Priority-Aware Secure Precoding Based on Multi-Objective Symbol Error Ratio Optimization

Jiankang Zhang, *Senior Member, IEEE*, Sheng Chen, *Fellow, IEEE*, Fasong Wang,
Soon Xin Ng, *Senior Member, IEEE*, Robert G. Maunder, *Senior Member, IEEE*, Lajos Hanzo, *Fellow, IEEE*

***Abstract*—The secrecy capacity based on the assumption of having continuous distributions for the input signals constitutes one of the fundamental metrics for the existing physical layer security (PHYS) solutions. However, the input signals of real-world communication systems obey discrete distributions. Furthermore, apart from the capacity, another ultimate performance metric of a communication system is its symbol error ratio (SER). In this paper, we pursue a radically new approach to PHYS by considering rigorous direct SER optimization exploiting the discrete nature of practical modulated signals. Specifically, we propose a secure precoding technique based on a multi-objective SER criterion, which aims for minimizing the confidential messages' SER at their legitimate user, while maximizing the SER of the confidential messages leaked to the illegitimate user. The key to this challenging multi-objective optimization problem is to introduce a priority factor that controls the priority of directly minimizing the SER of the legitimate user against directly maximizing the SER of the leaked confidential messages. Furthermore, we define a new metric termed as the security-level, which is related to the conditional symbol error probability of the confidential messages leaked to the illegitimate user. Additionally, we also introduce the secure discrete-input continuous-output memoryless channel (DCMC) capacity referred to as secure-DCMC-capacity, which serves as a classical security metric of the confidential messages, given a specific discrete modulation scheme. The impacts of both the channel's Rician factor and the correlation factor of antennas on the security-level and the secure-DCMC-capacity are investigated. Our simulation results demonstrate that the proposed priority-aware secure precoding based on the direct SER metric is capable of securing transmissions, even in the challenging scenario, where the eavesdropper has three receive antennas, while the legitimate user only has a single one.**

***Index Terms*—Physical layer security, wiretap channel, secrecy capacity, secure precoding, mean square error, symbol error rate, conditional error probability, multiple-input multiple-output**

I. Introduction

Wireless communications suffer from the risk of eavesdropping due to the broadcast nature of wireless channels. Recently, the concept of physical layer security (PHYS) [1]–[3] has attracted growing research interest from the wireless communications community. PHYS techniques are capable of securing the transmission by exploiting the physical characteristics of wireless channels, rather than relying on higher-layer encryption [4]. Wyner [2] proved that confidential messages can be securely transmitted to their destination in the presence of a wiretapper, whilst relying on the notion of secrecy capacity defined by Shannon [1]. Since then, the concept of secrecy capacity has become a fundamental metric in developing and investigating PHYS solutions [5]–[19].

Specifically, Csiszár and Korner [14] investigated the PHYS in a non-degraded channel, while the authors of [15] developed this concept further in the context of Gaussian channels. Moreover, PHYS was widely investigated in fading single-antenna channels [16] and multiple-antenna channels [7]. Secure multiple-antenna techniques have also been conceived for maximizing the achievable secrecy rates by designing transmit precoding (TPC) schemes [9], [12]. In particular, Khisti and Wornell [7] provided a metric of secrecy capacity for the Gaussian multi-antenna wiretap channel model to guide the design of a generalized singular value decomposition (GSVD)-based TPC design by maximizing the achievable throughput. However, a fraction of the secret messages may still be leaked to the eavesdropper, if the number of transmit antennas (TAs) is insufficiently large. Reboredo *et al.* [17] designed a linear zero-forcing (ZF) filter that minimizes the mean-squared error (MSE) between the legitimate users, whilst ensuring that the eavesdropper's MSE remains above a certain threshold. A similar beamforming scheme was developed for the multiple-input multiple-output (MIMO) wiretap channel [18] for maximizing the signal-to-leakage-plus-noise ratio (SLNR). Both the beamforming schemes developed in [17] and [18] rely on ZF precoding for cancelling the gain of the wiretap channels by imposing the orthogonal constraint between the wiretap channels and the beamforming matrix. The eavesdropper often invests more resources for eavesdropping on the confidential message delivered to the legitimate destination. Therefore, the scenario considered in [19], where the transmitter has multiple TAs, the destination has a single receive antenna (RA), and the eavesdropper has multiple RAs, is indeed realistic. Wang *et al.* [18] demonstrated that the ZF-based TPC attains a higher secrecy capacity than the GSVD-based TPC when the total combined number of RAs of the destination and of the eavesdropper is lower than that of the TAs.

At this point, it is worth revisiting the classical PHYS scenario, where the system is transmitting confidential messages to a legitimate user, while an eavesdropper attempts to

J. Zhang is with School of Electronics and Computer Science, University of Southampton, SO17 1BJ, U.K. J. Zhang is also with School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China. (E-mails: jz09v@ecs.soton.ac.uk).

S. Chen, S. X. Ng, R. Maunder and L. Hanzo are with School of Electronics and Computer Science, University of Southampton, SO17 1BJ, U.K. (E-mails: {sqc,sxn,rm,lh}@ecs.soton.ac.uk).

F. Wang is with School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China (E-mail: iefswang@zzu.edu.cn).

This work was supported in part by the Engineering and Physical Sciences Research Council projects EP/N004558/1, EP/P034284/1, EP/P034284/1, EP/P003990/1 (COALESCE), by the Royal Society's Global Challenges Research Fund Grant, by the European Research Council's Advanced Fellow Grant QuantCom, as well as in part by the National Natural Science Foundation of China under Grant 61571401 and the Innovative Talent of Colleges and University of Henan Province under grant 18HASTIT021.

intercept these confidential messages. In recent years, non-orthogonal transmission techniques have attracted substantial attention [20], [21], for example for connecting a huge number of Internet of Things (IoT) devices. More specifically, in a non-orthogonal broadcast scenario, a group of legitimate users share the same resources. Consequently, every user can also receive the transmissions destined for the other users of the group. A 'law-abiding' user should only decode the confidential messages designated to it. But since a user 'legitimately' receives all the confidential messages destined for the other users, it may also intentionally or unintentionally listen to the confidential messages destined for the other users. Hence, this user becomes an 'eavesdropper'. This PHYS scenario is more general and more challenging than the classical one, which motivates our current study. Although many of the conventional PHYS designs discussed previously may indeed also be applied, it is paramount to strike a compelling reliability versus security trade-off in this general scenario.

The fundamental concept of secrecy capacity in information-theory is based on the assumption that the input signal obeys a continuous Gaussian distribution. However, in practical digital communication systems, we use M-phase-shift keying (M-PSK), M-pulse-amplitude modulation (M-PAM) and M-quadrature amplitude modulation (M-QAM). The secrecy rate of a Gaussian wiretap channel conveying M-PAM input signals was studied in [22]. Bashar *et al.* [11], [23] investigated the secrecy rates of a MIMO system in the face of a single-eavesdropper (MIMO-SE) and multiple-eavesdropper (MIMO-ME) for finite-alphabet input signals. The key approach in these secrecy rate studies is to exploit the relationship between the mutual information (MI) and the MSE. The minimum MSE (MMSE) criterion has indeed been widely adopted in designing various communication systems, owing to its simplicity and analytical tractability. Nevertheless, the ultimate performance metric of a communication system is its bit error ratio (BER) or symbol error ratio (SER). However, minimizing the MSE in general does not lead to minimizing the BER, unless the input can be closely approximated by a Gaussian signal [24]. Transceiver designs based on the direct minimum BER (MBER) or direct minimum SER (MSER) criteria were conceived for various communication systems in [25]–[27], which demonstrate that the MBER transmitter design and the MBER receiver design outperform their corresponding MMSE counterparts.

The contributions of [25]–[27] however minimize the desired user's BER/SER rather than maximizing its security. The BER metric has been adopted for analyzing the security performance of various channel coding designs either for the classical wiretap channel or for the additive white Gaussian noise (AWGN) channel [28]–[32]. It is worth emphasizing that these treatises did not design channel coding PHYS solutions by optimizing the BER metric. Rather they mainly used the BER or BER-related metrics for analyzing channel coding designs as PHYS solutions either for the wiretap channel or for the AWGN channel. Similarly, the authors of [33] designed a secure orthogonal frequency division modulation with index modulation (OFDM-IM) system, and showed that it outperforms the conventional OFDM-IM, in terms of its BER. It can be seen that in the existing PHYS literature, there is a paucity of contributions on using the BER or SER as the design metric of secure TPC solution for MIMO communication systems.

Against the above background, in this paper, we propose a secure TPC solution for MIMO by directly optimizing a multi-objective SER metric, which is capable of increasing the reliability upon guaranteeing the secure transmission. Specifically, our joint design objective is to minimize the SER of the confidential messages transmitted to the designated user, while guaranteeing secure transmission by maximizing the SER of the confidential messages leaked to the eavesdropper. Explicitly, our contributions are

1) We proposed a new priority-aware secure TPC based on the multi-objective SER optimization criterion, which aims for minimizing the SER of the confidential messages transmitted to the designated user, while maximizing the SER of the confidential messages leaked to the eavesdropper, who is also a legitimate user of the system. This multi-objective optimization based design of secure TPC is achieved by introducing a priority factor that controls the priorities of minimizing the SER of the designated user against maximizing the SER of the leaked confidential messages. A flexible tradeoff between these two conflicting objectives is struck by adjusting this priority factor.
2) We define a new metric termed the security-level, which is a function of the conditional symbol error probability (CSEP) of the leaked confidential messages. The security-level is capable of assessing various secure TPC solutions by providing a directly optimized metric of the transmission integrity. We also introduce the novel notion of the secure discrete-input continuous-output memoryless channel (DCMC) capacity, secure-DCMC-capacity for short, for capturing the nature of practical discrete-constellation based modulated input signals. This directly represents the maximum attainable secure and reliable rate of the confidential messages, given a specific discrete modulation scheme.
3) The impact of the key parameters, such as the channel's Rician K-factor and the correlation factor of antennas on the security-level and the secure-DCMC-capacity are also investigated. Moreover, we have investigated the challenging scenario, when the eavesdropper is equipped with three receive antennas, while the legitimate user only has one. Our results demonstrate that the proposed priority-aware secure TPC scheme is capable of securing the transmission even under this hostile scenario.

The remainder of the paper is organized as follows. In Section II, the system model is presented, and the ZF-based as well as the MMSE-based TPC are also briefly reviewed. In Section III, the proposed secure TPC solution based on the multi-objective SER metric is derived. Then the differential evolutionary algorithm (DEA) used for finding the optimal secure TPC solution based on the priority-aware SER metric is presented. We also present a new metric, namely, the security-level of the confidential messages in a TPC system, in this section. In Section IV, we define the secure-DCMC-capacity for discrete modulated input signals, which serves as a classical secrecy capacity metric for evaluating the proposed solution. Our simulation results and discussions are presented in Section V, and the paper is concluded in Section VI.

II. System model

We consider a two-receiver MIMO broadcast system. However, all the derivations and analysis in this paper can be extended to the case of more than two receivers. The base station (BS) employs N_t TAs to support two users, denoted as user 1 and user 2, using a single frequency-time resource block. User 1 and user 2 are equipped with N_{r_1} and N_{r_2} antennas, respectively. We do not impose the assumption of $N_{r_1} = N_{r_2}$. This allows us to investigate challenging PHYS precoding design problems, where the confidential message of a vulnerable user equipped with a low number of antennas may be eavesdropped by another more sophisticated user, having more antennas. The total number of RAs is $N_r = N_{r_1} + N_{r_2}$. The MIMO system investigated is a full-rank one, where the number of TAs at the BS is no less than the total number of RAs. It is well known that $N_t > N_r$ is required in order for a MIMO system to achieve adequate performance when a linear precoding/detection technique is adopted. For the rank-deficient MIMO scenario, sophisticated nonlinear precoding/detection must be employed. For example, the authors of [34] proposed a generalized vector precoding to tackle this challenge in classical MIMO system without considering PHYS. Since we investigate a linear precoding based PHYS design, a full-rank MIMO system is considered.

Specifically, the BS transmits a pair of independent confidential messages, $\boldsymbol{s}_1 \in \mathbb{C}^{N_{r_1}}$ to user 1 and $\boldsymbol{s}_2 \in \mathbb{C}^{N_{r_2}}$ to user 2, respectively. The task of the BS is twofold. Firstly, it has to ensure that $\boldsymbol{s}_1$ is received by user 1 and $\boldsymbol{s}_2$ is received by user 2, reliably. Secondly, the message $\boldsymbol{s}_1$ intended for user 1 has to be kept secret from user 2, and the message $\boldsymbol{s}_2$ intended for user 2 has to be kept secret from user 1. Given these two conflicting objectives, the BS carries out secure precoding of the signals $\boldsymbol{s} = \left[\boldsymbol{s}_1^{\mathrm{T}}\ \boldsymbol{s}_2^{\mathrm{T}}\right]^{\mathrm{T}} \in \mathbb{C}^{N_r}$, in order to yield the transmit signal vector $\boldsymbol{x} \in \mathbb{C}^{N_t}$

$$\boldsymbol{x} = \sqrt{\lambda}\boldsymbol{W}\boldsymbol{s}, \tag{1}$$

where the TPC matrix $\boldsymbol{W} \in \mathbb{C}^{N_t \times N_r}$ is designed based on the downlink CSI estimated during the pilot training phase[1]. In (1), λ is a normalization factor that normalizes the average transmit power per data stream to unity, and hence λ is given by

$$\lambda = \frac{1}{E_s \mathsf{E}\left[\frac{1}{N_r}\mathrm{Tr}\{\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}}\}\right]}, \tag{2}$$

where E_s is the average power of each data stream, $\mathsf{E}[\cdot]$ denotes the expectation operator, and $\mathrm{Tr}\{\cdot\}$ is the matrix trace operator, while $(\cdot)^{\mathrm{H}}$ is the conjugate transpose operator. For fairness, the average powers per data stream are identical to E_s for the both users.

