

Optimal Closed-Form Designs for Directional Modulation with Practical Hardware Limitations

Zhongxiang Wei, Christos Masouros, Fan Liu, and Tongyang Xu

Department of Electronic and Electrical Engineering

University College London, London, UK

{zhongxiang.wei, c.masouros, fan.liu, and tongyang.xu.11}@ucl.ac.uk

Abstract—In this paper, directional modulation (DM) is investigated to enhance physical layer security. Practical transmitter designs are exploited under imperfect channel state information (CSI) and hardware limitations, such as finite-resolution phase shifters (PSs) at transmitter. Considering the most common scenario where eavesdroppers (Eves)’ information is completely unknown, we exploit the DM design to optimize legitimate users (LUs)’ receiving performance while randomizing the Eves’ received signal. Explicitly, tailored for the practical hardware limitations and imperfect CSI in realizing DM, we design optimal precoders in closed-form with Lagrangian and Karush-Kuhn-Tucker conditions, enhancing the practicality of the symbol-level based DM. Simulation demonstrates that the algorithm achieves lower symbol error rate (SER) at the LUs while deteriorating the Eves’ SER, leading to an improved secrecy rate over the benchmarks.

Index Terms—Directional modulation, Physical layer security, Hardware impairments, Imperfect channel estimation, Interference exploitation, Closed-form design.

I. INTRODUCTION

In the past decades, beamforming and jamming have been extensively investigated in terms of physical layer (PHY) security, which acts as a complement to secure wireless communications [1]. Conventionally, confidential signal is transmitted via the channels where the legitimate users (LUs) have better transmission condition over the eavesdroppers (Eves). For example, beamforming is designed such that the received power at the LUs is maximized with low power-level of leakage towards potential Eves, or the received signal at Eves is zero-forced with reduced received power at the LUs [2]. Also, isotropic [1] or spatial [3] artificial noise (AN) can be generated together with confidential signal to jam Eves. By the conventional beamforming and jamming designs, Eves’ received signal-to-noise ratio (SNR) is indeed degraded, whereas the same information is conveyed towards undesired directions by sidelobe. Hence, assuming Eves are equipped with high sensitivity receivers, the confidential messages intended for LUs can somehow be decoded by Eves [1].

Recently, directional modulation (DM) has attracted attention as a new technique to secure wireless communications [4] from the perspective of signal processing. Differently from conventional beamforming and jamming that provide directional power scaling to address PHY security, DM designs the received symbols at the LU directly, while relying on the spatial diversity of the channel to simultaneously distort

the constellation of the same signals in all directions other than the desired ones. Moreover, in DM systems, the rate of change of the complex weights of the antenna arrays at transmitter is exactly equivalent to the symbol rate, while that of conventional beamforming is based on the rate of change of the communication channel [5]. Hence, it is more difficult for potential Eves to estimate transmitter’s behavior. In addition, the advantages of DM also lie in high cost- and power-efficiency. By DM systems, power amplifiers (PA)s and phase shifters (PS)s are used to replace the expensive and power-consuming radio frequency (RF) chains and digital-to-analogue converters (DAC)s that are required in conventional digital or hybrid beamforming designs.

As a transmitter-side technique, symbols’ modulation of DM systems happens at antenna level instead of at the baseband by conventional beamforming design, and hence received beam-pattern at LUs’ receivers is treated as a spatial complex constellation point. As a pioneer, the authors in [4] and [5] implemented parasitic antennas or actively driven antenna array with configurable phase shifters (PSs) to construct DM. Later on, bit error rate and secrecy rate were suggested for evaluating the performance of DM system in [6]. Recently, the authors generalized the concept of DM systems into millimeter wave [7], multiple-input and multiple-output (MIMO) [8], spread spectrum systems [9]. In [10], the pseudo-inverse based least-norm method was utilized for multiuser DM systems. In [11], the barrier-method was used to derive the phase-array weights of DM systems, where the phase of the received signal is relaxed based on the concept of constructive interference (CI).

Some fundamental challenges, however, need to be addressed in DM systems. *The first challenge is that*, regardless of various DM structures and optimization objectives, system performance is essentially affected by the hardware impairments and imperfect CSI acquisition. Whereas, all the aforementioned DM schemes assumed perfect channel acquisition and hardware realization, such as infinite resolution PSs and noise excluded receivers [4]- [11]. In practice, the components required for realizing infinite resolution PSs are expensive, and finite resolution PSs are more cost-effective. Also, receiving noise at LUs’ receivers also inevitably distorts the desired beam pattern, which further leads to an increased symbol error rate (SER). Unfortunately, all of these practical issues have been ignored by the aforementioned researches. *The second challenge is*

that, since DM is required to operate at symbol-level rate, the closed-form optimal design is essential for DM realization. Towards that end, the closed-form design proposed in [11] is based on barrier-method, which is only optimal given the penalty factor approaching infinity. The closed-form result proposed in [10] is simply a ZF-based transmission and does not consider quality of service (QoS) of LUs, which may lead to a poor receiving performance at LUs end. More importantly, the closed-form designs in [10] and [11] do not capture any hardware impairments and are based on perfect CSI.

