Secure Directional Modulation with Few-Bit Phase Shifters: Optimal and Iterative-Closed-Form Designs

Zhongxiang Wei, *Member, IEEE,* Christos Masouros, *Senior Member, IEEE,* and Fan Liu, *Member, IEEE*

***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 constraints, such as finite-resolution phase shifters (PSs) and per-antenna power budget. Tailored for the practical issues in realizing DM, a series of practical scenarios are investigated. Starting from the scenario where eavesdroppers (Eve)s' information is completely unknown, corresponding designs are proposed to optimize legitimate users (LU)s' receiving performance while randomizing the Eves' received signal. When the Eves' CSI is imperfectly known, in the second scenario, the Eves' receiving performance is further deteriorated by imposing destructive interference to the Eves. For each scenario, three algorithms are proposed under hardware constraints and imperfect CSI, i.e. one direct-mapping algorithm suitable for high/moderate number of bits in PSs, one heuristic algorithm with improved receiving performance at the cost of complexity, and one iterative-closed-form algorithm with enhanced practicality of symbol-level based DM. Simulation demonstrates that the algorithms achieve lower symbol error rate (SER) at the LUs while significantly deteriorating the Eves' SER, leading to an improved secrecy throughput over the benchmarks.**

***Index Terms*—Directional modulation, Hardware impairments, Imperfect channel estimation, Interference exploitation, Iterative-closed-form precoding, Physical layer security**

I. Introduction

In the past decades, beamforming and jamming or a combination of the two 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 (LU)s have better transmission condition over the eavesdroppers (Eve)s. 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 nulled with the reduced received power at the LUs [2]. To further deteriorate Eves' receiving performance, artificial noise (AN) can be generated together with beamforming design to jam Eves. When the Eves' channel state information (CSI) is unknown at the transmitter, isotropic AN could be generated into the null space of the LUs' channel [1]. When the Eves' CSI is known at the transmitter, AN could be injected to the direction of Eves in a spatial manner, which is more efficient than the isotropic transmission [3]. By the conventional beamforming and jamming designs, Eves' received signal-to-interference-plus-noise ratio (SINR) is indeed degraded, whereas the same information is conveyed towards undesired directions by sidelobe. Hence, the confidential messages intended for LUs can somehow be decoded by Eves if the Eves are equipped with high sensitivity receivers [4].

Recently, directional modulation (DM) has attracted attention as a new technique to secure wireless communications from the perspective of signal processing [5]. 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. As a transmitter technique, symbols' modulation of DM systems happens at antenna level instead of at the baseband by conventional beamforming design, and the received beampatterns at LUs are treated as spatial complex constellation points. That is, the intended symbols are directly designed such that the LU's received beam has the same amplitude and phase of the intended data symbols [6]. Even if the Eves and LUs' channels are correlated, the Eves' receiving performance can also be deteriorated by intentionally imposing destructive interference to the Eves. 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 [7]. Hence, it is more difficult for potential Eves to estimate transmitter's behavior.

In terms of implementation of DM systems, there also has been extensive designs on the practical hardware realizations, such as parasitic antenna-based DM [6] [7], phase array-based DM [8] [9] [10] [11], Fourier transform synthesis-based DM [12], switch-array based DM [13] [14], and digital DM [15]. In recent years, there has been advanced actively driven antenna array-based DM, where power amplifiers (PA)s (or power attenuators) are cascaded to phase shifters (PS)s for constructing composite beampatterns [16] [17] [18], as shown in Fig. 1. Since the power and phase are jointly designed for constructing composite beampatterns based on the characteristics (i.e., fading) of the estimated channel, the DM in [16] [17] [18] can be both angle- and distance-dependent just like classical multiple-input and multiple-output (MIMO). In addition, the advantages of DM also lie in high cost- and power-efficiency, since the expensive and power-consuming radio frequency (RF) chains and digital-to-analogue converters (DAC)s of the conventional digital/hybrid beamforming (DBF/HBF) are not required. For illustration, Fig. 2 is demonstrated to show the

Zhongxiang Wei, Christos Masouros and Fan Liu are with the department of Electronic and Electrical Engineering at the University College London, London, UK. Email: {zhongxiang.wei, c.masouros, fan.liu}@ucl.ac.uk

This work was supported by the Engineering and Physical Sciences Research Council, UK, under project EP/R007934/1.

cost- and power-efficiency of the DM over conventional HBF systems. Without loss of generality, the partially-connected HBF is considered which consists of 4 RF chains and 2 PSs on each RF chain. It is observed that HBF dissipates high power on its RF chains and DACs, leading to 6 dB higher total power than the DM systems. Since energy efficiency (EE) is defined as the ratio between the achieved throughput and incurred power consumption, the EE of DM systems is also confirmed to be superior to that of HBF systems. Besides, there has been a variety of DM demonstrators, where secure waveform is synthesized with low cost and low power-consuming hardware. In [6], the parasitic antenna-based DM was built on the passively excited architecture, and later on the DM demonstrator based on the actively excited analogue phase arrays was presented in [9]. In [23], a digital DM demonstrator working at 2.4 GHz was constructed on the Wireless Open-Access Research Platform. In [24], the Fourier beamforming-based DM demonstrator can be considered as hardware realizations of the orthogonal vector DM synthesis approach. Also, there have been fruitful algorithm and optimization designs dedicated for DM systems, such as zero-forcing (ZF) like DM [16] [17], barrier-method based DM design [18], singular value decomposition (SVD) based DM [25], AN aided DM [26] [27] [28], and millimeter wave DM design [29]. In [16] [17], the concept of pseudo-inverse of channel matrix was utilized for multiuser communication. The authors in [25] proposed a DM synthesis scheme based on SVD operations. The authors in [26] [27] [28] investigated the joint design of multi-beam DM symbols and AN to secure wireless communications. In [29], a hybrid MIMO phased-array time-modulated DM was proposed to secure mmWave communications in line-of-sight (LOS) scenario, and it was further indicated that there is potential to extend the work into frequency diverse array (FDA)-based DM systems [30] [31], where a small frequency increment is applied across all the FDA elements to produce range-dependent beampattern. In [18], the barrier-method was used to derive the phase-array weights towards multiple directions in a MIMO system, where the phase of the received signal is relaxed based on the concept of constructive interference (CI). The received signal of the LUs is constructed to fall into a constructive region, in which the received signal is pushed away from the detection thresholds of the signal constellation. Hence, the increased distance to the detection thresholds can effectively improve the receiving performance. Related to DM systems, recent works have focused on exploiting CI through symbol level precoding. This was first introduced in [32] in the context of linear precoders, and then extended to optimization-based symbol level precoders [33] [34].

Some fundamental challenges, however, need to be addressed in DM systems. The first challenge is that, regardless of various DM structures and optimization designs, system performance is essentially affected by the hardware impairments and imperfect CSI. Whereas, all the aforementioned DM schemes assumed perfect CSI and hardware realization, such as infinite resolution PSs and noise excluded receivers. In practice, finite resolution PSs are more cost-effective [35], and receiving noise also inevitably distorts the desired beam pattern. Unfortunately, all of these practical issues have been

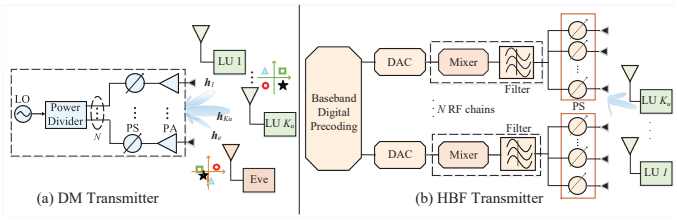

Fig. 1. Simplified system models for DM and HBF transmitters. By DM, signal is generated by applying actively driven elements, i.e. finite-resolution PSs and budget constrained PAs.

ignored by the aforementioned researches. The second challenge is that, existing designs are far from optimal. The design proposed in [18] is based on barrier-method, which is only solid given the penalty factor approaching infinity. The precoding design proposed in [16] [17] is simply based on pseudo inverse without considering quality of service (QoS) of LUs, which may lead to a poor receiving performance at LUs. More importantly, the designs in [16]-[18] do not capture hardware impairments and are based on perfect CSI. In addition, the employed total-power constraint in [16]-[18] failed to capture the typical architecture of DM transmitter, where per-antenna power constraint is more practical. The third challenge is that, indeed, according to the principle of DM, the received symbols at Eves are randomized due to the channel disparity among LUs and Eves. However, Eves may intercept a high volume of symbols in one specific frame and consequently be able to recover a fraction of the confidential messages with error correction coding, especially when the Eves' and LUs' channels are correlated. To this end, how to intentionally locate the Eves' signal into destructive regions, in which the Eves' received symbols are purposely constructed to be different from the confidential symbols, to further deteriorate the Eves' performance is still unknown.

To address the aforementioned outstanding issues, in this paper, we exploit 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 PHY security. To be more specific, imperfect CSI acquisition, finite-resolution PSs, per-antenna transmission power budget and receiving noise are considered in formulating the practical transmitter design.
2) We first 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 constraints, 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) We further exploit transmitter design when the Eves' CSI is imperfectly known at the transmitter. To be more specific, we refine the PHY security design for DM by

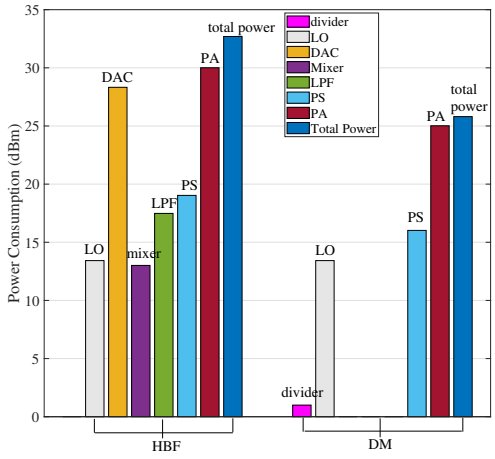

Fig. 2. An illustration of cost- and power-efficiency of DM systems over HBF systems. For clarity, assume there are K_u LUs requiring data streams. Since HBF requires that the number of RF chains should be no smaller than the total number of data streams for multi-user access, the HBF needs at least K_u RF chains (each RF chain mainly consists of a mixer and a low-pass filter), K_u DACs, 1 local oscillator, and a number of PSs. In comparison, DM only requires 1 local oscillator, 1 divider, and K_u PAs and PSs, which is evidently much less expensive than HBF structure. On the other hand, total power consumption of HBF is summarized as $P_{tot,HBF} = P_{LO} + K_u(P_{DAC} + P_{mixer} + P_f) + MP_{PS} + \frac{\sum ||\boldsymbol{w}||_2^2}{\varsigma}$ [19] [20], where $P_{LO}, P_{DAC}, P_{mixer}, P_f$, and P_{PS} denote the power consumption of local oscillator, DAC, mixer, filter, PS, respectively. M denotes the total number of PSs, depending on the partially-connected or fully-connected configuration of HBF structure. The last term $\frac{\sum ||\boldsymbol{w}||_2^2}{\varsigma}$ denotes the dissipated PAs power with precoding $\boldsymbol{w}$ and drain efficiency ς of the PAs. In comparison, the power consumption of DM consists of $P_{tot,DM} = P_{LO} + P_D + K_u P_{PS} + \frac{\sum P_t}{\varsigma}$, where P_D denotes the power consumption of divider, and $\frac{\sum P_t}{\varsigma}$ denotes the total transmission power of all the PAs. Evidently, if the transmission power consumed by DM is lower or comparable to that of HBF, the total power consumption of DM can be significantly reduced over HBF in terms of power efficiency. For fair comparison, the PAs power consumed by HBF (i.e., $\frac{\sum ||\boldsymbol{w}||_2^2}{\varsigma}$) and DM (i.e., $\frac{\sum P_t}{\varsigma}$) is obtained with the same symbol error rate (SER) requirements, i.e., 10^{-2}, at $K_u = 4$ LUs. The power consumption of different components is set to as $P_{DAC} = 170$ mW, $P_{PS} = 10$ mW, $P_{LO} = 22$ mW, $P_{mixer} = 5$ mW, $P_f = 14$ mW, $P_D = 1$ mW, and $\varsigma = 50$ % [19] [20] [21] [22].

intentionally pushing the Eves' received symbols into destructive regions of the signal constellation, which results in increased detection errors at the Eves. Hence, the LUs' symbols are explicitly protected from being intercepted on a symbol-level, and the LUs' SER performance is simultaneously maintained at a low level.