The signals $\boldsymbol{y}_i \in \mathbb{C}^{N_{r_i}}$ received by the receivers, $i = 1, 2$, can be expressed as

$$\boldsymbol{y}_i = \boldsymbol{H}_i\boldsymbol{x} + \boldsymbol{\varepsilon}_i,\ i = 1, 2, \tag{3}$$

where $\boldsymbol{H}_i \in \mathbb{C}^{N_{r_i} \times N_t}$ denotes the MIMO channel matrix from the BS to user i, and $\boldsymbol{\varepsilon}_i$ is the AWGN vector at receiver i having the covariance matrix of $2\sigma_\varepsilon^2 \boldsymbol{I}_{N_{r_i}}$. Here $\boldsymbol{I}_N$ denotes the $(N \times N)$ identity matrix. The signal to noise ratio (SNR) of the receive signal for RA n_r is defined by $\mathrm{SNR}_{n_r} = \frac{1}{2\sigma_\varepsilon^2}$, $\forall n_r \in \{1, 2, \cdots, N_r\}$. The channel matrix $\boldsymbol{H}_i$ is explicitly expressed as [35, p. 49]

$$\boldsymbol{H}_i = \sqrt{\frac{K_{\mathrm{Rice}}}{1 + K_{\mathrm{Rice}}}}\boldsymbol{H}_{\mathrm{d}_i} + \sqrt{\frac{1}{1 + K_{\mathrm{Rice}}}}\boldsymbol{H}_{\mathrm{r}_i},\ i = 1, 2, \tag{4}$$

where K_{Rice} is the K-factor of the Rician channel, $\boldsymbol{H}_{\mathrm{d}_i} = e^{\mathrm{j}\phi_i}$ is the deterministic component of Receiver-i's specular path arriving with uniformly distributed phase ϕ_i [35, p. 49], and $\boldsymbol{H}_{\mathrm{r}_i}$ is the scattered channel component that is the aggregation of the large number of reflected and scattered path components. In particular, the scattered channel component is given by

$$\boldsymbol{H}_{\mathrm{r}_i} = \left(\boldsymbol{R}_i^r\right)^{\frac{1}{2}}\boldsymbol{G}_i\left(\boldsymbol{R}^t\right)^{\frac{1}{2}},\ i = 1, 2, \tag{5}$$

where $\boldsymbol{R}^t \in \mathbb{C}^{N_t \times N_t}$ and $\boldsymbol{R}_i^r \in \mathcal{C}^{N_{r_i} \times N_{r_i}}$ are the spatial correlation matrices for the N_t TAs of the BS and the N_{r_i} RAs of user i, respectively, while $\boldsymbol{G}_i \in \mathbb{C}^{N_{r_i} \times N_t}$ has the independently identically distributed (i.i.d.) complex-valued entries, each obeying the complex Gaussian distribution of $\mathcal{CN}(0, 1)$. We generate the correlation matrices $\boldsymbol{R}^t$ and $\boldsymbol{R}_i^r$ according to the model of [36]. Explicitly, the l-th row and l'-th column element of the correlation matrix $\boldsymbol{R}$, where we have $\boldsymbol{R} = \boldsymbol{R}^t$ or $\boldsymbol{R}_i^r$, is generated as [36], [37]

$$\left[\boldsymbol{R}\right]_{[l,l']} = \left(\left[\boldsymbol{R}\right]_{[l',l]}\right)^{\ddagger} = \left(\rho e^{\mathrm{j}\theta}\right)^{|l-l'|}, \tag{6}$$

in which $(\cdot)^{\ddagger}$ is the conjugation operation, $\rho e^{\mathrm{j}\theta}$ is the correlation coefficient, ρ is the correlation factor between antennas, and θ is the phase of the coefficient. Additionally, $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ are uncorrelated, and both are assumed to be known to the BS. The impact of imperfect CSI will be investigated in our future work.

Based on the knowledge of $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$, the BS designs the TPC matrix $\boldsymbol{W}$ for striking a trade-off between the information reliability and information secrecy by enabling reliable transmission to the designated user, while securing the transmission by avoiding leakage to the other user. There are various design criteria for the TPC matrix $\boldsymbol{W}$, including the ZF-based TPC design [18] and the MMSE-based TPC design [38]. The contribution of this paper is to develop a priority-aware secure TPC design based on the multi-objective SER criterion, which will be presented in the next section.

[1] For a time division duplexing based system, the BS acquires the uplink CSI based on training symbols received from the uplink transmitters and exploits the reciprocity property of the uplink and downlink channels to design the TPC using the estimated uplink CSI. For a frequency division duplexing based system, the BS transmits pilots for the downlink receivers to acquire their respective CSI, which are quantized and fed back to the BS.

$$\bar{y}_1\big(n_{r_1}\big)=\sqrt{\lambda}\boldsymbol{H}_1[n_{r_1},:]\boldsymbol{W}[:,n_{r_1}]s_1\big(n_{r_1}\big)+\sum_{n_r=1,n_r\neq n_{r_1}}^{N_{r_1}}\sqrt{\lambda}\boldsymbol{H}_1[n_{r_1},:]\boldsymbol{W}[:,n_r]s(n_r)+\sum_{n_r=N_{r_1}+1}^{N_r}\sqrt{\lambda}\boldsymbol{H}_1[n_{r_1},:]\boldsymbol{W}[:,n_r]s(n_r), \quad (11)$$

III. Priority-aware Secure TPC Based on Multi-Objective SER Metric

In contrast to the traditional secure TPC solutions, which are designed based on information theory by assuming that the input signals are Gaussian distributed, we propose radically different priority-aware secure TPC design based on the multi-objective SER criterion for practical digital communication systems with discrete modulated signals, which is capable of balancing the priority of minimizing the SER of the confidential message to its designated user against maximizing the SER of the confidential message eavesdropped by the eavesdropper. Without loss of generality, we use the M-QAM modulation scheme for characterizing our multi-objective SER-based secure TPC solution. Given the total number of RAs of user 1 and user 2, N_r, there are $I = M^{N_r}$ potential transmitted symbol vectors $\boldsymbol{s}$. Each element of $\boldsymbol{s}$ is chosen from the M-QAM constellation

$$\mathcal{S} \triangleq \big\{s_{m,n}\big|s_{m,n} = z_m + \mathrm{j}z_n, 1 \le m, n \le \sqrt{M}\big\}, \quad (7)$$

where the real part of $s_{m,n}$ is $\Re\big[s_{m,n}\big] = z_m = 2m-\sqrt{M}-1$ and the imaginary part is $\Im\big[s_{m,n}\big] = z_n = 2n - \sqrt{M} - 1$. Therefore, the transmitted input signal vector $\boldsymbol{x}$ takes values from the signal set defined by

$$\mathcal{X} \triangleq \big\{\boldsymbol{W}\boldsymbol{s}\big|\boldsymbol{s} \in \underbrace{\{\mathcal{S}\times\mathcal{S}\times\cdots,\times\mathcal{S}\}}_{N_r}\big\}. \quad (8)$$

The size of $\mathcal{X}$ is obviously I. Based on the TPC model (1) with the normalization factor λ given by (2) as well as the channel model (3), the received signal vectors can be expressed as

$$\boldsymbol{y}_i = \sqrt{\lambda}\boldsymbol{H}_i\boldsymbol{W}\boldsymbol{s} + \boldsymbol{\varepsilon}_i, \ i = 1, 2. \quad (9)$$

When a confidential message is for user 1, user 2 may become an eavesdropper to the message, and vice versa. Accordingly, the CSEP of user 1 in decoding its confidential messages defines the legitimate-user's CSEP of user 1, while the eavesdropper's CSEP in decoding the confidential messages designated to user 1 defines the illegitimate-user's CSEP of user 2 eavesdropping on the confidential messages of user 1. Similarly, we can define the legitimate-user's CSEP of user 2 and the illegitimate-user's CSEP of user 1 eavesdropping on the confidential messages of user 2.

A. Legitimate-user conditional symbol error probability

Explicitly, the n_{r_1}-th element of $\boldsymbol{y}_1$ can be written as

$$y_1\big(n_{r_1}\big)=\sqrt{\lambda}\boldsymbol{H}_1[n_{r_1},:]\boldsymbol{W}\boldsymbol{s}+\varepsilon\big(n_{r_1}\big)=\bar{y}_1\big(n_{r_1}\big)+\varepsilon_1\big(n_{r_1}\big), \quad (10)$$

where $\boldsymbol{H}_1[n_{r_1},:]$ is the n_{r_1}-th row of $\boldsymbol{H}_1$, $\varepsilon\big(n_{r_1}\big)$ is the n_{r_1}-th element of $\boldsymbol{\varepsilon} = \big[\boldsymbol{\varepsilon}_1^{\mathrm{T}}\ \boldsymbol{\varepsilon}_2^{\mathrm{T}}\big]^{\mathrm{T}}$, which is equal to the n_{r_1}-th element of $\boldsymbol{\varepsilon}_1$, and the noise-free component $\bar{y}_1\big(n_{r_1}\big)$ is given by (11), in which $\boldsymbol{W}[:,n_r]$ denotes the n_r-th column of $\boldsymbol{W}$, $s_1\big(n_{r_1}\big)$ is the n_{r_1}-th element of $\boldsymbol{s}_1$, and $s(n_r)$ is the n_r-th element of $\boldsymbol{s}$. The first term in the right-hand side of (11) is the desired signal, the second term is the residual self-interference from the other data streams of the same user, and the third term is the residual multiuser interference from the other user.

Let $y_{R_1}\big(n_{r_1}\big) = \Re\big[y_1\big(n_{r_1}\big)\big]$. Since the BS has pre-equalized the MIMO channel by the TPC matrix $\boldsymbol{W}$ approximately, the residual self-interference and the residual multiuser interference in (11) are much smaller than the desired signal, and the receiver can simply use $y_{R_1}\big(n_{r_1}\big)$ to detect $s_{R_1}\big(n_{r_1}\big) = \Re\big[s_1\big(n_{r_1}\big)\big]$. Explicitly, $y_{R_1}\big(n_{r_1}\big)$ is used to estimate $s_{R_1}\big(n_{r_1}\big)$ according to the decision rule

$$\widehat{s}_{R_1}\big(n_{r_1}\big)=\begin{cases} z_1, & y_{R_1}\big(n_{r_1}\big) \le z_1 + 1, \\ z_m, & \begin{array}{l} z_m - 1 \le y_{R_1}\big(n_{r_1}\big) \le z_m + 1, \\ 2 \le m \le \sqrt{M} - 1 \end{array} \\ z_{\sqrt{M}}, & z_{\sqrt{M}} - 1 \le y_{R_1}\big(n_{r_1}\big). \end{cases} \quad (12)$$

For the 16-QAM modulation, i.e., for $\sqrt{M} = 4$, the conditional error probabilities of $\widehat{s}_{R_1}\big(n_{r_1}\big) \neq z_m$, given $\Re\big[s_1\big(n_{r_1}\big)\big] = z_m$, for $1 \le m \le 4$ are illustrated in Fig. 1 as the shaded areas. More specifically, the conditional error probability of $\widehat{s}_{R_1}\big(n_{r_1}\big) \neq z_1$ is the red shaded area, the conditional error probability of $\widehat{s}_{R_1}\big(n_{r_1}\big) \neq z_2$ is the blue shaded area, the conditional error probability of $\widehat{s}_{R_1}\big(n_{r_1}\big) \neq z_3$ is the yellow shaded area, and the conditional error probability of $\widehat{s}_{R_1}\big(n_{r_1}\big) \neq z_4$ is the green shaded area. Clearly, given $s_1\big(n_{r_1}\big)$, there are a total of $J = M^{(N_r-1)}$ potential transmitted symbol vectors for $\boldsymbol{s}$. Therefore, there are a total of J values for $\bar{y}_1\big(n_{r_1}\big)$ conditioned on $s_1\big(n_{r_1}\big)$, which are defined by

$$\big\{\bar{y}_1\big(n_{r_1}\big)\big|s_1\big(n_{r_1}\big)\big\} = \Big\{\bar{y}_1^{(j)}\big(n_{r_1}\big) = \bar{y}_{R_1}^{(j)}\big(n_{r_1}\big) + \mathrm{j}\bar{y}_{I_1}^{(j)}\big(n_{r_1}\big), \\ 1 \le j \le J\big|s_1\big(n_{r_1}\big)\Big\}, \quad (13)$$

where $\bar{y}_{R_1}^{(j)}\big(n_{r_1}\big) = \Re\Big[\bar{y}_1^{(j)}\big(n_{r_1}\big)\Big]$ and $\bar{y}_{I_1}^{(j)}\big(n_{r_1}\big) = \Im\Big[\bar{y}_1^{(j)}\big(n_{r_1}\big)\Big]$. Given the transmit signal component $s_1\big(n_{r_1}\big)$ and the TPC matrix $\boldsymbol{W}$, therefore, the conditional probability density function (CPDF) of $y_{R_1}\big(n_{r_1}\big)$ is a Gaussian mixture

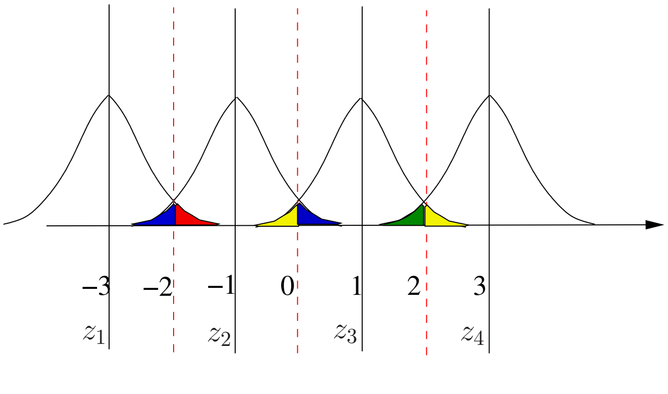


Fig. 1. Illustration of error probability for real-part symbol detection, where $\sqrt{M} = 4$.

$$y_2\big(n_{r_2}|n_{r_1}\big)=\underbrace{\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]s\big(n_{r_1}\big)+\sum_{n_r=1,n_r\neq n_{r_1}}^{N_{r_1}}\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_r]s\big(n_r\big)}_{\bar{y}_2\left(n_{r_2}|n_{r_1}\right)}+\underbrace{\sum_{n_r=N_{r_1}+1}^{N_r}\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_r]s\big(n_r\big)}_{\check{y}_2\left(n_{r_2}|n_{r_1}\right)}+\varepsilon_2\big(n_{r_2}\big), \tag{19}$$

given by

$$\begin{aligned} & f\left(y_{R_1}\big(n_{r_1}\big)\big|s_1\big(n_{r_1}\big),\boldsymbol{W}\right) \\ & =\frac{1}{\sqrt{2\pi}J\sigma_n}\sum_{j=1}^{J}\exp\left(-\frac{\left|y_{R_1}\big(n_{r_1}\big)-\bar{y}_{R_1}^{(j)}\big(n_{r_1}\big)\right|^2}{\sigma_\varepsilon^2}\right). \end{aligned} \tag{14}$$

This should be contrast with the ideal AWGN channel, where the CPDF is a Gaussian, i.e., the channel AWGN's PDF. The practical M-QAM constellation is symmetric, and $\sqrt{M}$ is an even integer. Thus, the conditional subsets of $\bar{y}_{R_1}\big(n_{r_1}\big)$ given $\Re\left[s_1\big(n_{r_1}\big)\right]=z_m$, $\left\{\bar{y}_{R_1}^{(j)}\big(n_{r_1}\big),1\le j\le J\middle|\Re\left[s_1\big(n_{r_1}\big)\right]=z_m\right\}$ for $1\le m\le\sqrt{M}$, satisfy the shift invariant property of [27]. As a result, the CPDFs of $y_{R_1}\big(n_{r_1}\big)$ conditioned on $\Re\left[s_1\big(n_{r_1}\big)\right]=z_m$, for $1\le m\le\sqrt{M}$, satisfy the shift property [27]. For $\sqrt{M}=4$, the shifted symmetric property of the four CPDFs is illustrated in Fig. 1.

