Polarization Sensitive Array Based Physical-Layer Security

Shiqi Gong, Chengwen Xing, Sheng Chen, Fellow, IEEE, and Zesong Fei

Abstract—We propose a framework exploiting the polarization sensitive array (PSA) to improve the physical layer security of wireless communications. Specifically, the polarization difference among signals is utilized to improve the secrecy rate of wireless communications, especially when these signals are spatially indistinguishable. We firstly investigate the PSA based secure communications for point-to-point wireless systems from the perspectives of both total power minimization and secrecy rate maximization. We then apply the PSA based secure beamforming designs to relaying networks. The secrecy rate maximization for relaying networks is discussed in detail under both the perfect channel state information and the polarization sensitive array pointing error. In the later case, a robust scheme to achieve secure communications for relaying networks is proposed. Simulation results show that the proposed PSA based algorithms achieve lower total power consumption and better security performance compared to the conventional scalar array designs, especially under challenging environments where all received signals at destination are difficult to distinguish in the spatial domain.

Index Terms—Physical layer security, polarization sensitive arrays, point-to-point wireless systems, relaying networks

I. INTRODUCTION

The issue of information security in wireless networks has attracted extensive attention in recent years considering the openness of wireless links [1], [2]. Traditionally, encryption techniques are utilized to ensure secure communications, which are generally applied in the upper layer of network and have a high design complexity [3]. Therefore, an intrinsic approach exploring the characteristics of wireless fading channels to improve information security emerges as a prominent technique, which is referred to as the physical layer security [4]. The fundamental theory for physical layer security was firstly established by Shannon [5]. Following Shannon’s work, Wyner [6] introduced the famous wiretap channel model and further defined the channel secrecy capacity. The work [7] proposed a Gaussian degraded wiretap channel which is widely used to model the wireless propagation environment.

Based on these pioneering theoretical concepts, a large amount of literature focusing on various design aspects of secure communications have sprung up. By applying multiple antennas at communication nodes to exploit spatial freedom, these researches aimed to significantly improve the physical layer security of wireless networks [8]–[11]. For example, an artificial noise scheme was proposed for wiretap channels in [8] to study the impact of antenna selection on security performance of multi-input multi-output (MIMO) two-way relaying networks. The work [9] introduced an effective method called cooperative jamming to confuse the eavesdropper deliberately.

With the aid of the game theory, a collaborative physical-layer security transmission scheme was designed in [10] to effectively balance the security performance among different links. All these works however assume that the wireless channels are ideally Rayleigh distributed, which ignores the influence of array directivity and correlation. A technique known as the directional modulation was also investigated to realize secure communications. In the work [12], the directional modulation technique was applied to the phased array to offer security. Specifically, by shifting each array element’s phase appropriately, the desired symbol phase and amplitude in a given direction is generated. The study [13] on the other hand adopted the directional modulation technique to enhance the security of multi-user MIMO systems. Different from the standard secrecy rate optimization, the secure communications of multi-user MIMO systems are achieved by increasing the symbol error rate at the eavesdropper. It can be seen that the directional modulation technique designs the weighting coefficients of the phased array. As will be shown, our polarization sensitive array (PSA) based technique designs the spatial pointing of each antenna to effectively extract the signals’ polarization information for realizing secure communications.

Generally, the polarization status, similar to the amplitude and phase, is a feature of the signal. Many researches have indicated that the direction-finding performance and short-wave communication quality can be improved by means of the polarization difference among signals [14]. However, in many practical communication scenarios, such as radar and electronic reconnaissance, the conventional scalar array (CSA) is widely deployed. In essence, the CSA is the uniformly spaced linear array with the same spatial properties in all its array elements. Generally, CSA is blind to the polarization status of signal and sensitive to the array aperture and signal wavelength [15]. Worse still, in some specific array alignment, a CSA may present the morbid response to the polarization status of signal. Different from the CSA, the PSA consists of a certain number of antennas with different spatial pointings, which can be utilized to extract the signal information more meticulously and comprehensively in a vector way [16], [17]. The spatial pointings of the PSA offer extra design degrees of freedom for physical layer security of wireless networks. In most practical wireless networks, jammer is typically introduced to effectively interfere with the eavesdropper, but it simultaneously causes the interference to the destination. When the jammer signal has approximately the same spatial properties as the source, the CSA based destination beamforming optimization is unable to suppress the interference, as it can only rely on the signals’ spatial characteristics. By contrast, since different polarization information can be extracted by the spatial pointings of PSA, the PSA based destination beamforming optimization is capable of suppressing the interference effectively, even when the signals are indistinguishable in the spatial domain.

S. Gong, C. Xing and Z. Fei are with School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China (E-mails: gsyxxt163.com, xingchengwen@gmail.com, feizesong@bit.edu.cn). S. Chen is with Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (E-mail: sqc@ecs.soton.ac.uk), and also with King Abdulaziz University, Jeddah 21589, Saudi Arabia.

arXiv:1601.05982v3 [cs.IT] 2 Oct 2017
Therefore, utilizing the PSA to realize secure communications for wireless networks can achieve superior performance over the CSA design.

However, most existing PSA related works focus on the problem of estimating the signal’s direction of arrival (DOA). In [18], a two-step maximum-likelihood signal estimation procedure was developed under the PSA. Based on the sparse polarization sensor measurements, the DOA estimation of the transmitted signal was conducted in [19]. There also exist some works specifically related to the optimization of dual-polarization array to enhance the system capacity. Compared to the single polarization array, the orthogonal dual polarization antenna can enhance MIMO spatial multiplexing gain remarkably by means of the eigenvalue ratio decomposition [20].

The study [21] designed a linear-polarized dual-polarization frequency reuse system to increase spectrum utilization and further improve the system capacity, while the work [22] compared three different transmission schemes for MIMO networks to achieve the maximum diversity under a dual-polarization channel model. All these works do not consider utilizing PSA to enhance secure communications.

Against the above background, this paper investigates the PSA based secure transmission strategy for wireless networks. Specifically, we first consider the PSA based secure communications for the point-to-point single-input multi-output (SIMO) network with the aid of jammer. In this case, the secure beamforming is firstly designed aiming at minimizing the total transmit power subject to the secrecy rate requirements. Then the secrecy rate maximization scheme is proposed to improve the secrecy capacity of SIMO network as much as possible. Further extending our research into the more complicated scenario where the relay is employed to enlarge the communication coverage of source nodes, we consider the secrecy rate maximization under both perfect channel state information (CSI) and imperfect PSA pointing, respectively. It is worth noting that convex optimization techniques [23] can be utilized to solve the optimization problems formulated in this paper effectively.

The rest of the paper is organized as follows. In Section II, the system model of PSA is briefly introduced. In Section III, the point-to-point secrecy beamforming is designed for SIMO networks, while the one-way relaying network is considered in Section IV, where the corresponding secrecy rate optimization problems are formulated. Section V presents the simulation results, and our conclusions are given in Section VI.

The normal-faced lower-case letters denote scalars, while bold-faced lower-case and upper-case letters stand for vectors and matrices, respectively. | | denotes the absolute value and \( \| \| \) denotes the Euclidean norm, while \( ( \cdot )^* \), \( ( \cdot )^T \), \( ( \cdot )^H \) and \( ( \cdot )^{-1} \) represent the conjugate, transpose, conjugate transpose and inverse operators, respectively. An optimal solution is marked by \( * \), while \( tr( \cdot ) \) and \( rank( \cdot ) \) denote the trace and rank of matrix, respectively. The \( n \)-th row of matrix \( A \) is given by \( A[n, \cdot] \), and the \( n \)-th row and \( m \)-th column element of \( A \) is \( A[n, m] \). \( A \succeq 0 \) means that \( A \) is a positive semidefinite matrix. The vector stacking operator \( vec(\cdot) \) stacks the columns of a matrix on top of one another, and \( \text{diag}\{u_1, \cdots, u_N\} \) is the diagonal matrix with the diagonal elements \( u_1, \cdots, u_N \).

\( I_N \) is the \( N \times N \) identity matrix, and \( 0_{n \times m} \) is the \( n \times m \) matrix with all zero elements. \( \alpha \sim \mathcal{CN}(0, \sigma^2 I) \) means that \( \alpha \) is a complex Gaussian distributed random vector with the zero mean vector \( 0 \) and the covariance matrix \( \sigma^2 I \), while \( \mathbb{E}\{\cdot\} \) is the expectation operator. The determinant operation is denoted by \( \det(\cdot) \), and \( \otimes \) denotes the Kronecker product. Finally, \( j = \sqrt{-1} \), and \( |a|^+ = \max\{0, a\} \).

II. POLARIZATION SENSITIVE ARRAY SYSTEM MODEL

Without loss of generality, we assume that a total of \( N_D \) antennas are located in the \( y \)-axis and the distance \( d_q \) between the adjacent antennas is half wavelength, as illustrated in Fig. 1 (a). Here two plane electromagnetic (EM) signals are considered, i.e., the desired EM signal \( s_d \) and the jamming EM signal \( s_j \). They arrive at the \( N_D \) antennas of the PSA from different incident angles. As is well known, the EM wave is traveling in a single direction, where the electric component and the magnetic component are perpendicular to each other as well as perpendicular to this propagation direction. Taking the electric component as an example, we define the transverse electric field vectors of the EM signal \( s_k \) as

\[
e_{e_k}(t) = e_{h_k}(t) + e_{v_k}(t), \quad k = d, j,
\]

where \( e_{h_k}(t) \) and \( e_{v_k}(t) \) are the electric field projections on the \( e_{h_k} \) and \( e_{v_k} \) directions, respectively. As a result, the magnetic field biases of the EM signal are \( e_{v_k} \) and \( -e_{h_k} \), respectively, for keeping the orthogonality [24]. Furthermore, it is assumed that the EM signals are completely polarized signals which means that the time varying \( e_{h_k}(t) \) and \( e_{v_k}(t) \) can be formulated as an ellipse. As described in Fig. 1 (b), \( \alpha_k \) and \( \beta_k \) are the polarization orientation and ellipse angle, respectively, which represent the trace of the EM signal's electric vector and are thereafter called the POA for short. According to the EM theory [19]–[22], [24]–[26], we can express the EM signal in a vector form with its DOA \( (\theta_k, \varphi_k) \) and POA \( (\alpha_k, \beta_k) \) as follows

\[
\hat{s}_k = \mathbb{E}\{\theta_k, \varphi_k\} \mathbf{R}(\alpha_k) \mathbf{\ell}(\beta_k) = [\hat{s}_k(1) \cdots \hat{s}_k(N)]^T, \quad k = d, j,
\]

where \( \theta_k \) and \( \varphi_k \) are the azimuth and elevation angles of the EM signal \( s_k \), respectively, while

\[
\mathbb{E}\{\theta_k, \varphi_k\} = \begin{bmatrix} e_{h_k} & e_{v_k} \\ e_{v_k} & -e_{h_k} \end{bmatrix} = \begin{bmatrix} -\sin \theta_k \cos \varphi_k \cos \theta_k \\ \cos \theta_k \cos \varphi_k \sin \theta_k \\ 0 \end{bmatrix} = \begin{bmatrix} -\sin \varphi_k \cos \theta_k \\ \cos \varphi_k \cos \theta_k \\ \sin \theta_k \end{bmatrix} \begin{bmatrix} -\sin \varphi_k \\ \cos \varphi_k \sin \theta_k \\ 0 \end{bmatrix}
\]
\[ R(\alpha_k) = \begin{bmatrix} \cos \alpha_k & -\sin \alpha_k \\ \sin \alpha_k & \cos \alpha_k \end{bmatrix} \quad \text{and} \quad \ell(\beta_k) = \begin{bmatrix} \cos \beta_k \\ \sin \beta_k \end{bmatrix}. \quad (4) \]

\( \Xi(\theta_k, \varphi_k) \) is the steering matrix of \( s_k \), which is composed of the electric and magnetic field bases of the EM signal, while \( R(\alpha_k) \) and \( \ell(\beta_k) \) are the corresponding rotation and ellipticity matrix of \( s_k \), respectively. \[26\].