To address the aforementioned outstanding issues, in this paper, we exploit closed-form DM designs with practical issues, and our contributions are summarized as:

- 1) To the best of our knowledge, it is the first work explicitly addressing the fundamental issues of DM systems for enhancing physical layer security. To be more specific, imperfect CSI acquisition, finite-resolution PSs, per-antenna power budget and receiving noise are considered in formulating the practical transmitter design.
- 2) We consider the most common scenario, where the LUs' CSI is imperfectly obtained but the potential Eves' CSI is completely unknown at the transmitter. Under the imperfect CSI and hardware impairments, we maximize the Euclidean distance in the signal constellation between the LUs' received signals and the decision thresholds and hence minimize the LUs' SER, while concurrently randomizing the Eves' received signal benefiting from the channel disparity among the LUs and Eves.
- 3) For the considered scenario, we propose a robust algorithm that is tailored for imperfect CSI and hardware limitations. The optimal results are given in closed-forms with Lagrangian and Karush-Kuhn-Tucker (KKT) conditions, enhancing the practicality of the symbol-level enabled DM systems.
- 4) Based on the concept of CI, the LUs' received symbols are designed to fall into the constructive regions while the Eves' received symbols are confined into destructive regions. Hence, higher degrees of freedom (DoFs) are endorsed for system design over the fixed phase DM design in [4]- [10].

Notations: Matrices and vectors are represented by boldface capital and lower case letters, respectively. $\|\cdot\|$ denotes the Euclidean vector norm. \mathbf{A}^H and $\text{Tr}(\mathbf{A})$ denote the Hermitian transpose and trace of matrix \mathbf{A} . $\text{diag}(\mathbf{A})$ returns a diagonal matrix with diagonal elements from matrix \mathbf{A} and $\text{diag}(\mathbf{a})$ stacks the elements of vector \mathbf{a} into a diagonal matrix. $\mathbf{A} \succeq 0$ denotes \mathbf{A} a positive semi-definite matrix. Superscript \Re and \Im denote the real and imaginary parts, respectively. \mathbf{I}_n means a n -by- n identity matrix. $\mathbb{C}^{N \times M}$ and $\mathbb{H}^{N \times M}$ denote sets of $N \times M$ matrices and Hermitian matrices with complex entries.

II. SYSTEM MODEL AND RELAXED PHASE DM

In this section, system model is demonstrated in II-A. The strict and relaxed phase based DM designs are briefly introduced II-B.

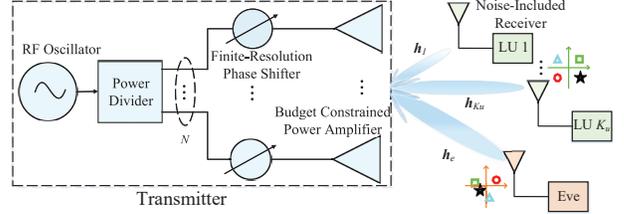


Fig. 1. Simplified system models for DM, where signal is generated by applying finite-resolution PSs and budget constrained PAs.

A. System Model

We consider DM systems with actively driven elements [11]. Assume that the transmitter is equipped with N antennas and hence the same number of PSs. There are K_u LUs and K_e non-colluded Eves, and each of them is equipped with single antenna for simplicity. The system model is depicted by Fig. 1. LUs' CSI is obtained by channel estimation in the training phase, based on channel reciprocity as in [11]. Define $\mathbf{h}_k = \hat{\mathbf{h}}_k + \mathbf{e}_k$ as the channel from the transmitter side to LU k , $\forall k \in K_u$, where $\hat{\mathbf{h}}_k \in \mathbb{C}^{1 \times N}$ and $\mathbf{e}_k \in \mathbb{C}^{1 \times N}$ denote the estimated CSI and estimation error, respectively. By classic channel estimation approaches, such as minimum mean square error (MMSE), the element of the error vector can be modeled by a Gaussian distributed variable as $[e_k]_n \sim \mathcal{CN}\{0, \sigma_e^2\}$, $\forall n \in N$, with variance σ_e^2 . Eves' CSI is assumed to be completely unknown [11]. Define $\phi \in \mathbb{C}^{N \times 1}$ as the PS design while $\mathbf{p} \in \mathbb{C}^{N \times 1}$ as transmission power at the transmitter side. We consider a practical finite resolution PSs and per-antenna power budget. Let $\mathbb{F} = \{1, \phi, \phi^2, \dots, \phi^{n_{ps}-1}\}$ denote the set of available phase and $\phi = e^{j2\pi/n_{ps}}$. $n_{ps} = 2^b$ is the number of realizable phase angles and b is the number of bits in the resolution of PSs. Hence, the received signal at LU k can be written as

$$y_k = \mathbf{h}_k(\phi \circ \mathbf{p}) + n_k, \quad \forall k \in K_u, \quad (1)$$

where operator \circ denotes the pair-wise Hadamard product. n_k denotes the receiving noise at LU k , following Gaussian distribution such that $n_k \sim \mathcal{CN}(0, \sigma_n^2)$, $\forall k \in K_u$. Evidently, by considering finite-resolution PSs, we need to ensure that $\phi(n) \in \mathbb{F}$, $\forall n \in N$.