Referring to the decision rule (12) and the illustration of Fig. 1, therefore, the legitimate-user CSEP of $\widehat{s}_{R_1}\big(n_{r_1}\big)\neq z_1$ can be evaluated as

$$\begin{aligned} P_{E,R_1}^{(n_{r_1},z_1)}(\boldsymbol{W}) &= \int\limits_{z_1+1}^{+\infty} f\left(y_{R_1}\big(n_{r_1}\big)\big|s_1\big(n_{r_1}\big),\boldsymbol{W}\right)d\,y_{R_1}\big(n_{r_1}\big) \\ &=\frac{1}{J}\sum_{j=1}^{J}Q\Big(C_{R_1,n_{r_1}}^{(j,z_1)}(\boldsymbol{W})\Big), \end{aligned} \tag{15}$$

where

$$C_{R_1,n_{r_1}}^{(j,z_1)}(\boldsymbol{W})=\frac{(z_1+1)-\bar{y}_{R_1}^{(j)}\big(n_{r_1}\big)}{\sigma_\varepsilon}, \tag{16}$$

$$Q(x)=\frac{1}{2\pi}\int\limits_{x}^{+\infty}\exp\left(-\frac{u^2}{2}\right)d\,u. \tag{17}$$

Again the legitimate-user CSEP (15) should be contrast to the one for the ideal AWGN channel which is a single Q-function. Following the derivation in Appendix A, the average legitimate-user CSEP of user 1 is given by

$$\begin{aligned} P_{E,1}^{l(1)}(\boldsymbol{W}) &=\frac{1}{N_{r_1}}\sum_{n_{r_1}=1}^{N_{r_1}}P_{E,1}^{(n_{r_1})}(\boldsymbol{W}) \\ &\approx\frac{4\big(\sqrt{M}-1\big)}{N_{r_1}\sqrt{M}}\sum_{n_{r_1}=1}^{N_{r_1}}P_{E,R_1}^{(n_{r_1},z_1)}, \end{aligned} \tag{18}$$

where $P_{E,1}^{(n_{r_1})}(\boldsymbol{W})$ denotes the average legitimate-user CSEP of $\widehat{s}_1\big(n_{r_1}\big)\neq s_1\big(n_{r_1}\big)$.

In the same way, we can derive the average legitimate-user CSEP of user 2 $P_{E,2}^{l(2)}(\boldsymbol{W})$.

B. Illegitimate-user conditional symbol error probability

To investigate the illegitimate-user CSEP of user 2 eavesdropping on the confidential messages of user 1, we rewrite the received signal $y_2\big(n_{r_2}\big)$ at the n_{r_2}-th RA of user 2 for eavesdropping on the confidential signal $s\big(n_{r_1}\big)$ as (19), where $\bar{y}_2\big(n_{r_2}|n_{r_1}\big)$ is the noise-free part containing the signal of user 1, which takes its value from the set $\left\{\bar{y}_2^{(j)}\big(n_{r_2}|n_{r_1}\big),1\le j\le J\right\}$, $\check{y}_2\big(n_{r_2}|n_{r_1}\big)$ is the interference imposed by user 2's own signal, and $\varepsilon_2\big(n_{r_2}\big)$ is the n_{r_2}-th element of $\boldsymbol{\varepsilon}_2$. When user 2 attempts to decode user 1's confidential data $s\big(n_{r_1}\big)$, the best strategy is as follows. First, user 2 can attempt to cancel out its self-interference contaminating its received signal $y_2\big(n_{r_2}|n_{r_1}\big)$ using its own detected data. Since the TPC matrix is designed to ensure that a user can reliably decode its own confidential messages, the detected data of user 2's are correct with a very high probability. Hence this self cancellation is effective and will reduce the second sum $\check{y}_2\big(n_{r_2}|n_{r_1}\big)$ in (19) to almost zero. Secondly, since user 2 has N_{r_2} RAs and hence has the N_{r_2} received signals $y_2\big(n_{r_2}|n_{r_1}\big)$ for $1+N_{r_1}\le n_{r_2}\le N_{r_2}+N_{r_1}$, it can attempt some form of received combining using these N_{r_2} signals to mitigate the self-interference of user 1's data streams, i.e., to reduce the first sum in (19), so that the probability of successful eavesdropping on $s\big(n_{r_1}\big)$ is significantly improved.

The worst-case security scenario is therefore as follows: user 2 decodes its own data perfectly, thus becomes able to perform perfect self cancellation, and it has managed to acquire the TPC matrix $\boldsymbol{W}_1$ for user 1, thus it is able to perform receive combining for its received user-1's signal components by all its antennas. Consequently, the BS must design the secure TPC matrices to ensure that even under this worst-case security scenario, the above eavesdropper strategy will fail. The rationale of such a design approach is plausible. If the BS can ensure that even under this worst-case security scenario, the eavesdropper fails to decode the other user's confidential messages, it will certainly ensure security under all the other situations that are less favourable for the eavesdropper, namely, when the eavesdropper cannot perfectly cancel out its own self-interference and/or it has no knowledge of the other user's TPC matrix.

Specifically, the BS can first assume that user 2 can perfectly cancel the self-interference, when it eavesdrops on the confidential signal $s\big(n_{r_1}\big)$. Under this assumption, (19) becomes

$$y_2\big(n_{r_2}|n_{r_1}\big)=\bar{y}_2\big(n_{r_2}|n_{r_1}\big)+\varepsilon_2\big(n_{r_2}\big). \tag{20}$$

Secondly, the BS also assumes that user 2 has managed to acquire or steal $\boldsymbol{W}_1$. It is widely exploited that the maximum-ratio combiner (MRC) is an optimal linear combiner[2] for maximizing the diversity gain of multiple independent channels. Thus the BS will assume that user 2 adopts the MRC for maximally improving its successful eavesdropping probability. That is, the BS assumes that user 2 decodes the confidential signal $s_1\left(n_{r_1}\right)$ of user 1 according to

$$\widetilde{y}_2\left(n_{r_1}\right) = \frac{\sum\limits_{n_{r_2}=1}^{N_{r_2}} \left(\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right)^* y_2\left(n_{r_2}|n_{r_1}\right)}{\sum\limits_{n_{r_2}=1}^{N_{r_2}} \left|\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right|^2}. \tag{21}$$

In other words, the eavesdropper, user 2, can use $\widehat{y}_{R_2}\left(n_{r_1}\right) = \Re\left[\widetilde{y}_2\left(n_{r_1}\right)\right]$ to detect $s_{R_1}\left(n_{r_1}\right)$ based on the decision rule (2). The CPDF of $\widetilde{y}_{R_2}\left(n_{r_1}\right)$ given the transmitted signal $s_1\left(n_{r_1}\right)$ and the TPC matrix $\boldsymbol{W}$ is a Gaussian mixture given by

$$\begin{aligned} & f\left(\widetilde{y}_{R_2}\left(n_{r_1}\right)\middle|s\left(n_{r_1}\right),\boldsymbol{W}\right) \\ & = \frac{1}{\sqrt{2\pi}J\widetilde{\sigma}_\varepsilon}\sum_{j=1}^{J}\exp\left(\frac{-\left|\widetilde{y}_{R_2}\left(n_{r_1}\right)-\bar{y}_{R_2}^{(j)}\left(n_{r_1}\right)\right|^2}{\widetilde{\sigma}_\varepsilon^2}\right), \end{aligned} \tag{22}$$

where $\bar{y}_{R_2}^{(j)}\left(n_{r_1}\right) = \Re\left[\bar{y}_2^{(j)}\left(n_{r_1}\right)\right]$ and $\bar{y}_2^{(j)}\left(n_{r_1}\right)$ is the j-th possible noise-free component of the MRC output, which is given by

$$\bar{y}_2^{(j)}\left(n_{r_1}\right) = \frac{\sum\limits_{n_{r_2}=1}^{N_{r_2}} \left(\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right)^* \bar{y}_2^{(j)}\left(n_{r_2}|n_{r_1}\right)}{\sum\limits_{n_{r_2}=1}^{N_{r_2}} \left|\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right|^2}, \tag{23}$$

while $\widetilde{\sigma}_\varepsilon^2$ is the effective variance of the noise at the output of the MRC, which is given by

$$\begin{aligned} \widetilde{\sigma}_\varepsilon^2 &= \frac{\sigma_\varepsilon^2 \sum\limits_{n_{r_2}=1}^{N_{r_2}} \left|\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right|^2}{\left(\sum\limits_{n_{r_2}=1}^{N_{r_2}} \left|\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right|^2\right)^2} \\ &= \frac{\sigma_\varepsilon^2}{\sum\limits_{n_{r_2}=1}^{N_{r_2}} \left|\sqrt{\lambda}\boldsymbol{H}_2[n_{r_2},:]\boldsymbol{W}[:,n_{r_1}]\right|^2}. \end{aligned} \tag{24}$$

Let $\widehat{s}_{R_2}\left(n_{r_1}\right)$ be the eavesdropper's estimate of user-1's signal $s_{R_1}\left(n_{r_1}\right)$. The illegitimate-CSEP of $\widehat{s}_{R_2}\left(n_{r_1}\right) \neq z_1$ is given by

$$\begin{aligned} P_{E,R_2}^{(n_{r_1},z_1)}(\boldsymbol{W}) &= \int\limits_{z_1+1}^{+\infty} f\left(\widetilde{y}_{R_2}\left(n_{r_1}\right)\middle|s\left(n_{r_1}\right),\boldsymbol{W}\right)d\widetilde{y}_{R_2}\left(n_{r_1}\right) \\ &= \frac{1}{J}\sum_{j=1}^{J} Q\left(C_{R_2,n_{r_1}}^{(j,z_1)}(\boldsymbol{W})\right), \end{aligned} \tag{25}$$

where

$$C_{R_2,n_{r_1}}^{(j,z_1)}(\boldsymbol{W}) = \frac{(z_1+1)-\bar{y}_{R_2}^{(j)}\left(n_{r_1}\right)}{\widetilde{\sigma}_\varepsilon}. \tag{26}$$

As detailed in Appendix B, we can arrive at the illegitimate-CSEP of user 2 eavesdropping on user 1's confidential messages under this worst-case security scenario, which is given by

$$\begin{aligned} P_{E,2}^{ill(1)}(\boldsymbol{W}) &= \frac{1}{N_{r_1}}\sum_{n_{r_1}=1}^{N_{r_1}} P_{E,2}^{(n_{r_1})}(\boldsymbol{W}) \\ &\approx \frac{4\left(\sqrt{M}-1\right)}{N_{r_1}\sqrt{M}}\sum_{n_{r_1}=1}^{N_{r_1}} P_{E,R_2}^{(n_{r_1},z_1)}(\boldsymbol{W}). \end{aligned} \tag{27}$$

Clearly, this illegitimate-CSEP is the lower bound that represents the best achievable SER of user 2, who is eavesdropping on user 1's confidential messages. In reality, the eavesdropping user 2 will have a much higher CSEP, when it eavesdrops on user 1's confidential message, since in most practical cases, user 2 does not know $\boldsymbol{W}_1$.

The lower bound of the average illegitimate-CSEP of user-1 eavesdropping on user-2's confidential messages, $P_{E,1}^{ill(2)}(\boldsymbol{W})$, can be derived in the same way. Without causing misunderstanding, we will also refer to the lower-bound illegitimate-CSEPs $P_{E,2}^{ill(1)}(\boldsymbol{W})$ and $P_{E,1}^{ill(2)}(\boldsymbol{W})$ as the illegitimate-CSEPs.

C. The optimization problem of priority-aware secure precoding

In order to secure transmissions, the BS should design $\boldsymbol{W}$ for minimizing the legitimate-CSEPs $P_{E,1}^{l(1)}(\boldsymbol{W})$ and $P_{E,2}^{l(2)}(\boldsymbol{W})$, while maximizing the illegitimate-CSEPs $P_{E,2}^{ill(1)}(\boldsymbol{W})$ and $P_{E,1}^{ill(2)}(\boldsymbol{W})$. This is a challenging multi (two)-objective optimization problem. Intuitively, the most secure case when user-2 eavesdropping on the confidential message of user-1 is that it can only randomly guess user-1's message. This has a SER of $\frac{M-1}{M}$ for the M-QAM signal. Thus, the most secure TPC is the one that achieves $P_{E,2}^{ill(1)}(\boldsymbol{W}) \rightarrow \frac{M-1}{M}$, and maximizing $P_{E,2}^{ill(1)}(\boldsymbol{W})$ corresponds to minimizing $\left|P_{E,2}^{ill(1)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$. Similarly, maximizing $P_{E,1}^{ill(2)}(\boldsymbol{W})$ is equivalent to minimizing $\left|P_{E,1}^{ill(2)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$. Thus, the optimal secure TPC solution $\boldsymbol{W}^\star$ should simultaneously minimize $P_{E,1}^{l(1)}(\boldsymbol{W})$ and $P_{E,2}^{l(2)}(\boldsymbol{W})$ as well as $\left|P_{E,2}^{ill(1)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$ and $\left|P_{E,1}^{ill(2)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$. Since this is a challenging two-objective optimization problem, the optimal solution set forms an optimal Pareto front, which may be obtained by an evolutionary multi-objective algorithm [39]–[41], albeit at an extremely high computational complexity. Moreover, in a practical system, even when such an optimal Pareto solution set is found, a trade-off must be struck between the information reliability, i.e., minimizing $P_{E,1}^{l(1)}(\boldsymbol{W})$ and $P_{E,2}^{l(2)}(\boldsymbol{W})$, and information security, namely, minimizing $\left|P_{E,2}^{ill(1)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$ and $\left|P_{E,1}^{ill(2)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$. This corresponds to selecting a particular point on the Pareto front to meet the required trade-off between the two conflicting objectives.

[2] Note that user 2 may also employ sophisticated non-linear receiver combining, which may achieve a slightly better eavesdropping performance. Nevertheless, we adopt the MRC, which allows us to derive a closed-form expression for our ensuing analysis.

$$P_E^{(s)}(\boldsymbol{W}) = \xi\left(P_{E,1}^{l(1)}(\boldsymbol{W}) + P_{E,2}^{l(2)}(\boldsymbol{W})\right) + (1-\xi)\left(\left|P_{E,2}^{ill(1)}(\boldsymbol{W}) - \frac{M-1}{M}\right| + \left|P_{E,1}^{ill(2)}(\boldsymbol{W}) - \frac{M-1}{M}\right|\right), \tag{28}$$

Considering this practical perspective, therefore, we combine the two conflicting objectives, $P_{E,1}^{l(1)}(\boldsymbol{W})$ and $P_{E,2}^{l(2)}(\boldsymbol{W})$ as well as $\left|P_{E,2}^{ill(1)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$ and $\left|P_{E,1}^{ill(2)}(\boldsymbol{W}) - \frac{M-1}{M}\right|$, into a single objective with the priority factor $\xi \in [0,\ 1]$, which defines the trade-off between information reliability and information security. More explicitly, the above challenging multi-objective optimization problem is transferred into a single-objective optimization by introducing the following metric termed as the weighted-CSEP for designing the optimal TPC matrix $\boldsymbol{W}$ given in (28), where the legitimate-priority factor ξ and illegitimate-priority factor $(1-\xi)$ represent the weighting factors for the legitimate-CSEPs and illegitimate-CSEPs, respectively. A larger value of ξ indicates a higher priority of minimizing the legitimate-CSEPs. By contrast, a smaller ξ or a larger value of $(1-\xi)$ indicates a higher priority of maximizing illegitimate-CSEPs.