In addition to the polarization of EM signals, the antenna polarization should also be considered. It is noted that only short dipole antennas are adopted in our work, and thus the array magnetic response can be neglected. Besides, the polarization sensitive matrix \( P \) which represents the polarization characteristics of the array is defined by the spatial pointing angles of the \( N_D \) antennas of the PSA, i.e., \( (\theta(e,n), \varphi(e,n)) \) for \( 0 \leq n \leq N_D - 1 \), where \( \theta(e,n) \) and \( \varphi(e,n) \) are the azimuth and elevation pointing angle of the \( n \)th antenna of the PSA, respectively. Mathematically, we have

\[
P = [P_e]_0 = \begin{bmatrix} p_{e,x}^{(0)} & p_{e,y}^{(0)} & p_{e,z}^{(0)} \\ p_{e,x}^{(1)} & p_{e,y}^{(1)} & p_{e,z}^{(1)} \\ \vdots & \vdots & \vdots \\ p_{e,x}^{(N_D-1)} & p_{e,y}^{(N_D-1)} & p_{e,z}^{(N_D-1)} \end{bmatrix}, \quad (5)
\]

with

\[
\begin{bmatrix} p_{e,x}^{(n)} \\ p_{e,y}^{(n)} \\ p_{e,z}^{(n)} \end{bmatrix} = G_e \begin{bmatrix} \sin \varphi(e,n) \cos \theta(e,n) \\ \sin \varphi(e,n) \sin \theta(e,n) \\ \cos \varphi(e,n) \end{bmatrix}, \quad 0 \leq n \leq N_D - 1, \quad (6)
\]

where \( G_e \) (generally taking the value of 1) is the antenna gain when the polarization status of the EM signal perfectly matches the antenna. Note that the matrix \( 0 \) included in \( P \) indicates that the array magnetic response is ignored. In addition, for the matrix \( P_e \), we have

\[
\|P_e[n + 1, \cdot]\|^2 = 1, \quad 0 \leq n \leq N_D - 1. \quad (7)
\]

It is worth emphasizing that different from [19], where the PSA consists of the aligned short dipole antennas, each antenna of the PSA in our paper is deployed with a different spatial pointing angle, which becomes an optimization variable for secure communications.

Furthermore, the space phase matrix \( U_k \) of the EM signal \( s_k \) impinging on the PSA is given by

\[
U_k = \text{diag}\{u_{k,0}, u_{k,1}, \ldots, u_{k,N_D-1}\}, \quad (8)
\]

\[
u_{k,n} = e^{-j2\pi (\xi(\theta_k, \varphi_k) + \lambda_k n) / \lambda_k}
\]

\[
e^{j\pi n \sin \varphi_k \sin \theta_k}, \quad k = d, j, \quad 0 \leq n \leq N_D - 1, \quad (9)
\]

where \( \xi(\theta_k, \varphi_k) = -[\sin \varphi_k \cos \theta_k \quad \sin \varphi_k \sin \theta_k \quad \cos \varphi_k] \) denotes the propagation vector of the EM signal \( s_k \), \( r_n = [0, n d_a, 0]^T \) is the position vector of the \( n \)th polarization antenna, and \( \lambda_k \) is the wavelength of \( s_k \). Based on (2), (5) and (8), the spatio-polarized manifold for the EM signal \( \tilde{s}_k \) is defined as

\[
a_{\theta_k, \varphi_k, \alpha_k, \beta_k} = U_k P \tilde{s}_k = U_k P \Xi(\theta_k, \varphi_k) R(\alpha_k) \ell(\beta_k), \quad (10)
\]

for \( k = d, j \). For notational convenience, we will simplify \( a_{\theta_k, \varphi_k, \alpha_k, \beta_k} \) as \( a_k \) in the sequel.

For the sake of maximizing secrecy rate, the PSA’s spatial pointings need to be optimized. In order to perform this optimization conveniently, the formulation (10) is rewritten as

\[
a_k = U_k [P_e]_0 \tilde{s}_k = U_k P \Xi(\theta_k, \varphi_k) R(\alpha_k) \ell(\beta_k) = Q_k p, \quad (11)
\]

for \( k = d, j \), where \( p = [p_{e,x}^{(0)} \ldots p_{e,x}^{(N_D-1)} \ldots p_{e,y}^{(0)} \ldots p_{e,y}^{(N_D-1)} \ldots p_{e,z}^{(0)} \ldots p_{e,z}^{(N_D-1)}]^T\)

\[
= \text{vec}(P_e) \in \mathbb{R}^{3N_D}, \quad (12)
\]

\[
Q_k = [U_k \otimes \tilde{s}_k(1) U_k \otimes \tilde{s}_k(2) U_k \otimes \tilde{s}_k(3)] \in \mathbb{C}^{N_D \times 3N_D}. \quad (13)
\]

Clearly, the new vector \( p \) denotes the PSA’s spatial pointings and thus becomes our optimization variables.

III. POINT-TO-POINT SECRECY BEAMFORMING DESIGN

We consider the simplest but most representative wiretap channel as a source, a destination and an eavesdropper. In most cases, the capacity of the wiretap channel is higher than the main channel owing to the concealment and intention of the eavesdropper. In order to realize secure communications, we introduce a jammer to disturb the eavesdropper sufficiently. In this four-terminal network as depicted in Fig. 2, the source \( S \) and jammer \( J \) are equipped with single antenna, while the eavesdropper \( E \) and the destination \( D \) are equipped with \( N_E \) and \( N_D \) antennas, respectively. More importantly, in our work, the \( N_D \)-antenna PSA at destination \( D \) is assumed instead of the conventional CSA to fully show the advantage of PSA for secure communications.

Let \( h_{m,n} \sim \mathcal{C}\mathcal{N}(0, \sigma^2_m) \) be the channel gain vector from node \( m \) to node \( n \), where \( m = S, J \) and \( n = E \). Furthermore, we assume far field communications related to destination \( D \), and we denote \( h_{SD} \) and \( h_{JD} \) as the channel gains from source \( S \) and jammer \( J \) to the reference antenna (the first antenna) of the PSA at destination \( D \), respectively. It is worth pointing out that the eavesdropper \( E \) in our work is a legitimate, active but non-intended receiver, which means that \( E \) can simultaneously transmit signals to other nodes and intercept the confidential signal from source. Based on this assumption, the CSI of eavesdropper \( E \) is available through a training-based channel estimation technique. For the sake of improving security performance of the SIMO network, a beamforming vector \( \omega_d = [\omega_0 \ \omega_1 \cdots \omega_{N_D-1}]^T \) satisfying

\[1\] Our work can easily be extended to the more general case, where the eavesdropper is also equipped with the PSA of \( N_E \) antennas. In fact, in this case, all our designs and algorithms remains applicable and effective. Due to the space limitation, the detailed discussions are omitted here.
\[
\begin{align*}
\left( \begin{pmatrix} P_j h_{JE} h_{JE}^H + \sigma_s^2 I_{N_E} \end{pmatrix}^{-1} h_{SE} h_{SE}^H \right) & = \\
& \left( \begin{pmatrix} P_j h_{JE} h_{JE}^H + \sigma_s^2 I_{N_E} \end{pmatrix}^{-1} h_{SE} \right) \left( \begin{pmatrix} P_j h_{JE} h_{JE}^H + \sigma_s^2 I_{N_E} \end{pmatrix}^{-1} h_{SE} \right) = \\
& \lambda_{\text{max}} \sum_{\theta_{\text{max}}} \mathbf{P} S + P_J, \\
\text{s.t.} & \quad \begin{cases} 
1 + \sigma S^2 \mathbf{p}^H (\mathbf{S}^H) \mathbf{Q} \mathbf{Q}^H \mathbf{Q} \mathbf{p} + P_J |h_{SJ}^2| \mathbf{Q} \mathbf{p} + \sigma \mathbf{p} S^2 \mathbf{P} S^2 |h_{SD}^2| |h_{SJ}^2|^2 \mathbf{C}^2, \\
\geq 2 \mathbf{Q} \mathbf{p} (1 + P_J \mathbf{S}^H h_{SE} (P_j h_{JE} h_{JE}^H + \sigma_s^2 I_{N_E}^{-1} h_{SE}), \\
\text{tr} (\mathbf{p}^H \mathbf{F}_{h_p}) = 1, 0 \leq n \leq N_D - 1, \quad P_S \geq 0, P_J \geq 0.
\end{cases}
\end{align*}
\]

\[
\min_{P_S, P_J, p} \quad P_S + P_J,
\]

where \( \omega_d \) is a real vector. 

Based on (14) as well as (15) and (19), we formulate the received SINRs at destination \( D \) and eavesdropper \( E \) as

\[
\text{SINR}_D = \frac{P_S |h_{SD}|^2 |\omega_d^H \mathbf{Q} \mathbf{p}|}{\omega_d^H (\sigma^2 I_{N_D} + P_J |h_{JD}|^2 \mathbf{Q}_p \mathbf{p}^T \mathbf{Q}_j^H) \omega_d}, \\
\text{SINR}_E = \frac{P_S (\omega_e^H \mathbf{h}_{SE} |h_{SE}^H \omega_e^*|}{\omega_e^H \left( P_j h_{JE} h_{JE}^H + \sigma_s^2 I_{N_E} \right) \omega_e^*} = P_S \mathbf{h}_{SE}^H \left( P_j h_{JE} h_{JE}^H + \sigma_s^2 I_{N_E} \right)^{-1} h_{SE},
\]

respectively, where \( p^T = p^H \) applies because \( p \) is a real vector. To realize secure communication of the SIMO network, the security metric called the maximum achievable secrecy rate [6] is considered, which is defined as follows

\[
R_{\text{sec}} \leq [I(y_D, \hat{s}_d) - I(y_E, \hat{s}_d)]^+, 
\]

where \( R_{\text{sec}} \) denotes the achievable secrecy rate, \( I(y_D, \hat{s}_d) \) is the mutual information between source and destination, and \( I(y_E, \hat{s}_d) \) is the mutual information between source and eavesdropper. With the assumption of Gaussian wireless channels, \( I(y_D, \hat{s}_d) \) and \( I(y_E, \hat{s}_d) \) can readily be calculated as

\[
I(y_D, \hat{s}_d) = \log_2 (1 + \text{SINR}_D) \quad \text{and} \quad I(y_E, \hat{s}_d) = \log_2 (1 + \text{SINR}_E).
\]
optimization objective for the PSA spatial pointings\). Thus the maximum achievable secrecy rate of the SIMO network is formulated as

$$R_{\text{sec}}^{\text{max}} = \log_2 \left( \frac{P_s |h_{SD}|^2 |\omega_d|_d^2 Q_d P_p^T|^2}{1 + P_s h_{SE}^H (P_{j} h_{JE} h_{JE}^H + \sigma_d^2 I_N) h_{SE}} \right)^{1/2}.$$

(23)

For the point-to-point SIMO network, we consider two optimization problems, which are the total power minimization under secrecy rate constraint and the secrecy rate maximization under transmit power constraints, respectively.