4) For all the above considered scenarios, we propose three robust algorithms tailored for imperfect CSI and hardware impairments in DM systems. The first direct-mapping algorithm achieves a fast convergence rate and is favourable given a high resolution PS. The second heuristic algorithm further improves the LUs' receiving performance in an iteration manner, and offers a preferable solution when employing low/moderate resolution PSs. The third algorithm is given in iterative-closed-form with Lagrangian and Karush-Kuhn-Tucker (KKT) conditions, further enhancing the practicality of the symbol-level enabled DM systems.
5) The conventional DM techniques contain the constructed symbols within a region around the nominal point in the modulated signal constellation, which requires a strict phase on the constructed symbols [8]-[17]. In our work, the phases of constructed symbols are not necessary to be strictly fixed, based on the concept of CI. To be specific, the received symbols of LUs are designed to fall into the constructive regions while the Eves' received symbols are confined into destructive regions. Hence, higher degrees of freedom (DoF)s are endorsed for DM transmitter design over the existing fixed-phase DM designs.

Notations: Matrices and vectors are represented by boldface capital and lower case letters, respectively. $|\cdot|$ denotes the absolute value. $||\cdot||$ denotes the norm operation. $\boldsymbol{A}^H$ and $\boldsymbol{A}^T$ denote the Hermitian transpose and transpose of a matrix $\boldsymbol{A}$. diag $(\boldsymbol{A})$ returns a diagonal matrix with diagonal elements from a matrix $\boldsymbol{A}$ and diag $(\boldsymbol{a})$ stacks the elements of vector $\boldsymbol{a}$ into a diagonal matrix. Superscript $\Re$ and $\Im$ denote the real and imaginary parts, respectively. $\boldsymbol{I}_n$ means a n-by-n identity matrix. $\mathbb{C}^{N\times M}$ denotes the set of $N \times M$ matrix.

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 and II-C, respectively.

A. System Model

We consider DM systems with actively driven elements [18]. 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(a). LUs' CSI is obtained by channel estimation in the training phase, based on channel reciprocity as in [17] [18]. Note that in DM systems, only the intended symbols change in symbol-level, which can be naturally known by the transmitter. While the users' CSI may only change in block level (known as block fading), we only need to update LUs' CSI in block level. Hence, acquiring the users' CSI in DM systems makes no difference compared to that in conventional beamforming systems, which has been extensively utilized in the DM related works in [16]-[18]. Define $\boldsymbol{h}_k = \tilde{\boldsymbol{h}}_k + \boldsymbol{e}_k$ as the channel from the transmitter to the LU k, $\forall k \in K_u$, where $\tilde{\boldsymbol{h}}_k \in \mathbb{C}^{1\times N}$ and $\boldsymbol{e}_k \in \mathbb{C}^{1\times N}$ denote the estimated CSI and estimation error, respectively. By classic channel estimation method, such as minimum mean square error (MMSE), the element of the error vector can be modeled by a Gaussian distributed variable as $[\boldsymbol{e}_k]_n \sim \mathbb{CN}\{0, \sigma_e^2\}$, $\forall n \in N$, with variance σ_e^2 [36]. The Eves' CSI is assumed to be completely unknown in section III, while in Sections IV we further consider advanced designs in the case where the Eve's CSI is imperfectly known. Define $\boldsymbol{\phi} \in \mathbb{C}^{N\times 1}$ as phase and $\boldsymbol{p} \in \mathbb{C}^{N\times 1}$ as transmission power. We consider a practical finite resolution PSs and per-antenna power budget. Let $\mathbb{F} = \{1, \phi, \phi^2, ..., \phi^{n_{ps}-1}\}$ 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

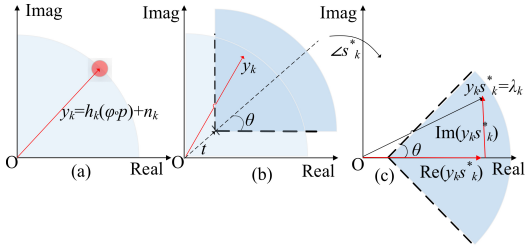

Fig. 3. QPSK for illustration. (a) Fixed phase DM: the received signal is expected to be in a proximity region around the constellation point. (b) Relaxed phase DM: the received signal y_k falls into constructive region (dark blue area). The design pushes the symbol away from the original decision thresholds of the constellation and hence optimizes receiving performance. (c) After rotation by $\angle s_k^*$, $\Re\{y_k s_k^*\}$ and $\Im\{y_k s_k^*\}$ are projected on real and imaginary axis, according to the trigonometry.

resolution of PSs. Hence, the received signal at LU k can be written as

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

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

B. Strict and Relaxed Phase based DM

1) Strict Phase based DM Design: By the strict phase based DM systems in Fig. 3(a), the received signal y_k should have exactly same phase and amplitude of the desired symbol of LU k, such as $[\tilde{\boldsymbol{h}}_1(\boldsymbol{\phi} \circ \boldsymbol{p}), \tilde{\boldsymbol{h}}_2(\boldsymbol{\phi} \circ \boldsymbol{p}), ..., \tilde{\boldsymbol{h}}_{K_u}(\boldsymbol{\phi} \circ \boldsymbol{p})] = [\sqrt{\gamma_1}s_1, \sqrt{\gamma_2}s_2, ..., \sqrt{\gamma_{Ku}}s_{K_u}]$, where s_k denotes the desired symbol for the LU k and $\sqrt{\gamma_k}$ denotes the desired amplitude that relates to the LU's SNR requirement. Since the constructed signal may be impaired by practical issues, such as imperfect CSI and hardware realizations, a higher value of signal-to-noise ratio (SNR) requirement can be set to place the constructed signal away from the detection threshold. Obviously, 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 thresholds of the signal constellation. Furthermore, the LUs can still correctly detect the received signal with the increased DoFs at the transmitter. The CI concept has been thoroughly discussed in the recent literature, and to avoid extensive repetition we refer the readers to [37] for details. According to the geometrical interpretation in Fig. 3(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. 3(c), the received signal of the LU k falling into constructive regions is equivalent to satisfying the following equation.

$$\begin{aligned}|\Im\{(\boldsymbol{h}_k(\boldsymbol{\phi} \circ \boldsymbol{p}) + n_k)s_k^*\}| \leq \\ (\Re\{(\boldsymbol{h}_k(\boldsymbol{\phi} \circ \boldsymbol{p}) + n_k)s_k^*\} - t)\tan\theta, \ \forall k \in K_u,\end{aligned} \tag{2}$$

where s_k is the desired symbol of the LU k and s_k^* denotes its conjugate. $\theta = \frac{\pi}{M}$, where M denotes the constellation size. (2) inherently indicates inter-beam interference has been utilized as a beneficial effect. 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 estimation error, receiving noise, finite resolution of PSs and per-antenna power budget, (2) may not be always satisfied. Hence, we write (2) in a probabilistic manner as

$$\begin{aligned}\Pr\{|\Im\{(\boldsymbol{h}_k(\boldsymbol{\phi} \circ \boldsymbol{p}) + n_k)s_k^*\}| \leq \\ (\Re\{(\boldsymbol{h}_k(\boldsymbol{\phi} \circ \boldsymbol{p}) + n_k)s_k^*\} - t)\tan\theta\} \geq \Gamma, \ \forall k \in K_u,\end{aligned} \tag{3}$$

where Γ is the probability threshold of satisfying (2). Evidently, Γ can be set to a high value, indicating (2) is satisfied with high probability. In other words, the probability of the LUs' signal falling into constructive regions is not lower than Γ. Note that the receiver only needs to detect and decode the received signal directly, according to the amplitude and phase of the constructed beampatterns, but does not need to know the CSI or the prior-information of the desired symbols. Importantly, note that DM removes the need for channel equalization at the LU's receiver. Since the DM symbols are designed to fall exactly at the constructive regions of the received constellation at the LUs, there is no need for the LUs to equalize for the channel phase. Critically, this also avoids the need for channel estimation at the LUs.

III. DM Design without Eve's Information

In a number of practical scenarios, it is impossible to obtain the Eves' CSI, since passive Eves only intercept confidential messages but do not actively launch attack. In this section, we investigate system design without the knowledge of the Eves' CSI. Problem formulation is given in subsection III-A and three algorithms are proposed in III-B-1), III-B-2) and III-B-3), respectively. Finally, PHY security performance is discussed in section III-C.

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. In particular with respect to imperfect CSI, we take a probabilistic approach where a robust precoder based on the CSI error distribution is designed. Hence, the optimization is given as

$$
\begin{aligned}
P1 \ &: \underset{\boldsymbol{\phi},\boldsymbol{p}}{\text{argmax}} \ t, \\
\text{s.t } &(C1): \Pr\{|\Im\{(\boldsymbol{h}_k(\boldsymbol{\phi}\circ\boldsymbol{p})+n_k)s_k^*\}| \leq \\
&\quad (\Re\{(\boldsymbol{h}_k(\boldsymbol{\phi}\circ\boldsymbol{p})+n_k)s_k^*\}-t)\tan\theta\} \geq \Gamma, \ \forall k\in K_u, \\
&(C2): \boldsymbol{p}^H\boldsymbol{A}_n\boldsymbol{p} \leq p_{max}, \forall n\in N, \\
&(C3): \boldsymbol{\phi}(n)\in\mathbb{F}, n\in N,
\end{aligned} \tag{4}
$$

where p_{max} denotes the per-antenna maximum available transmission power, and $\boldsymbol{A}_n = \text{diag}\ \{\underbrace{0,...,0}_{n-1},1,\underbrace{0,...,0}_{N-n}\}$, $\forall n\in N$, 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 PA lower than the available 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 the 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. Power and Phase Optimization Design

The optimization problem P1 involves infinite possibilities of receiving noise and CSI estimation error, as well as finite choice of phase designs. To access the optimization problem, we first decompose constraint (C1) into

$$
\begin{aligned}
&\Pr\{|\Im\{(\tilde{\boldsymbol{h}}_k+\boldsymbol{e}_k)(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}+\Im\{n_ks_k^*\}| \leq \\
&(\Re\{(\tilde{\boldsymbol{h}}_k+\boldsymbol{e}_k)(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}+\Re\{n_ks_k^*\}-t)\tan\theta\} \geq \Gamma, \forall k\in K_u.
\end{aligned} \tag{5}
$$

Since the noise n_k and CSI estimation error $\boldsymbol{e}_k$ follow Gaussian distribution with different variance, we know that the linear combination of $\Im\{n_ks_k^*\}$, $\Re\{n_ks_k^*\}$, $\Im\{\boldsymbol{e}(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}$, and $\Re\{\boldsymbol{e}(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}$ still follow Gaussian distribution with a modified variance. Hence, collecting all the above uncertainty related terms in to a variable $\bar{n}_k$ yields [1]

$$
\begin{cases}
\Pr\{\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\} \leq (\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}-t)\tan\theta+\bar{n}_k\} \geq \Gamma, \\
\Pr\{-\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\} \leq (\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}-t)\tan\theta+\bar{n}_k\} \geq \Gamma,
\end{cases} \tag{6}
$$

where $\bar{n}_k \sim \mathbb{CN}(0,(1+\tan^2\theta)(\frac{N\sigma_e^2||(\boldsymbol{\phi}\circ\boldsymbol{p})||_2^2}{2}+\frac{\sigma_n^2}{2}))$. 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 $\mathbb{CN}(0,(\frac{N^2\sigma_e^2p_{max}+\sigma_n^2}{2\cos^2\theta})$, and the two inequalities in (6) can be seen as cumulative distribution function (cdf) of a Gaussian distributed variable. Normalizing the variance of $\bar{n_k}$ yields (7), as shown on top of next page. Apparently, (7) serves as cdf of the standard Gaussian distributed variables. Denote $\Phi^{-1}(\cdot)$ as the inverse cdf of a standard Gaussian variable. (7) is written as

$$
\begin{cases}
\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\} \leq (\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}-t)\tan\theta-\Theta, \\
-\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\} \leq (\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}-t)\tan\theta-\Theta,
\end{cases} \tag{8}
$$

where $\Theta = \frac{\Phi^{-1}(\Gamma)\sqrt{N^2\sigma_2^2p_{max}+\sigma_n^2}}{\sqrt{2}\cos\theta}$. Now the probabilistic constraint (C1) has been transformed into robust constraints in (8), and the next difficulty lies in the combination constraint (C3) due to the finite-resolution of PSs. In the following subsections, three algorithms are proposed to solve the optimization problems.