The optimal priority-aware secure TPC matrix $\boldsymbol{W}_{\text{MSER}}$ based on the multi-objective SER criterion of (28) is defined by the following optimization problem:

$$\boldsymbol{W}_{\text{MSER}} = \arg\min_{\boldsymbol{W}} P_E^{(s)}(\boldsymbol{W}). \tag{29}$$

Intuitively, $\boldsymbol{W}_{\text{MSER}}$ is a particular solution point on the optimal Pareto front of the solutions that reflects where our 'priority' is in terms of minimizing the legitimate-CSEPs and maximizing the illegitimate-CSEPs, with the trade off between the two conflicting optimization objectives specified by the priority factor ξ.

D. *Differential evolution algorithm aided multi-objective SER based TPC*

There is no closed-form solution for the optimal secure TPC matrix $\boldsymbol{W}_{\text{MSER}}$, and a numerical optimization must be adopted to obtain $\boldsymbol{W}_{\text{MSER}}$. For example, a gradient algorithm was invoked for finding the MSER/MBER solution for the systems without considering PHYS [27]. However, gradient-based algorithm may become trapped at locally optimal points. Hence, we opt for using the DEA for solving the optimization problem (29). As an efficient global optimization algorithm, DEA [42]–[44] is capable of finding a globally optimal solution for a wide variety of optimization scenarios with a near-unity probability, provided that a sufficiently computational complexity quantified in terms of the number of evolutionary generations is affordable [46], [47]. This has been characterized in [45]–[47] for wireless system designs, but without considering their PHYS. Furthermore, both the design and the probability of the DEA's convergence are detailed in [45]–[47]. For the sake of completeness, below we summarize our DEA designed for solving the optimization problem (29), which requires optimization over continuous spaces.

1) **Initialization**. The DEA commences its evolution by randomly generating an initial population of P_S candidate vectors, denoted by

$$\widehat{\boldsymbol{w}}_{1,p_s} = [\widehat{w}_{1,p_s,1}\widehat{w}_{1,p_s,2}\cdots\widehat{w}_{1,p_s,A}]^{\text{T}} \in \mathbb{C}^A, 1 \le p_s \le P_S, \tag{30}$$

where P_S is the population size, and $A = N_t \cdot N_r$. Each $\widehat{\boldsymbol{w}}_{1,p_s}$ represents a potential solution, and the first index 1 in $\widehat{\boldsymbol{w}}_{1,p_s}$ indicates that this is the first generation. A size-P elite-archive deposits the $100P\%$ best candidate vectors of the current population.

2) **Mutation**. The aim of mutation is to prevent the premature convergence to a local optimum without thoroughly exploring the search-space. Hence, at the g-th generation, the mutation perturbs the candidate solutions by perturbing the selected base population vector $\widehat{\boldsymbol{w}}_{g,p_s}$ with a mutant vector, which is generated by two appropriately scaled and randomly selected difference vectors. Explicitly, the mutation operation is given by

$$\widetilde{\boldsymbol{w}}_{g,p_s} = \widehat{\boldsymbol{w}}_{g,p_s} + \lambda_{p_s}\left(\widehat{\boldsymbol{w}}_{g,p}^{\text{elite}} - \widehat{\boldsymbol{w}}_{g,p_s}\right) + \lambda_{p_s}\left(\widehat{\boldsymbol{w}}_{g,p_{r_1}} - \widehat{\boldsymbol{w}}_{g,p_{r_2}}\right), \tag{31}$$

where $\widehat{\boldsymbol{w}}_{g,p}^{\text{elite}}$ is randomly selected from the elite-archive, and $1 \le p_{r_1}, p_{r_2} \le P_S$ are two random integer values, which also satisfy $p_{r_1} \ne p_{r_2}$, $p_{r_1} \ne p_s$ and $p_{r_2} \ne p_s$, while $\lambda_{p_s} \in (0,\ 1]$ denotes the scaling factor, which is randomly generated for each individual according to the normal distribution with the mean μ_λ and the standard deviation σ_λ.

3) **Crossover**. To avoid premature convergence and to increase the diversity of the population, the crossover operation generates a trial candidate vector by exchanging some elements of a target vector and a donor vector. Specifically, the a-th element of the trial vector $\breve{\boldsymbol{w}}_{g,p_s}$ is generated according to

$$\breve{w}_{g,p_s,a} = \begin{cases} \widetilde{w}_{1,p_s,a}, & \text{rand}_a(0,1) \le C_{p_s}, \\ \widehat{w}_{g,p_s,a}, & \text{rand}_a(0,1) > C_{p_s}, \end{cases} \tag{32}$$

where $\widetilde{w}_{g,p_s,a}$ and $\widehat{w}_{g,p_s,a}$ are the a-th elements of the donor vector $\widetilde{\boldsymbol{w}}_{g,p_s}$ and the target vector $\widehat{\boldsymbol{w}}_{g,p_s}$, respectively, and the random number generator $\text{rand}_a(0,1)$ generates a uniformly distributed random value in the range of $[0,\ 1)$, while C_{p_s} denotes the crossover probability that determines whether the a-th element of a target vector will be replaced by its donor vector, and it obeys the normal distribution with the mean μ_c and the standard deviation σ_c.

4) **Selection**. The selection operation compares the target vectors and the trial vectors to decide which survives into the next generation. Explicitly, we first convert $\widehat{\boldsymbol{w}}_{g,p_s}$ and $\breve{\boldsymbol{w}}_{g,p_s}$ into the target and trial matrices $\widehat{\boldsymbol{W}}_{g,p_s}$ and $\breve{\boldsymbol{W}}_{g,p_s}$, respectively. Then whether $\widehat{\boldsymbol{w}}_{g,p_s}$ or $\breve{\boldsymbol{w}}_{g,p_s}$ survives into the next generation is decided according to

$$\widehat{\boldsymbol{w}}_{g+1,p_s} = \begin{cases} \widehat{\boldsymbol{w}}_{g,p_s}, \text{if } P_E^{(s)}\left(\widehat{\boldsymbol{W}}_{g,p_s}\right) \le P_E^{(s)}\left(\breve{\boldsymbol{W}}_{g,p_s}\right), \\ \breve{\boldsymbol{w}}_{g,p_s}, \text{if } P_E^{(s)}\left(\widehat{\boldsymbol{W}}_{g,p_s}\right) > P_E^{(s)}\left(\breve{\boldsymbol{W}}_{g,p_s}\right). \end{cases} \tag{33}$$

The selection operation maintains constant population size of P_S.

5) **Adaptation**. The mean of the crossover probability μ_c and the mean of the scaling factor μ_λ are adaptively

$$\mathcal{I}_1^{l(1)}(s_1(n_{r_1});y_1(n_{r_1}))=\log_2(M)-\frac{1}{M}\sum_{m=1}^{M}\int f\left(y_1(n_{r_1})\middle|s_1^{(m)}(n_{r_1}),\boldsymbol{W}\right)\log_2\frac{\sum\limits_{m'=1}^{M} f\left(y_1(n_{r_1})\middle|s_1^{(m')}(n_{r_1}),\boldsymbol{W}\right)}{f\left(y_1(n_{r_1})\middle|s_1^{(m)}(n_{r_1}),\boldsymbol{W}\right)}dy_1(n_{r_1}). \tag{38}$$

$$\mathcal{I}_2^{ill(1)}(s_1(n_{r_1});\widetilde{y}_2(n_{r_1}))=\log_2(M)-\frac{1}{M}\sum_{m=1}^{M}\int f\left(\widetilde{y}_2(n_{r_1})\middle|s_1^{(m)}(n_{r_1}),\boldsymbol{W}\right)\log_2\frac{\sum\limits_{m'=1}^{M} f\left(\widetilde{y}_2(n_{r_1})\middle|s_1^{(m')}(n_{r_1}),\boldsymbol{W}\right)}{f\left(\widetilde{y}_2(n_{r_1})\middle|s_1^{(m)}(n_{r_1}),\boldsymbol{W}\right)}d\widetilde{y}_2(n_{r_1}), \tag{40}$$

updated according to

$$\mu_c =(1-\kappa)\mu_c + \kappa\cdot \mathrm{mean}_A\left(\mathcal{S}_c\right), \tag{34}$$

$$\mu_\lambda =(1-\kappa)\mu_\lambda + \kappa\cdot \mathrm{mean}_L\left(\mathcal{S}_\lambda\right), \tag{35}$$

where the factor κ controls the rate of adaption, $\mathrm{mean}_A(\cdot)$ represents the arithmetic average, and $\mathrm{mean}_L(\mathcal{S}_\lambda)$ is the Lehmer mean of $\mathcal{S}_\lambda$, which is defined by $\sum_{\lambda_{p_s}\in\mathcal{S}_\lambda}\lambda_{p_s}^2\big/\sum_{\lambda_{p_s}\in\mathcal{S}_\lambda}\lambda_{p_s}$, while $\mathcal{S}_c$ denotes the set of successful crossover probabilities, and $\mathcal{S}_\lambda$ is the set of successful scaling factors in generating survived candidate vectors.

6) **Termination**. The evolution is terminated when either of the following two criteria is met:

C1. The pre-defined maximum number of generations $G_{\max}$ for evolution has been exhausted.

C2. There is no improvement in the *weighted-CSEP* value of the best candidate in the population for Δ_g generations.

E. Security-level of the confidential message

In general, a PHYS solution must balance the system's information reliability and information security. The secrecy capacity, which takes into account both the information reliability and information security, has been used as a fundamental metric in developing and investigating PHYS solutions. In practice, there is also a need to evaluate the system's information security separately to answer the question of how secure the confidential messages are. This motivates us to introduce the concept of security-level. As mentioned-above, the illegitimate-CSEPs $P_{E,j}^{ill(i)}(\boldsymbol{W})$, $i,j=1,2$, $i\neq j$, quantify the information security of the given PYHS TPC design $\boldsymbol{W}$. Hence, the security-level of user i for a given $\boldsymbol{W}$ can be defined as

$$L_i^{(s)}(\boldsymbol{W})=100\left(1-\left|\frac{P_{E,j}^{ill(i)}(\boldsymbol{W})}{\frac{M-1}{M}}-1\right|\right), i,j=1,2, i\neq j, \tag{36}$$

which takes a value from 0 to 100 to represent the security-level of user i from low to high. In particular, $L_i^{(s)}(\boldsymbol{W})=100$ indicates that there is no leakage at all of user i's confidential messages to user-j, and they are completely secure. By contrast, $L_i^{(s)}(\boldsymbol{W})=0$ indicates that user i's confidential messages are completely exposed to user-j's eavesdropping, since user j can correctly decode them.

The security level only considers the information security aspect of the system. The information reliability of the system is the other important consideration, which of course can be quantitatively measured by the legitimate-CSEPs. In the next section, we introduce the secure-DCMC-capacity, which is an extension to the classical security capacity, to serve as a security capacity metric of the confidential messages, by considering both the DCMC-capacity for the legitimate user's confidential message and the DCMC-capacity for the leakage of the legitimate user's confidential message to the eavesdropper.

IV. Secure MI with Discrete Input Signals

We now investigate the MI of confidential messages destined to the legitimate-user and that leaked to the illegitimate-user for M-QAM signals. For notational convenience, we also number the M constellation points of $\mathcal{S}$ given in (7) by $m=1,2,\cdots,M$. Since the M-QAM symbol points are equiprobable, the probability of $s_1(n_{r_1})$ assuming the m-th symbol point is $p\big(s_1^{(m)}(n_{r_1})\big)=\frac{1}{M}$ for $m=1,2,\cdots,M$. Similar to the set (13), given $s_1(n_{r_1})=s_1^{(m)}(n_{r_1})$ and $\boldsymbol{W}$, there are J possible values for the noise-free component of $y_1(n_{r_1})$, denoted by the set $\left\{\widetilde{\bar{y}}_1^{(j)}(n_{r_1}), 1\leq j\leq J\right\}$. The CPDF of $y_1(n_{r_1})$ conditioned on $s_1^{(m)}(n_{r_1})$ and $\boldsymbol{W}$ is given by

$$\begin{aligned} & f\left(y_1(n_{r_1})\middle|s_1^{(m)}(n_{r_1}),\boldsymbol{W}\right) \\ & = \frac{1}{2\pi J\sigma_\varepsilon^2}\sum_{j=1}^{J}\exp\left(-\frac{\left|y_1(n_{r_1})-\widetilde{\bar{y}}_1^{(j)}(n_{r_1})\right|^2}{2\sigma_\varepsilon^2}\right). \end{aligned} \tag{37}$$

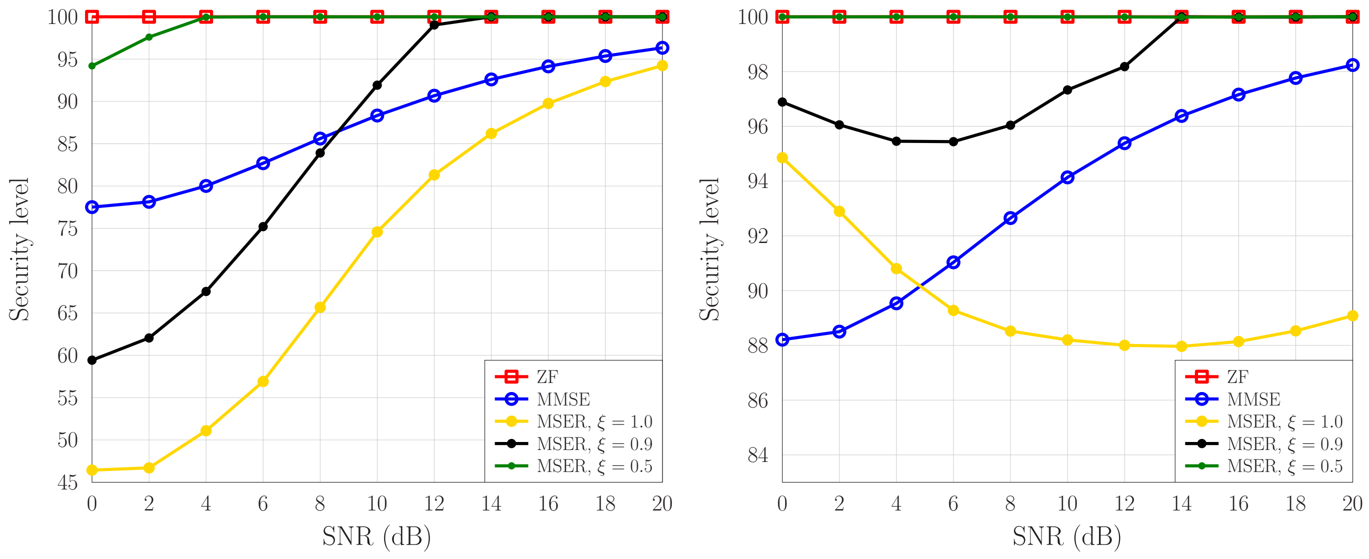
The MI $\mathcal{I}_1^{l(1)}(s_1(n_{r_1});y_1(n_{r_1}))$ then represents the DCMC capacity of the confidential message related to legitimate user 1's n_{r_1}-th antenna, which can be shown to be given by (38).