A. Total Power Minimization

The optimization problem is defined as the one that minimizes the total transmit power of the SIMO network subject to the minimum secrecy rate constraint $R_{\text{sec}}^{\text{min}}$, that is,

$$\min_{P_s, P_j, \omega_d} P_S + P_j, \quad \text{s.t.} \quad \log_2 \left( \frac{P_s |h_{SD}|^2 |\omega_d|_d^2 Q_d P_p^T|^2}{1 + P_s h_{SE}^H (P_{j} h_{JE} h_{JE}^H + \sigma_d^2 I_N) h_{SE}} \right)^{1/2} \geq R_{\text{sec}}^{\text{min}},$$

(24)

where $P_S = P_S + P_j$, and the problem (24) is obtained, similar to the derivation of $\omega_d^{\text{opt}}$ as

$$\omega_d^{\text{opt}} = \frac{(\sigma_d^2 I_{N_D} + P_j) |h_{JD}|^2 Q_d h_{DP}^T Q_d^H}{|| (\sigma_d^2 I_{N_D} + P_j) |h_{JD}|^2 Q_d h_{DP}^T Q_d^H ||}.$$

(26)

Next we substitute (26) into (24) to reformulate the total power minimization problem as (27), which is given at the top of this page. Unfortunately, because of the nonlinear and coupled term $C_p$, which is given by

$$C_p = p^T Q_d^H Q_d p - p^T Q_d^H Q_d p = 0,$$

(28)

the optimization problem (27) is generally nonconvex and difficult to solve directly. Hence we propose a suboptimal algorithm for the optimization problem (27), i.e., (24). With this method, the optimization of $p$ is performed independently from $P_S$ and $P_j$. Specifically, since the received desired signal strength at destination $D$ in the SIMO network satisfies

$$P_S |h_{SD}|^2 |\omega_d|_d^2 |Q_d P_p^T|^2 \leq P_S |h_{SD}|^2 |\omega_d|_d^2 |Q_d P_p^T|^2 \leq P_S |h_{SD}|^2 \text{tr}(Q_d h_{DP}^T),$$

(29)

we can consider the term $P_S |h_{SD}|^2 \text{tr}(Q_d h_{DP}^T)$ as the optimization objective for the PSA spatial pointings $p$ by introducing $P_c = pp^T$. Thus, the secrecy optimization problem with respect to $p$ can be formulated as

$$\max_{P_c} \quad P_S |h_{SD}|^2 \text{tr}(Q_d h_{DP}^T), \quad \text{s.t.} \quad P_c \geq 0, \quad \text{rank}(P_c) = 1, \quad \text{tr}(Q_d h_{DP}^T) = 0,$$

(30)

where the constraint $\text{tr}(Q_d h_{DP}^T) = 0$ indicates that the interference introduced by jammer $J$ to destination $D$ can be canceled completely. However, the problem (30) is nonconvex and NP-hard due to the rank-1 constraint.

In order to find an efficient way of solving the optimization (30), we firstly relax it to a standard semidefinite programming (SDP) problem by neglecting the rank-1 constraint temporarily. Then the penalty based method [29] is utilized to obtain the finally rank-1 satisfied solution for the problem (30). To be specific, let $P_c^{\text{opt}}$ be the optimal solution of (30) without considering the rank-1 constraint. Then $\text{tr}(Q_d^H Q_d P_c^{\text{opt}})$ is actually an upper bound of $\text{tr}(Q_d^H Q_d P_c)$ in the objective function of the problem (30). With the penalty based method, this $P_c^{\text{opt}}$ is adopted as the initial point $P_c^{(0)}$ for the iterative optimization given in (31):

$$P_c^{(i+1)} = \arg \min_{P_c} \text{tr}(P_c) - \lambda_{\text{max}}(P_c^{(i)}) \quad \text{s.t.} \quad \text{tr}(Q_d^H Q_d P_c) \leq \gamma, \quad P_c \geq 0, \quad \text{tr}(Q_d^H Q_d P_c) = 0,$$

(31)

where the auxiliary variable $\gamma$ satisfying $0 \leq \gamma \leq \text{tr}(Q_d^H Q_d P_c^{\text{opt}})$, and the superscript $(i)$ denotes the iteration number, while $\lambda_{\text{max}}(P_c^{(i)})$ is the maximum eigenvalue of $P_c^{(i)}$ and $\varphi_{\text{max}}^{(i)}$ denotes the corresponding eigenvector. For a fixed $\gamma$, we can obtain the optimal rank-1 satisfied solution $P_c^{\text{opt}}$ by solving the optimization problem (31) iteratively, and the corresponding optimal $P_c^{\text{opt}}$ is calculated through the eigenvalue decomposition of $P_c^{\text{opt}}$. We utilize the bisection method [30] to perform one-dimensional search for obtaining the optimal auxiliary variable $\gamma^*$, so as to obtain the optimal solution $P^*$. The convergence of utilizing this penalty based method to solve the problem (31) is proved in Appendix.

Once the optimal $P^*$ is given, the optimal $\omega_d^*$ and the SINR at destination are derived respectively from (26) and (20) as

$$\omega_d^* = \text{tr}(Q_d P^*) \quad \text{SINR}_D = \sigma_s^2 P_s |h_{SD}|^2 ||Q_d P^*||^2.$$  

(32)

(33)

By substituting $P^*$ and $\omega_d^*$ into the original problem (24), the reformulated total power minimization problem is given by

$$\min_{P_s, P_j} \quad P_S + P_j, \quad \text{s.t.} \quad \log_2 \left( \frac{1 + P_s h_{SE}^H (P_{j} h_{JE} h_{JE}^H + \sigma_d^2 I_N) h_{SE}}{1 + P_s h_{SE}^H (P_{j} h_{JE} h_{JE}^H + \sigma_d^2 I_N) h_{SE}} \right) \geq R_{\text{sec}}^{\text{max}}, \quad P_S \geq 0, \quad P_j \geq 0.$$

(34)
After performing some mathematical transformations, we have
\[
\begin{align*}
\min_{P_S, P_J} & \quad P_S + P_J, \\
s.t. & \quad \sigma^2 (2R^0_{sec} - 1) + (2R^0_{sec} - 1) \| h_{JE} \|^2 P_J \\
+ & \left( 2R^0_{sec} \| h_{SE} \|^2 \sigma^2 - \sigma^2 | h_{SD} |^2 \right) | Q_d P^* |^2 P_S \\
+ & \left( 2R^0_{sec} \sigma^2 - \sigma^2 a \right) P^* - \| h_{SE} \|^2 | Q_d P^* |^2 \| h_{JE} \|^2 \| P_S P_J \leq 0, \\
& \quad P_S \geq 0, \quad P_J \geq 0,
\end{align*}
\]
where \( a = \| h_{SE} \|^2 \| h_{JE} \|^2 - \| h_{SE} \|^2 \| h_{JE} \|^2 \). For effectively solving the optimization problem (35), we consider different cases of the required secrecy rate threshold \( R^0_{sec} \), which corresponds to different optimal solutions of \( P_S + P_J \). Firstly, two bounds of \( R^0_{sec} \) are defined as
\[
\begin{align*}
R_1 &= \log_2 \left( \frac{\sigma^2 | h_{SD} |^2 | Q_d P^* |^2}{\sigma^2 \| h_{SE} \|^2 \sigma^2} \right), \\
R_2 &= \log_2 \left( \frac{\sigma^2 | h_{SD} |^2 | Q_d P^* |^2}{\sigma^2 \| h_{SE} \|^2 \sigma^2} \right),
\end{align*}
\]
Based on (36) and (37), the following three cases of \( R^0_{sec} \) are discussed.

1) Case 1. \( R_1 < R^0_{sec} < R_2 \): In this case, the optimization problem (35) is actually a standard geometric programming (GP) problem, which is
\[
\begin{align*}
\min_{P_S, P_J} & \quad P_S + P_J, \\
s.t. & \quad g_2 P_S^2 + g_3 P_J^2 + g_1 P_S^2 P_J^2 - 1 \\
& \quad P_S \geq 0, \quad P_J \geq 0,
\end{align*}
\]
where
\[
\begin{align*}
g_1 &= (\sigma^2 | h_{SD} |^2 | Q_d P^* |^2) - \sigma^2 \| h_{SE} \|^2 \| h_{JE} \|^2 \sigma^2 - \sigma^2, \\
g_2 &= (\sigma^2 | h_{SD} |^2 | Q_d P^* |^2) - \sigma^2 \| h_{SE} \|^2 \| h_{JE} \|^2 \sigma^2 - \sigma^2, \\
g_3 &= (\sigma^2 | h_{SD} |^2 | Q_d P^* |^2) - \sigma^2 \| h_{SE} \|^2 \| h_{JE} \|^2 \sigma^2 - \sigma^2.
\end{align*}
\]
Obviously, this optimization can be efficiently solved using the convex optimization technique to yield corresponding optimal total transmit power \( P_S^* + P_J^* \).

2) Case 2. \( R^0_{sec} \leq R_1 \): In fact, the expression \( R_1 \) denotes the maximum secrecy rate of the SIMO network without introducing jammer \( J \) under a high SINR condition. If \( R^0_{sec} \leq R_1 \) is required, it makes no sense to introduce jammer \( J \) and thus \( P_J = 0 \) is desired. Therefore, the optimization problem (35) is transformed into
\[
\begin{align*}
\min_{P_S} & \quad P_S, \\
s.t. & \quad (2R^0_{sec} \| h_{SE} \|^2 \sigma^2 - \sigma^2 | h_{SD} |^2 | Q_d P^* |^2) P_S \\
& \quad + \sigma^2 (2R^0_{sec} - 1) \| h_{SE} \|^2 \| h_{SD} \|^2 \sigma^2 P_S \| h_{JE} \|^2 \| Q_d P^* \|^2 \| h_{SE} \|^2 | Q_d P^* |^2 \| h_{JE} \|^2 \| P_S \geq 0,
\end{align*}
\]
which has the optimal source transmit power \( P_S^* \) as
\[
P_S^* = \frac{\sigma^2 (2R^0_{sec} - 1)}{2R^0_{sec} \| h_{SE} \|^2 \| h_{SD} \|^2 | Q_d P^* |^2}.
\]
In this case, the optimal total power consumption is then given by \( P_S^* + P_J^* = P_S^* \).

3) Case 3. \( R^0_{sec} \geq R_2 \): When jammer \( J \) is introduced to promote secure communications of the SIMO network, the maximum achievable secrecy rate is expressed as \( R_2 \). That is, if the required secrecy rate threshold \( R^0_{sec} \geq R_2 \), the optimization problem (35) is infeasible.

In summary, by combining the optimization problems (31), (32) and (35), the total power minimization problem (24) can be solved efficiently in a suboptimal way by optimizing the PSA spatial pointings \( p \), the receive beamforming vector \( \omega_d \), and the total transmit power \( P_S + P_J \), separately.

B. Secrecy Rate Maximization

We now investigate the secrecy rate maximization of the SIMO network subject to the total transmit power constraint \( P_{max} \). Similar to the total power minimization of (24), the secrecy rate optimization problem is formulated as
\[
\begin{align*}
\max_{P_S, P_J, \omega_d, p} & \quad \log_2 \frac{1 + \| h_{SE} \|^2 \| h_{JE} \|^2 \| Q_d P^* \|^2}{1 + \| h_{SE} \|^2 \| h_{JE} \|^2 \| Q_d P^* \|^2} \\
s.t. & \quad \tr(p^T F_s p) = 1, \ 0 \leq n \leq N_D - 1, \\
& \quad P_S + P_J \leq P_{max}, \quad P_S \geq 0, \quad P_S \geq 0.
\end{align*}
\]
Likewise, the problem (44) is difficult to solve directly. However, it is known that the secrecy rate maximization problem with total power constraint is equivalent to the total power minimization problem with the secrecy rate threshold in essence. As a result, we can also apply the proposed suboptimal algorithm for problem (24) to the problem (44). The concrete solutions are presented as follows. Firstly, according to (30), the PSA spatial pointings \( P \) is optimized to maximize the received signal strength at destination with eliminating the interference introduced by jammer. Then the joint optimization among remaining variables \( \{ P_S, P_J, \omega_d \} \) is performed. Particularly, the optimal \( \omega_d \) for problem (44) is not related to \( \{ P_S, P_J \} \) due to the zero interference \( \tr(Q_j^H Q_j P_c) = 0 \) required in (30). As such, we can derive the optimal \( \omega_d \) by maximizing the destination SINR as in (32). Further, the joint optimization of \( \{ P_S, P_J \} \) is presented in the following problem (45) based on the obtained \( P \) and \( \omega_d \).