B. Strict and Relaxed Phase based DM

1) *Strict Phase based DM Design:* By the strict-phase based DM systems in Fig. 2(a), the received signal should have exactly same phase and amplitude of the desired symbol of LUs, such as $[\hat{\mathbf{h}}_1(\phi \circ \mathbf{p}), \hat{\mathbf{h}}_2(\phi \circ \mathbf{p}), \dots, \hat{\mathbf{h}}_{K_u}(\phi \circ \mathbf{p})] = [\sqrt{\gamma}s_1, \sqrt{\gamma}s_2, \dots, \sqrt{\gamma}s_{K_u}]$, where s_k denotes the desired symbol for LU k and $\sqrt{\gamma}$ denotes the desired amplitude that relates to LUs' SNR requirement. Since the phase needs to be aligned with that of the desired symbols, the strict phase decreases the DoFs and consequently the LUs' receiving performance.

2) *Relaxed Phase based DM Design:* Based on concept of CI, the received signal is not necessary to be aligned with the intended symbols, but is pushed away from the detection

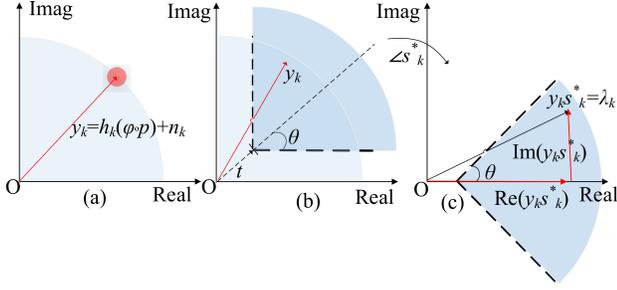


Fig. 2. QPSK for illustration. (a) Conventional fixed phase DM design. (b) Relaxed phase DM design, where the received signal y_k falls into constructive region (dark blue area). (c) After rotation by $\angle s_k^*$, $\Re\{y_k s_k^*\}$ and $\Im\{y_k s_k^*\}$ are mapped on real and imaginary axis, according to the trigonometry.

thresholds of the signal constellation. Furthermore, the LUs can still correctly detect the received signal with the increased DoFs at the transmitter [12]. The CI concept has been thoroughly discussed in the recent literature, and to avoid extensive repetition we refer the readers to [3] for details. According to the geometrical interpretation in Fig. 2(b), a constructive region (dark blue area) for the received signal on each LU is given, for the example of QPSK modulation. The constructive area of the constellation is defined as the area where the distances from the decision thresholds are increased. By rotating the received signal y_k and mapping it into real and imaginary parts, as shown in Fig. 2(c), the received signal of LU k falling into constructive regions is equivalent to satisfying the CI constraint $|\Im\{(\mathbf{h}_k(\phi \circ \mathbf{p}) + n_k)s_k^*\}| \leq (\Re\{(\mathbf{h}_k(\phi \circ \mathbf{p}) + n_k)s_k^*\} - t)\tan\theta$, where s_k is the desired symbol of LU k and superscript $*$ denotes its conjugate. $\theta = \frac{\pi}{M}$, where M denotes the constellation size. Physically, a larger value of t pushes the constructive region away from the detection threshold. Hence, lower SER at the LUs and higher robustness against hardware impairments are presented. However, due to the uncertainty of estimation error and receiving noise, the inequality above may not be always satisfied with the finite resolution of PSs, imperfect CSI and per-antenna power budget. Hence, we write it in a probabilistic manner as

$$\Pr\{|\Im\{(\mathbf{h}_k(\phi \circ \mathbf{p}) + n_k)s_k^*\}| \leq (\Re\{(\mathbf{h}_k(\phi \circ \mathbf{p}) + n_k)s_k^*\} - t)\tan\theta\} \geq \Gamma, \quad (2)$$

where Γ is the probability threshold of satisfying the CI constraint. Evidently, Γ can be set to a high value, indicating the CI constraint is satisfied with high probability.

III. CLOSED-FORM DM DESIGN UNDER IMPERFECT CSI AND HARDWARE LIMITATIONS

In a number of practical scenarios, Eves' CSI is unknown, since passive Eves only intercept confidential messages but do not actively launch attack. Hence, in this section, we investigate DM design without knowledge of the Eves' CSI.

A. Problem Formulation

We target to maximize the value of t , subject to multiple constraints. As discussed, t physically represents the Euclidean distance in the signal constellation between the LUs' received

signals and the decision thresholds. Hence, maximizing t can optimize receiving performance at the LUs and improve robustness against hardware impairments and imperfect CSI. Hence, the optimization is given as

$$\begin{aligned} P1 : & \operatorname{argmax}_{\phi, \mathbf{p}} t, \\ \text{s.t. } & (C1) : \Pr\{|\Im\{(\mathbf{h}_k(\phi \circ \mathbf{p}) + n_k)s_k^*\}| \leq \\ & (\Re\{(\mathbf{h}_k(\phi \circ \mathbf{p}) + n_k)s_k^*\} - t)\tan\theta\} \geq \Gamma, \forall k \in K_u, \\ & (C2) : \mathbf{p}^H \mathbf{A}_n \mathbf{p} \leq p_{max}, \forall n \in N, \quad (C3) : \phi(n) \in \mathbb{F}, n \in N, \end{aligned} \quad (3)$$

where p_{max} denotes the per-antenna transmission power budget. $\mathbf{A}_n = \operatorname{diag}\{\underbrace{0, \dots, 0}_{n-1}, 1, \underbrace{0, \dots, 0}_{N-n}\}$, $\forall n \in N$, is an auxiliary

matrix. Evidently, constraint (C1) probabilistically guarantees that the received signal at each LU falls into the desired detectable constellation region, considering the effect of imperfect CSI and hardware constraints. Constraint (C2) constrains the maximum transmission power at each antenna lower than the constraint p_{max} , while constraint (C3) denotes that the phase of all the PSs is only from the finite set \mathbb{F} . Note that no explicit secrecy constraint is considered in P1. It is because desired symbols are only dedicatedly designed for the LUs, and the received signal of potential Eves is randomized across the constellation panel due to channel disparity, which is the design principle of DM systems.