Thus the sum DCMC-capacity of confidential messages to legitimate user 1 is formulated as

$$C_{\text{DCMC},1}^{l(1)}(\boldsymbol{W})=\sum_{n_{r_1}=1}^{N_{r_1}}\mathcal{I}_1^{l(1)}\left(s_1(n_{r_1});y_1(n_{r_1})\right). \tag{39}$$

Similarly, the MI $\mathcal{I}_2^{ill(1)}\left(s_1(n_{r_1});\widetilde{y}_2(n_{r_1})\right)$ represents the DCMC capacity of the confidential message related to user 1's n_{r_1}-th antenna leaked to illegitimate user 2, which is given by (40), where the noise-free part of $\widetilde{y}_2(n_{r_1})$ given $s_1^{(m)}(n_{r_1})$ and $\boldsymbol{W}$ takes the value from the set $\left\{\widetilde{\bar{y}}_2^{(j)}(n_{r_1}), 1\leq j\leq J\right\}$, and the CPDF of $\widetilde{y}_2(n_{r_1})$ given $s_1^{(m)}(n_{r_1})$ and $\boldsymbol{W}$ takes the form

$$\begin{aligned} & f\left(\widetilde{y}^{(2)}(n_{r_1})\middle|s_1^{(m)}(n_{r_1}),\boldsymbol{W}\right) \\ & = \frac{1}{2\pi J\widetilde{\sigma}_\varepsilon^2}\sum_{j=1}^{J}\exp\left(-\frac{\left|\widetilde{y}_2(n_{r_1})-\widetilde{\bar{y}}_2^{(j)}(n_{r_1})\right|^2}{2\widetilde{\sigma}_\varepsilon^2}\right). \end{aligned} \tag{41}$$



(a) security-level of user 1

(b) security-level of user 2

Fig. 2. Comparison of the security-level performance of two users for three designs, under $K_{\text{Rice}} = 0$ and $\rho = 0$.

The sum DCMC-capacity of user 1's confidential message leaked to user 2 is then defined as

$$C^{ill(1)}_{\text{DCMC},2}(\boldsymbol{W}) = \sum_{n_{r_1}=1}^{N_{r_1}} \mathcal{I}^{ill(1)}_2 \left(s_1(n_{r_1}); \widetilde{y}_2(n_{r_1})\right). \quad (42)$$

Finally, we can define the secure-DCMC-capacity of user 1's confidential messages as

$$C^{(s)}_{\text{DCMC},1}(\boldsymbol{W}) = C^{l(1)}_{\text{DCMC},1}(\boldsymbol{W}) - C^{ill(1)}_{\text{DCMC},2}(\boldsymbol{W}). \quad (43)$$

In the same way, we arrive at the secure-DCMC-capacity of user 2's confidential messages $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W})$.

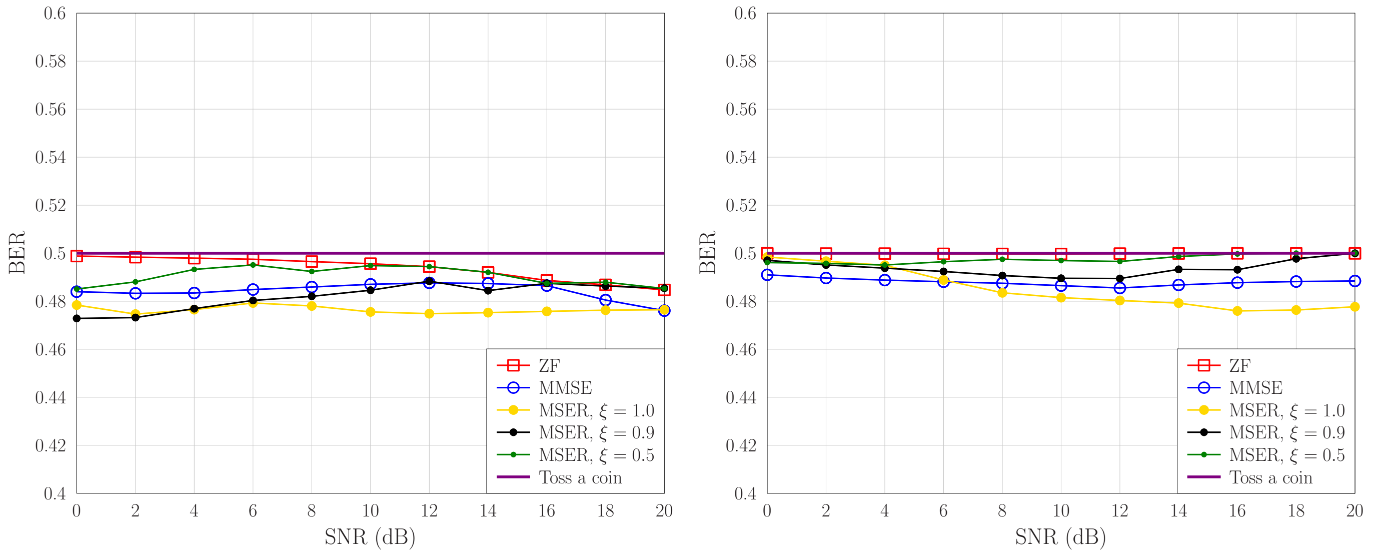
V. Simulation Results

In our investigations, the users have different numbers of RAs, to reflect practical systems where the numbers of data streams transmitted to the users can be different. Explicitly, we consider a two-user non-orthogonal based broadcast system, where the BS employs $N_t = 4$ TAs, user 1 has a single RA and user 2 is equipped with 3 RAs. The 4-QAM signaling is employed. Clearly, the security of user 1's confidential message faces a quite challenge, as the potential eavesdropper has more antennas. Simulation results are provided for evaluating the security-level, the SER of confidential messages and the secure-DCMC-capacity for the proposed priority-aware secure TPC based on the multi-objective SER optimization, denoted as MSER for short, using the ZF-based TPC [18] and the MMSE-based TPC [38] as two benchmarks. Furthermore, the impacts of some key system parameters on the achievable secure system performance are also investigated. The DEA of Subsection III-D is used to solve the optimization problem (29). The population size is set to $P_S = 100$, and the two stopping criteria are specified by $G_{\max} = 500$ and $\Delta_g = 50$.

A. The impact of priority factor

The Rician K-factor is set to $K_{\text{Rice}} = 0$, i.e., the channel is Rayleigh distributed, and the antenna correlation is set $\rho = 0$. Fig. 2 depicts the security-level performance, $L^{(s)}_1(\boldsymbol{W})$ and $L^{(s)}_2(\boldsymbol{W})$, as the functions of the user SNR for the three secure TPC schemes, where the impact of the priority factor ξ on the performance of the priority-aware MSER-based secure TPC design is also investigated. As expected, the ZF-based TPC always attains the maximum security-level, as it completely removes the leakage of the legitimate user's confidential message to the illegitimate user. By comparison, the security-level of the MMSE-based TPC is poorer and it cannot reach the maximum security-level even under high-SNR conditions, since there always exists some leakage of the legitimate user's confidential message to the eavesdropper. With $\xi = 0.5$, which means that our MSER-based TPC assigns the equal weight to minimizing the legitimate-user CSEP and to maximizing the illegitimate-user CSEP, it attains the maximum security-level for user 1 for SNR ≥ 4 dB and achieves the maximum security-level for user 2 for the whole range of SNRs tested. With $\xi = 0.9$, which means that the design weighs more heavily on information reliability than information security, our MSER design can only attain the maximum security-level for user 1 for SNR ≥ 13 dB, and it can only achieve the maximum security-level for user 2, when SNR ≥ 14 dB. Not surprisingly, with $\xi = 1.0$, which means that our MSER TPC completely ignores the maximization of the illegitimate-user CSEP, it cannot attain the maximum security-level. Also as expected, with the exception of the ZF TPC, the achievable security-level of user 1 is poorer than that of user 2 for the other two TPC designs, which simply demonstrates the fact that user 1's confidential messages are more vulnerable to leakage, since the eavesdropper, user 2, has more antennas.

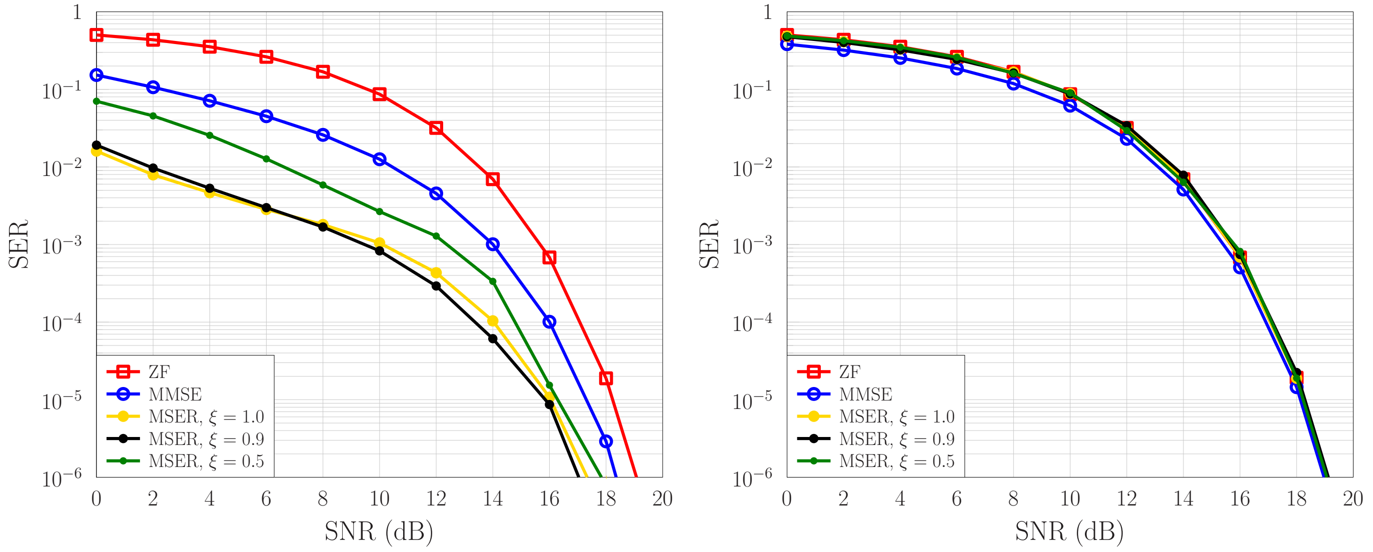
The previous simulation results confirm that the ZF-based TPC design attains the maximum information security with no leakage of the legitimate user's confidential message. The consequence of this is that the legitimate user's information bits will appear to be purely random to the eavesdropper, and regardless which eavesdropping strategy is adopted by the eavesdropper, it can only decode the legitimate user's information bits correctly with the probability close to that of



(a) BER of user 1 eavesdropping on user 2

(b) BER of user 2 eavesdropping on user 1

Fig. 3. Comparison of the BER performance of eavesdropper tempering with the other user's confidential messages for three designs, under $K_{\text{Rice}} = 0$ and $\rho = 0$.



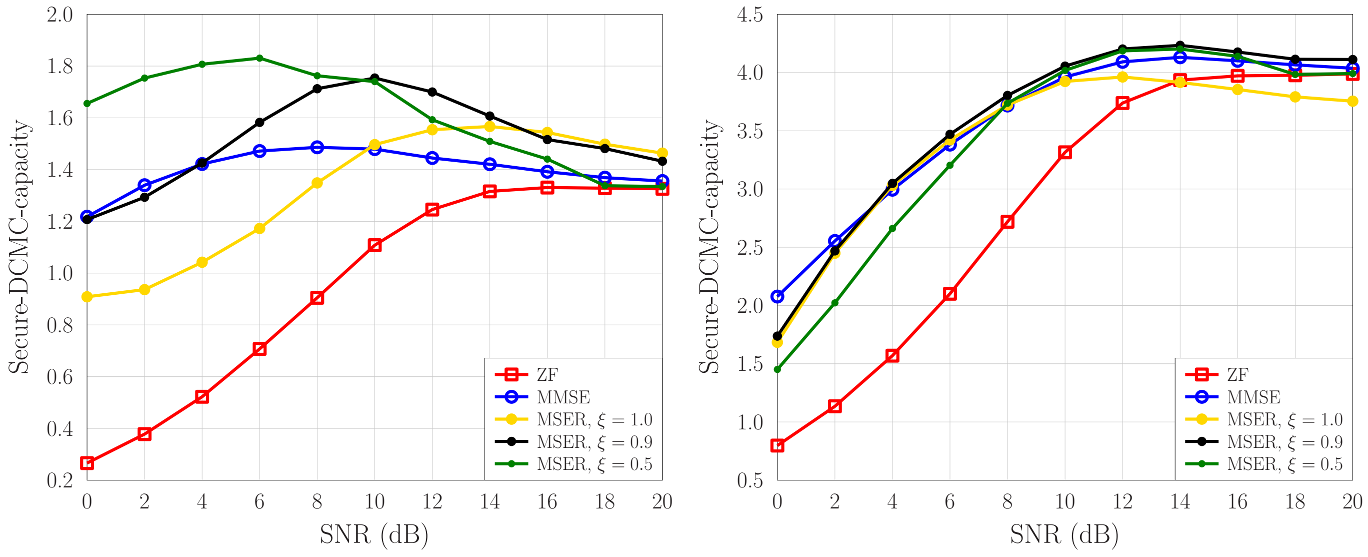
(a) SER of user 1

(b) SER of user 2

Fig. 4. Comparison of the SER performance of confidential messages for three designs, under $K_{\text{Rice}} = 0$ and $\rho = 0$.

randomly tossing a coin. In other words, in the system based on the ZF TPC, the BER of the eavesdropper tempering the other user's confidential data should be equal or very close to 0.5. Fig. 3 compares the BER performance of the eavesdropper tempering with the other user's confidential messages for the three designs. Observe from Fig. 3 that the ZF-based TPC indeed ensures that the eavesdropper has the highest BER equal or very close to 0.5 when it decodes the legitimate user's confidential message. Also from Fig. 3, it can be seen that our MSER TCP design with $\xi = 0.5$ imposes the second highest BER, also very close to the maximum BER value of 0.5, on the eavesdropper for tempering with the other user's confidential messages. This agrees with the results of Fig. 2.