\[
\begin{align*}
\max_{P_S, P_J} & \quad \log_2 \frac{1 + \| h_{SE} \|^2 \| h_{JE} \|^2 | Q_d P^* |^2}{1 + \| h_{SE} \|^2 \| h_{JE} \|^2 | Q_d P^* |^2} \\
s.t. & \quad P_S + P_J \leq P_{max}, \quad P_S \geq 0, \quad P_S \geq 0,
\end{align*}
\]
It is natural that the optimal solution of the problem (45) is achieved when the constraint \( P_S + P_J = P_{max} \) holds. Therefore, we further rewrite the problem (45) as
\[
\max_{0 \leq P_S \leq P_{max}} \ f(P_S),
\]
where
\[
f(P_S) = \frac{l_1 P_S^2 - l_4 P_S - l_1}{l_3 P_S^2 - l_2 P_S - l_1},
\]
and
\[
\begin{align*}
l_1 &= \sigma^2 + P_{max} \| h_{JE} \|^2, \\
l_2 &= \| h_{SE} \|^2 - \| h_{JE} \|^2 + P_{max} l_3, \\
l_3 &= \sigma^2 - \sigma^2 a, \\
l_4 &= \sigma^2 | h_{SD} |^2 \| Q_d P^* |^2 (P_{max} \| h_{JE} \|^2 + \sigma^2) - \| h_{JE} \|^2, \\
l_5 &= \sigma^2 | h_{SD} |^2 | h_{SD} |^2 | h_{JE} |^2.
\end{align*}
\]
It can be seen that the optimization problem (46) is an unconstrained quadratically fractional function maximization problem, whose the optimal solution $P^*_S$ can easily be derived by the quadratic discriminant method, which is

$$P^*_S = \min \{ P_{\text{max}}, P'_S \}, \quad (49)$$

with

$$P'_S = \left[ \frac{-l_1(l_3-l_5)+\sqrt{l_1^2(l_3-l_5)^2-l_1(l_3l_4-l_5l_2)(l_4-l_2)}}{l_3l_4-l_5l_2} \right]^+. \quad (50)$$

Once the optimal $P^*_S$ is obtained, the optimal $P^*_j = P_{\text{max}} - P^*_S$. Given the optimal source and jammer transmit powers $P^*_S$ and $P^*_j$, we can accordingly determine the maximum achievable secrecy rate of the SIMO network via (23). It is worth reiterating that the ‘optimal’ PSA spatial pointing vector $P^*$, the receive beamforming vector $\omega^*_d$, the transmit power pairs $P^*_S$ and $P^*_j$ so obtained do not offer an optimal solution of the optimization problem (44). Rather they only provide a suboptimal solution.

IV. RELAY AIDED SECRECY BEAMFORMING DESIGN

We now extend the secure beamforming design to the relaying network with PSA. Specifically, two cases are considered, where the first case assumes that the perfect CSI in the relay network is available and the other one considers the imperfect PSA spatial pointings. For the both cases, we aim at improving the secrecy rate of the relaying network as much as possible.

A. Secrecy Rate Maximization with Perfect CSI

Similar to Section III, the scalar $h_{mn} \sim \mathcal{CN}(0, \sigma_m^2)$ denotes the flat-fading and quasi-static channel from node $m$ to node $n$ where $m = S, J$ and $n = E$, while $h_{SR}$ and $h_{JR}$ denote the channel gains from source $S$ and jammer $J$ to the reference antenna of the relay’s PSA, respectively. Furthermore, the CSI of eavesdropper $E$ is assumed to be available. Based on these assumptions, the received signals at the $N_R$ antennas of relay $R$ in the MAC phase can be expressed as

$$y_R = \tilde{Q}_d \tilde{p}_h_{SR} \sqrt{P_S} \tilde{s}_d + \tilde{Q}_j \tilde{p}_h_{JR} \sqrt{P_j} \tilde{s}_j + n_R, \quad (51)$$

where $\tilde{s}_d$ and $\tilde{s}_j$ are the transmit signals of source $S$ and jammer $J$, respectively, with $E\{ |\tilde{s}_d|^2\} = E\{ |\tilde{s}_j|^2\} = 1$, $P_S$ and $P_j$ are the transmit powers of source $S$ and jammer $J$, respectively, while $n_R \in \mathbb{C}^{N_R}$ is the Gaussian noise vector at relay $R$ whose elements follow the distribution $\mathcal{CN}(0, \sigma_E^2)$. The spatio-polarized manifold matrices $Q_k \in \mathbb{C}^{N_k \times 3N_R}$ for $k = d, j$ are defined similarly to (13), and the relay’s PSA spatial pointing vector $\tilde{p} \in \mathbb{R}^{3N_R}$ is defined similarly to (12). The wiretapped signal at $E$ in this phase is given by

$$y_E^{(1)} = h_{SE} \sqrt{P_S} \tilde{s}_d + h_{JE} \sqrt{P_j} \tilde{s}_j + n_E^{(1)}$$

$$= h_{SE} \sqrt{P_S} \tilde{s}_d + n_E^{(1)}, \quad (52)$$

where the additive Gaussian noise $n_E^{(1)}$ follows the distribution $\mathcal{CN}(0, \sigma_E^2)$, and $n_R^{(1)} = h_{JE} \sqrt{P_j} \tilde{s}_j + n_E^{(1)}$.

In the BC phase, relay $R$ utilizes the amplify-and-forward (AF) strategy to forward the received signal $y_R$. To be specific, the retransmitted signal is $y_R = W y_R$, where $W \in \mathbb{C}^{N_R \times N_R}$ denotes the AF beamforming matrix. Thus, the transmit power of $R$ is given by

$$P_R = P_S |h_{SR}|^2 |W \tilde{Q}_d \tilde{p}|^2 + P_j |h_{JR}|^2 |W \tilde{Q}_j \tilde{p}|^2$$

$$+ \sigma^2 \text{tr}(WW^H). \quad (53)$$

Simultaneously, jammer $J$ sends the interference signal $\tilde{s}_j$ with power $P_j^{(2)}$ to $D$. Let $h_{RD} \in \mathbb{C}^{1 \times N_R}$ and $h_{RE} \in \mathbb{C}^{1 \times N_R}$ be the channel gain vectors from the $N_R$ antennas of relay $R$ to destination $D$ and eavesdropper $E$, respectively, while $h_{JD}$ denotes the channel gain from $J$ to $D$. Then the received signals at $D$ and $E$ are formulated respectively as

$$y_D = h_{RD} \tilde{Q}_d \tilde{p}_h_{SR} \sqrt{P_S} \tilde{s}_d + n_D$$

$$= h_{RD} \tilde{Q}_d \tilde{p}_h_{SR} \sqrt{P_S} \tilde{s}_d + n_D, \quad (54)$$

$$y_E^{(2)} = h_{RE} \tilde{Q}_j \tilde{p}_h_{SR} \sqrt{P_j} \tilde{s}_j + n_E^{(2)}$$

$$= h_{RE} \tilde{Q}_j \tilde{p}_h_{SR} \sqrt{P_j} \tilde{s}_j + n_E^{(2)}. \quad (55)$$

Due to the fact that relay $R$ adopts the PSA as the transmit array, its antenna correlation matrix $R_{\text{cor}} \in \mathbb{C}^{N_R \times N_R}$ must be considered, whose elements follow the exponential model of $R_{\text{cor}}[n, m] = p^{\lceil |n-m| \rceil}$ for $1 \leq n, m \leq N_R$ with constant $p$ [31]. The additive Gaussian noises at destination $D$ and eavesdropper $E$ are $n_D \sim \mathcal{CN}(0, \sigma_D^2)$ and $n_E^{(2)} \sim \mathcal{CN}(0, \sigma_E^2)$.

Fig. 3. A two-hop network with the polarization sensitive array having $N_R$ antennas at relay.
respectively, while the equivalent noise-plus-interference terms $\tilde{n}_D$ and $\tilde{n}_E^{(2)}$ are given by

\[
\tilde{n}_D = h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} h_{JR} \sqrt{p_{J}^{(1)} s_j} + \sqrt{p_{J}^{(2)} s_j} + K_e,
\]

\[
\tilde{n}_E^{(2)} = h_{RE} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} h_{JE} \sqrt{p_{J}^{(1)} s_j} + \sqrt{p_{J}^{(2)} s_j} + K_e.
\]

(56)

(57)

Clearly, the total amount of information leakage to $E$ comes from both $S$ and $R$, as indicated in (52) and (55). Hence, the wiretapped information in the relay network is given by

\[
y_E = \begin{bmatrix}
h_{SE} \\
h_{RE} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} h_{SR}
\end{bmatrix} \sqrt{P_S \tilde{s}_d} + \begin{bmatrix}
\tilde{n}_E^{(1)} \\
\tilde{n}_E^{(2)}
\end{bmatrix}.
\]

(58)

The covariance matrix $O_E$ of $\tilde{n}_E$ and $O_D = E[\tilde{n}_D^{2}]$ are given by (59) and (60), respectively, at the top of the next page, in which $K_e = p_{J}^{(1)}|h_{JE}|^2 + \sigma_e^2|h_{RE} R_{cor}^{\frac{1}{2}} W|^2 + \sigma^2_d$. Correspondingly, the achievable secrecy rate region of this relaying network is

\[
\tilde{R}_{sec} \leq \left[ \tilde{I}(y_d, \tilde{s}_d) - \tilde{I}(y_e, \tilde{s}_d) \right]^+,
\]

(61)

in which the mutual information between source $S$ and destination $D$ and the mutual information between source $S$ and eavesdropper $E$ are given respectively by

\[
\tilde{I}(y_d, \tilde{s}_d) = \log_2(1 + P_S|h_{SR}|^2|h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} |O_D),
\]

\[
\tilde{I}(y_e, \tilde{s}_d) = \log_2 \det \left( I_2 + P_S H_E H_E^{\dagger} O_E^{-1} \right).
\]

(62)

(63)

The optimization problem for the proposed secure beamforming design is formulated as

\[
\max_{P_j^{(1)}, P_j^{(2)}, W, \tilde{p}} \log_2 \frac{1 + P_S|h_{SR}|^2|h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} |^2}{\det \left( I_2 + P_S H_E H_E^{\dagger} O_E^{-1} \right)},
\]

\[
\text{s.t.} \quad \text{tr}(\tilde{p}^{\dagger} F_0 \tilde{p}) = 1, \quad 0 \leq n \leq N_R - 1,
\]

\[
P_S|h_{SR}|^2 ||\tilde{W} \tilde{Q}_d \tilde{p} ||^2 + P_{J}^{(1)} |h_{JR}|^2 ||\tilde{W} \tilde{Q}_j \tilde{p} ||^2 
+ \sigma_e^2 \text{tr}(H_W H_W^{\dagger}) \leq P_{max},
\]

\[
0 \leq P_{J}^{(1)} + P_{J}^{(2)} \leq P_{max}.
\]

(64)

where the definition of $\tilde{R}_n \in \mathbb{R}^{3N_R \times 3N_R}$ is similar to that of $F_n$ given in Section III-A, while $P_{max}$ and $P_{max}^*$ are the maximum relay and jammer transmit powers, respectively. It can be observed that the objective function of this problem is a product of two correlated generalized Rayleigh quotients and is obviously nonconvex. Thus this optimization is difficult to solve directly. Since eavesdropper $E$ is a legitimate although not an intended receiver, we assume that the perfect CSI of $E$ is available. Then the following operations are performed.

1) As the perfect CSI of $E$ is available, the beamforming matrix $W$ is designed to satisfy $h_{RE} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} = 0$. Thus the information leakage from $R$ to $E$ is canceled completely. With this beamforming matrix design, jammer $J$ does not need to transmit signal $s_j$ to decrease the information leakage caused by $R$, which means that $P_{J}^{(2)} = 0$.

2) As destination $D$ is disturbed by the forwarded jammer signal $\tilde{s}_j$ from the MAC phase, the beamforming matrix $W$ should be designed to satisfy $h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} = 0$ to eliminate the interference to $D$ caused by jammer $J$ completely.

3) Since only jammer signal $\tilde{s}_j$ is utilized to decrease the information leakage to $E$ in the MAC phase and $P_{J}^{(2)} = 0$, we can set $P_{J}^{(1)} = P_{max}^*$ to interfere eavesdropper maximally. Thus the power allocation for jammer $J$ is determined.