1) Direct-mapping algorithm: Evidently, the pair-wise Hadamard product of $\boldsymbol{\phi}$ and $\boldsymbol{p}$ serves as an equivalent transmission vector. Hence, we can solve the optimization problem P1 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. Hence, define an equivalent transmission vector $\boldsymbol{x} = \boldsymbol{\phi}\circ\boldsymbol{p}$. After removing constraint (C3) the problem is given as

$$
\begin{aligned}
P2 \ &: \underset{\boldsymbol{\phi},\boldsymbol{p}}{\text{argmax}} \ t, \\
\text{s.t } &(C1): \ \Im\{\tilde{\boldsymbol{h}}_k\boldsymbol{x}s_k^*\} \leq (\Re\{\tilde{\boldsymbol{h}}_k\boldsymbol{x}s_k^*\}-t)\tan\theta-\Theta, \text{ and} \\
&\quad -\Im\{\tilde{\boldsymbol{h}}_k\boldsymbol{x}s_k^*\} \leq (\Re\{\tilde{\boldsymbol{h}}_k\boldsymbol{x}s_k^*\}-t)\tan\theta-\Theta, \forall k\in K_u, \\
&(C2): \boldsymbol{x}^H\boldsymbol{A}_n\boldsymbol{x} \leq p_{max}, \forall n\in N,
\end{aligned} \tag{9}
$$

which is a standard convex second-order cone (SOC) programming and can be readily solved by commercial optimization tool, i.e. CVX. After obtaining the optimal vector $\boldsymbol{x}^*$, we map it to the closest point in the feasible set $\mathbb{F}$ for the consideration of finite-resolution PSs. Hence, the final PS and power vectors are designed as

$$
\hat{\boldsymbol{\phi}}(n) = \mathbb{Q}(\frac{\boldsymbol{x}^*(n)}{|\boldsymbol{x}^*(n)|_2}), \text{ and } \hat{\boldsymbol{p}}(n) = |\boldsymbol{x}^*(n)|_2, \ \forall n\in N, \tag{10}
$$

where the operator $\mathbb{Q}(\cdot)$ maps a complex unit-norm variable to the nearest point in the set $\mathbb{F}$. For the optimization problem in P2, since it has been transformed into a standard convex optimization problem, and can be readily solved by CVX with interior-point method. Its convergence is naturally guaranteed, as the interior-point method is known to converge [36]. Now, we are able to devise the whole algorithm, as summarized in Algorithm 1. By considering imperfect CSI and hardware constraints, i.e., finite-resolution PS, per-antenna power budget as well as receiving noise, we first handle the uncertainty and transform the probabilistic constraint (C1) into a robust linear constraint, and then the transformed problem can be readily solved by CVX. Afterwards, only one extra mapping step is needed to get the final result of phase $\hat{\boldsymbol{\phi}}$ and power $\hat{\boldsymbol{p}}$.

2) Heuristic Optimization: In subsection III-B-1), the proposed low-complexity direct-mapping algorithm may not be favourable given a low or moderate resolution PS, where the quantized result $\hat{\boldsymbol{\phi}}$ selected from $\mathbb{F}$ may be far from the ideal result. Hence, in this part, we propose a heuristic

[1] $\Pr\{|X|\leq c\}\geq\Gamma$ is equivalent to $\Pr\{-X\leq c, X\leq c\}\geq\Gamma$. However, considering the complicated optimization problems, presenting the optimal precoding design with the joint probability may be infeasible. Moreover, the optimal precoding may not exist unless the joint probability satisfying some strict conditions. Hence, to strike a good tradeoff between system performance and complexity, we approximate $\Pr\{|X|\leq c\}\geq\Gamma$ to $\Pr\{X\leq c\}\geq\Gamma$ and $\Pr\{-X\leq c\}\geq\Gamma$. More important, given a high value of Γ, the approximation is tight and has been widely utilized in robust optimization design.

$$\begin{cases} \Pr\{\frac{(\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}-t)\tan\theta-\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}}{\frac{\sqrt{N^2\sigma_e^2 p_{max}+\sigma_n^2}}{\sqrt{2}\cos\theta}} \geq \frac{\bar{n}_k}{\frac{\sqrt{N^2\sigma_e^2 p_{max}+\sigma_n^2}}{\sqrt{2}\cos\theta}}\} \geq \Gamma, \\ \Pr\{\frac{(\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}-t)\tan\theta+\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}}{\frac{\sqrt{N^2\sigma_e^2 p_{max}+\sigma_n^2}}{\sqrt{2}\cos\theta}} \geq \frac{\bar{n}_k}{\frac{\sqrt{N^2\sigma_e^2 p_{max}+\sigma_n^2}}{\sqrt{2}\cos\theta}}\} \geq \Gamma, \end{cases} \tag{7}$$

Algorithm 1 Direct-mapping algorithm, without Eves' Information

Input: LUs' estimated channel $\tilde{\boldsymbol{h}}_k$, for $\forall k \in K_u$, maximum power p_{max}, finite-resolution set $\mathbb{F}$, and intended symbol vector $\boldsymbol{s}$ for the LUs.
Output: Optimal PS design $\hat{\boldsymbol{\phi}}$ and optimal power $\hat{\boldsymbol{p}}$.
1: Solve optimization problem P2. Do $\hat{\boldsymbol{\phi}}(n) = \mathbb{Q}(\boldsymbol{\phi}^*(n))$ and $\hat{\boldsymbol{p}}(n) = |\boldsymbol{x}^*(n)|_2, \forall\, n \in N$.

algorithm to provide a superior performance over the direct-mapping algorithm, at the cost of increased complexity. The principle of the heuristic algorithm is to iteratively optimize one of the variables $\boldsymbol{\phi}$ and $\boldsymbol{p}$ assuming the other being fixed. For example, we can extract the contribution of $\boldsymbol{p}$ and seek to find its optimum with a fixed $\boldsymbol{\phi}$. Then assuming power vector $\boldsymbol{p}$ being fixed, we turn to optimize phase $\boldsymbol{\phi}$. Such operations are iteratively run until the algorithm converges to an optimum point. Revisiting problem P1, the variables $\boldsymbol{\phi}$ and $\boldsymbol{p}$ are coupled by Hadamard product in (C1). Hence, we transform the Hadamard product $\boldsymbol{\phi}\circ\boldsymbol{p}$ into a simpler form $\boldsymbol{\phi}\circ\boldsymbol{p} = (\sum_{n=1}^{N}\phi(n)\boldsymbol{A_n})\boldsymbol{p}$. Without loss of generality, we first optimize $\boldsymbol{p}$ assuming $\boldsymbol{\phi}$ being fixed. Denote j as the index of the j-th iteration, and the pre-fixed value of $\boldsymbol{\phi}^{(j)}(n)$, $\forall n \in N$, can be randomly selected from $\mathbb{F}$ or call Algorithm 1 to calculate. Now, we have the optimization with respect to the $\boldsymbol{p}$ as

$$\begin{aligned} P3\ &: \underset{\boldsymbol{p}}{\text{argmax}}\ t, \\ \text{s.t}\ (C4)&: \Pr\{|\Im\{\tilde{\boldsymbol{h}}_k(\sum_{n=1}^{N}\boldsymbol{\phi}^{(j)}(n)\boldsymbol{A_n})\boldsymbol{p}s_k^*\}| \leq \\ &(\Re\{\tilde{\boldsymbol{h}}_k(\sum_{n=1}^{N}\boldsymbol{\phi}^{(j)}(n)\boldsymbol{A_n})\boldsymbol{p}s_k^*\} - t)\tan\theta\} \geq \Gamma, \forall k \in K_u, \\ &(C5): \boldsymbol{p}^H\boldsymbol{A}_n\boldsymbol{p} \leq p_{max},\ (C6): \boldsymbol{\phi}^{(j)}(n) \in \mathbb{F}, n \in N. \end{aligned} \tag{11}$$

Since the value of $\boldsymbol{\phi}^{(j)}(n), n \in N$, at the j-th iteration has been pre-set to guarantee the validity of (C6), (C6) can be readily removed from P3. Then by handling the uncertainty terms introduced by the imperfect CSI and receiving noise, (C4) can be similarly written as $|\Im\{\tilde{\boldsymbol{h}}_k(\sum_{n=1}^{N}\phi^{(j)}(n)\boldsymbol{A_n})\boldsymbol{p}s_k^*\}| \leq (\Re\{\tilde{\boldsymbol{h}}_k(\sum_{n=1}^{N}\phi^{(j)}(n)\boldsymbol{A_n})\boldsymbol{p}s_k^*\} - t)\tan\theta - \Theta$. Hence, P3 is equivalently written as $P3\ : \underset{\boldsymbol{p}}{\text{argmax}}\ t$, s.t $(C4)$, $(C5)$: $\boldsymbol{p}^H\boldsymbol{A}_n\boldsymbol{p} \leq p_{max}, \forall n \in N$, which is a standard convex optimization and can be readily solved by CVX. After obtaining optimal power $\boldsymbol{p}^*$, we update $\boldsymbol{p}^{(j)} = \boldsymbol{p}^*$ and turn to optimize $\boldsymbol{\phi}$ with known value of $\boldsymbol{p}^{(j)}$. By extracting the contribution of $\boldsymbol{\phi}$, the optimization problem turns into

$$\begin{aligned} P4\ &: \underset{\boldsymbol{\phi}}{\text{argmax}}\ t, \\ \text{s.t}\ (C7)&: |\Im\{\tilde{\boldsymbol{h}}_k(\sum_{n=1}^{N}\boldsymbol{p}^{(j)}(n)\boldsymbol{A_n})\boldsymbol{\phi}s_k^*\}| \leq \\ &(\Re\{\tilde{\boldsymbol{h}}_k(\sum_{n=1}^{N}\boldsymbol{p}^{(j)}(n)\boldsymbol{A_n})\boldsymbol{\phi}s_k^*\} - t)\tan\theta - \Theta, \\ &(C8): \boldsymbol{\phi}^H\boldsymbol{A}_n\boldsymbol{\phi} \leq 1, \end{aligned} \tag{12}$$

where the maximal power constraint in (C8) is normalized as the power budget has been captured by the intermediate variable $\boldsymbol{p}^{(j)}$. Since P4 can be readily solved by CVX, we can obtain the optimal result ϕ^* and then quantize it with (10) for the consideration of finite-phase.

Algorithm 2 Heuristic algorithm, without Eves' Information

Input: LUs' estimated channel $\tilde{\boldsymbol{h}}_k$, for $\forall k \in K_u$, maximum power p_{max}, finite-resolution set $\mathbb{F}$, and intended symbol vector $\boldsymbol{s}$ for the LUs, maximum iteration number $\max_{\text{ite}}$.
Output: Optimal PS design $\hat{\boldsymbol{\phi}}$ and optimal power $\hat{\boldsymbol{p}}$.
1: Set an initial feasible set, i.e., calling Algorithm 1 or simply selecting from $\mathbb{F}$ to obtain $\hat{\boldsymbol{\phi}}$. Let $\boldsymbol{\phi}^{(0)} = \hat{\boldsymbol{\phi}}$.
2: **for** j=0: $\max_{\text{ite}}$ or until convergence **do**
3: With given value of $\boldsymbol{\phi}^{(j)}$, solve P3 and obtain an intermediate optimal power design $\boldsymbol{p}^*$.
4: Update $\boldsymbol{p}^{(j)} = \boldsymbol{p}^*$. With given value of $\boldsymbol{p}^{(j)}$, solve P4 and obtain intermediate optimal phase $\boldsymbol{\phi}^*$.
5: Do $\hat{\boldsymbol{\phi}}(n) = \mathbb{Q}(\boldsymbol{\phi}^*(n)), \forall\, n \in N$. Set $j = j+1$ and update $\boldsymbol{\phi}^{(j)} = \hat{\boldsymbol{\phi}}$.
6: **end for**

In conclusion, the power $\boldsymbol{p}$ (in optimization P3) and phase $\boldsymbol{\phi}$ (in optimization P4) are optimized iteratively assuming the other variable being fixed, and the iterative optimization is operated until convergence. The whole heuristic algorithm is summarized in Algorithm 2. In particular, optimizations P3 and P4 are both standard convex problems and their convergences are naturally guaranteed. Hence, the convergence of the inner layer of the proposed heuristic algorithm is confirmed. For proving the convergence of heuristically updating the power $\boldsymbol{p}$ and phase $\boldsymbol{\phi}$ in the outer layer, let us denote the objective function by $t(\boldsymbol{\phi}, \boldsymbol{p})$ and assume $\boldsymbol{\phi}_0$ and $\boldsymbol{p}_0$ are initial values of phase $\boldsymbol{\phi}$ and power $\boldsymbol{p}$. We have demonstrated optimizing $\boldsymbol{p}$ with fixed $\boldsymbol{\phi}_0$ in P3 is a standard convex function, and hence its convergence is readily obtained. Assuming P4 gives us $\boldsymbol{\phi}^*$ with fixed $\boldsymbol{p} = \boldsymbol{p}^*$, we can then quantize the obtained $\boldsymbol{\phi}^*$ into the set $\mathbb{F}$ of available phases for the consideration of finite phase constraint. Although the quantization of $\boldsymbol{\phi}^*$ may result in deviation from the optimal phase $\boldsymbol{\phi}^*$, heuristically optimizing $\boldsymbol{\phi}$ and $\boldsymbol{p}$ still monotonically pushes the results closer to the global or local optimum, such that $t(\boldsymbol{\phi}_0, \boldsymbol{p}_0) \leq t(\boldsymbol{\phi}_0, \boldsymbol{p}^*) \leq \cdots \leq t(\boldsymbol{\phi}^*, \boldsymbol{p}^*)$, which means the heuristic algorithm monotonically converges to the stationary

point. Due to the near-optimality, the concept of heuristic algorithm has been extensively utilized in multiple variables involved optimizations, such as joint precoder/combiner design in HBF systems [35].