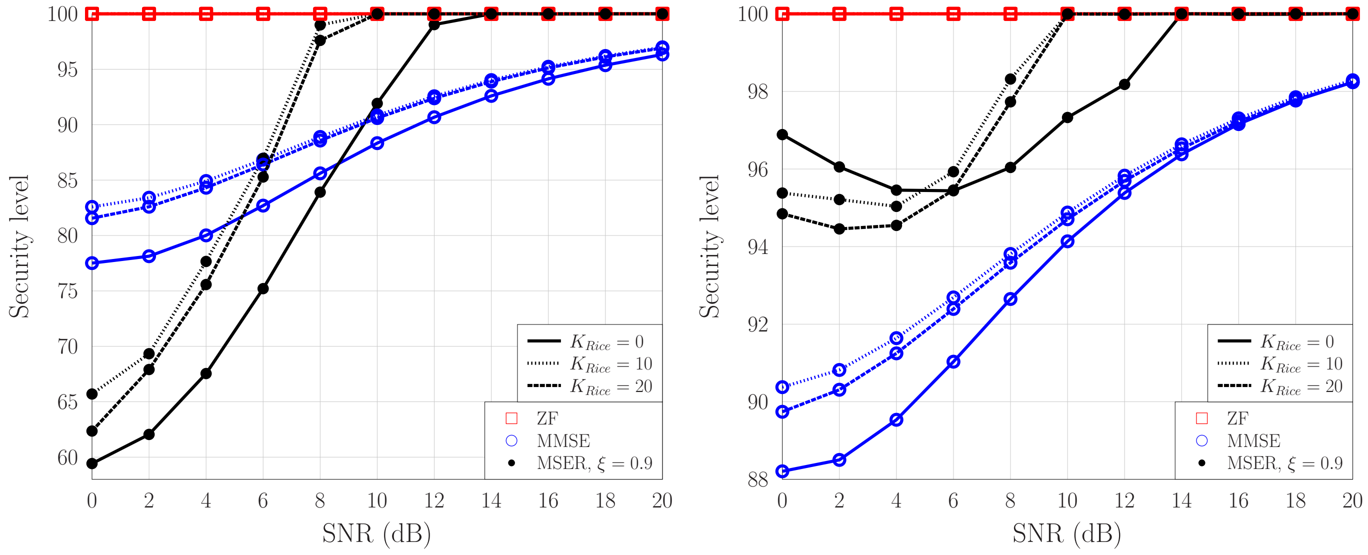
Having examined the information security of the three designs, we now turn our attention to their information reliability performance. Fig. 4 shows the achievable SER performance, $P_{E,1}^{l(1)}(\boldsymbol{W})$ and $P_{E,2}^{l(2)}(\boldsymbol{W})$, as the functions of the user SNR for the three designs. The effective MIMO system for user 1 consists of two TAs and one RA. For this type of 'overloaded' systems, the MMSE design outperforms the ZF scheme in terms of achievable SER, while our MSER design significantly outperforms the MMSE-based scheme. This is confirmed by the results of Fig. 4(a). For user 1, the SER performance of our MSER-based solutions having the priority factors of $\xi = 1.0$ and 0.9 are better than the SER associated with $\xi = 0.5$. This makes sense, since higher ξ means placing higher emphasis on minimizing the SER of the legitimate user. Also observe from Fig. 4(a) that the SER curves associated with $\xi = 1.0$ and 0.9 are very close. By contrast, the effective MIMO system for user 2 consists of two TAs and three RAs. Since the number of outputs is higher than the number of inputs, the signals are more Gaussian like and, therefore, in terms of SER, the ZF,



(a) Secure-DCMC-capacity of user 1

(b) Secure-DCMC-capacity of user 2

Fig. 5. Comparison of the secure-DCMC-capacity performance of two users for three designs, under $K_{\text{Rice}} = 0$ and $\rho = 0$.



(a) security-level of user 1

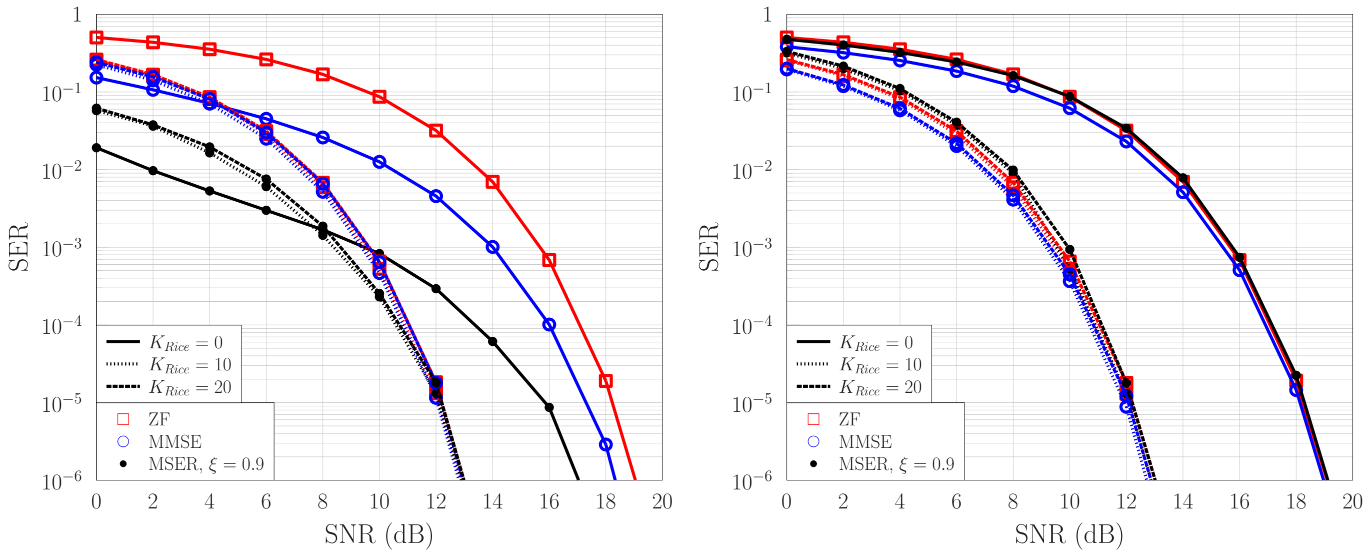
(b) security-level of user 2

Fig. 6. Comparison of the security-level performance of two users for three designs, under $\rho = 0$ and different K_{Rice}.

MMSE and MSER solutions are typically indistinguishable [24]. This is confirmed by the results of Fig. 4(b).

The secure-DCMC-capacity, which takes into account both the information reliability and information security, characterizes the overall security performance. In Fig. 5, $C^{(s)}_{\text{DCMC},1}(\boldsymbol{W})$ and $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W})$ are studied for the three designs. As expected, the results obtained confirm that the MMSE TPC attains higher secure-DCMC-capacity than the ZF TPC for both users. Observe from Fig. 5(a) that for user 1, our MSER design with $\xi = 0.5$ attains higher secure-DCMC-capacity than the MMSE design, while the MSER TPC with $\xi = 0.9$ has similar secure-DCMC-capacity to that of the MMSE TPC for SNR ≤ 5 dB, but the former has higher secure-DCMC-capacity for SNR > 5 dB. With $\xi = 1.0$, $C^{(s)}_{\text{DCMC},1}(\boldsymbol{W}_{\text{MSER}})$ is lower than $C^{(s)}_{\text{DCMC},1}(\boldsymbol{W}_{\text{MMSE}})$ for SNR < 10 dB, but becomes higher than the latter for SNR > 10 dB. Regarding user 2, it can be seen from Fig. 4(b) that with $\xi = 0.9$, $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W}_{\text{MSER}})$ is similar to $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W}_{\text{MMSE}})$. With $\xi = 1.0$, $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W}_{\text{MSER}})$ is similar to $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W}_{\text{MMSE}})$ for SNR < 10 dB but the former is lower than the latter for SNR > 10 dB. With $\xi = 0.5$, $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W}_{\text{MSER}})$ is lower than $C^{(s)}_{\text{DCMC},2}(\boldsymbol{W}_{\text{MMSE}})$ for SNR < 8 dB, but the former becomes similar to the latter when SNR > 8 dB.

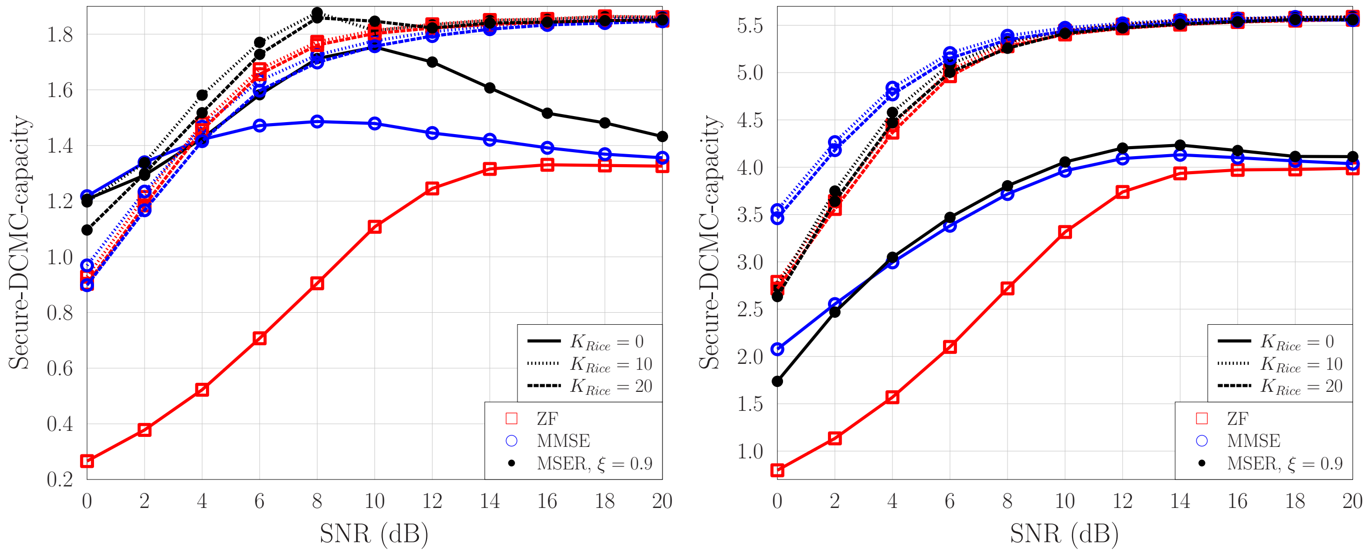
By observing the results of Figs. 2 to 5, it can be seen that for our priority-aware secure TPC design based on the multi-objective SER optimization, the priority factor of $\xi =$ 0.5 to 0.9 strikes beneficial trade-off between maximizing the security-level and minimizing the SER for the legitimate user, especially for the challenging case of user 1. Since the secure-DCMC-capacity of our MSER-based TPC design with $\xi = 0.9$ are overall better for both users than those with $\xi = 0.5$ and 1.0, in the following investigation, we set the priority factor to $\xi = 0.9$ for the MSER-based TPC.



(a) SER of user 1

(b) SER of user 2

Fig. 7. Comparison of the SER performance of confidential messages for three designs, under $\rho = 0$ and different K_{Rice}.



(a) Secure-DCMC-capacity of user 1

(b) Secure-DCMC-capacity of user 2

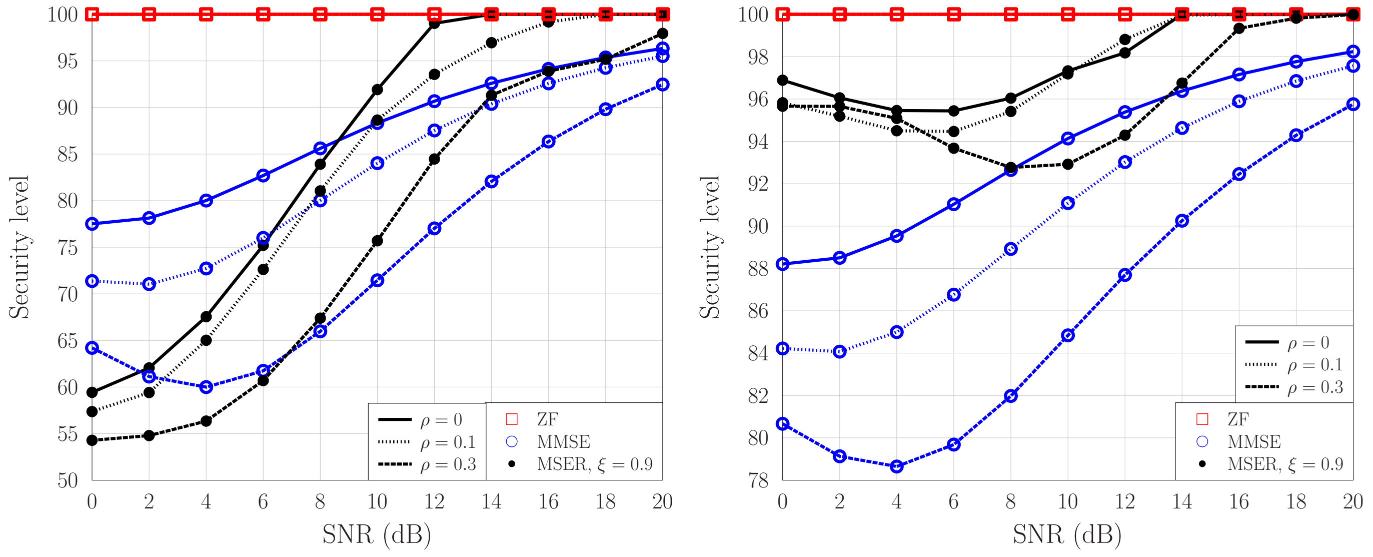
Fig. 8. Comparison of the secure-DCMC-capacity performance of two users for three designs, under $\rho = 0$ and different K_{Rice}..

B. The impact of Rician factor

By setting the antenna correlation to $\rho = 0$, we investigate the impact of Rician factor. Fig. 6 compares the security-levels of the three designs. Similar conclusions to those for Fig. 2 can be drawn. In particular, the ZF TPC always guarantees the maximum security-level of confidential messages. Our MSER TPC with the priority factor of $\xi = 0.9$ is capable of attaining the maximum security-level for sufficiently high SNRs, while the MMSE TPC is unable to attain the maximum security-level. Also for the MMSE and MSER schemes, the achievable security-level of user 1 is poorer than that of user 2. Additionally, for these two schemes, the security-levels under $K_{\text{Rice}} = 10$ and 20 are clearly better than those under $K_{\text{Rice}} = 0$. Furthermore, the $K_{\text{Rice}} = 10$ scenario is marginally better than that of $K_{\text{Rice}} = 20$.