B. Optimization Solution

In this subsection, we propose a closed-form result to enhance the practicality of DM systems. The optimization problem P1 involves infinite possibilities of receiving noise and CSI estimation error, as well as finite choice of phase design. To access the optimization problem, we first handle constraint (C1). Decomposing constraint (C1) yields

$$\Pr\{|\Im\{(\tilde{\mathbf{h}}_k + \mathbf{e}_k)(\phi \circ \mathbf{p})s_k^*\} + \Im\{n_k s_k^*\}| \leq (\Re\{(\tilde{\mathbf{h}}_k + \mathbf{e}_k)(\phi \circ \mathbf{p})s_k^*\} + \Re\{n_k s_k^*\} - t)\tan\theta\} \geq \Gamma, \quad (4)$$

for $\forall k \in K_u$. It is observed that the linear combination of $\Im\{n_k s_k^*\}$, $\Re\{n_k s_k^*\}$, $\Im\{\mathbf{e}(\phi \circ \mathbf{p})s_k^*\}$, and $\Re\{\mathbf{e}(\phi \circ \mathbf{p})s_k^*\}$ still follow Gaussian distribution with a modified variance. Hence, we collect all the above uncertainty related terms in to a variable \bar{n}_k , and (4) is given as

$$\begin{cases} \Pr\{\Im\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} \leq (\Re\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} - t)\tan\theta + \bar{n}_k\} \geq \Gamma, \\ \Pr\{-\Im\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} \leq (\Re\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} - t)\tan\theta + \bar{n}_k\} \geq \Gamma, \end{cases} \quad (5)$$

$\forall k \in K_u$. $\bar{n}_k \sim \mathcal{CN}(0, (1 + \tan^2\theta)(\frac{N\sigma_e^2|\phi \circ \mathbf{p}|_2^2}{2} + \frac{\sigma_n^2}{2}))$. Intuitively, in P1 we try to maximize the value of t , and hence the transmitters need to dissipate all the transmission power p_{max} . As a result, the distribution of \bar{n}_k can be approximately written as $\mathcal{CN}(0, (\frac{N^2\sigma_e^2 p_{max} + \sigma_n^2}{2\cos^2\theta}))$, and the two inequalities in (5) can be seen as cumulative distribution function (cdf) of a Gaussian distributed variable. Normalizing the variance of \bar{n}_k and defining $\Phi^{-1}(\cdot)$ as the inverse cdf of a standard Gaussian variable, we have

$$\begin{cases} \Im\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} \leq (\Re\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} - t)\tan\theta - \Theta, \\ -\Im\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} \leq (\Re\{\tilde{\mathbf{h}}_k(\phi \circ \mathbf{p})s_k^*\} - t)\tan\theta - \Theta, \end{cases} \quad (6)$$

where $\Theta = \frac{\Phi^{-1}(\Gamma)\sqrt{N^2\sigma_2^2p_{max}+\sigma_n^2}}{\sqrt{2\cos\theta}}$. Now the probabilistic constant (C1) has been transformed into robust constraints in (6).

Evidently, the pair-wise Hadamard product of ϕ and \mathbf{p} serves as an equivalent transmission vector. Hence, define an equivalent transmission vector $\mathbf{x} = \phi \circ \mathbf{p}$. We then introduce auxiliary variables $\lambda_k = \tilde{\mathbf{h}}_k \mathbf{x} s_k^*$, $\forall k \in K_u$. λ_k physically represents the rotated received signal $y_k s_k^*$, as depicted in Fig. 2(c). Then the optimization P1 can be equivalently written as

$$\begin{aligned} P2 : \underset{\mathbf{x}}{\operatorname{argmax}} \quad & t, \\ \text{s.t. } (\tilde{C}1) : & |\Im\{\lambda_k\}| \leq (\Re\{\lambda_k\} - t)\tan\theta - \Theta, \quad \forall k \in K_u, \\ (C2) : & \mathbf{x}^H \mathbf{A}_n \mathbf{x} \leq p_{max}, \quad \forall n \in N, \\ (C3) : & \phi(n) \in \mathbb{F}, n \in N, \quad (C4) : \lambda_k = \tilde{\mathbf{h}}_k \mathbf{x} s_k^*, \quad \forall k \in K_u, \end{aligned} \quad (7)$$