3) Iterative-closed-form algorithm: In subsections 1) and 2), we have proposed two algorithms for optimizing the LUs' receiving performance with CVX solver. In this subsection, we further propose an iterative-closed-form result to further reduce the computational complexity with favorable receiving performance at the LUs. Recalling the problem P1, we first introduce auxiliary variables $\lambda_k = \tilde{\boldsymbol{h}}_k \boldsymbol{x} s_k^*,\ \forall k \in K_u$. λ_k physically represents the rotated received signal $y_k s_k^*$, as depicted in Fig. 3(c). Then the optimization problem can be equivalently written as

$$\begin{aligned} P5\ &: \underset{\boldsymbol{x}}{\text{argmax}}\ t, \\ \text{s.t}\ &(C9) : |\Im\{\lambda_k\}| \le (\Re\{\lambda_k\} - t)\tan\theta - \Theta,\ \forall k \in K_u, \\ &(C10) : \boldsymbol{x}^H \boldsymbol{A}_n \boldsymbol{x} \le p_{max}, \forall n \in N, \\ &(C11) : \lambda_k = \tilde{\boldsymbol{h}}_k \boldsymbol{x} s_k^*,\ \forall k \in K_u, \\ &(C12) : \boldsymbol{\phi}(n) \in \mathbb{F}, n \in N. \end{aligned} \tag{13}$$

Note that the term $\tilde{\boldsymbol{h}}_k \boldsymbol{x} s_k^*$ in (C9) has been replaced by λ_k, $\forall k \in K_u$. The per-antenna constraint (C10) imposes high difficulty on obtaining the iterative-closed-form result. Hence, to tackle the optimization, we can replace the per-antenna constraint by a total power constraint such that $\boldsymbol{x}^H \boldsymbol{x} \le N p_{max}$. After obtaining the optimal result, the power on each PA violating the individual power constraint will be reduced to its maximal power p_{max} to satisfy the original power constraint in (C10). We first remove constraint $(C12)$ and write the Lagrangian of P5 as

$$\begin{aligned} L = &-t + \sum_{k=1}^{K_u} \mu_k [\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta] + \\ &\sum_{k=1}^{K_u} v_k [-\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta] + \\ &\mu_0 (\boldsymbol{x}^H \boldsymbol{x} - N p_{max}) + \delta_k \sum_{k=1}^{K_u} (\tilde{\boldsymbol{h}}_k \boldsymbol{x} s_k^* - \lambda_k), \end{aligned} \tag{14}$$

where μ_k, v_k, μ_0 and δ_k are the Lagrangian multipliers. Taking derivative L with respect $\boldsymbol{x}$, we have $\frac{\partial L}{\partial \boldsymbol{x}} = \sum_{k=1}^{K_u} (\delta_k \tilde{\boldsymbol{h}}_k s_k^*) + \mu_0 \boldsymbol{x}^H = 0$, which further yields

$$\boldsymbol{x} = \sum_{k=1}^{K_u} (s_k \tilde{\boldsymbol{h}}_k^H \gamma_k), \tag{15}$$

where $\gamma_k = -\frac{\delta_k}{\mu_0},\ \forall k \in K_u$. Based on (15), we write $\boldsymbol{x}$ in a compact form as $\boldsymbol{x} = \tilde{\boldsymbol{H}}^H (\boldsymbol{\Upsilon} \circ \boldsymbol{s})$, where $\tilde{\boldsymbol{H}}^H = [\tilde{\boldsymbol{h}}_1^H, \tilde{\boldsymbol{h}}_2^H, ..., \tilde{\boldsymbol{h}}_{K_u}^H]$ and $\boldsymbol{\Upsilon} = [\gamma_1, \gamma_2, ..., \gamma_{K_u}]^T$. Also, constraint $(C11)$ can be written in a compact form as $\tilde{\boldsymbol{H}}(\boldsymbol{x} \circ \boldsymbol{s}^*) = \boldsymbol{\Lambda}$, where $\boldsymbol{\Lambda} = [\lambda_1, \lambda_2, ..., \lambda_{K_u}]^T$. Based on the two compact forms, we finally obtain the optimal result $\boldsymbol{x}^*$ as

$$\boldsymbol{x}^* = \tilde{\boldsymbol{H}}^H (\tilde{\boldsymbol{H}} \tilde{\boldsymbol{H}}^H)^{-1} \boldsymbol{\Lambda} \circ \boldsymbol{s}. \tag{16}$$

Remark 1: As indicated by (16), the vector $\boldsymbol{x}$ is related to the LUs' intended symbols $\boldsymbol{s}$ and channel $\tilde{\boldsymbol{H}}$, 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 LUs' channel information $\tilde{\boldsymbol{H}}$ and the intended symbols $\boldsymbol{s}$ are known by the transmitter, the optimal $\boldsymbol{x}^*$ is directly obtained with known value of $\boldsymbol{\Lambda}$, which can be simply calculated by solving the dual problem of P5. As suggested in (16), we now present how to find the optimal value of $\boldsymbol{\Lambda}$ to yield $\boldsymbol{x}^*$. Based on the fact that $\mu_0 > 0$, substituting (16) into constraint $(C10)$ yields $\boldsymbol{\Lambda}^H \boldsymbol{T} \boldsymbol{\Lambda} = N p_{max}$, where $\boldsymbol{T} = \text{diag}(\boldsymbol{s}^H)(\tilde{\boldsymbol{H}} \tilde{\boldsymbol{H}}^H)^{-1} \text{diag}(\boldsymbol{s})$. Since the elements of $\boldsymbol{\Lambda}$ and $\boldsymbol{T}$ are complex variables, we separate and stack their real and imaginary parts into new variables $\hat{\boldsymbol{\Lambda}}$ and $\hat{\boldsymbol{T}}$, such that $\hat{\boldsymbol{\Lambda}} = [\Re\{\boldsymbol{\Lambda}^T\}, \Im\{\boldsymbol{\Lambda}^T\}]^T$ and $\hat{\boldsymbol{T}} = [\Re\{\boldsymbol{T}\}, -\Im\{\boldsymbol{T}\}; \Im\{\boldsymbol{T}\}, \Re\{\boldsymbol{T}\}]$. It is easy to prove the validation of $\hat{\boldsymbol{\Lambda}}^T \hat{\boldsymbol{T}} \hat{\boldsymbol{\Lambda}} = N p_{max}$. Since the effect of constraint $(C11)$ has been captured in (16), constraint $(C11)$ can be omitted. Now, an equivalent problem of P5 can be given as

$$P5(a) : \underset{\boldsymbol{x}}{\text{argmax}}\ t,\ \text{s.t}\ (C9),\ (C13) : \hat{\boldsymbol{\Lambda}}^T \hat{\boldsymbol{T}} \hat{\boldsymbol{\Lambda}} = N p_{max}, \tag{17}$$

whose Lagrangian can be written as

$$\begin{aligned} L = &-t + \hat{a}_0 (\hat{\boldsymbol{\Lambda}}^T \hat{\boldsymbol{T}} \hat{\boldsymbol{\Lambda}} - N p_{max}) + \\ &\sum_{k=1}^{K} \hat{\mu_k} [\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta] + \\ &\sum_{k=1}^{K} \hat{v_k} [-\Im\{\lambda_k\} - (\Re\{\lambda_k\} - t)\tan\theta + \Theta]. \end{aligned} \tag{18}$$

For simplicity, we introduce a vector $\boldsymbol{\eta}$ to stack the Lagrangian multipliers such as $\boldsymbol{\eta} = [\hat{\mu_1}, \hat{\mu_2}, ..., \hat{\mu}_{K_u}, \hat{v_1}, \hat{v_2}, ..., \hat{v}_{K_u}]^T$ and introduce an auxiliary matrix $\boldsymbol{S} = [\boldsymbol{I}, -\frac{\boldsymbol{I}}{\tan\theta}; \boldsymbol{I}, \frac{\boldsymbol{I}}{\tan\theta}]$, where the identify matrix $\boldsymbol{I} \in \mathbb{C}^{K_u \times K_u}$. Taking derivative L with respect to $\hat{\boldsymbol{\Lambda}}$, we have $\frac{\partial L}{\partial \hat{\boldsymbol{\Lambda}}} = 2\hat{a_0} \hat{\boldsymbol{T}} \hat{\boldsymbol{\Lambda}} - \boldsymbol{S}^T \boldsymbol{\eta} = \boldsymbol{0}$. Substituting it into $(C13)$ yields $\hat{a_0} = \frac{\sqrt{\boldsymbol{\eta}^T \boldsymbol{V}^{-1} \boldsymbol{\eta}}}{4 N p_{max}}$, where $\boldsymbol{V}^{-1} = \boldsymbol{S} \hat{\boldsymbol{T}}^{-1} \boldsymbol{S}^T$. Since P5(a) is a convex optimization problem and its strong duality holds, its dual problem is given as

$$\begin{aligned} P5(b) :\ &\max_{\boldsymbol{\eta}}\ \hat{a}_0 (\hat{\boldsymbol{\Lambda}}^T \hat{\boldsymbol{T}} \hat{\boldsymbol{\Lambda}} - N p_{max}) + \boldsymbol{1}\boldsymbol{\eta}\Theta - \boldsymbol{\eta}^T \boldsymbol{S} \hat{\boldsymbol{\Lambda}} \\ &= -\sqrt{N p_{max} \boldsymbol{\eta}^T \boldsymbol{V}^{-1} \boldsymbol{\eta}} - \Theta, \\ &\text{s.t.}\ \boldsymbol{1}\boldsymbol{\eta} = 1, \boldsymbol{\eta} \ge \boldsymbol{0}, \end{aligned} \tag{19}$$

where $\boldsymbol{1}$ 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

$$P5(c) :\ \min_{\boldsymbol{\eta}}\ \boldsymbol{\eta}^T \boldsymbol{V}^{-1} \boldsymbol{\eta},\ \text{s.t.}\ \boldsymbol{1}\boldsymbol{\eta} = 1, \boldsymbol{\eta} \ge \boldsymbol{0}, \tag{20}$$

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 quadratic solvers [38] [39] [40]. When obtaining the optimal value of $\boldsymbol{\eta}$ by solving P5(c), the value of $\boldsymbol{\Lambda}$ is naturally obtained.

Now, we are able to devise the whole algorithm, as summarized in Algorithm 3. The optimal transmission vector $\boldsymbol{x}^*$ is obtained by solving the simple quadratic optimization problem in P5(c). Afterwards, the power of each PA violating the individual power constraint will be reduced to its maximal power p_{max}, and phase of each PS is quantized with Eq. (10).

Algorithm 3 Iterative-closed-form algorithm, without Eves' information

Input: LUs' estimated channel $\tilde{\boldsymbol{h}}_k$, for $\forall k \in K_u$, maximum power p_{max}, finite-resolution set $\mathbb{F}$, and intended symbol vector $\boldsymbol{s}$ for the LUs.

Output: Optimal phase $\hat{\boldsymbol{\phi}}$ and transmission power $\hat{\boldsymbol{p}}$.

1: Solve P5(c) and obtain the closed-form optimal vector $\boldsymbol{x}^*$.

2: Set $\boldsymbol{p}_n = p_{max}$ if the n-th PA violates its power constraints, $\forall n \in N$. Calculate final phase design $\hat{\boldsymbol{\phi}}$ and power design $\hat{\boldsymbol{p}}$, according to Eq. (10).

C. Receiving Performance at Potential Eves

In this subsection, we discuss the security performance when the Eves' CSI is unknown at the transmitter. Without Eves' CSI, PHY security cannot be explicitly guaranteed, which is a common scenario in DM systems [8]-[29] and conventional DBF/HBF systems [41]-[44]. A well-established approach in DBF/HBF systems is to generate isotropic AN along the null-space of the LUs' channel, whereas it is still a best-effort method. Now we present that in fact, the similar design principle has been utilized in the proposed algorithm for the first scenario.