The impact of the Rician K-factor on the achievable SER performance is depicted in Fig. 7 for the three solutions. Similar to Fig. 4, it can be seen that for user 1, our MSER design attains much better SER performance than the ZF and MMSE solutions for a given K_{Rice}. For user 2, the three solutions have similar SER performance for a given K_{Rice}. Additionally, for any of the three designs and for both users, the SER performance achieved under $K_{\text{Rice}} = 10$ and 20 are very close, and they are better than that attained under $K_{\text{Rice}} = 0$ as expected.

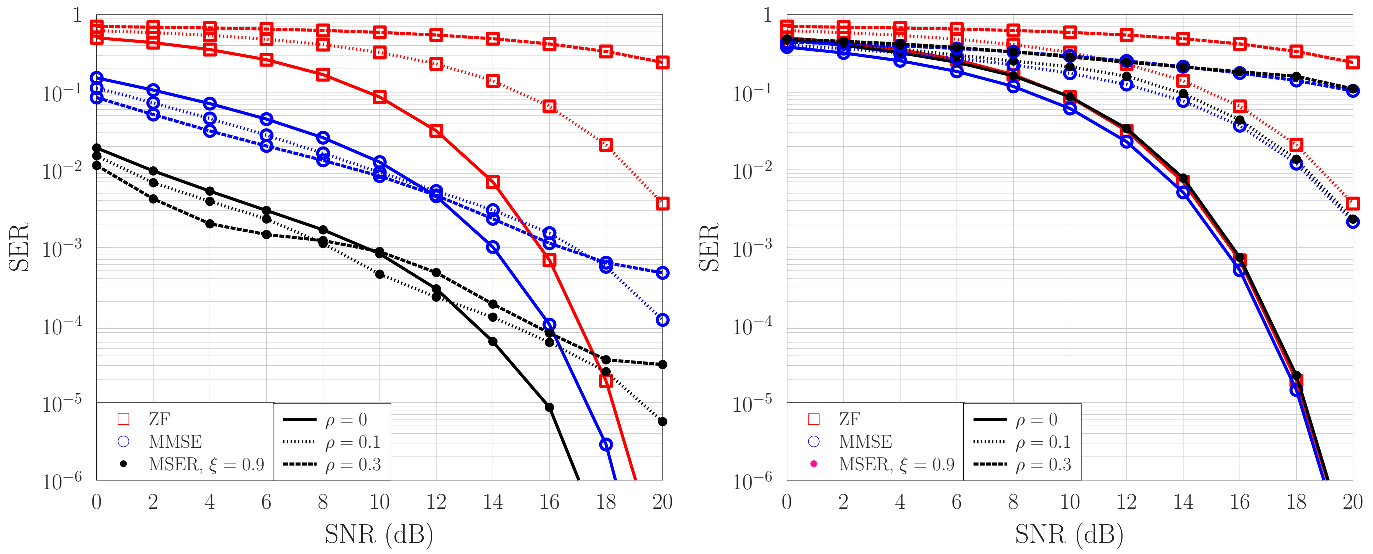
The impact of K_{Rice} on the secure-DCMC-capacity performance is investigated in Fig. 8 for the three designs. Observe from Fig. 8(a) that for user 1, the secure-DCMC-capacity of our MSER TPC is generally better than those of the MMSE and ZF solutions. Also for any of the three designs, the secure-DCMC-capacity of user 1 under $K_{\text{Rice}} = 10$ and 20 are very similar, and they are better than that attained under $K_{\text{Rice}} = 0$. The last observation is also true for user 2, as can be seen from Fig. 8(b). Also for user 2, the secure-DCMC-capacity



(a) security-level of user 1

(b) security-level of user 2

Fig. 9. Comparison of the security-level performance of two users for three designs, under $K_{\text{Rice}} = 0$ and different ρ.



(a) SER of user 1

(b) SER of user 2

Fig. 10. Comparison of the SER performance of confidential messages for three designs, under $K_{\text{Rice}} = 0$ and different ρ.

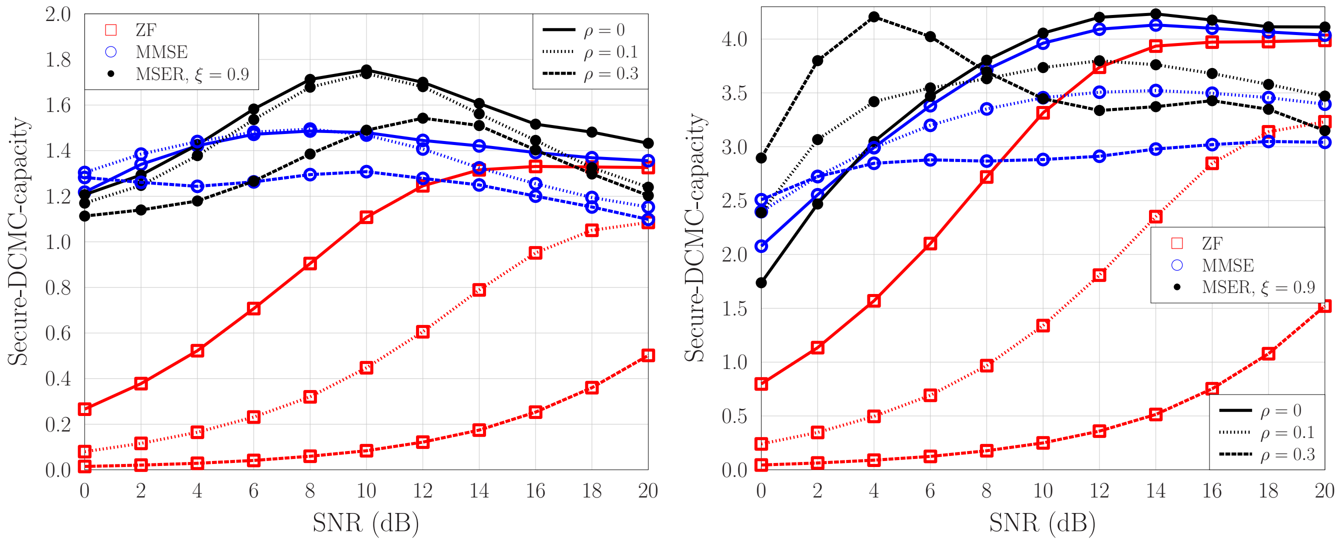
of the MMSE solution under $K_{\text{Rice}} = 10$ and 20 are better than those of the MSER and ZF designs when SNR < 8 dB. Under $K_{\text{Rice}} = 0$, which simply repeats Fig. 5(b), the MSER and MMSE solutions for user 2 exhibit similar performance, and they significantly outperform the ZF design.

C. The impact of correlation factor between antennas

With the Rician factor set to $K_{\text{Rice}} = 0$, the impact of antenna correlation ρ on the achievable security-level for the three TPC designs is studied in Fig. 9. As expected, the security-level of the ZF design is not affected by ρ, since it always attains the maximum security-level. By contrast, the correlation factor has clear impact on the MSER-based and MMSE-based solutions. For these two designs, lower ρ leads to better security-level performance. Fig. 9(a) shows that for user 1, our MSER-based TPC outperforms the MMSE-based TPC, in terms of security level, when SNR > 9 dB, while Fig. 9(b) shows that for user 2, our MSER-based TPC always achieves better security-level than the MMSE-based solution.

Fig. 10 investigates the impact of ρ on the SER performance of confidential messages for the three solutions. Generally, a higher correlation factor results in a higher SER for confidential messages. The SER performance of the ZF TPC is particularly sensitive to ρ, which degrades dramatically as ρ increases. This is in contrast to the security-level of the ZF solution, which is not affected by ρ at all. It is seen from Fig. 10(a) that for user 1, our MSER-based TPC typically outperforms the MMSE-based TPC, while the MMSE-based design significantly outperforms the ZF-based solution, in terms of the SER performance. As for user 2, Fig. 10(b) indicates that the MSER-based and MMSE-based solutions have similar SER performance, and they outperform the ZF-based design when antenna correlation exists.

The impact of the correlation factor on the secure-DCMC-



(a) Secure-DCMC-capacity of user 1

(b) Secure-DCMC-capacity of user 2

Fig. 11. Comparison of the secure-DCMC-capacity of two users for three designs, under $K_{\text{Rice}} = 0$ and different ρ.

capacity is investigated in Fig. 11. For all the three designs, generally increasing ρ leads to reduction in secure-DCMC-capacity. An exception is the MSER-based TPC for user 2 under low SNR conditions, where significantly higher secure-DCMC-capacity is achieved for higher ρ, as clearly seen from Fig. 11(b). The results of Fig. 11 show that our MSER TPC achieves significantly higher secure-DCMC-capacity than the MMSE solution for the both users, while the ZF TPC has the lowest secure-DCMC-capacity. The secure-DCMC-capacity of the ZF solution is particularly sensitive to ρ.

D. Discussions

In our proposed priority-aware TPC-aided PHYS solution based on the multi-objective SER optimization designed for the generic non-orthogonal based broadcast system, we minimize the SER of the confidential messages transmitted to the legitimate user, whilst maximizing the SER of the confidential messages leaked to the eavesdropper. In the simulation-based investigations, we compare our proposed solution to the existing ZF-based TPC and MMSE-based TPC in terms of three key metrics. Explicitly, we use the security-level of the confidential messages which is an information security metric that quantifies how secure the confidential messages are in the presence of an eavesdropper. Secondly, we employ the SER of the confidential messages which is an information reliability metric quantifies the SER of the confidential messages decoded by the legitimate user. Finally, the secure-DCMC-capacity is used which is an overall security metric that takes into account both the information reliability and information security of the system.

The security scenario of user 1 is particularly hostile, because this single-antenna user faces the potential eavesdropper, user 2, armed with more resource – three antennas. Therefore, securing the transmissions to user 1 is very challenging. Additionally, the equivalent MIMO system for user 1 is an overloaded MIMO system consisting of two TAs and one RA. Therefore, achieving the reliable transmissions to user 1 is also very challenging. It is for this type of challenging scenarios that our priority-aware design based on the multi-objective SER criterion is particularly effective. Compared to traditional secure TPC designs, such as the ZF-based TPC and the MMSE-based TPC, our design is capable of striking a flexible trade-off between minimizing the SER of the legitimate user's confidential messages and maximizing the SER of the leaked confidential messages to the eavesdropper. Consequently, it attains much better overall security performance than the ZF and MMSE designs. Specifically, the simulation results demonstrate the following:

1) In terms of security-level of confidential messages, our solution significantly outperforms the MMSE TPC, and the security-level performance of our design is much closer to that of the ZF TPC, which is known to always guarantee the maximum security-level. Our results also show that for sufficiently high SNRs, our MSER TPC attains the maximum security-level too, which means no leakage of confidential messages at all for high SNRs.
2) In terms of SER of confidential messages, as expected, our MSER design significantly outperforms the MMSE design. The SER of confidential messages for the ZF design is considerably worse than that of the MMSE design. This is because the SER of confidential messages is scarified by the ZF design in pursuit zero leakage of confidential messages. By contrast, our design strikes a flexible balance between the SER and the leakage of confidential messages.
3) In terms of overall security performance, i.e., secure-DCMC-capacity, it is well known that the MMSE TPC outperforms the ZF TPC, since the former does attempt to strike a trade-off between the SER and the leakage of confidential messages. Not surprisingly, our MSER TPC attains significantly higher secure-DCMC-capacity than the MMSE design. This confirms that our design strikes an optimal trade-off between the SER and the leakage of confidential messages, and it is capable of providing the highest overall security performance.

Compared to user 1, the security scenario of user 2 is

$$P_{E,R_1}^{(n_{r_1},z_m)}(\boldsymbol{W})=\int\limits_{z_m+1}^{+\infty} f\left(y_{R_1}(n_{r_1})\middle|s_1(n_{r_1}),\boldsymbol{W}\right)dy_{R_1}(n_{r_1})+\int\limits_{-\infty}^{z_m-1} f\left(y_{R_1}(n_{r_1})\middle|s_1(n_{r_1}),\boldsymbol{W}\right)dy_{R_1}(n_{r_1})=2P_{E,R_1}^{(n_{r_1},z_1)}(\boldsymbol{W}). \quad (44)$$

very favourable, because this three-antenna user has a weak potential eavesdropper – user 1 having only one antenna. Therefore, for each of the MSER and MMSE designs, the achievable security-level of user 2 is much higher than that of user 1. Since the equivalent MIMO system for user 2 is a two-input three-output system, the SERs of confidential messages for the three designs are typically similar. More specifically,

1) In terms of security-level of confidential messages, again the MSER-based design is closer to the ZF-based design, and it is better than the MMSE-based design.
2) In terms of SER of confidential messages, the three designs typically achieve similar performance, especially when there exists no antenna correlation. By contrast, for high antenna correlation, the performance of the ZF-based solution becomes inferior to those of the MMSE-based and MSER-based solutions.
3) In terms of secure-DCMC-capacity, the MMSE-based and MSER-based solutions are typically very close, and they considerably outperform the ZF-based TPC.

As the ZF TPC completely removes the leakage of confidential messages, its security-level is independent of both the Rician factor K_{Rice} and antenna correlation ρ for both users. But its SER of confidential messages and secure-DCMC-capacity are very sensitive to K_{Rice} and ρ. Typically, for the ZF TPC, the SER performance of legitimate user achievable under the Rayleigh channel ($K_{\text{Rice}}=0$) is considerably worse than under the Rician channel ($K_{\text{Rice}}=10$ and 20). Moreover, a higher ρ significantly degrades the achievable secure-DCMC-capacity of the ZF solution. For the MMSE and MSER solutions, the achievable security-level, SER of confidential messages and secure-DCMC-capacity are better under the Rician channel ($K_{\text{Rice}}=10$ and 20) than under the Raleigh channel ($K_{\text{Rice}}=0$). Furthermore, increasing ρ typically degrades the achievable security-level, SER of confidential messages and secure-DCMC-capacity performance for these two designs, with some exceptions to the SER and secure-DCMC-capacity of the MSER-based design under low-SNR conditions.

VI. Conclusions

In this paper, we have studied the physical layer security for a generic non-orthogonal based MIMO broadcast system from the radically new SER perspective, rather than from the classical ergodic capacity view of information theory. In particular, we have proposed a new priority-aware secure TPC design based on the multi-objective SER optimization, which is capable of striking a flexible trade-off between minimizing the SER of the legitimate user and maximizing the SER of the confidential messages leaked to the eavesdropper. To add the evaluation of various TPC based PHYS solutions for MIMO, we have introduced three metrics, namely, the security-level of confidential messages, which quantifies how secure the confidential messages remain in the presence of an eavesdropper, the standard SER of confidential messages, and the new secure-DCMC-capacity, which takes into account both the security-level and SER of confidential messages and, therefore, it quantifies the overall security performance. Our detailed analysis together with extensive simulation results have demonstrated that our proposed priority-aware MSER-based TPC outperforms the existing secure TPC designs, such as the ZF-based and MMSE-based solutions. More specifically, in terms of delivering confidential messages at a low SER, while maintaining a high security-level of confidential messages, our proposed priority-aware MSER-based TPC design has been shown to be very effective, particularly in a challenging scenario of our specific example where the eavesdropper is equipped with three receive antennas, while the legitimate user only has a single one.

