1987.

[37] D. Bliss, K. Forsythe, and A. Chan, "MIMO wireless communication," *Lincoln Lab. J.*, vol. 15, no. 1, pp. 97–126, 2005.

[38] M.-X. Chang and Y. T. Su, "Performance analysis of equalized OFDM systems in Rayleigh fading," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 721–732, Oct. 2002.

Salah Eddine Zegrar received the B.E. degree in electric electronics engineering from Gebze Technical University, Turkey, in 2019. He is currently pursuing the Ph.D. degree with the Communications, Signal Processing, and Networking Center (CoSiNC), Istanbul Medipol University, Turkey. His research focuses on 5G and beyond radio access technologies, physical layer security, interference management, waveform design, joint radar (sensing) and communication designs, and next-generation Wi-Fi.

Haji M. Furqan received the B.E. and M.Sc. degrees in electrical engineering from the COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan, in 2012 and 2014, respectively, and the Ph.D. degree from Istanbul Medipol University, Turkey. He is currently a Post-Doctoral Researcher at Istanbul Medipol University. His research focuses on physical layer security, cooperative communication, adaptive index modulation, OFDM, V2X, 5G systems, and wireless channel modeling and characterization.

Hüseyin Arslan (Fellow, IEEE) received the B.S. degree from Middle East Technical University (METU), Ankara, Turkey, in 1992, and the M.S. and Ph.D. degrees from Southern Methodist University (SMU), Dallas, TX, USA, in 1994 and 1998, respectively.

From January 1998 to August 2002, he was with the Research Group of Ericsson, where he was involved with several projects related to 2G and 3G wireless communication systems. Since August 2002, he has been with the Electrical Engineering Department, University of South Florida, where he is currently a Professor. In December 2013, he joined Istanbul Medipol University to found the Engineering College, where he has worked as the Dean of the School of Engineering and Natural Sciences. In addition, he has worked as a part-time Consultant for various companies and institutions, including Anritsu Company and The Scientific and Technological Research Council of Turkey. He conducts research in wireless systems, with emphasis on the physical and medium access layers of communications. He has been collaborating extensively with key national and international industrial partners and his research has generated significant interest in companies, such as InterDigital, Anritsu, NTT DoCoMo, Raytheon, Honeywell, and Keysight Technologies. Collaborations and feedback from industry partners has significantly influenced his research. In addition to his research activities, he also has contributed to wireless communication education. He has integrated the outcomes of his research into education which lead him to develop a number of courses at the University of South Florida. He has developed a unique "Wireless Systems Laboratory" course (funded by the National Science Foundation and Keysight Technologies), where he was able to teach not only the theory but also the practical aspects of wireless communication system with the most contemporary test and measurement equipment. His current research interests are on 5G and beyond radio access technologies, physical layer security, interference management (avoidance, awareness, and cancellation), cognitive radio, multi-carrier wireless technologies (beyond OFDM), dynamic spectrum access, co-existence issues, non-terrestial communications (high altitude platforms), joint radar (sensing), and communication designs.

Dr. Arslan has served as the general chair, the technical program committee chair, the session and symposium organizer, the workshop chair, and a technical program committee member for several IEEE conferences. He is a member of the Editorial Board for the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and the *Sensors* journal. He has also served as a member of the Editorial Board for the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and several other scholarly journals by Elsevier, Hindawi, and Wiley Publishing. He is an IEEE Distinguished Lecturer.