Let us write the e-th Eve's channel $\boldsymbol{g}_e$ in the form of $\boldsymbol{g}_e = \sqrt{\rho}\boldsymbol{h}_k + \sqrt{1-\rho}\boldsymbol{\epsilon}$. 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 $\boldsymbol{\epsilon} \in \mathbb{CN}(0, \boldsymbol{I}_N)$ is a random vector independent of $\boldsymbol{h}_k$ [45]. In particular, $\rho = 0$ means the k-th LU and e-th Eve's channels are un-correlated. Hence, the received signal at the e-th Eve can be equivalently written as $y_e = \sqrt{\rho}\boldsymbol{h}_k^T\boldsymbol{x} + \sqrt{(1-\rho)}\boldsymbol{\epsilon}^T\boldsymbol{x} + n_e$, where $\boldsymbol{x}$ denotes the equivalent transmitting vector and n_e denotes the receiving noise at the e-th Eve. The first term represents the symbol of interest that is tailored for the k-th LU while the second term is a random vector varying in each transmission. Hence, the random term $\sqrt{(1-\rho)}\boldsymbol{\epsilon}^T\boldsymbol{x}$ can be utilized to randomize the distribution of the Eve' received signal and thus degrade the signal detection performance of the Eves. Similar methodology can be observed for conventional null-space AN based PHY security systems [41]-[44]. For this purpose, the power of $\sqrt{(1-\rho)}\boldsymbol{\epsilon}^T\boldsymbol{x}$ should be large enough to guarantee sufficient randomization to the phase of the Eve's received signal. With unknown $\boldsymbol{\epsilon}$, the average power of $\boldsymbol{\epsilon}^T\boldsymbol{x}$ can be approximated as $\mathbb{E}\{|\boldsymbol{\epsilon}^T\boldsymbol{x}|^2\} \approx \mathrm{Tr}(\boldsymbol{x}^H\mathbb{E}\{\boldsymbol{\epsilon}\boldsymbol{\epsilon}^H\}\boldsymbol{x}) = ||\boldsymbol{x}||^2$. Since we intend to maximize the Euclidean distance t in the signal constellation between the LUs' received signals and the decision thresholds, a high power $||\boldsymbol{x}||^2$ will be utilized at transmitter side in the optimizations. That is to say, the beam leakage $\boldsymbol{\epsilon}^T\boldsymbol{x}$ is maximized under the available power budget and acts as the null-space AN to jam the Eve in a statistical manner.

In fact, even when the LU and Eve are located in the same direction from the transmitter, their actual channels may still be different due to small scale fading, multipath and communication distance. Hence, by utilizing the channel disparity, PHY security is still obtainable (with reduced secrecy performance compared to the scenario that LUs' and Eves' channels are uncorrelated). Please not that in the rare case that the potential Eve has exactly same CSI to the LU, none of the DM and conventional DBF/HBF beamforming systems is able to guarantee PHY security, where conventional authentication/encryption is more suitable to be implemented for providing security in this case. Hence, a more meaningful scenario for evaluating the PHY security performance is when Eves' and LUs' channels are highly correlated. An example is plotted in Fig. 4 by the iterative-closed-form algorithm. It is observed that when the Eve and LU's channels are uncorrelated ($\rho = 0$ in Fig. (b)), the received signals of the Eves are randomized in the constellation panel, and hence SER of intercepting any LU is $1/M$. Nevertheless, when the correlation factor ρ increases in Figs. (c)-(d), the Eve's received signal gradually becomes similar to that of the first LU, and it is easier to intercept the LU's messages. Especially with a lower coding rate (more redundant channel coding bit in Fig. (e)), i.e., 1/4 coding rate, the Eve's block error rate (BLER) is reduced given a high channel correlation factor.

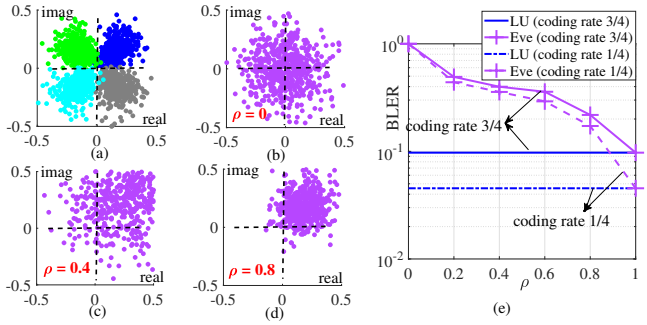

Fig. 4. QPSK and $\boldsymbol{s} = [\frac{1+1i}{\sqrt{2}}, \frac{1-1i}{\sqrt{2}}, \frac{-1+1i}{\sqrt{2}}, \frac{-1-1i}{\sqrt{2}}]$ for illustration, where cyclic redundancy check (CRC) and low-density parity-check (LDPC) coding chain is applied. For brevity, assume the Eve' channel is correlated with the first LU' channel (whose received symbols are denoted in blue). (a) The LUs' received signal is located into their constructive regions. (b)-(d) The Eve's received signal gradually becomes similar to that of the first LU (dark blue dots) with a higher correlation factor ρ.

IV. DM Design with Eves' Imperfect CSI

In Sec. III, we have investigated system design without the Eves' CSI. As discussed, the probability of Eves' intercepting increases when the Eves and LUs' channels are correlated. Aided by the symbol-level operation in DM, however, we can further deteriorate the Eves' performance when the Eves' CSI is imperfectly known by the transmitter. In the section IV-A, when the Eves' CSI is imperfectly known, the problem formulation is proposed to optimize the LUs' receiving performance while purposely deteriorating the Eve's performance in a symbol level. Then in section IV-B, we show how to find destructive regions to accommodate the Eves' symbols. Finally, three subsequent algorithms are demonstrated in section IV-C.

A. Problem Formulation

Denote the e-th Eve's channel as $\boldsymbol{g}_e = \tilde{\boldsymbol{g}}_e + \boldsymbol{e}_e$, where $\tilde{\boldsymbol{g}} \in \mathbb{C}^{1\times N}$ and $\boldsymbol{e}_e \in \mathbb{C}^{1\times N}$ denote the estimated CSI and estimation error for the e-th Eve. Since the Eves' targets are not known by the transmitter, it may be difficult to present a general geometric interpretation for accommodating the Eves' signal into destructive regions. However, we can construct artificial symbols for the Eves, which to the most extend breaks down the Eves' intercepting behaviour in a symbol level and hence the volume of the symbols being intercepted in any frame is significantly reduced. Defining s_e as the artificial symbol constructed for the e-th Eve, we have

$$\begin{aligned} P6 \ &: \underset{\boldsymbol{\phi},\boldsymbol{p}}{\text{argmax}} \ t, \\ \text{s.t} \ &(C13) : \Pr\{|\Im\{(\boldsymbol{h}_k(\boldsymbol{\phi}\circ\boldsymbol{p})+n_k)s_k^*\}| \leq \\ &\qquad (\Re\{(\boldsymbol{h}_k(\boldsymbol{\phi}\circ\boldsymbol{p})+n_k)s_k^*\} - t)\tan\theta\} \geq \Gamma, \forall k \in K_u, \\ &(C14) : \Pr\{|\Im\{(\boldsymbol{g}_e(\boldsymbol{\phi}\circ\boldsymbol{p})+n_k)s_e^*\}| \leq \\ &\qquad (\Re\{\boldsymbol{g}_e(\boldsymbol{\phi}\circ\boldsymbol{p})+n_k)s_e^*\}\tan\theta\} \geq \Gamma, \forall e \in K_e, \\ &(C15) : \boldsymbol{p}^H\boldsymbol{A}_n\boldsymbol{p} \leq p_{max}, \ (C16) : \boldsymbol{\phi}(n) \in \mathbb{F}, n \in N. \end{aligned} \tag{21}$$

In particular, constraint $(C14)$ guarantees the received symbol of the e-th Eve is purposely constructed as an artificial symbol s_e, $\forall e \in K_e$. Note that the variable t is omitted from $(C14)$. It is because we only need to push the Eve's symbols into the destructive regions, but it is not necessary to consume high power to move the Eve's symbol far from the originate. By handling the uncertainties in $(C13)$ and $(C14)$, we have

$$\begin{aligned} &(C13) : |\Im\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\}| \leq \\ &\qquad (\Re\{\tilde{\boldsymbol{h}}_k(\boldsymbol{\phi}\circ\boldsymbol{p})s_k^*\} - t)\tan\theta - \Theta, \forall k \in K_u, \\ &(C14) : |\Im\{\tilde{\boldsymbol{g}}_e(\boldsymbol{\phi}\circ\boldsymbol{p})s_e^*\}| \leq \\ &\qquad (\Re\{\tilde{\boldsymbol{g}}_e(\boldsymbol{\phi}\circ\boldsymbol{p})s_e^*\})\tan\theta - \Theta, \forall e \in K_e, \end{aligned} \tag{22}$$

To solve the optimization problem, we first need to find how to construct the "artificial symbol" s_e for the e-th Eve, $\forall e \in K_e$. Hence, in subsection IV-B, we first propose a series of schemes for creating the artificial symbols, each of them with different design objectives.

B. Schemes for Creating Artificial Symbols

Evidently, when there are empty constellation quadrants not occupied by the LUs' desired symbols, we can directly let s_e fall into the empty constellation quadrant that has largest euclidean distance with LUs' constellation quadrants, which is a common scenario when the constellation size is greater or equal to the number of LUs, such as $M \geq K_u$. When there is no empty constellation quadrant in one specific symbol-level duration, we further propose the following schemes to find a constellation quadrant for accommodating the Eve's symbol s_e, $\forall e \in K_e$.

1) Priority based Scheme: We first address the case where the LUs have different confidentiality requirements. Starting from the LU with the highest priority, we protect its constellation quadrant by removing it from the available constellation quadrants for accommodating the Eves' symbols. Then we delete the constellation quadrant occupied by the LU with the second high priority from accommodating the Eves' symbols. By doing so, the available quadrant is deleted one by one until the last quadrant is left for accommodating the Eves' symbols. Physically, the priority based scheme guarantees that the LUs with higher priority can be well protected in a symbol level, while sacrificing security of the LUs with low priority.

2) The Least Number of LUs based Scheme: By the least number of LUs based scheme, we find the constellation quadrant that is occupied by the least number of LUs, which is then used for accommodating the Eves' artificial symbol s_e. Physically, the least LU scheme guarantees that the Eves can only intercept the least number of LUs in a symbol level.

3) Round Robin based Scheme: By the round robin based scheme, we observe the history of each LU being intercepted. For example, in a frame-level duration, we find the LU being intercepted the most and protect it by deleting its constellation quadrant from accommodating the Eves' symbol. Hence, when the last quadrant is left, it is used to accommodate the Eves' smybol. Physically, the round robin based scheme addresses the security fairness among LUs.

C. Phase and Power Optimization Design

After purposely constructing the artificial symbol s_e for the Eves, we are ready to solve P6. Again, one direct-mapping, one heuristic based and one iterative-closed-form algorithm are proposed.

1) Direct-mapping algorithm: We first solve P6 without the consideration of (C16), and then map the obtained result into the closest point from $\mathbb{F}$. Removing constraint (C16) that involves finite resolution PS, P6 can be given as

$$\begin{aligned} &P7 : \underset{\boldsymbol{\phi},\boldsymbol{p}}{\text{argmax}} \ t, \\ &\text{s.t} \ (C17) : (22), \ (C15) : \boldsymbol{p}^H\boldsymbol{A}_n\boldsymbol{p} \leq p_{max}, n \in N, \end{aligned} \tag{23}$$

which is a convex optimization problem and can be readily solved by CVX. Afterwards, (10) is called to obtain the final power and phase designs. Since the convergence is similar to the proof we presented for Algorithm 1, it is omitted for brevity.

2) Heuristic algorithm: Now we propose a heuristic algorithm for further improving the LUs' performance while purposely jamming the Eves. The principle is to optimize one of the variables $\boldsymbol{p}$ and $\boldsymbol{\phi}$ assuming the other being fixed. With a similar optimization structure of P7, we first find a feasible $\boldsymbol{\phi}^{(j)}$ as our initial stage, and optimize power vector $\boldsymbol{p}$ with the given value of $\boldsymbol{\phi}^{(j)}$. After obtaining $\boldsymbol{p}^*$, we update $\boldsymbol{p}^{(j)} = \boldsymbol{p}^*$ and turn to optimize $\boldsymbol{\phi}$ with the fixed $\boldsymbol{p}^{(j)}$. The power and phase are iteratively optimized until convergence. Since it has similar structure with Algorithm 2, the mathematics and convergence discussions are omitted from brevity.