Note that the term $\tilde{\mathbf{h}}_k \mathbf{x} s_k^*$ has been replaced by λ_k , $\forall k \in K_u$. The next difficulty lies in the combination constraint (C3) due to the finite-resolution of PSs and (C2) due to per-antenna power constraint. To obtain a closed-form result, we can replace the per-antenna constraint in (C2) by a total power constraint such that $\mathbf{x}^H \mathbf{x} \leq Np_{max}$. After obtaining the closed-form result, the power on each antenna violating the individual power constraint will be reduced to its maximal power p_{max} to satisfy the original power constraint in (C2). For the finite-resolution constraint of PSs, we can first solve the optimization problem P2 without constraint (C3), and then quantize the obtained result to the closest point in the feasible set \mathbb{F} to address the finite-resolution constraint. Now, we can write the Lagrangian of transformed version of P2 as

$$\begin{aligned} L = & -t + \sum_{k=1}^{K_u} \mu_k [\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta] + \\ & \sum_{k=1}^{K_u} v_k [-\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta] + \\ & \mu_0 (\mathbf{x}^H \mathbf{x} - Np_{max}) + \delta_k \sum_{k=1}^{K_u} (\tilde{\mathbf{h}}_k \mathbf{x} s_k^* - \lambda_k), \end{aligned} \quad (8)$$

where μ_k, v_k, μ_0 and δ_k are Lagrangian multipliers. Taking derivative L with respect \mathbf{x} , we have

$$\frac{\partial L}{\partial \mathbf{x}} = \sum_{k=1}^{K_u} (\delta_k \tilde{\mathbf{h}}_k s_k^*) + \mu_0 \mathbf{x}^H = 0, \quad (9)$$

which further yields $\mathbf{x} = \sum_{k=1}^{K_u} (s_k \tilde{\mathbf{h}}_k^H \gamma_k)$ with $\gamma_k = -\frac{\delta_k}{\mu_0}$, $\forall k \in K_u$. Now, we write \mathbf{x} in a compact form as $\mathbf{x} = \tilde{\mathbf{H}}^H (\mathbf{Y} \circ \mathbf{s})$, where $\tilde{\mathbf{H}}^H = [\tilde{\mathbf{h}}_1^H, \tilde{\mathbf{h}}_2^H, \dots, \tilde{\mathbf{h}}_{K_u}^H]$ and $\mathbf{Y} = [\gamma_1, \gamma_2, \dots, \gamma_{K_u}]^T$. Also, constraint (C4) can be written in a compact form as $\tilde{\mathbf{H}}(\mathbf{x} \circ \mathbf{s}^*) = \mathbf{\Lambda}$, where $\mathbf{\Lambda} = [\lambda_1, \lambda_2, \dots, \lambda_{K_u}]^T$. Based on the two compact forms, we finally obtain the closed-form of optimal \mathbf{x}^* as

$$\mathbf{x}^* = \tilde{\mathbf{H}}^H (\tilde{\mathbf{H}} \tilde{\mathbf{H}}^H)^{-1} \mathbf{\Lambda} \circ \mathbf{s}, \quad (10)$$

which indicates the vector \mathbf{x} is related to the LUs' intended symbols \mathbf{s} and channel $\tilde{\mathbf{H}}$, which is completely different from conventional precoding design that the precoding vector is only related to channel but independent from the desired symbols.

Since the estimated LUs' channel $\tilde{\mathbf{H}}$ and the intended symbols \mathbf{s} are known by the transmitter, the closed-form of optimal \mathbf{x}^* is directly obtained with known value of $\mathbf{\Lambda}$, which can be simply calculated by solving the dual problem of P2. As suggested in Eq. (10), we now present how to find the optimal value of $\mathbf{\Lambda}$ to yield \mathbf{x}^* . Based on the fact that $\mu_0 > 0$, substituting (10) into constraint (C2) yields $\mathbf{\Lambda}^H \mathbf{T} \mathbf{\Lambda} = Np_{max}$, where $\mathbf{T} = \operatorname{diag}(\mathbf{s}^H) (\tilde{\mathbf{H}} \tilde{\mathbf{H}}^H)^{-1} \operatorname{diag}(\mathbf{s})$. Since the elements of $\mathbf{\Lambda}$ and \mathbf{T} are complex variables, we separate and stack their real and imaginary parts into new variables $\hat{\mathbf{\Lambda}}$ and $\hat{\mathbf{T}}$, such that $\hat{\mathbf{\Lambda}} = [\Re\{\mathbf{\Lambda}^T\}, \Im\{\mathbf{\Lambda}^T\}]^T$ and $\hat{\mathbf{T}} = \begin{bmatrix} \Re\{\mathbf{T}\} & -\Im\{\mathbf{T}\} \\ \Im\{\mathbf{T}\} & \Re\{\mathbf{T}\} \end{bmatrix}$. It is easy to prove the validation of $\hat{\mathbf{\Lambda}}^T \hat{\mathbf{T}} \hat{\mathbf{\Lambda}} = Np_{max}$. Since the effect of constraint (C4) has been captured in (10), constraint (C4) can be omitted from the equivalent problem of P2 as

$$P3 : \underset{\mathbf{\Lambda}}{\operatorname{argmax}} \quad t, \text{ s.t. } (\tilde{C}1), (C5) : \hat{\mathbf{\Lambda}}^T \hat{\mathbf{T}} \hat{\mathbf{\Lambda}} = Np_{max}, \quad (11)$$

whose Lagrangian can be written as

$$\begin{aligned} L = & -t + \hat{a}_0 (\hat{\mathbf{\Lambda}}^T \hat{\mathbf{T}} \hat{\mathbf{\Lambda}} - Np_{max}) + \\ & \sum_{k=1}^K \hat{\mu}_k [\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta] + \\ & \sum_{k=1}^K \hat{v}_k [-\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta]. \end{aligned} \quad (12)$$