With the operations 1) to 3), the information leakage only occurs in the MAC phase, and the mutual information

\[
\tilde{I}(y_d, \tilde{s}_d) = \log_2 \left( 1 + \frac{P_S|h_{SR}|^2}{\sigma^2_e + \sigma^2_d + P_{max}^* |h_{JE}|^2} \right).
\]

(65)

(66)

Thus the secrecy rate maximization problem (64) can be re-expressed as

\[
\max_{W, \tilde{p}} \log_2 \frac{1 + P_S|h_{SR}|^2|h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} |^2}{\sigma^2_e + \sigma^2_d + P_{max}^* |h_{JE}|^2},
\]

\[
\text{s.t.} \quad \text{tr}(\tilde{p}^{\dagger} F_0 \tilde{p}) = 1, \quad 0 \leq n \leq N_R - 1,
\]

\[
h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} = 0, \quad h_{RE} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} = 0,
\]

\[
P_S|h_{SR}|^2 ||\tilde{W} \tilde{Q}_d \tilde{p} ||^2 + P_{max}^* |h_{JR}|^2 ||\tilde{W} \tilde{Q}_j \tilde{p} ||^2 
+ \sigma_e^2 \text{tr}(H_W H_W^{\dagger}) \leq P_{max}^*.
\]

(67)

Unfortunately, this problem is still neither convex nor concave with respect to $W$ and $\tilde{p}$. Similar to solving (24), we propose an iterative suboptimal algorithm to solve (67) effectively.

1) Optimization of $W$: When the PSA spatial pointing vector is fixed to $\tilde{p} = \tilde{p}^{(l-1)}$ where $l$ is the outer iteration index and $\text{tr}(\tilde{p}^{(l-1)^{\dagger}} F_0 \tilde{p}^{(l-1)}) = 1$ for $0 \leq l \leq N_R - 1$, the problem (67) is transformed into

\[
\max_{W} \log_2 \frac{1 + P_S|h_{SR}|^2|h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} |^2}{\sigma^2_e + \sigma^2_d + P_{max}^* |h_{JE}|^2},
\]

\[
\text{s.t.} \quad \text{tr}(\tilde{p}^{\dagger} F_0 \tilde{p}) = 1, \quad 0 \leq n \leq N_R - 1,
\]

\[
h_{RD} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} = 0, \quad h_{RE} R_{cor}^{\frac{1}{2}} W \tilde{Q}_d \tilde{p} = 0,
\]

\[
P_S|h_{SR}|^2 ||\tilde{W} \tilde{Q}_d \tilde{p} ||^2 + P_{max}^* |h_{JR}|^2 ||\tilde{W} \tilde{Q}_j \tilde{p} ||^2 
+ \sigma_e^2 \text{tr}(H_W H_W^{\dagger}) \leq P_{max}^*.
\]

(68)
\[
\mu = \left( (G_{je}^{(l-1)\perp})^\top (P_{R}^{\text{max}} G_h + P_S |h_{SR}|^2 R_{d}^{(l-1)} + P_{J}^{\text{max}} |h_{JR}|^2 R_{j}^{(l-1)} + \sigma^2 \mathbf{I}_{N_R}^\perp) G_{je}^{(l-1)\perp} \right)^{-1} (G_{je}^{(l-1)\perp})^\top g_d^{(l-1)}, \tag{78}
\]
\[
c(p^{(l-1)}) = \sqrt{P_{R}^{\text{max}} / \left( \mu^\top (G_{je}^{(l-1)\perp})^\top (P_S |h_{SR}|^2 R_{d}^{(l-1)} + P_{J}^{\text{max}} |h_{JR}|^2 R_{j}^{(l-1)} + \sigma^2 \mathbf{I}_{N_R}^\perp) G_{je}^{(l-1)\perp} \mu \right)}. \tag{79}
\]

After some manipulations, (68) can be rewritten as

\[
\begin{align*}
\max_{\omega_R} \quad & 1 + P_S |h_{SR}|^2 |\omega|^4 (G_{je}^{(l-1)\perp})^\top \omega_R, \\
\text{s.t.} \quad & (g_{k}^{(l-1)})^\top \omega_R = 0, \quad (g_{l}^{(l-1)})^\top \omega_R = 0, \\
& \omega_R^\top (P_S |h_{SR}|^2 R_{d}^{(l-1)} + P_{J}^{\text{max}} |h_{JR}|^2 R_{j}^{(l-1)} + \sigma^2 \mathbf{I}_{N_R}^\perp) \omega_R \leq P_{R}^{\text{max}},
\end{align*} \tag{69}
\]

where
\[
\omega_R = \text{vec}(W) \in \mathbb{C}^{N_R^2}, \tag{70}
\]
\[
g_{k}^{(l-1)} = (\hat{Q}_k p^{(l-1)})^\top \otimes (h_{RD} R_{d}^{(l-1)})^\top \in \mathbb{C}^{N_R^2}, \tag{71}
\]
\[
g_{l}^{(l-1)} = (\hat{Q}_l p^{(l-1)})^\top \otimes (h_{RE} R_{d}^{(l-1)})^\top \in \mathbb{C}^{N_R^2}, \tag{72}
\]
\[
G_{d}^{(l-1)} = g_{d}^{(l-1)}(\omega_R)^\top, \tag{73}
\]
\[
G_{h} = (I_{N_R} \otimes (h_{RD} R_{d}^{(l-1)})^\top) (I_{N_R} \otimes (h_{RE} R_{d}^{(l-1)})^\top), \tag{74}
\]
\[
R_{d}^{(l-1)} = (\hat{Q}_d ^{\top} p^{(l-1)})^\top \otimes I_{N_R} \otimes (h_{RD} R_{d}^{(l-1)})^\top \otimes I_{N_R}, \tag{75}
\]

Let \( G_{je}^{(l-1)\perp} \) be the projection matrix onto the null space of \( G_{je}^{(l-1)} = [g_{j}^{(l-1)}, g_{e}^{(l-1)}]^\top \). Then the \( N_R^2 \)-dimensional relay beamforming vector is denoted as \( \omega_R = G_{je}^{(l-1)\perp} \omega_R \), which transforms the original optimization variable \( \omega_R \) into \( \omega_R \). Thus, the problem (69) can be rewritten as

\[
\max_{\omega_R} \quad 1 + P_S |h_{SR}|^2 |\omega_R|^4 (G_{je}^{(l-1)\perp})^\top \omega_R, \\
\text{s.t.} \quad \omega_R^\top (P_S |h_{SR}|^2 R_{d}^{(l-1)} + P_{J}^{\text{max}} |h_{JR}|^2 R_{j}^{(l-1)} + \sigma^2 \mathbf{I}_{N_R}^\perp) \omega_R \leq P_{R}^{\text{max}},
\]

The problem in (76) is also a generalized Rayleigh quotient problem, which has the closed-form solution
\[
\tilde{\omega}_{R}^{(l)} = c(p^{(l-1)}) \mu, \tag{77}
\]
with \( \mu \) and \( c(p^{(l-1)}) \) given by (78) and (79), respectively, at the top of this page. Once the optimal \( \tilde{\omega}_{R}^{(l)} \) is obtained, the optimal \( \tilde{W}^{(l)} \) can be derived based on \( \omega_R^{(l)} = G_{je}^{(l-1)\perp} \tilde{\omega}_{R}^{(l)} \).

2) Optimization of \( \tilde{p} \): Given \( W^{(l)} \), the optimization problem (67) is rewritten as

\[
\max_{\tilde{p}} \quad 1 + P_S |h_{SR}|^2 |\tilde{p}|^4 (W^{(l)})^\top (R_{d}^{(l-1)})^\top h_{RD} h_{RD} R_{d}^{(l-1)} W^{(l)} \tilde{Q}_d \tilde{p},
\]

s.t. \( \tilde{p}^\top F_n \tilde{p} = 1, \quad 0 \leq n \leq N_R - 1, \quad \tilde{p} \geq 0, \quad \text{rank}(\tilde{p}_c) = 1, \quad \tilde{p}_c \geq 0, \quad \text{tr} (\hat{F}_n^\top \hat{F}_n \tilde{p}_c) = 1, \quad e_{d,j} \leq \tilde{p} \leq \tilde{p}_c, \quad \text{tr} (\hat{F}_n^\top \hat{F}_n \tilde{p}_c) = 1, \tag{81}
\]

Then the feasible \( \tilde{p} \) must be in the null-space of \( \tilde{P}_c^{(l)} \). Therefore, \( \tilde{p} = \tilde{P}_c^{(l)\perp} \tilde{p}_c \), where \( \tilde{P}_c^{(l)\perp} \) denotes the projection matrix onto the null space of \( \tilde{P}_c^{(l)} \) and \( \tilde{p}_c \) is the equivalent variable vector to be optimized. By defining the Hermitian matrix \( \tilde{P}_c = \tilde{p}_c \tilde{p}_c^\top \), the problem (80) is rewritten as

\[
\max_{\tilde{P}_c} \quad P_S |h_{SR}|^2 |\tilde{P}_c| \tilde{p}_c, \\
\text{s.t.} \quad \text{tr} (\hat{F}_n^\top \hat{F}_n \tilde{P}_c) = 1, \quad 0 \leq n \leq N_R - 1, \quad \tilde{P}_c \geq 0, \quad \text{rank}(\tilde{P}_c) = 1, \tag{82}
\]

It is observed that the problem (82) becomes a standard SDP problem if the rank-1 constraint is not considered. Similar to solving (30), we utilize the penalty based method to solve (82). The corresponding iterative optimization problem (86) is given at the bottom of this page, where the superscript \( [l] \) denotes the inner iteration index, and \( \tilde{\omega}_{\text{max}} \) is the eigenvector corresponding to the maximum eigenvalue \( \lambda_{\text{max}}(\tilde{P}_c^{(l)}) \). Note

\[
\tilde{P}_{c}^{[l+1]} = \arg \min_{\tilde{P}_c} \text{tr}(\tilde{F}_n \tilde{p}_c) - \lambda_{\text{max}}(\tilde{P}_c) - \text{tr}(\tilde{\omega}_{\text{max}}(\tilde{P}_c) \tilde{p}_c) - \text{tr}(\tilde{R}_d^\top \tilde{P}_c),
\]

s.t. \( \text{tr}(\tilde{R}_d^\top \tilde{P}_c) \leq \tilde{\gamma}_d, \quad \text{tr}(P_S |h_{SR}|^2 G_{d}^{(l)} + P_{J}^{\text{max}} |h_{JR}|^2 G_{j}^{(l)} \tilde{P}_c) \leq P_{R}^{\text{max}} - \sigma^2 \text{tr}(W^{(l)} (W^{(l)})^\top), \tag{86}
\]

\[
\tilde{P}_c \geq 0, \quad \text{tr}(\tilde{F}_n \tilde{P}_c) = 1, \quad 0 \leq n \leq N_D - 1.
\]
the bisection method are jointly applied to iteratively solve (86) to obtain the optimal rank-1 constraint. Furthermore, the penalty based method and the eigenvalue decomposition on the optimal solution obtained in Subsection IV-A, the optimal PSA pointing, which has the Cholesky decomposition, can be obtained by the eigenvalue decomposition on \( \tilde{P}^{[0]} \). Since the iterative optimization (86) has exactly the same form as the iterative algorithm for solving (86) is guaranteed.

Thus, instead of jointly optimizing \( \tilde{p} \) and \( W \), we optimize \( W \) and \( \tilde{p} \) separately in an iterative procedure involving steps 1 and 2. Specifically, with the initial iteration index \( l = 1 \) and a feasible initial \( \tilde{p}^{[l-1]} \), we obtain the optimal beamforming matrix \( W^{[l]} \) using the closed-form solution (77). Then with \( W^{[l]} \), the optimal PSA pointing vector \( \tilde{p}^{[l]} \) is determined by solving (86) iteratively. Because the pair \( (W^{[l]}, \tilde{p}^{[l]}) \) is feasible in next iteration to obtain \( (W^{[l+1]}, \tilde{p}^{[l+1]}) \), the objective function in the original problem (67) is monotonously increasing and it converges to the maximum value as the iteration index increases. Hence, when a preset termination criterion is met, the procedure yields the optimal beamforming matrix \( W^* \) and the optimal PSA pointing \( \tilde{p}^* \).