3) Iterative-closed-form algorithm: Defining $\lambda_k = \tilde{\boldsymbol{h}}_k\boldsymbol{x}s_k^*$ and $\chi_e = \tilde{\boldsymbol{h}}_e\boldsymbol{x}s_e^*$ yields

$$
\begin{aligned}
P8 \ &: \underset{\boldsymbol{x}}{\text{argmax}} \ t, \\
\text{s.t.} \ &(C18): |\Im\{\lambda_k\}| \leq (\Re\{\lambda_k\} - t)\tan\theta - \Theta, \forall k \in K_u, \\
&(C19): |\Im\{\chi_e\}| \leq \Re\{\chi_e\}\tan\theta - \Theta, \forall e \in K_e, \\
&(C20): \boldsymbol{x}^H \boldsymbol{A}_n \boldsymbol{x} \leq p_{max}, \forall n \in N, \\
&(C21): \tilde{\boldsymbol{h}}_k \boldsymbol{x} \boldsymbol{s}_k^* = \lambda_k, \forall k \in K_u, \\
&(C22): \tilde{\boldsymbol{g}}_e \boldsymbol{x} \boldsymbol{s}_e^* = \chi_e, \forall e \in K_e,
\end{aligned} \tag{24}
$$

Similarly, we replace the individual power constraint $(C20)$ with $\boldsymbol{x}^H\boldsymbol{x} \leq Np_{max}$, and obtain the iterative-closed-form result with the Lagrangian and KKT conditions. After obtaining the optimal result $\boldsymbol{x}^*$, the power of PA violating the power constraint is reduced to p_{max}. Evidently, P8 has a similar structure with P5. After a series of derivation, the optimal result is given as

$$
\boldsymbol{x}^* = \tilde{\boldsymbol{E}}^H(\tilde{\boldsymbol{E}}\tilde{\boldsymbol{E}}^H)^{-1}\boldsymbol{\Pi} \circ \hat{\boldsymbol{s}}, \tag{25}
$$

where $\tilde{\boldsymbol{E}} = [\tilde{\boldsymbol{h}}_1, ..., \tilde{\boldsymbol{h}}_{K_u}, \tilde{\boldsymbol{g}}_1, ..., \tilde{\boldsymbol{g}}_{K_e}]$ represents the equivalent channel matrix by padding the Eves' channels, $\hat{\boldsymbol{s}} = [s_1, ..., s_{K_u}, s_e, ..., s_{K_e}]^T$ denotes the equivalent symbol vector containing the desired symbols for the LUs and artificial symbols for the Eves, and $\boldsymbol{\Pi} = [\lambda_1, ..., \lambda_K, \chi_1, ..., \chi_{K_e}]$. Note that $\boldsymbol{\Pi}$ can be similarly obtained by solving the dual problem of P8, where the derivation is omitted for brevity. Afterwards, we reduce the power of the PA which dissipates more power than its constraint p_{max}, and finally the phase and power are designed with Eq. (10). Now, we are able to devise the whole algorithm. We first construct artificial symbols for the Eves by calling the schemes in subsection IV-B. Then we optimize the power and phase by the three algorithms listed in subsection IV-C.

Algorithm 4 Optimal power and phase design with the Eves' imperfect CSI

Input: LUs' estimated channel $\tilde{\boldsymbol{h}}_k$, $\forall k \in K_u$, Eve's estimated channel $\tilde{\boldsymbol{g}}_e$, $\forall e \in K_e$, power budget p_{max}, finite resolution set $\mathbb{F}$, and intended symbol vector $\boldsymbol{s}$ of the LUs.

Output: Optimal PS $\hat{\boldsymbol{\phi}}$ and power $\hat{\boldsymbol{p}}$.

1: Create artificial symbol s_e, $\forall e \in K_e$, as presented in section IV-B.
2: Obtain the optimal power and phase design by the direct-mapping, heuristic or iterative-closed-form algorithm.
3: Set $\boldsymbol{p}_n = p_{max}$ if the n-th PA violates its power constraints, $\forall n \in N$. Calculate final phase design $\hat{\boldsymbol{\phi}}$ and power design $\hat{\boldsymbol{p}}$, according to Eq. (10).

V. Complexity Analysis

In this section, the computational complexities of the proposed algorithms are evaluated. [2] For the direct-mapping algorithm (in P2), it contains $2K_u$ linear constraints and N SOC constraints. For the heuristic algorithm, it iteratively optimizes $\boldsymbol{p}$ (in P3) or $\boldsymbol{\phi}$ (in P4) assuming the other being fixed, until convergence is achieved with l_i iterations. For the iterative-closed-form algorithm, its complexity is closely related to solving the optimization problem P5(c), which is subject to $2K_u + 1$ linear constraint only. On the other hands, when potential Eves' CSI can be imperfect known at the transmitter, we are able to intentionally deteriorate Eves' receiving performance. In particular, the complexity of constructing artificial symbols is at the level of $\mathcal{O}(K_u)$. Afterwards, the complexities of the subsequent three algorithms are slightly higher than the corresponding algorithms in the first scenario, due to the additional constraints on making the Eves' received signal equivalent to the artificial symbols. For the pseudo-inverse based DM [17], its complexity is dominated by generating the pseudo-inverse matrix of the equivalent multiuser MISO channel $\boldsymbol{H}$. The pseudo-inverse matrix can be obtained by the conventional SVD approach or Cholesky decomposition [47], which have been shown to offer similar complexity. The overall complexities of the proposed algorithms are summarized in TABLE I. It is observed that the proposed algorithms have polynomial time computational complexity. The heuristic algorithms have the highest complexity as it needs to iteratively update phase and power until convergence. In comparison, the iterative-closed-form algorithm enjoys the lowest complexity. On the other hand, when the Eves' CSI can be imperfectly known at transmitter, we can further deteriorate the Eves' receiving performance with additional optimization constraints, whereas the complexities are slightly higher than the corresponding algorithms in the first scenario.

[2] For convex formulations that involve linear matrix inequality (LMI) and SOC constraints, their complexities can be evaluated as $\ln(\frac{1}{\tau})\sqrt{c_b}(c_{form} + c_{fact})$ [46]. Specifically, $\ln(\frac{1}{\tau})$ relates to the accuracy setup. $\sqrt{c_b}$ represents the barrier parameter measuring the geometric complexity of the conic constraints. c_{form} and c_{fact} represent the complexities cost on forming and factorization of $n \times n$ matrix of the linear system. We refer readers to [46] for details.

VI. Simulation Results

We present the simulated performance in this section. The central frequency is set to 2 GHz with 180 kHz bandwidth, a typical narrow bandwidth transmission scenario. Per-antenna transmission power budget is $p_{max} = 10$ dBm. The number of antennas and PSs are set to $N = 5$ at the transmitter. The number of bits in the resolution of PS is set to $b = 4$ bits except in Fig. 5 (c). Without loss of generality, we adopt QPSK modulation and assume that there are $K_u = 4$ LUs and $K_e = 1$ Eve. 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 $\sigma_n^2 = 10^{-3}$ and Rayleigh fading is considered [17] [18]. LUs' probabilistic threshold for guaranteeing SINR requirement is set to $\Gamma = 0.99$. CSI estimation error is set to $\sigma_e^2 = 10^{-4}$ except in Fig. 5 (d). Besides, the most related DM designs, pseudo inverse [17] and barrier method based [18], are selected as benchmarks. For fair comparison, the optimal phase and power of [17] and [18] are subsequently mapped by Eq. (10) considering the finite-resolution of PSs.

We first demonstrate the LUs' SER when the Eves' CSI is completely unknown at the transmitter. Fig. 5 (a) demonstrates the impact of power budget on the LUs' SER. It can be observed that the ideal case (perfect CSI acquisition and infinite resolution of PSs) achieves the best SER performance, followed by the global optimum algorithm that is achieved by

TABLE I. Complexity analysis with accuracy factor τ, where $n_1 = \mathcal{O}(N)$, $n_2 = \mathcal{O}(2K_u)$, and $n_3 = \mathcal{O}(2K_u + 2K_e)$.

Without Eves' CSI	Direct-mapping algorithm	$\ln[\frac{1}{\tau}]\sqrt{2K_u + 2N}[2n_1K_u + 2n_1^2K_u + n_1N^3 + n_1^3] + \mathcal{O}(N)$
	Heuristic algorithm	$l_i\big(\ln\frac{1}{\tau}\big)\sqrt{2K_u + 2N}[[2n_1K_u + 2n_1^2K_u + n_1N^3 + n_1^3] + \mathcal{O}(N) + [2n_1K_u + 2n_1^2K_u + n_1N^3 + n_1^3]\big)$
	Iterative-closed-form algorithm	$\ln[\frac{1}{\tau}]\sqrt{2K_u + 1}[2n_2 + 2n_2^2 + n_2^3] + \mathcal{O}(N)$
With Eves' imperfect CSI	Direct-mapping algorithm	$\ln[\frac{1}{\tau}]\sqrt{2(K_u + K_e) + 2N}(2n_1K_u + 2n_1^2(K_u + K_e) + n_1N^3 + n_1^3] + \mathcal{O}(N)$
	Heuristic algorithm	$l_i\ln[\frac{1}{\tau}]\sqrt{2(K_u + K_e) + 2N}\big([2n(K_u + K_e) + 2n_1^2(K_u + K_e) + n_1N^3 + n_1^3] + \mathcal{O}(N) + [2n_1(K_u + K_e) + 2n_1^2(K_u + K_e) + n_1N^3 + n_1^3]\big)$
	Iterative-closed-form algorithm	$\ln[\frac{1}{\tau}]\sqrt{2K_u + 1}[2n_3 + 2n_3^2 + n_3^3] + \mathcal{O}(N)$
Benchmarks	Barrier method DM [18]	$\ln(\frac{1}{\tau})\sqrt{2K_u}[2n_1K_u + 2n_1^2K_u + n_1^3] + \mathcal{O}(N)$
	Pseudo-inverse based DM [17]	$24K_u^3 + 16K_u^2N + K_u + 2K_uN + 8K_u^2N$

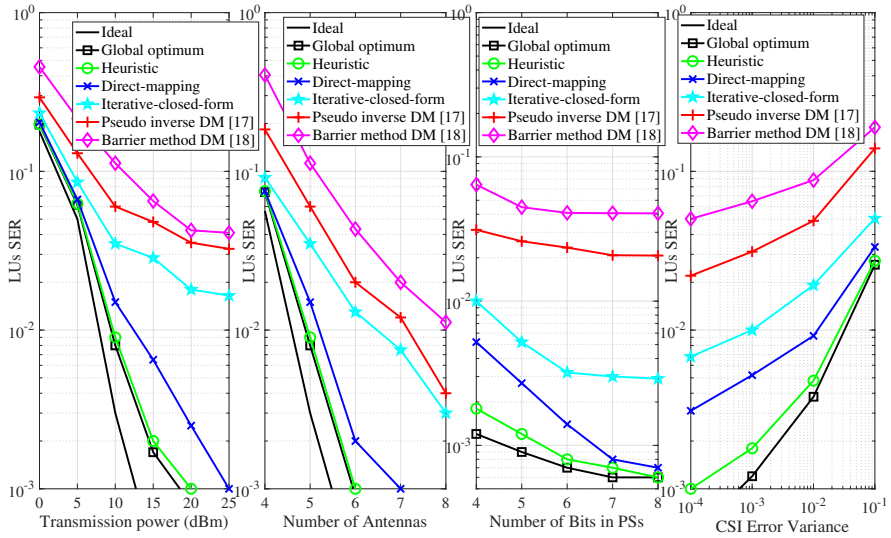

Fig. 5. When the Eves' information is completely unknown: (a) the impact of power budget p_{max} on the LUs' SER, where $b = 4$ bits and $N = 5$. (b) The impact of number of antennas on the LUs' SER performance, where $b = 4$ bits and $p_{max} = 10$ dBm. (c) The impact of number of bits of resolution of PS on the LUs' SER, where $N = 6$ and $p_{max} = 15$ dBm. (d) The impact of CSI error variance on the LUs' SER, where $b = 4$ bits, $N = 6$ and $p_{max} = 15$ dBm.

exhaustively searching all the combinations of the available phases with high complexity. While by the proposed heuristic algorithm, the phase and power are iteratively optimized until convergence, which achieves a desirable SER close to the global optimum. Also, it shows that the direct-mapping algorithm achieves an inferior SER compared to the heuristic algorithm. For the iterative-closed-form algorithm, its SER is slightly higher than the direct-mapping algorithm. It is because the iterative-closed-form algorithm first replaces the per-antenna power constraint by a total power constraints to tackle the optimization, and then reduces the power of PAs violating the individual power constraint to the maximum power p_{max}, leading to the loss of optimality. As comparisons, the two benchmarks show much higher SER compared to our proposed algorithms. In particular, the barrier method DM [18] shows the worst SER performance, since it aims to allocate the received signals of 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 pseudo-inverse based DM [17] also obtains inferior SER over our proposed algorithms, since the fixed phase DM design limits the DoFs for transmitter design. Besides, it can be seen that with a high power budget p_{max}, SER of all the algorithms can be effectively reduced. Fig. 5 (b) demonstrates SER performance with different number of antennas (also PSs) at the transmitter side. Since increasing the number of antennas improves DoFs of channel diversity and hence the DoFs for transmitter design, the LUs' SER of all algorithms can be effectively reduced. Again, the LUs' SER performance by the heuristic algorithm approaches the ideal case, even with a low number of antennas. While the number of the antennas needs to be doubled by the barrier-method algorithm to achieve the same SER performance. Also, the proposed algorithms outperform the two benchmarks with different number of antennas. Fig. 5 (c) shows the LUs' SER with different number of bits in resolution of PSs. Benefiting from the infinite-resolution PS, the LUs' SER under the ideal case remains unchanged with the value of b (equals to 0 in Fig. 5 (c)). By the heuristic and direct-mapping algorithms, the LUs' SER approaches the global optimum when b is high enough, i.e. $b \geq 5$ bits. It is because with high resolution at PS, one can always find a phase $\hat{\phi}$ from the set $\mathbb{F}$ that is close to the ideal design. For the iterative-closed-form algorithm, it has a higher level of error floor, which is caused by handling the per-antenna constraint (C10), as we discussed in Fig.