Appendix

A. The average legitimate-user CSEP of user 1's confidential messages

By exploiting the shift symmetric property of the CPDF of (14), the legitimate-user CSEP of $\widehat{s}_{R_1}(n_{r_1})\neq z_m$, for $2\leq m\leq\sqrt{M}-1$, can be expressed as (44).

The legitimate-user CSEP of $\widehat{s}_{R_1}(n_{r_1})\neq z_{\sqrt{M}}$ is similarly given by

$$\begin{aligned}P_{E,R_1}^{(n_{r_1},z_{\sqrt{M}})}(\boldsymbol{W})=&\int\limits_{-\infty}^{z_{\sqrt{M}}-1} f\left(y_{R_1}(n_{r_1})\middle|s_1(n_{r_1}),\boldsymbol{W}\right)dy_{R_1}(n_{r_1})\\ =&P_{E,R_1}^{(n_{r_1},z_1)}(\boldsymbol{W}).\end{aligned} \quad (45)$$

All the legitimate constellation symbols in the M-QAM set $\mathcal{S}$ can be assumed to be equiprobable, and the average legitimate-user CSEP of $\Re\left[\widehat{s}_1(n_{r_1})\right]\neq\Re\left[s_1(n_{r_1})\right]$ is given by

$$\begin{aligned}P_{E,R_1}^{(n_{r_1})}(\boldsymbol{W})=&\frac{1}{\sqrt{M}}\sum_{m=1}^{\sqrt{M}}P_{E,R_1}^{(n_{r_1},z_m)}(\boldsymbol{W})\\ =&\frac{2\left(\sqrt{M}-1\right)}{\sqrt{M}}P_{E,R_1}^{(n_{r_1},z_1)}(\boldsymbol{W}).\end{aligned} \quad (46)$$

Similarly, the average legitimate-user CSEP of $\Im\left[\widehat{s}_1(n_{r_1})\right]\neq\Im\left[s_1(n_{r_1})\right]$ is given by

$$\begin{aligned}P_{E,I_1}^{(n_{r_1})}(\boldsymbol{W})=&\frac{1}{\sqrt{M}}\sum_{n=1}^{\sqrt{M}}P_{E,I_1}^{(n_{r_1},z_n)}(\boldsymbol{W})\\ =&\frac{2\left(\sqrt{M}-1\right)}{\sqrt{M}}P_{E,I_1}^{(n_{r_1},z_1)}(\boldsymbol{W}),\end{aligned} \quad (47)$$

where

$$\begin{aligned}P_{E,I_1}^{(n_{r_1},z_1)}(\boldsymbol{W})=&\int\limits_{z_1+1}^{+\infty} f\left(y_{I_1}(n_{r_1})\middle|s_1(n_{r_1}),\boldsymbol{W}\right)dy_{I_1}(n_{r_1})\\ =&\frac{1}{J}\sum_{j=1}^{J}Q\left(C_{I_1,n_{r_1}}^{(j,z_1)}(\boldsymbol{W})\right),\end{aligned} \quad (48)$$

with $C^{(j,z_1)}_{I_1,n_{r_1}}(\boldsymbol{W}) = \frac{(z_1+1)-\bar{y}^{(j)}_{I_1}\left(n_{r_1}\right)}{\sigma_\varepsilon}$.

Due to the constellation symmetry, $P^{(n_{r_1})}_{E,I_1}(\boldsymbol{W}) = P^{(n_{r_1})}_{E,R_1}(\boldsymbol{W})$. Then, the average legitimate-user CSEP of $\widehat{s}_1\left(n_{r_1}\right) \neq s_1\left(n_{r_1}\right)$ is readily given by

$$\begin{aligned} P^{(n_{r_1})}_{E,1}(\boldsymbol{W}) &= P^{(n_{r_1})}_{E,R_1}(\boldsymbol{W}) + P^{(n_{r_1})}_{E,I_1}(\boldsymbol{W}) - P^{(n_{r_1})}_{E,R_1}(\boldsymbol{W}) \cdot P^{(n_{r_1})}_{E,I_1}(\boldsymbol{W}) \\ &= 2P^{(n_{r_1})}_{E,R_1}(\boldsymbol{W}) - \left(P^{(n_{r_1})}_{E,R_1}(\boldsymbol{W})\right)^2 \approx 2P^{(n_{r_1})}_{E,R_1}(\boldsymbol{W}). \end{aligned} \tag{49}$$

By average $P^{(n_{r_1})}_{E,1}(\boldsymbol{W})$ over $1 \leq n_{r_1} \leq N_{r_1}$ as well as noting (46), the average legitimate-user CSEP of user 1 is readily derived in (18).

B. The illegitimate-CSEP of user 2 eavesdropping on user 1's confidential messages

The illegitimate-user CSEP of $\widehat{s}_{R_2}\left(n_{r_1}\right) \neq z_m$, $2 \leq m \leq \sqrt{M}-1$, can be derived as

$$P^{(n_{r_1},z_m)}_{E,R_2}(\boldsymbol{W}) = 2P^{(n_{r_1},z_1)}_{E,R_2}(\boldsymbol{W}). \tag{50}$$

Likewise, the illegitimate-user CSEP of $\widehat{s}_{R_2}\left(n_{r_1}\right) \neq z_{\sqrt{M}}$ is given by

$$P^{(n_{r_1},z_{\sqrt{M}})}_{E,R_2}(\boldsymbol{W}) = P^{(n_{r_1},z_1)}_{E,R_2}(\boldsymbol{W}). \tag{51}$$

Because all the symbols in the M-QAM set $\mathcal{S}$ are equiprobable, the average illegitimate-CSEP of user 2 eavesdropping on the real signal $\Re\left[s_1\left(n_{r_1}\right)\right]$ is

$$P^{(n_{r_1})}_{E,R_2}(\boldsymbol{W}) = \frac{2(\sqrt{M}-1)}{\sqrt{M}} P^{(n_{r_1},z_1)}_{E,R_2}(\boldsymbol{W}). \tag{52}$$

Since the square M-QAM constellation is symmetric between the real-part and imaginary-part, the average illegitimate-CSEP of user 2 eavesdropping on $\Im\left[s_1\left(n_{r_1}\right)\right]$ is given by

$$\begin{aligned} P^{(n_{r_1})}_{E,I_2}(\boldsymbol{W}) &= \frac{2(\sqrt{M}-1)}{\sqrt{M}} P^{(n_{r_1},z_1)}_{E,I_2}(\boldsymbol{W}) \\ &= \frac{2(\sqrt{M}-1)}{\sqrt{M}} P^{(n_{r_1},z_1)}_{E,R_2}(\boldsymbol{W}). \end{aligned} \tag{53}$$

Hence the average illegitimate-CSEP of user 2 eavesdropping on $s_1\left(n_{r_1}\right)$ can be expressed as

$$P^{(n_{r_1})}_{E,2}(\boldsymbol{W}) \approx 2P^{(n_{r_1})}_{E,R_2}(\boldsymbol{W}). \tag{54}$$

Then by averaging over $1 \leq n_{r_1} \leq N_{r_1}$, the average illegitimate-CSEP of user-2 eavesdropping on user-1's confidential messages, $P^{ill(1)}_{E,2}(\boldsymbol{W})$, is readily given in (27).

References

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[4] 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, Third Quarter 2014.

[5] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of linear precoding for secrecy in the MIMO broadcast channel," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1701–1713, Sep. 2013.

[6] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[7] A. Khisti and G. W. Wornell, "Secure transmission with multiple antenna - part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[8] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814–1825, Aug. 2015.

[9] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, First Quarter 2017.

[10] H. M. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565–2578, May 2019.

[11] S. Bashar, Z. Ding, and C. Xiao, "On secrecy rate analysis of MIMO wiretap channels driven by finite-alphabet input," *IEEE Trans. Commun.*, vol. 60, no. 12, pp. 3816–3825, Dec. 2012.

[12] S. Gong, C. Xing, S. Chen, and Z. Fei, "Secure communications for dual-polarized MIMO systems," *IEEE Trans. Signal Process.*, vol. 65, no. 16, pp. 4177–4192, Aug. 2017.

[13] Y. Cao, N. Zhao, G. Pan, Y. Chen, L. Fan, M. Jin, and M. Alouini, "Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay," *IEEE Trans. Commun.*, vol. 67, no. 8, pp. 5574–5587, Aug. 2019.

[14] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[15] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[16] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[17] H. Reboredo, J. Xavier, and M. R. D. Rodrigues, "Filter design with secrecy constraints: The MIMO Gaussian wiretap channel," *IEEE Trans. Signal Process.*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[18] K. Wang, X. Wang, and X. Zhang, "SLNR-based transmit beamforming for MIMO wiretap channel," *Wireless Personal Commun.*, vol. 71, no. 1, pp. 109–121, Jul. 2013.

[19] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. National Academy of Sciences of the USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[20] L. Dai, B. Wang, Z. Ding, Z. Wang, S. Chen, and L. Hanzo, "A survey of non-orthogonal multiple access for 5G," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2294–2323, Third Quarter 2018

[21] D. Xu, Y. Li, J. Li, H. Pan, S. Chen, and J. Crowcroft, "A survey of opportunistic offloading," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2190–2236, Third Quarter 2018.

[22] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian wiretap channels with M-PAM inputs," in *Proc. 2010 European Wireless Conf.* (Lucca, Italy), Apr. 12-15, 2010, pp. 774–781.

[23] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 527–529, Apr. 2011.

[24] S. Chen, "Adaptive minimum bit-error-rate filtering," *IEE Proc. Vision, Image and Signal Process.*, vol. 151, no. 1, pp. 76–85, Feb. 2004.

[25] S. Chen, N. N. Ahmad, and L. Hanzo, "Adaptive minimum bit error rate beamforming," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 341–348, Mar. 2005.

[26] S. Chen, A. Livingstone, and L. Hanzo, "Minimum bite-error rate design for space-time equalization-based multiuser detection," *IEEE Trans. Commun.*, vol. 54, no. 5, pp. 824–832, May 2006.

[27] S. Chen, A. Livingstone, H.-Q. Du, and L. Hanzo, "Adaptive minimum symbol error rate beamforming assisted detection for quadrature amplitude modulation," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1140–1145, Apr. 2008.

[28] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 883–894, Jun. 2012.

[29] I.-M. Kim, B.-H. Kim, and J. K. Ahn, "BER-based physical layer security with finite codelength: Combining strong converse and error amplification," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3844–3857, Sep. 2016.

[30] K. Kwon, T. Kim, and J. Heo, “Pre-coded LDPC coding for physical layer security,” *EURASIP J. Wireless Commun. and Networking*, pp. 1–18, 2016.

[31] M. A. M. Albashier, A. Abdaziz, and H. Abd. Ghani, “Performance analysis of physical layer security over different t-error correcting codes,” in *Proc. TENCON 2017* (Penang, Malaysia), Nov. 5-8, 2017, pp. 875–878.

[32] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, “Physical layer security for ultra-reliable and low-latency communications,” *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.

[33] Y. Lee, H. Jo, Y. K0, and J. Choi, “Secure index and data symbol modulation for OFDM-IM,” *IEEE Access*, vol. 5, pp. 24959–24974, 2017.

[34] W. Yao, S. Chen, and L. Hanzo, “Generalised MBER-based vector precoding design for multiuser transmission,” *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 739–745, Feb. 2011.

[35] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press: Cambridge, UK, 2005.

[36] B. Lee, J. Choi, J.-Y. Seol, D. J. Love, and B. Shim, “Antenna grouping based feedback compression for FDD-based massive MIMO systems,” *IEEE Trans. Commun.*, vol. 63, no. 9, pp. 3261–3274, Sep. 2015.

[37] C. Martin and B. Ottersten,, “Asymptotic eigenvalue distributions and capacity for MIMO channels under correlated fading,” *IEEE Trans. Wireless Commun.*, vol. 3, no. 4, pp. 1350–1359, Jul. 2004.

[38] P. I. da Cruz, R. Suyama, and M. B. Loiola, “Wireless physical-layer security using precoding and an active eavesdropper,” in *Proc. XXXV Simposio Brasileiro de Telecomunicacoes e Processamento de Sinais* (Sao Pedro, Brazil), Sep. 3-6, 2017, pp. 999–1003.

[39] E. Zitzler, L. Thiele, M. Laumanns, C. M. Fonseca, and V. G. da Fonseca, “Performance assessment of multiobjective optimizers: An analysis and review,” *IEEE Trans. Evolutionary Computation*, vol. 7, no. 2, pp. 117–132, Apr. 2003.

[40] C. A. Coello Coello, “Evolutionary multi-objective optimization: A historical view of the field,” *IEEE Computational Intelligence Magazine*, vol. 1, no. 1, pp. 28–36, Feb. 2006.

[41] S. F. Page, S. Chen, C. J. Harris, and N. M. White, “Repeated weighted boosting search for discrete or mixed search space and multiple-objective optimisation,” *Applied Soft Computing*, vol. 12, no. 9, pp. 2740–2755, 2012.

[42] K. V. Price, R. M. Storn, J. A. Lampinen, “Differential Evolution — A Practical Approach to Global Optimization”, Springer-Verlag Berlin Heidelberg 2005.

[43] A. Qin, V. Huang, P. Suganthan, “Differential evolution algorithm with strategy adaptation for global numerical optimization,” IEEE Transaction on Evolutionary Computation, vol. 13, no. 2, pp. 398–417, 2009.

[44] R. M. Storn, K. V. Price, “Differential evolution–a simple and efficient heuristic for global optimization over continuous spaces,” Journal of global optimization, vol. 11, no. 4, pp. 341–359, 1997.

[45] J. Zhang, S. Chen, X. Mu, and L. Hanzo, “Turbo multi-user detection for OFDM/SDMA systems relying on differential evolution aided iterative channel estimation,” *IEEE Trans. Commun.*, vol. 60, no. 6, pp. 1621–1633, Jun. 2012.

[46] J. Zhang, S. Chen, X. Mu, and L. Hanzo, “Benchmarking capabilities of evolutionary algorithms in joint channel estimation and turbo multi-user detection/decoding,” in *Proc. CEC 2013* (Cancun, Mexico), Jun. 20-23, 2013, pp. 3354–3362.

[47] J. Zhang, S. Chen, X. Mu, and L. Hanzo, “Evolutionary-algorithm-assisted joint channel estimation and turbo multiuser detection/decoding for OFDM/SDMA” *IEEE Trans. Veh. Technol.*, vol. 63, no. 3, pp. 1204–1222, Mar. 2014.