The complexity of this proposed algorithm mainly comes from the iterative SDP optimization (86) for deriving the PSA spatial pointing vector. According to [32], the computational complexity of a standard SDP problem is on the order of

\[
C_{\text{SDP}} = O((M_{\text{std}} N_{\text{std}}^3 + M_{\text{std}} N_{\text{std}}^2 + N_{\text{std}}^5 M_{\text{std}}^3) \log(1/\epsilon)) \tag{87}
\]

where \( M_{\text{std}} \) is the number of semidefinite cone constraints and \( N_{\text{std}} \) is the dimension of the semidefinite cone, while \( \epsilon \) is the accuracy imposed to solve the SDP problem. Thus the per-iteration complexity of our proposed algorithm is

\[
C_{\text{per-ite}} = O(((3N_R)^3 + (3N_R)^2 + (3N_R)^5) \log(1/\epsilon)) \tag{88}
\]

B. Robust Design for Maximizing Secrecy Rate

In the previous subsection, we obtain the optimal PSA pointing \( \tilde{p}^* \). In most practical deployments, however, the actual array spatial pointing implemented will deviate from this ideal one, due to the antenna distortion, operational environment factors or installation errors. Therefore, it is necessary to design a robust beamforming under an imperfect PSA pointing realization \( \tilde{p}_{\text{act}} \). There exist two types of array pointing errors. One is modeled as a deterministic matrix with bounded norm, and the other is unbounded and denoted by a statistical model of unknown parameters. For simplicity, we only consider the design of robust relay beamforming \( W_{\text{rb}} \), for the bounded PSA pointing error type. Specifically, an ellipsoid model is utilized to model the PSA spatial pointing error as

\[
\tilde{p}_{\text{act}} = \tilde{p}^* + \Delta \tilde{p}, \quad \Delta \tilde{p} \in P = \{ \Delta \tilde{p} : \Delta \tilde{p}^H C \Delta \tilde{p} \leq 1 \}, \tag{89}
\]

where \( \tilde{p}^* \) is the optimal PSA pointing for the relaying network obtained in Subsection IV-A, \( \Delta \tilde{p} \) is the elliptical array pointing error, and the matrix \( C > 0 \) determines the accuracy degree of the PSA pointing, which has the Cholesky decomposition of \( C = C^* (C^*)^H \). If the elements of \( C \) tend to infinity, the PSA pointing error approaches zero, i.e., the actual array structure is perfect. On the other hand, if the elements of \( C \) approach 0, the PSA pointing is extremely inaccurate.

By considering the array pointing error, the resulting robust secrecy rate maximization problem (90) is formulated at the top of this page. This optimization is highly complicated, and we make some operational assumptions in order to simplify it. First, the robust beamforming matrix \( W_{\text{rb}} \) is designed to satisfy

\[
h_{\text{rb}}^T R_{\text{cor}}^2 W_{\text{rb}} Q_d = 0 \text{ to cancel the information leakage from } \tilde{R} \text{ to } E \text{ completely. Second, } P_j^{[1]} = P_j^{\text{max}} \text{ and } P_j^{[2]} = 0 \text{ are also applied to the robust beamforming optimization with the same reasons as given in Subsection IV-A. Under these conditions, (90) can be reformulated as the optimization problem (91) given at the top of this page, where } \bar{R}_k = (h_{\text{rb}}^T R_{\text{cor}}^2 W_{\text{rb}} Q_k)^H h_{\text{rb}}^T R_{\text{cor}}^2 W_{\text{rb}} Q_k \text{, } k = d, j, \text{ and the lower bound of } \bar{\gamma} \text{ is zero, while the upper bound of } \hat{\gamma} \text{ is calculated based on the optimal } \tilde{p}^* \text{ and } W^* \text{ from the perfect CSI case.}
The first two constraints in the optimization problem (91) can be expressed as (92) and (93), respectively, given at the top of this page, where \( a = 2^2(1+P_S)[h_{SE}|^2/(\sigma^2 + P_{max}|h_{JE}|^2)] - 1 \). To promote the standard SDP formulation for the robust secrecy beamforming design, we employ the S-procedure lemma [33] to transform (92) and (93) into the linear matrix inequalities and, consequently, the optimization problem (91) is reformulated as

\[
\begin{align*}
\max \quad & \tilde{\gamma}, \\
\text{s.t.} \quad & u_1 C + \Phi_{P, J} \Phi_{P, J}^H \tilde{p}^* - u_1 - \sigma^2 a (1+||h_{RD} R_{cor}^{1/2} W_{rh}||^2), \\
& u_2 C - \Phi_{J, D} \Phi_{J, D}^H \tilde{p}^* - \sigma^2 \text{tr}(W_{rh} W_{rh}^H), \\
& \text{tr}(\tilde{Q}_d W_{rb}^H) = 0, \quad u_1 > 0, \quad u_2 > 0,
\end{align*}
\]

where

\[
t_1 = (\tilde{p}^H)^H \Phi_{P, J} \Phi_{P, J}^H \tilde{p}^* - u_1 - \sigma^2 a (1+||h_{RD} R_{cor}^{1/2} W_{rh}||^2), \\
t_2 = P_{max}^j - u_2 - (\tilde{p}^H)^H \Phi_{J, D} \Phi_{J, D}^H \tilde{p}^* - \sigma^2 \text{tr}(W_{rh} W_{rh}^H), \\
\Phi_{P, J} = P_S|h_{SD}|^2 \tilde{Q}_d - \alpha P_{max}^j |h_{JR}|^2 \tilde{R}_j, \\
\Phi_{J, D} = P_S|h_{SR}|^2 \tilde{Q}_d W_{rh}^H W_{rh} \tilde{Q}^*_d + P_{max}^j |h_{JR}|^2 \tilde{Q}_d W_{rh}^H W_{rh} \tilde{Q}^*_d.
\]

The optimization (94) is still nonconvex with respect to \( W_{rh} \). Similar to solving (80), some mathematical transformations are applied to reformulate (94) into a standard SDP problem with a rank-1 constraint. Specifically, by defining

\[
W_{rb}^H = \text{vec}(W_{rh}) \text{vec}(W_{rh})^H \in \mathbb{C}^{N_R^2 \times N_R^2},
\]

the problem (94) is transformed into

\[
\begin{align*}
\max \quad & \tilde{\gamma}, \\
\text{s.t.} \quad & u_1 C + \Phi_{P, J} \Phi_{P, J}^H \tilde{p}^* \\
& u_2 C - \Phi_{J, D} \Phi_{J, D}^H \tilde{p}^* \\
& \text{tr}(\tilde{Q}_d W_{rb}^H) = 0, \quad W_{rb} \succeq 0, \quad \text{rank}(W_{rb}) = 1, \\
& u_1 > 0, \quad u_2 > 0,
\end{align*}
\]

where

\[
t_1 = (\tilde{p}^H)^H \Phi_{P, J} \Phi_{P, J}^H \tilde{p}^* - u_1 - \sigma^2 a (1+||h_{RD} R_{cor}^{1/2} W_{rh}||^2), \\
t_2 = P_{max}^j - u_2 - (\tilde{p}^H)^H \Phi_{J, D} \Phi_{J, D}^H \tilde{p}^* - \sigma^2 \text{tr}(W_{rh} W_{rh}^H), \\
\Phi_{P, J} = P_S|h_{SD}|^2 \tilde{Q}_d (W_{rh})^H \tilde{Q}_d - \alpha P_{max}^j |h_{JR}|^2 \tilde{R}_j, \\
\Phi_{J, D} = P_S|h_{SR}|^2 \tilde{Q}_d W_{rh}^H W_{rh} \tilde{Q}^*_d + P_{max}^j |h_{JR}|^2 \tilde{Q}_d W_{rh}^H W_{rh} \tilde{Q}^*_d.
\]

In the simulation study, the DOA of desired signal \( s_d \) is specified by \( (\theta_j, \varphi_d) = (90^\circ) \), and its POA is given by \( (\alpha_d = -30^\circ, \beta_d = 0^\circ) \). For jammer signal \( s_j \), its DOA is \( (\theta_j, 90^\circ) \) with \( \theta_j \in [0, \pi] \), and its POA is \( (\alpha_j, \beta_j) \) with \( \alpha_j \in [-\pi/2, \pi/2] \) and \( \beta_j \in [-\pi/2, \pi/2] \). Thus, the spatial and polarization distances between \( s_d \) and \( s_j \) are given respectively by \( \Delta_s = |\theta_j - 40^\circ| \) and \( \Delta_p = \arccos(\cos 2\beta_d \cos 2\beta_j \cos (2\alpha_d - 2\alpha_j)) + \sin 2\beta_d \sin 2\beta_j \) [34]. The 8-antenna PSA is considered in our simulations and the antenna spacing is half of the transmit signal wavelength. In the SIMO network, the eavesdropper is equipped with \( N_E = 6 \) antennas. All channel coefficients are generated independently according to \( \mathcal{CN}(0, 1) \) and the power of the receive additive noise is \( \sigma^2 = \sigma^2 = 1 \). In order to solve the standard convex optimization problems such as the GP (38) and the SDP (86) efficiently, the software toolbox CVX [32] is used. Under this simulation setting, we perform numerical evaluations for the point-to-point SIMO network and the relaying network, respectively. In order to demonstrate the advantages of PSA, the standard CSA based technique is utilized as a comparison. Specifically, instead of employing the 8-element PSA, the destination \( D \) also employs the CSA with 8 antennas in the SIMO network case, while the relay \( R \) is also equipped with the 8-element CSA in the relay network case. All the results are averaged over 500 Monte Carlo simulations.

### V. Simulation Results

For different DOAs of the jammer signal \( s_j \), Table I presents the optimized spatial pointings of the 8-antenna PSA for both the SIMO network and the relaying network is presented. The corresponding optimal destination beamforming and relay beamforming can be derived from (32) and (77), respectively.

#### A. The SIMO Network

We first consider the security performance of the SIMO network with the proposed algorithm for optimizing the receive beamforming, power allocation and PSA spatial pointings.

1) **Total power minimization**: With the 8-antenna PSA, Fig. 4 depicts the minimum power consumption of the SIMO network as the function of the secrecy rate threshold \( R_{sec}^0 \), under three different polarization distances \( \Delta_p \) with the DOA of jammer signal \( s_j \) given by \( (35^\circ, 90^\circ) \), which is slightly difficult from the DOA \( (40^\circ, 90^\circ) \) of desired signal \( s_d \). Thus, the spatial distance between \( s_d \) and \( s_j \) is only \( \Delta_s = 5^\circ \), which is considered to be very small. Three POA values considered

\[\text{Note that our work can also be extended easily to the planar array case with the different spatial phase matrix. Moreover, since the spatial phase matrix is not related to any optimization variable, the simulation conclusions obtained by applying the planar array are similar to that in Section V.}\]
for $s_j$ are $(\alpha_j, \beta_j) \in \{(−30^\circ, 0^\circ), (−20^\circ, 0^\circ), (−30^\circ, 20^\circ)\}$, corresponding to three polarization distances $\Delta_p = 0^\circ, 20^\circ$ and $40^\circ$, respectively. It is obvious that the minimum total power consumption is a monotonically increasing function of the required secrecy rate $R_{\text{sec}}^0$, as clearly indicated in Fig. 4. Also observe from Fig. 4 that for the PSA, increasing $\Delta_p$ leads to reduction in the total power consumption, which confirms that the polarization difference between the two signals is beneficial to improve the power efficiency of the PSA based SIMO network. As a comparison, the minimum total power consumption required by the CSA based SIMO network with the POA of $s_j$ given by $(−30^\circ, 0^\circ)$ is also plotted in Fig. 4, where it can be seen that the CSA needs consume more than 4 dB of power to achieve the required $R_{\text{sec}}^0$, compared with the PSA. This is because the CSA cannot utilize the signals’ polarization information to improve performance.