For simplicity, we introduce a vector $\boldsymbol{\eta}$ to stack the Lagrangian multipliers such as $\boldsymbol{\eta} = [\hat{\mu}_1, \dots, \hat{\mu}_{K_u}, \hat{v}_1, \dots, \hat{v}_{K_u}]^T$ and introduce an auxiliary matrix $\mathbf{S} = \begin{bmatrix} \mathbf{I} & -\frac{\mathbf{I}}{\tan\theta} \\ \mathbf{I} & \frac{\mathbf{I}}{\tan\theta} \end{bmatrix}$ with the identify matrix $\mathbf{I}_{K_u \times K_u}$. Taking derivative L with respect to $\hat{\mathbf{\Lambda}}$, we have

$$\frac{\partial L}{\partial \hat{\mathbf{\Lambda}}} = 2\hat{a}_0 \hat{\mathbf{T}} \hat{\mathbf{\Lambda}} - \mathbf{S}^T \boldsymbol{\eta} = 0. \quad (13)$$

Substituting it into (C5) yields $\hat{a}_0 = \frac{\sqrt{\boldsymbol{\eta}^T \mathbf{V}^{-1} \boldsymbol{\eta}}}{4Np_{max}}$, where $\mathbf{V}^{-1} = \mathbf{S}^T \hat{\mathbf{T}}^{-1} \mathbf{S}^T$. Since P3 is a convex optimization problem and its strong duality holds, its dual problem is given as

$$\begin{aligned} P4 : \max_{\boldsymbol{\eta}} \quad & \hat{a}_0 (\hat{\mathbf{\Lambda}}^T \hat{\mathbf{T}} \hat{\mathbf{\Lambda}} - Np_{max}) + \mathbf{1} \boldsymbol{\eta} \Theta - \boldsymbol{\eta}^T \mathbf{S} \hat{\mathbf{\Lambda}}, \\ & = -\sqrt{Np_{max} \boldsymbol{\eta}^T \mathbf{V}^{-1} \boldsymbol{\eta}} - \Theta, \\ \text{s.t. } & \mathbf{1} \boldsymbol{\eta} = 1, \boldsymbol{\eta} \geq 0, \end{aligned} \quad (14)$$

where $\mathbf{1}$ is a row vector and all elements equal to 1. Since the square root operation in the objective function is monotonic and the second term is a constant. The optimization problem has the same optimal result as follows

$$P5: \min_{\boldsymbol{\eta}} \boldsymbol{\eta}^T \hat{\mathbf{V}}^{-1} \boldsymbol{\eta}, \text{ s.t. } \mathbf{1}\boldsymbol{\eta} = 1, \boldsymbol{\eta} \geq 0, \quad (15)$$

which is a simple quadratic optimization problem over a simplex. It has already been shown in the existing literature that quadratic optimization can be efficiently solved and its convergence can be easily guaranteed with existing solvers [13]. When obtaining the optimal value of $\boldsymbol{\eta}$ by solving P5, the value of \mathbf{A} is naturally obtained, and also the value of vector \mathbf{x}^* is confirmed.

Now, we are able to devise the whole algorithm, namely robust closed-form DM (Robust-cf-DM). The optimal transmission vector \mathbf{x}^* is obtained by solving the simple quadratic optimization problem in P5. Afterwards, the power of each antenna violating the individual power constraint will be reduced to its maximal power p_{max} . Finally, we map it to the closest point in the feasible set \mathbb{F} for the consideration of finite-resolution PSs. Hence, the final phase design is given as

$$\hat{\phi}(n) = \mathbb{Q}\left(\frac{\mathbf{x}^*(n)}{|\mathbf{x}^*(n)|_2}\right), \quad \forall n \in N, \quad (16)$$

where the operator $\mathbb{Q}(\cdot)$ maps a complex unit-norm variable to the nearest point in the set \mathbb{F} .

IV. SECURITY PERFORMANCE AND COMPLEXITY

In this section, we first discuss the PHY security performance, and then present the analytical complexity of the proposed algorithm.

A. Receiving Performance at Potential Eves

Since potential Eves' CSI is unknown at the transmitter, PHY security may not be explicitly guaranteed, which is a common scenario for the PHY security designs in DM systems [4]- [11] and conventional DBF/HBF systems [1] [14]. That is, PHY security is addressed benefiting from the channel's disparity among the LUs and Eves, where the received symbols of the Eves are naturally randomized.