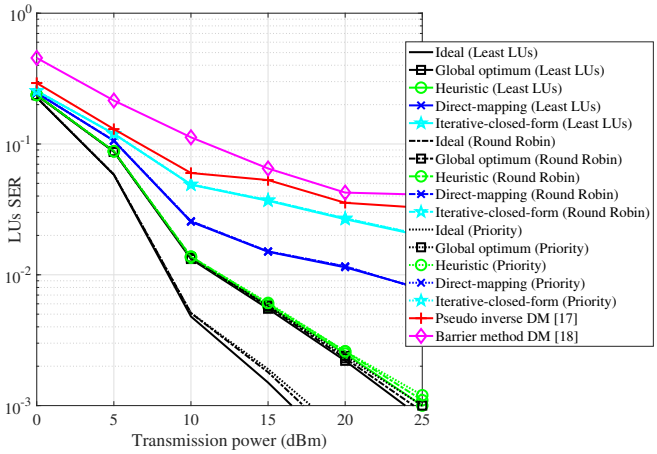

Fig. 6. The impact of power budget p_{max} on the LUs' SER, when the Eves' CSI is imperfectly known. $b = 4$ bits and $N = 5$.

5 (a). Fig. 5 (d) shows the impact of CSI uncertainty on the SER performance. It can be observed that the proposed algorithms always outperform the benchmarks. In comparison, the benchmarks ignore the impact of imperfect CSI, and the LUs' SER improves significantly with a coarse CSI quality.

Fig. 6 shows the LUs' SER when the Eves' CSI is imperfectly known at the transmitter. Since the transmitter needs to intentionally scramble the Eves while guaranteeing a low receiving SER at the LUs, the LUs' SER is slightly higher that of the first scenario, indicating there is a trade-off between optimizing the LUs' SER and deteriorating the Eves' SER. Whereas, the proposed algorithms still achieve a much lower SER for the LUs over the benchmarks. On the other hand, it can be observed that with priority, least LUs and round robins schemes for constructing artificial symbols, the LUs are able to achieve similar SER performance. It is because the priority, least LUs and round robins schemes are used to intentionally scramble Eves, and their impacts are reflected in terms of PHY security against Eves, as will be shown in Fig. 7.

Fig. 7 presents the probability density function (pdf) of the number of the intercepted symbols in each frame. Without loss of generality, LTE type 2 protocol is considered where each frame typically consists 140 symbols. (a) shows that, when the Eves' CSI is completely unknown, the Eves can averagely intercept 35 symbols in each frame. However, if the Eves and LUs' channels are correlated, i.e. $\rho = 0.4$ in (e), the Eves can intercept up to 100 symbols in a frame. On the other hand, when the Eves' CSI is imperfectly available at the transmitter, the number of the intercepted symbols can be significantly reduced by intentionally constructing artificial symbols for the Eves, even though the Eves and LUs' channels are correlated. In particular, (b) and (f) show when the priority scheme is applied for constructing artificial symbols, the LUs with higher priorities can be well protected, and the Eves only intercept 7-8 symbols on average. For the least LUs in (c) and (g), the number of the intercepted symbols centers at 10 symbols, whereas the pdf is more tailed by the least LUs scheme. It is because the least LUs scheme aims to protect the most of LUs, and one LU may be frequently intercepted if its symbols are always different from others'. Also, for the round robin scheme in (d) and (h), all the LUs are equally protected while the average number of the intercepted symbols is slightly higher than that in (c) and (g).

Fig. 8 demonstrates the throughput performance by the proposed algorithms with BPSK and 8PSK modulations respectively, where the Eves' CSI is unknown for illustration purpose. The use of throughput rather than the capacity as a performance metric is justified by the fact that DM is modulation dependent, which does not support the assumption of Gaussian signals. Following [50], we define the sum-throughput as $T = \sum_{k=1}^{K_u}(1 - BLER_k) \times \log_2 M$ where $BLER_k$ denotes the k-th LU's block error rate and can be obtained in simulation directly. $\log_2(M)$ is the bit information per symbol and K_u is the number of the LUs. It is observed that 8PSK achieves higher throughput with a high available transmission power, i.e., 10-40 dBm, while BPSK outperforms 8PSK given a low/moderate transmission power, i.e., 0-10 dBm. It is because while a higher order modulation is able to carry more bits per symbol, it needs a higher transmission power to achieve the same receiving performance with a low order modulation. It suggests modulation scheme can be properly selected according to the transmission power budget, enabling higher throughput achieved at the LUs. In addition, it has been revealed in Fig. (4) that with a low coding rate of QPSK modulation, a lower BLER performance can be achieved at the LUs due to the increased redundancy correction bits. Hence, a higher throughput is also endorsed by a low coding rate, which is not demonstrated due to the page limit.

Fig. 9 shows the impact of channel correlation on the secrecy-throughput. We use secrecy-throughput [4] [48] [49] rather than secrecy-capacity [3] as a performance metric to evaluate the proposed designs, calculated as [4] $T_{secrecy,k} = (T_k - T_e)[1 - \Pr(T_k > C_k)][1 - \Pr(T_e < C_e)]$. The term $\Pr(T_k > C_k)$ denotes the reliability outage probability occurring when the k-th LU's throughput T_k exceeds its capacity C_k, while the term $\Pr(T_e < C_e)$ denotes secrecy outage probability occurring when the e-th Eve throughput T_e is lower than its capacity C_e. Since DM is modulation dependent and does not support the Gaussian signal, the LUs and Eves' capacities are not calculable. Nevertheless, since T_k and T_e are the maximum throughputs with particular constellation and also are the actual instantaneous throughputs, the reliability and secrecy outage can be naturally guaranteed. As shown in Fig. 9 (a), when the Eves' CSI is unknown, security is addressed by the channel disparity. As a result, the secrecy throughput decreases with a higher value of ρ. However, since the proposed algorithms endorse a low SER and thus a high throughput for the LUs, the achieved secrecy throughput always outperforms the two benchmarks. On the other hand, when the Eves' CSI is imperfectly known, we can construct artificial symbols to intentionally jam the Eves. Even though Eves' channels are correlated with that of LUs, the confidential symbols being intercepted is maintained at a low level as demonstrated in Fig. 7. As a result in Fig. 9 (b), the secrecy throughput of the proposed algorithms only slightly decreases when ρ increases. It is because by pushing

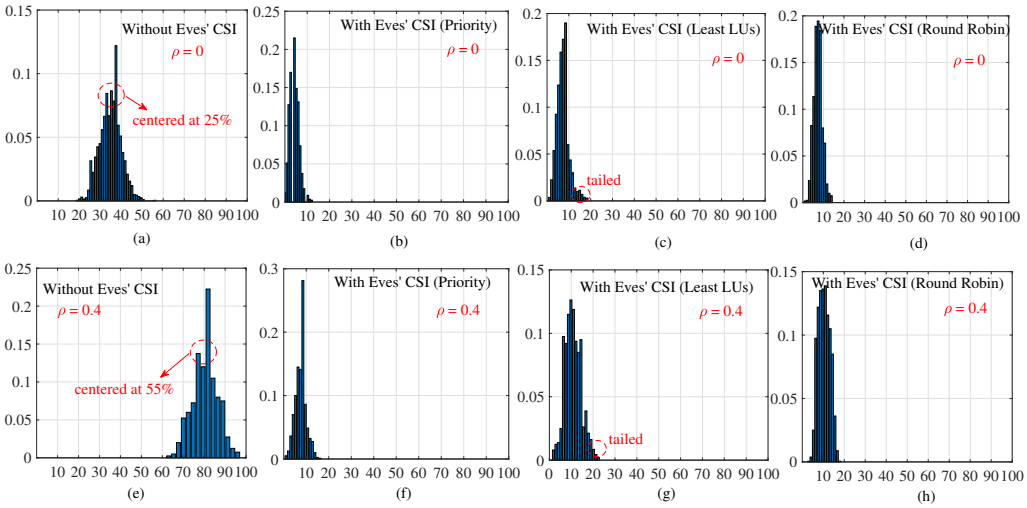

Fig. 7. The pdf of the number of the intercepted symbols, where the iterative-closed-form algorithm is applied for illustration.

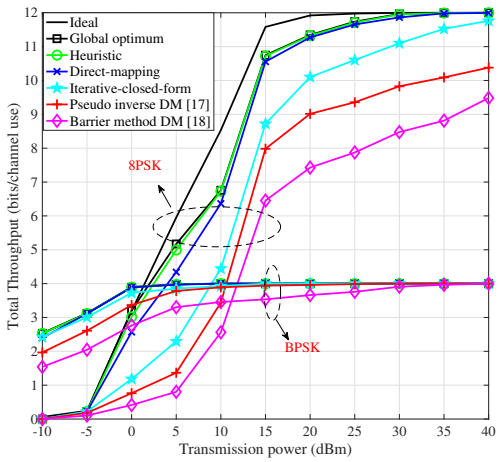

Fig. 8. Total achievable throughput of the LUs with BPSK and 8PSK modulations, where $b = 4$ bits and $N = 5$.

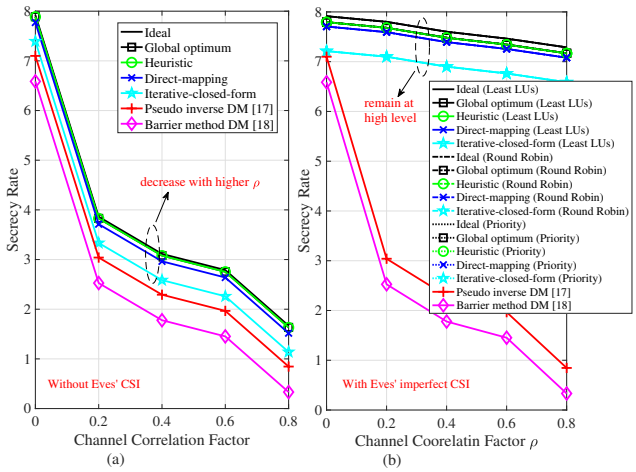

Fig. 9. Secrecy throughput comparisons with different values of channel correlation factor ρ. (a) the Eves' information is completely unknown. (b) the Eves' CSI is imperfectly obtained, where $b = 4$ bits, $N = 5$ and $p_{max} = 10$ dBm.

the Eves' signal into destructive regions, the Eves' throughput is significantly degraded. However, the LUs' throughput is also slightly reduced as a part of the transmission power is spared for jamming the Eves. It suggests a trade-off between improving the LUs' and deteriorating the Eves' performance.

Fig. 10 shows the average running time of different algorithms versus the number of LUs, where the first scenario (Eves' CSI is completely unknown) is considered as an example. It can be seen that the proposed iterative-closed-form algorithm almost requires the same running time with the simple pseudo-inverse operation in [17]. Since the pseudo-inverse has been extensively utilized for low-complexity ZF precoder/combiner design, the proposed iterative-closed-form algorithm is indeed practical and applicable in low-cost and power devices that have limited computation ability. In addition, for the CVX based heuristic and direct-mapping algorithms, they achieve better system performance at the cost of increased complexity, whereas they still require much lower running time compared to the global optimum that exhaustively searches all the combinations of the available phases. In summary, the proposed three robust algorithms make different trade-off between system performance and complexity, fully exploiting the applicability of the optimizations with heterogeneous performance requirements and computation ability.