We then change the DOA of $s_j$ to $(10^\circ, 90^\circ)$, and repeat the same experiment. The results obtained are shown in Fig. 5. Compared with Fig. 4, we observe that the power consumptions of the both CSA-based and PSA-based SIMO networks are greatly reduced, because we have a large spatial difference $\Delta_s = 30^\circ$ between $s_d$ and $s_j$. From Fig. 5, it can be seen that the three minimum power consumption curves of the PSA for the three different polarization distances $\Delta_p$ become very close. This phenomenon demonstrates that the polarization difference $\Delta_p$ has little effect on the network performance when the two signals have a sufficiently large spatial distance. The results of Fig. 5 again confirm the advantage of the PSA over the CSA, as the former achieves 2 dB saving in power consumption in comparison with the latter.

Additionally, Fig. 6 depicts the minimum total power consumption of the PSA SIMO network as the function of DOA $(\theta_j, 90^\circ)$ of $s_j$ under three different polarization distances $\Delta_p$ and given the secrecy rate threshold $R_{\text{sec}}^0 = 2.5$ bits/s/Hz. It can be seen that as the DOA difference between $s_d$ and $s_j$,
Again, increasing the polarization distance reduces in power consumption, as clearly shown in Fig. 6.

The minimum total power consumption as the function of the DOA (θj, 90°) of sj under different polarization distances Δp and given Psel = 2.5 bits/s/Hz.

The achievable secrecy rate as the function of the DOA (θj, 90°) of sj under different polarization distances Δp and given Psel = 2.5 bits/s/Hz.

The achievable secrecy rate as the function of the DOA (θj, 90°) of sj given Pmax = 12 dB. It can be seen that for a given Δp, the achievable secrecy rate is reduced rapidly as the spatial separation between sd and sj, Δa = |θj − 40°|, decreases, and when Δa → 0, the achievable secrecy rate reaches the minimum value. It is also clear that the achievable secrecy rate increases with the increase of the polarization separation Δp. Moreover, the influence of Δp to the achievable secrecy rate is particularly strong when the two signals are near spatially inseparable, while the influence of Δp becomes very small when the signals are sufficiently separable in the spatial domain. Note that at Δp = 0 and Δa = 0, the secrecy rate is zero. As a comparison, the secrecy rate of the CSA-based SIMO network under Δp = 0° is also given in Fig. 7, where it is apparent that the PSA significantly outperforms the CSA.

Next we increase Pmax to 14 dB and expand the range of θj from [0°, 90°] to [0°, 180°]. Given Δp = 0, Fig. 8 compares the achievable secrecy rate of the PSA SIMO network with that of the CSA SIMO network. As expected, both the PSA and CSA attain a zero secrecy rate at θj = 40°, as at this point, both Δa = 0 and Δp = 0. However, it is further noticed that for the CSA, the secrecy rate also deteriorates to zero when the DOA of sj is (140°, 90°). This is owing to the symmetric fuzzification and is referred to as grating lobe. By contrast, the secure communication of the SIMO network employing PSA is realized without introducing grating lobes, which is another significant advantage of the PSA over the CSA.

B. The Relaying Network

We now investigate the secure communication of the relay aided network. The DOAs and POAs of the incident signals ˜s and ˜s are the same as those given in Section V-A for the SIMO network. We concentrate on the maximum secrecy rate of the relaying network obtained by the iterative algorithm proposed in Section IV-A, assuming a perfect realization of the PSA pointing vector, but the robust design with imperfect realization of the PSA pointing vector is also studied.

1) The secrecy rate maximization for the relaying network: First, we demonstrate the convergence of our proposed iterative optimization algorithm given in Section IV-A. Specifically, we choose the POA (0°, 0°) for ˜sj, i.e., we consider the case of Δp = 2|αj + 30°| = 60°, and we set ˜P = 14 dB, Pmax = 25 dB and Pmax = 10 dB. Fig. 9 depicts the convergence performance of the proposed iterative optimization algorithm under both the spatially separable and spatially inseparable cases. It can be seen from Fig. 9 that for the case of Δa > 0, the algorithm takes l = 3 outer iterations to converge, while for the case of Δa = 0, the algorithm converges within l = 6 outer iterations. Moreover, the choice of the initial 0 does not seem to affect the algorithm’s convergence performance.

In Fig. 10, the achievable secrecy rate of the PSA relaying network is depicted as the function of the source transmit power P, under different DOA (θj, 90°) and POA (αj, 0°).
of jammer signal $\tilde{s}_j$ with the maximum relay power $P_{S_j}^{\text{max}} = 25$ dB and the maximum jammer power $P_{J_j}^{\text{max}} = 10$ dB. Obviously, the achievable secrecy rate is a monotonically increasing function of $P_S$ but it exhibits a saturation trend for large $P_S$. This is because increasing $P_S$ also increases the information leakage from source $S$ to eavesdropper $E$, while the relay transmit power $P_{R_j}^{\text{max}}$ is limited. Therefore, the achievable secrecy rate cannot go arbitrarily high. With the DOA of $\tilde{s}_j$ given by $65^\circ, 90^\circ$, which is distinguishable from the DOA $40^\circ, 90^\circ$ of $s_d$, the influence of the polarization distance $\Delta_p$ between $\tilde{s}_d$ and $\tilde{s}_j$ on the achievable secrecy rate is very small. However, when $\tilde{s}_j$ and $s_d$ are spatially inseparable with $\Delta_a = 0^\circ$, the influence of $\Delta_a$ becomes significant, and a larger $\Delta_a$ leads to a larger achievable secrecy rate. Also observe from Fig. 10 that under the condition of $\Delta_a = 0^\circ$ and $\Delta_p = 0^\circ$, the achievable secrecy rate of the PSA relaying network is very small.

Fig. 11 compares the achievable secrecy rates of the PSA and CSA relaying networks given the DOA $(\theta_j, 90^\circ)$ for $\tilde{s}_j$ with $\theta_j \in [0^\circ, 90^\circ]$, $P_{S_j}^{\text{max}} = 10$ dB and $P_S = 15$ dB. In this case, the POA of $\tilde{s}_j$ is given by $(\alpha_j, 0^\circ)$, and the polarization distance between $s_d$ and $\tilde{s}_j$ is $\Delta_p = 2(|\alpha_j + 30^\circ|)$. The results of Fig. 11 demonstrate that the PSA based relaying network significantly outperforms the CSA based relaying network, in terms of achievable secrecy rate. Similar to the SIMO network case, at $\Delta_a = 90^\circ$, the achievable secrecy rates of both the PSA and CSA relaying networks deteriorate to their minimum values. In particular, under the condition of $\Delta_a = 0^\circ$ and $\Delta_p = 0^\circ$, the secrecy rate of the CSA relaying network is zero but the secrecy rate of the PSA relaying network is a small nonzero value. Furthermore, by increasing the polarization separation $\Delta_p$ to nonzero, the secrecy rate of the PSA relaying network can be increased considerably, because the PSA can effectively utilize the polarization information.

2) Robust design with imperfect realization of the PSA pointing: We next illustrate our robust beamforming optimization design for the PSA relaying network with imperfect PSA pointing realization. We set the PSA pointing error bound to $C = 100 I_{S_j E}$. In order to reduce the computation complexity, we consider the 4-antenna PSA. In Fig. 12, the achievable secrecy rates of three designs as the functions of $P_s$, under different DOA and POA settings of $\tilde{s}_j$ with the 4-antenna PSA as well as $P_{S_j}^{\text{max}} = 10$ dB and $P_{R_j}^{\text{max}} = 25$ dB.
PSA pointing solution $\hat{\mathbf{p}}^*$, which is the curve under the title ‘Perfect PSA’ in Fig. 12. However, in practice, there usually exists PSA pointing implementation error, and the optimal design of $\hat{\mathbf{p}}^*$ is actually implemented as $\hat{\mathbf{p}}^* + \Delta \mathbf{p}$, which is the curve under the title ‘Non-robust PSA’ in Fig. 12. Obviously, this implementation is far from optimal, and the actual secrecy rate achieved is significantly lower than that obtained with the perfect implementation of $\hat{\mathbf{p}}^*$. Under the imperfect implementation of $\hat{\mathbf{p}}^* + \Delta \mathbf{p}$, our robust beamforming optimization design presented in Section IV-B is capable of regaining considerable secrecy rate performance, which is shown in Fig. 12 under the title ‘Robust PSA’.

C. Extension to the PSA based eavesdropper

As mentioned before, our work can also be easily extended to the case where the PSA is deployed at the eavesdropper. Note that the PSA-based eavesdropper can effectively suppress the interference with approximate spatial properties as the source, and further improve the wiretap capability. In order to illustrate the good performance of the PSA-based eavesdropper, we perform the following two simulations for total power minimization and secrecy rate maximization, respectively.

Particularly, we assume that the eavesdropper is equipped with a PSA with $N_E = 6$ antennas. Besides, the DOA and POA of the desired signal $s_d$ impinging on PSA at eavesdropper are assumed to be $(30^\circ, 90^\circ)$ and $(-30^\circ, 0^\circ)$, respectively. For jammer signal $s_j$, its DOA at eavesdropper is $(25^\circ, 90^\circ)$ and its POA is $((\alpha_{jE}, \beta_{jE})$. Based on this, the polarization distance at eavesdropper between $s_d$ and $s_j$ is defined as $\Delta p_e$, which is similar to that of the polarization distance at destination $\Delta p$. Note that in the following two simulations, $\Delta p = 20^\circ$ is fixed. In Fig. 13, the total power consumption of the SIMO network versus the secrecy rate threshold $P_{sec}$ under different polarization distances $\Delta p_e$ is studied. Here, both the eavesdropper equipped with the CSA and PSA (also named CSA-Eve and PSA-Eve), are considered. Firstly, we find that for both CSA-Eve and PSA-Eve, the total power consumption increases with $P_{sec}$. Secondly, it is clear that the total power consumption for PSA-Eve case increases with $\Delta p_e$, which due to the fact that the wiretap capability of PSA-Eve is enhanced by enlarging the polarization distance $\Delta p_e$. More importantly, compared to the case of CSA-Eve, the total power consumption for PSA-Eve case is evidently higher under the arbitrary polarization distance $\Delta p_e$, which indicates that more transmit power is required to suppress the interception of PSA-Eve and further achieve the secrecy rate threshold.

In Fig. 14, the achievable secrecy rate versus the DOA ($\theta_j, 90^\circ$) of $s_j$ for both PSA-Eve and CSA-Eve case is shown. The same parameters in Fig. 1 are adopted, and the total transmit power $P_S + P_j = 12dB$ is assumed. Based on this, we naturally find that for both PSA-Eve and CSA-Eve, when the DOA ($\theta_j, 90^\circ$) of $s_j$ is near to that of the desired signal, i.e. $|\theta_j - 40^\circ| < 10^\circ$, the secrecy rate performance evidently deteriorates due to the similar spatial characteristics between the desired signal and the jammer signal. Besides, with the increase of polarization distance $\Delta p_e$, i.e., from $\Delta p_e = 10^\circ$ to $\Delta p_e = 20^\circ$, the PSA-Eve can utilize more polarization difference to improve the wiretap rate and further reduce the achievable secrecy rate. More importantly, compared to the case of CSA-Eve, the lower achievable secrecy rate of PSA-Eve is observed, which is attributed to the better wiretap capability of PSA-Eve.