For clarification, let us write the e -th Eve's channel \mathbf{g}_e in the form of $\mathbf{g}_e = \sqrt{\rho}\mathbf{h}_k + \sqrt{1-\rho}\boldsymbol{\epsilon}$. The parameter $\rho \in [0, 1]$ measures the strength of the channel correlation between the k -th LU and e -th Eve's channels and $\boldsymbol{\epsilon} \in \mathbb{C}\mathcal{N}(0, \mathbf{I}_N)$ is a random vector independent of \mathbf{h}_k . In particular, $\rho = 0$ means the k -th LU and e -th Eve's channels are independent. Hence, the received signal at the e -th Eve can be calculated as $y_e = \sqrt{\rho}\mathbf{h}_k^T \mathbf{x} + \sqrt{(1-\rho)}\boldsymbol{\epsilon}^T \mathbf{x} + n_e$, where \mathbf{x} denotes the equivalent transmitting vector and n_e denotes the receive of noise at the e -th Eve. In fact, the first term represents the symbol of interest that tailored for the k -th LU while the second term is a random vector varying at the symbol level. Hence, the random term $\sqrt{(1-\rho)}\boldsymbol{\epsilon}^T \mathbf{x}$ can be used to randomize the Eve's received signal and thus deteriorate the Eve's signal detection. To this end, the power of $\sqrt{(1-\rho)}\boldsymbol{\epsilon}^T \mathbf{x}$ needs to be large enough to guarantee sufficient randomization to the phase of the Eve's received signal. With unknown $\boldsymbol{\epsilon}$, the average power of $\boldsymbol{\epsilon}^T \mathbf{x}$ can be approximated as $\mathbb{E}\{|\boldsymbol{\epsilon}^T \mathbf{x}|^2\} \approx \text{Tr}(\mathbf{x}^H \mathbb{E}\{\boldsymbol{\epsilon}\boldsymbol{\epsilon}^H\}\mathbf{x}) = \|\mathbf{x}\|^2$. Since we intend to maximize the Euclidean distance t in the

TABLE I
COMPLEXITY ANALYSIS WITH ACCURACY FACTOR τ , WHERE $n_1 = \mathcal{O}(N)$
AND $n_2 = \mathcal{O}(2K_u)$.

Closed-form DM	$\ln[\frac{1}{\tau}]\sqrt{2}[2n_2 + 2n_2^2 + n_2^3] + \mathcal{O}(N)$
Barrier method DM [11]	$\ln(\frac{1}{\tau})\sqrt{2K_u n_1}[2K_u + 2n_1 K_u + n_1^2] + \mathcal{O}(N)$
Least-norm DM [10]	$24K_u^3 + 16K_u^2 N + K_u + 2K_u N + 8K_u^2 N$

signal constellation between the LUs' received signals and the decision thresholds, a high power $\|\mathbf{x}\|^2$ will be utilized at transmitter side in the optimizations. That is to say, the beam leakage $\boldsymbol{\epsilon}^T \mathbf{x}$ is maximized under the available power budget and acts as the null-space AN to jam the Eve in a statistical manner.

B. Complexity Analysis

In this section, the computational complexities of the proposed algorithms are compared with the mostly related works in [10] and [11]. For the proposed algorithm, its complexity is closely related to solving the optimization problem P5, which is subject to 2 linear constraint only. For the least-norm DM [10], its complexity is dominated by generating the pseudo-inverse matrix of equivalent multiuser MISO channel \mathbf{H} . The pseudo-inverse matrix can be obtained by the conventional SVD approach or Cholesky decomposition [15]. The overall complexities of the algorithms are summarized in TABLE I. It is observed that the complexity of the proposed algorithm goes as low as that of SVD or Cholesky decomposition, which have been extensively used in practical ZF/MMSE precoding due to its low computational complexity.

V. SIMULATION RESULTS

We present the simulated performance in this section. The central frequency is set to 2 GHz with 1 MHz bandwidth. Per-antenna transmission power budget is $p_{max} = 10$ dBm. The numbers of antennas and PSs are set to $N = 5$ at the transmitter. Without loss of generality, we adopt QPSK modulation and assume that there are $K_u = 4$ LUs and $K_e = 1$ Eves. The intended symbols for the LUs are randomly generated. LDPC coding chain in the 5G new radio and CRC are employed with 3/4 coding rate. The variance of noise is set to $\sigma_n^2 = 10^{-3}$. LUs' probabilistic threshold for guaranteeing SINR requirement is set to $\Gamma = 0.99$. CSI estimation error is set to $\sigma_e^2 = 10^{-4}$. Besides, the most related DM designs, least-norm based [10] and barrier-method based [11], are selected as benchmarks. For fair comparison, the optimal PS and power designs of [10] and [11] are subsequently mapped by Eq. (16) considering the infinite-resolution of PSs.

In Fig. 3, it can be observed that the proposed algorithm achieves the lowest SER performance and the LUs' SER is always maintained at a low level with different resolutions of PSs, demonstrating a strong robustness against hardware limitations and imperfect CSI. As comparisons, the two benchmarks show much higher SER compared to our proposed algorithm. In particular, the barrier method DM [11] shows the worst SER performance, since it aims to allocate the received signals of

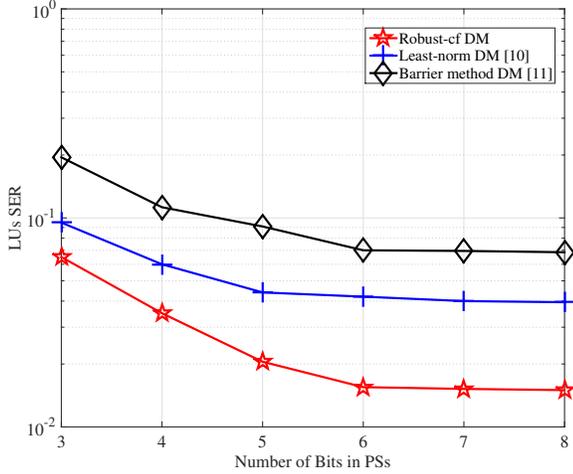


Fig. 3. SER performance comparisons with different resolutions of PSs.