VII. CONCLUSIONS

In this paper, we have investigated practical transmitter design under imperfect channel estimation and critical hardware impairments for realizing DM systems. When the Eves' information is completely unavailable at transmitter, phase and power designs have been jointly designed to optimize receiving

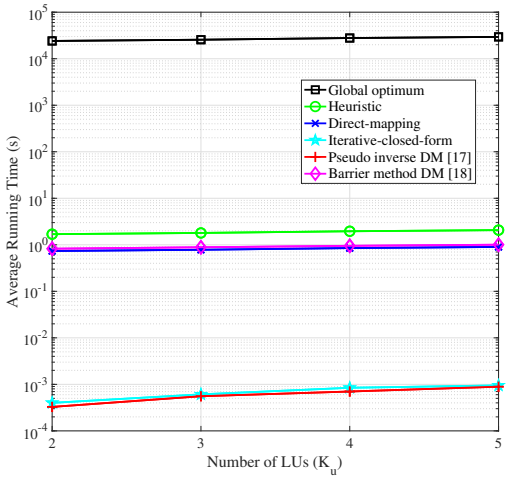

Fig. 10. The impact of the total number of users on the execution time, where p_{max}= 10 dBm, $b = 3$ bits and $N = 5$.

performance at the LUs while simultaneously randomizing the Eves' received signal. Then, when the Eves' CSI is imperfectly known at the transmitter, we further intentionally construct the Eves' signal into destructive region and protect the LUs in a symbol-level, which enables a more dedicatedly scrambling to the Eves. In all the above scenarios, three tailored algorithms are 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 or deteriorating the Eves' receiving performance. Our simulation results have showed that the proposed algorithms endorse much lower SER at the LUs, compared to the benchmarks in [17] and [18]. Especially, when the Eves' CSI is imperfectly known at the transmitter, the Eves' SER can be significantly deteriorated by the proposed algorithms over the benchmarks, which to the most extend breaks down the Eves' intercepting behaviour in a symbol-level. Hence, the secrecy throughput of the proposed algorithms is significantly improved over the benchmarks.

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, H. Zhang, I. S. Ansari, and K. A. Qaraqe, "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] Q. Li and L. Yang, "Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information," *IEEE Trans. Inf. Foren. Sec.*, vol. 13, no. 10, pp. 2628-2638, Oct. 2018.

[4] 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.

[5] E. J. Baghdady, "Directional signal modulation by means of switched spaced antennas," *IEEE Trans. Commun.*, vol. 38, no. 4, pp. 399-403, Apr. 1990.

[6] 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.

[7] A. Babakhani, "Near-field direct antenna modulation," *IEEE Microw. Mag.*, vol. 10, no. 1, pp. 36-46, Feb. 2009.

[8] M. P. Daly, "DM technique for phased arrays," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, pp. 2633-2640, Sep. 2009.

[9] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, pp. 1545-1550, May 2010.

[10] M. P. Daly and J. T. Bernhard, "Beamsteering in pattern re-configurable arrays using directional antenna," *IEEE Trans. Antennas Propag*, vol. 58, no. 7, pp. 2259-2265, Jul. 2010.

[11] 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.

[12] Y. Ding, "DM radiation pattern considerations," *IET Microw. Ant. Propag.*, vol. 7, no. 15, pp. 1201-1206, Dec. 2013.

[13] N. Valliappan, A. Lozano, and R. W. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3231-3245, Aug. 2013.

[14] N. N. Alotaibi and K. A. Hamdi, "Switched phase-array transmission architecture for secure milliliter-wave wireless transmission," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1303-1312, Mar. 2016.

[15] Y. Ding and V. Fusco, "A vector approach for the analysis and synthesis of directional modulation transmitters," *IEEE Trans. Antennas Propag.*, vol. 62, no. 1, pp. 361-370, Jan. 2014.

[16] M. Hafez and H. Arslan, "On directional modulation: An analysis of transmission scheme with multiple directions," *In Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 459-263.

[17] 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.

[18] A. Kalantari, M. Soltanalian, 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.

[19] S. Domouchtsidis, C. G. Tsinos, S. Chatzinotas, and B. Ottersten, "Symbol-level precoding for low complexity transmitter architectures in large-scale antenna array systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 2, pp. 852-863, Feb. 2019.

[20] L. N. Ribeiro, S. Schwarz, M. Rupp, and A. L. F. de Almeida, "Energy efficiency of mmwave massive mimo precoding with low-resolution DACs," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 2, pp. 298-312, May 2018.

[21] M. Mohsenpour and C. E. Saavedra, "Variable 360 vector-sum phase shifter with coarse and fine vector scaling," *IEEE Trans. Micro. Theory Tech.*, vol. 64, no. 7, pp. 2113-2120, Jul. 2016.

[22] S. Jorgensen, *Modelling of power dissipation in CMOS DACs,* Master thesis of Linkoping University, 2002, [Online] http://www.diva-portal.org/smash/get/diva2:18651/FULLTEXT01.pdf

[23] Y. Ding and V. Fusco, "Experiment of digital directional modulation transmitters," *Forum Electromagn. Res. Methods Appl. Technol.*, vol. 11, pp. 1–9, Oct. 2015.

[24] Y. Ding, Y. Zhang, and V. Fusco, "Fourier Rotman lens enabled directional modulation transmitter," *Int. J. Antennas Propag.*, vol. 15, pp. 1-13, Apr. 2015.

[25] Y. Ding, "MIMO-inspired synthesis of DM systems," *IEEE Antennas Propag. Lett.*, vol. 15, pp. 580-584, Mar. 2016.

[26] F. Shu, L. Xu, J. Wang, W. Zhu, and X. Zhou, "Artificial noise aided secure multicast precoding for directional modulation systems," *IEEE Trans. Veh. Tech.*, vol. 67, no. 7, pp. 6658-6662, Jul. 2018.

[27] T. Xie, J. Zhu, and Y. Li, "Artificial noise aided zero-forcing synthesis approach for secure multi-beam directional modulation," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 276-279, Nov. 2017.

[28] R. M. Christopher and D. K. Borah, "Iterative convex optimization of multi-beam directional modulation with artificial noise," *IEEE Commun. Lett.*, vol. 22, no. 8, pp. 1712-1716, Aug. 2018.

[29] W. Wang and Z. Zheng, "Hybrid MIMO and phased-array directional modulation for physical layer security in mmWave wireless communications," *IEEE Joural on Sel. Area in Commun.*, vol. 36, no. 7, pp. 1383-1396, Jul. 2018.

[30] W. Wang, "Frequency diverse array antenna: New opportunities," *IEEE Antennas Propag. Mag.*, vol. 57, no. 2, pp. 145–152, Apr. 2015.

[31] W. Wang, H. C. So, and A. Farina, "An overview on time/frequency modulated array processing," *IEEE J. Sel. Topics Signal Process.*, vol. 11, no. 2, pp. 228–246, Mar. 2017.

[32] C. Masouros and E. Alsusa, "Dynamic linear precoding for the exploitation of known interference in MIMO broadcast systems," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1396–1404, Mar. 2009.

[33] C. Masouros, M. Sellathurai, and T. Ratnarajah, "Vector perturbation based on symbol scaling for limited feedback MISO downlinks," *IEEE Trans. Sig. Proc.*, vol. 62, no. 2, pp. 562-571, Feb. 2014.

[34] M. Alodeh, S. Chatzinotas, and B. Ottersten, "Constructive multiuser interference in symbol level precoding for the MISO downlink channel," *IEEE Trans. Signal Process.*, vol. 63, no. 9, pp. 2239–2252, May 2015.

[35] F. Sohrabi and W. Yu, "Hybrid digital and analog beamforming design for large-scale antenna arrays," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 501-513, Apr. 2016.

[36] S. Boyd, Stanford University [2008, Winter Quarter] *Linear dynamical systems*, [Online] Available: https://stanford.edu/class/ee363/lectures/estim.pdf

[37] Z. Wei, C. Masouros, K. Wong, and X. Kang, "Multi-cell interference exploitation: a new dimension in cell coordination," *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 1303-1312, Oct. 2019.

[38] S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge, U.K.: Cambridge Univ. Press, 2004.

[39] A. Li and C. Masouros, "Interference exploitation precoding made practical: optimal closed-form solutions for PSK modulations," *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7661-7676, Nov. 2018.

[40] D. P. Bertsekas, *Convex optimization algorithms*, Belmont, MA, USA Athena Scientific, 2015.

[41] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. VTC Fall'15*, Boston, USA, 2012.

[42] X. Zhou and M. R. Mckay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Vech. Technol.,* vol. 59, no. 8, pp. 3831-3841, Oct. 2010.

[43] X. Zhang, X. Zhou, and M. R. Mckay, "On the design of artificial noise aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Vech. Technol.*, vol. 62, no. 5, pp. 2170-2182, Jun. 2013.

[44] T. Zheng, H. Wang, J. Yuan, D. Towsley, and M. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.,* vol. 63, no. 11, 4347-4362, Nov. 2015.

[45] Q. Xu, P. Ren, and A. L. Swindlehurst, "Rethinking secure precoding via interference exploitation: a smart eavesdropper perspective," 2019, [Online], Available: arXiv:1908.03174

[46] K. Wang, A. M. So, W. Ma, and C. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690-5715, Nov. 2014.

[47] L. Vandenberghe, *Applied numerical computing,* University Lecture, Dept. Elect. Eng., UCLA, Los Angeles, USA, 2012.

[48] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. M. Merolla, "Applications of LDPC codes to the wiretap channel" *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933-2945, Aug. 2007.

[49] D. Klinc, J. Ha, S. W. Mclaughlin, J. Barros, and B. J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 532-540, Sept. 2011.

[50] P. V. Amadori and C. Masouros, "Large scale antenna selection and precoding for interference exploitation," *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4529–4542, Oct. 2017.

Zhongxiang Wei (S'15–M'17) received the Ph.D. degree in electrical and electronics engineering from the University of Liverpool (UOL), Liverpool, U.K., in 2017. From March 2016 to March 2017, he was with the Institution for Infocomm Research, Agency for Science, Technology, and Research (A*STAR), Singapore, as a Research Assistant. From March 2017 to October 2017, he was a Visiting Student with the Wireless Networks and Communications Group, Harbin Institute of Technology (HIT), Shenzhen, China. He is currently a Research Associate of electrical and electronics engineering with University College London (UCL), U.K. He has authored and co-authored more than 40 research papers published on top-tier journals and international conferences. His research interests include constructive interference design, green communications, millimeter-wave communications, and algorithm design. He has acted as a TPC member or the Session Chair of various international conferences. He was a recipient of an Exemplary Reviewer of the IEEE TRANSACTION ON WIRELESS COMMUNICATIONS in 2016, the Graduate China National Scholarship Award in 2012, and the A*STAR Research Attachment Programme (ARAP) Studentship in 2016.

Christos Masouros (SMIEEE, MIET) received the Diploma degree in Electrical and Computer Engineering from the University of Patras, Greece, in 2004, and MSc by research and PhD in Electrical and Electronic Engineering from the University of Manchester, UK in 2006 and 2009 respectively. In 2008 he was a research intern at Philips Research Labs, UK. Between 2009-2010 he was a Research Associate in the University of Manchester and between 2010-2012 a Research Fellow in Queen's University Belfast. In 2012 he joined University College London as a Lecturer. He has held a Royal Academy of Engineering Research Fellowship between 2011-2016.

He is currently a Full Professor in the Information and Communication Engineering research group, Dept. Electrical and Electronic Engineering, and affiliated with the Institute for Communications and Connected Systems, University College London. His research interests lie in the field of wireless communications and signal processing with particular focus on Green Communications, Large Scale Antenna Systems, Communications and Radar Co-existence, interference mitigation techniques for MIMO and multicarrier communications. He was the recipient of the Best Paper Awards in the IEEE GlobeCom 2015 and IEEE WCNC 2019 conferences, and has been recognised as an Exemplary Editor for the IEEE Communications Letters, and as an Exemplary Reviewer for the IEEE Transactions on Communications. He is an Editor for IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, the IEEE Open Journal of Signal Processing, and Editor-at-Large for IEEE Open Journal of the Communications Society. He has been an Associate Editor for IEEE Communications Letters, and a Guest Editor for IEEE Journal on Selected Topics in Signal Processing issues "Exploiting Interference towards Energy Efficient and Secure Wireless Communications" and "Hybrid Analog/Digital Signal Processing for Hardware-Efficient Large Scale Antenna Arrays". He is currently Chair of the IEEE Special Interest Group on Energy Harvesting and an elected member of the EURASIP SAT Committee on Signal Processing for Communications and Networking.

Fan Liu (Member, IEEE) received the Ph.D. and the BEng. degrees from Beijing Institute of Technology, Beijing, China, in 2018 and 2013, respectively. He has been a visiting Ph.D. student in the Department of Electronics and Electrical Engineering, University College London between 2016-2018, where he is currently a Marie Curie Research Fellow. He was the recipient of the Best Ph.D. Thesis Award of Chinese Institute of Electronics in 2019, and the Marie Curie Individual Fellowship in 2018. He has been named as an Exemplary Reviewer for the IEEE Transactions on Wireless Communications, the IEEE Transactions on Communications and the IEEE Communications Letters. He has served as the organizer and Co-Chair of the IEEE ICC 2020 Workshop on Communication and Radar Spectrum Sharing, as well as of the ICASSP 2021 Special Session on Intelligent Sensing and Communications. He is an Editor of the IEEE Communications Letters, and is the Founding Member of the IEEE Wireless Communications Technical Committee (WTC) Special Interest Group (SIG) on Integrated Sensing and Communication (ISAC). He has authored and co-authored more than 40 research papers published on top-tier journals and conferences. His research interests include vehicular network, massive MIMO and mmWave communications, and radar signal processing.