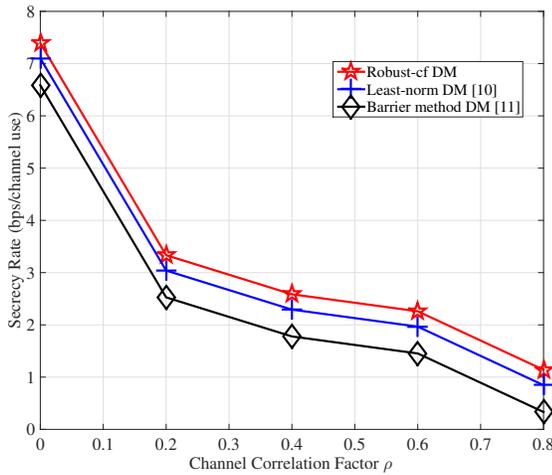


Fig. 4. Secrecy rate comparisons with different values of channel correlation factor ρ , where the number of bits in the resolution of PS is $b = 4$ bits.

the LUs into the wanted regions with minimal transmission power, and the LUs' SER performance may be deteriorated significantly in the presence of hardware impairments and imperfect CSI. The least-norm DM [10] also obtains inferior SER over our proposed algorithm, since the fixed phase DM design in [10] limits the DoFs for transmitter design. Also, it is observed all the algorithms achieve a superior SER given a high resolution of PSs.

Fig. 4 shows the impact of correlation among the LUs and Eves' channels on the secrecy rate [16]. Since the Eves' received signal is randomized benefiting from the channel disparity in DM designs, the Eves' rate is much lower than that of the LUs. Hence, positive secrecy rate is always maintained by DM designs. Nevertheless, it is observed that the secrecy rate is reduced when channel correlation increases. It is because with higher correlation, the Eves' received signal becomes similar to that of LUs, and hence Eves' SER is refined. As

a result, the achievable secrecy rate decreases with a higher value of ρ . Also, since the proposed algorithm endorses a low SER and hence a high throughput for the LUs, the secrecy rate achieved by the proposed algorithm always outperforms the two benchmarks.

VI. CONCLUSIONS

In this paper, we have investigated practical transmitter design under imperfect channel estimation and critical hardware limitations for realizing DA systems. Phase and power have been jointly designed to optimize receiving performance at the LUs while simultaneously randomizing the Eves' received signals. A closed-form algorithm is proposed to push the received signals of the LUs away from the decision threshold based on the concept of relaxed-phase DM design, while simultaneously randomizing the Eves' receiving performance. Our simulation results have showed that the proposed algorithm endorses much lower SER at the LUs. Also, the secrecy rate of the proposed algorithm is significantly improved over the benchmarks in [10] and [11], guaranteeing a reasonable security performance even with a high correlation factor among the LUs and Eves' channels.

REFERENCES

- [1] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 2180-2189, Jun. 2008.
- [2] H. Lei *et al.*, "Secrecy outage analysis for SIMO underlay cognitive radio networks over generalized-K fading channels," *IEEE Trans. Signal Process. Lett.*, vol. 23, no. 8, pp. 1106-1110, Aug. 2016.
- [3] Z. Wei and C. Masouros, "User-centric distributed antenna transmission: secure precoding and antenna selection with interference exploitation," <https://arxiv.org/pdf/1812.05046.pdf>
- [4] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Transmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuit*, vol. 43, no. 12, pp. 2674-2692, Dec. 2008.
- [5] M. P. Daly, "DM technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633-2640, Sep. 2009.
- [6] Y. Ding and V. Fusco, "Establishing metrics for assessing the performance of directional modulation systems," *IEEE Trans. Antennas Propag.*, vol. 62, no. 5, pp. 2745-2755, May 2014.
- [7] N. N. Alotaibi and K. A. Hamdi, "Switched phase-array transmission architecture for secure millimeter-wave wireless transmission," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303-1312, Mar. 2016.
- [8] W. Wang and Z. Zheng, "Hybrid MIMO and phased-array DM for PHY security in mmWave wireless communications," *IEEE Journal on Sel. Area in Commun.*, vol. 36, no. 7, pp. 1383-1396, Jul. 2018.
- [9] T. Hong, M. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, pp. 1417-1420, Nov. 2011.
- [10] M. Hafez, M. Yusuf, T. Khattab, T. Elfouly, and H. Arslan, "Secure spatial multiple access using directional modulation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 1, pp. 563-573, Jan. 2018.
- [11] A. Kalantari, S. Maleki, S. Chatzinotas, and B. Ottersten, "Directional modulation via symbol-level precoding: a way to enhance security," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1478-1493, Dec. 2016.
- [12] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Vector perturbation based on symbol scaling for limited feedback misodownlinks" *IEEE Trans. Sig. Proc.*, vol. 62, no. 2, pp. 562-571, Feb. 2014.
- [13] D. P. Bertsekas, *Convex optimization algorithms*, Belmont, MA, USA Athena Scientific, 2015.
- [14] T. Zheng, H. Wang, J. Yuan, and M. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 63, no. 11, pp. 4347-4362, Nov. 2015.
- [15] L. Vandenbergh, *Applied numerical computing*, University Lecture, Dept. Elect. Eng., UCLA, Los Angeles, USA, 2012.
- [16] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. on Wireless Commun.*, vol. 14, no. 11, pp. 63-77, Nov. 2015.