VI. CONCLUSIONS

In this paper, a joint beamforming, power allocation and PSA pointing optimization has been proposed for wireless communications. Our main contribution has been to apply the polarization sensitive array to improve the security performance of wireless communications. Specifically, by utilizing the polarization difference among signals, the interference caused by jammer to destination is greatly reduced while the information leakage to eavesdropper is minimized, even when these signals are spatially indistinguishable. Two communication scenarios, the PSA based SIMO network and the PSA...
aided relay network, have been considered. For the former scenario, both total transmit power minimization and secrecy rate maximization have been performed. For the relaying network assuming perfect CSI, both secrecy rate maximization designs under perfect and imperfect PSA spatial pointing implementations have been obtained. Since all the optimization problems involved are nonconvex with complicated constraints and/or objectives, alternative suboptimal algorithms have been proposed which enable us to apply convex optimization techniques to solve the transformed optimization problems efficiently. Extensive simulation results have demonstrated the effectiveness of our proposed PSA based techniques for enhancing physical-layer security. In particular, it has been shown that the improvement of maximum achievable secrecy rate of wireless networks by the proposed PSA techniques over the standard CSA techniques is remarkable.

APPENDIX

The convergence of the proposed iterative algorithm to solve the optimization problem (31) was demonstrated in [29]. Here we prove the convergence of this algorithm.

Firstly, we define the following objective function

\[ f(P_c) = \text{tr}(P_c) - \lambda_{\text{max}}(P_c) - \text{tr} \left( \vartheta_{\text{max}} \vartheta_{\text{max}}^H (P_c - P_c^{(t)}) \right) \]

\[ = \text{tr}(P_c) - \lambda_{\text{max}}(P_c). \tag{99} \]

Then the lower bound of \( f(P_c) \) is zero according to the following lemma.

**Lemma 1** For an arbitrary square matrix \( A \), it holds that \( \text{tr}(A) - \lambda_{\text{max}}(A) \geq 0 \), in which the equality is guaranteed if and only if rank(\( A \)) = 1 is satisfied.

Next, we modify \( f(P_c) \) into the following penalty function

\[ \tilde{f}(P_c^{(t+1)}) = \min_{P_c} \text{tr}(P_c) - \lambda_{\text{max}}(P_c^{(t)}) \]

\[ - \text{tr} \left( \vartheta_{\text{max}}^{(t)} \vartheta_{\text{max}}^{(t)}^H (P_c - P_c^{(t)}) \right), \tag{100} \]

where \( \text{tr}(P_c) - \lambda_{\text{max}}(P_c^{(t)}) - \text{tr} \left( \vartheta_{\text{max}}^{(t)} \vartheta_{\text{max}}^{(t)}^H (P_c - P_c^{(t)}) \right) \) is the objective function in the \((t + 1)\)th iteration of (31).

Let \( P_c^{(t)} \) be the optimal matrix obtained at the \( t \)th iteration of (31). Using \( P_c^{(t)} \) in the iterative optimization procedure yields the optimal matrix \( P_c^{(t+1)} \) at the \((t + 1)\)th iteration, which is feasible. Clearly, the optimized \( \tilde{f}(P_c^{(t+1)}) \) satisfies

\[ \tilde{f}(P_c^{(t+1)}) = \text{tr}(P_c^{(t+1)}) - \lambda_{\text{max}}(P_c^{(t)}) \]

\[ - \text{tr} \left( \vartheta_{\text{max}}^{(t)} \vartheta_{\text{max}}^{(t)}^H (P_c^{(t+1)} - P_c^{(t)}) \right) \]

\[ \leq \text{tr}(P_c^{(t+1)}) - \lambda_{\text{max}}(P_c^{(t)}) \]

\[ - \text{tr} \left( \vartheta_{\text{max}}^{(t)} \vartheta_{\text{max}}^{(t)}^H (P_c^{(t+1)} - P_c^{(t)}) \right) \]

\[ = f(P_c^{(t)}). \tag{101} \]

For an arbitrary Hermitian matrix \( Z \), the following relationship holds

\[ \text{tr} \left( \vartheta_{\text{max}} \vartheta_{\text{max}}^H (Z - P_c^{(t)}) \right) = \vartheta_{\text{max}}^H Z \vartheta_{\text{max}} - \vartheta_{\text{max}}^H P_c^{(t)} \vartheta_{\text{max}} \]

\[ = \vartheta_{\text{max}}^H Z \vartheta_{\text{max}} - \lambda_{\text{max}}(P_c^{(t)}) \leq \lambda_{\text{max}}(Z) - \lambda_{\text{max}}(P_c^{(t)}). \tag{102} \]

Therefore, we further obtain

\[ \lambda_{\text{max}}(P_c^{(t+1)}) - \lambda_{\text{max}}(P_c^{(t)}) \geq \text{tr} \left( \vartheta_{\text{max}}^{(t)} \vartheta_{\text{max}}^{(t)}^H (P_c^{(t+1)} - P_c^{(t)}) \right). \tag{103} \]

Based on (103), the function \( f(P_c^{(t+1)}) \) satisfies

\[ f(P_c^{(t+1)}) = \text{tr}(P_c^{(t+1)}) - \lambda_{\text{max}}(P_c^{(t+1)}) \]

\[ \leq \text{tr}(P_c^{(t+1)}) - \lambda_{\text{max}}(P_c^{(t)}) - \lambda_{\text{max}}(P_c^{(t+1)}) \]

\[ \leq f(P_c^{(t)}) \], \tag{104} \]

where the first inequality and the second inequality hold due to (103) and (101), respectively.

Thus, given an initial feasible \( P_c^{(0)} \), the optimization problem (31) can be iteratively solved to obtain a sequence \( P_c^{(t)} \), \( t = 1, 2, \ldots \), whose rank approaches 1. Since this iteration procedure is monotonically decreasing, in terms of the objective function \( f(P_c^{(t)}) \), as shown in (104), which has a lower bound of zero based on Lemma 1, it is naturally converged. Consequently, we conclude that the iterative optimization problem (31) based on the penalty function method converges to a rank-1 solution.

**REFERENCES**

[1] X. Wang and P. Yi, “Security framework for wireless communications in smart distribution grid,” IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 809–818, Dec. 2011.

[2] Y. W. P. Hong, P.-C. Lan and C.-C. J. Kuo, “Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches,” IEEE Signal Process. Mag., vol. 30, no. 5, pp. 29–40, Sep. 2013.

[3] A. P. Sawiluk, Z. J. Khan, and S. G. Akojwar, “Power optimization of wireless sensor networks using encryption and compression techniques,” in Proc. ICESC 2014 (Nagpur, India), Jan. 9-11, 2014, pp. 222–227.

[4] W. Trappe, “The challenges facing physical layer security,” IEEE Com mun. Mag., vol. 53, no. 6, pp. 16–20, Jun. 2015.

[5] C. Shannon, “Communication theory of secrecy systems,” Bell System Technical J., vol. 28, no. 4, pp. 656–715, Oct. 1949.

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

[7] S. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap chan nel,” IEEE Trans. Inf. Theory, vol. 24, no. 4, pp. 451–463, Jul. 1978.

[8] Z. Ding, Z. Ma and P. Fan, “Asymptotic studies for the impact of antenna selection on secure two-way relaying communications with artificial noise,” IEEE Trans. Wireless Commun., vol. 13, no. 4, pp. 2189–2203, Apr. 2014.

[9] F. Zhu, F. Gao, M. Yao, and H. Zou, “Joint information- and jamming-beamforming for physical layer security with full duplex base station,” IEEE Trans. Signal Process., vol. 62, no. 10, pp. 6391–6401, Dec. 2014.

[10] L. Zhang, Y. Cai, R. C. de Lamare, and M. Zhao, “Robust multi-branch Tomlinson-Harashima source and relay precoding scheme in nonregenerative MIMO relay systems,” in Proc. VTC-2013 Spring (Dresden, Germany), Jun. 2-5, 2013, pp. 1–5.

[11] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, “QoS-based transmit procedure is monotonically decreasing, in terms of the object-

[12] F. Zhao, “Joint information- and jamming-beamforming for physical layer security with full duplex base station,” IEEE Trans. Signal Process., vol. 62, no. 24, pp. 6391–6401, Dec. 2014.

[13] A. Kalantari, M. Soltanian, 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.
A. D. Nesic and D. A. Nesic, “Printed planar 8 × 8 array antenna with circular polarization for millimeter wave application,” *IEEE Antennas Wireless Propagation Lett.*, vol. 11, pp. 744–747, 2012.

M. Costa, A. Richter, and V. Koivunen, “Unified array manifold decomposition based on spherical harmonics and 2-D Fourier basis,” *IEEE Trans. Signal Process.*, vol. 58, no. 9, pp. 4634–4645, Sep. 2010.

W. C. Y. Lee and Y. Yeh, “Polarization diversity system for mobile radio,” *IEEE Trans. Commun.*, vol. 20, no. 5, pp. 912–923, Oct. 1972.

P. L. Carro and J. de Mingo, “Polarization diversity with genetic parallel printed dipole antennas for Bluetooth and WiMAX applications,” in *Proc. VTC-2006 Fall (Montreal, Canada)*, Sep. 25-28, 2006, pp. 1–5.

A. J. Weiss and B. Friedlander, “Maximum likelihood signal estimation for polarization sensitive arrays,” *IEEE Trans. Antennas Propag.*, vol. 41, no. 7, pp. 918–925, Jul. 1993.

H. Chen, Q. Wan, Y. P. Liu, and A. M. Huang, “A sparse signal reconstruction perspective for direction-of-arrival estimation with a distributed polarization sensitive array,” in *Proc. IEEE WCSP 2009 (Nanjing, China)*, Nov. 13-15, 2009, pp. 1–5.

S. Namba, N. Miyazaki, Y. Hirota, and Y. Kishi, “MIMO capacity estimation based on single and dual polarization MIMO channel measurements,” in *Proc. 16th Asia Pacific Conf. Commun.* (Auckland, New Zealand), Oct. 31-Nov. 3, 2010, pp. 313-318.

J. Wu and M. C. Wu, “Dual-polarization frequency reuse with frequency band shifting allocation,” *IEEE Trans. Veh. Technol.*, vol. 49, no. 6, pp. 2244–2256, Nov. 2000.

B. Vrigneau, J. Letessier, P. Rostaing, and L. Collin, “Max-min precoder performances in a polarization diversity MIMO channel,” in *Proc. 40th Asilomar Conf. Signals Syst. and Comput.* (Pacific Grove, CA), Oct. 29-Nov. 1, 2006, pp. 1613–1619.

A. B. Gershman, N. D. Sidiropoulos, S. Shahbazpanahi, M. Bengtsson, and B. Ottersten, “Convex optimization-based beamforming,” *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 62–75, May 2010.

C. A. Balanis, *Antenna Theory: Analysis and Design* (3rd Edition). Hoboken, NJ: John Wiley & Sons, 2005.

V. N. Tatarkinov, “The use of the emergence principle as a new step in the electromagnetic waves polarization theory at the scattering by complex random radar objects,” in *Proc. MIKON 2006 (Krakow, Poland)*, May 22-24, 2006, pp. 511–518.

A. Nehorai, K.-C. Ho, and B. T. G. Tan, “Minimum-noise variance beamformer with an electromagnetic vector sensor,” *IEEE Trans. Signal Process.*, vol. 47, no. 3, pp. 601–618, Mar. 1999.

G. Barriac, R. Mudumbai, and U. Madhow, “Distributed beamforming for information transfer in sensor networks,” in *Proc. IPSN 2004 (Berkeley, CA)*, Apr. 26-27, 2004, pp. 81–88.

H. M. Wang, Q. Yin, and X. G. Xia, “Distributed beamforming for physical-layer security of two-way relay networks,” *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

H. M. Wang, M. Luo, Q. Yin, and X. G. Xia, “Hybrid cooperative beamforming and jamming for physical layer security of two-way relay networks,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

C. Lameiro, J. Via and I. Santamaria, “Amplify-and-forward strategies in the two-Way relay channel with analog Tx-Rx beamforming,” *IEEE Trans. Veh. Technol.*, vol. 62, no. 2, pp. 642-654, Feb. 2013.

M. Ding and S. D. Blostein,”MIMO minimum total MSE transceiver design with imperfect CSI at both ends,” *IEEE Trans. Signal Process.*, vol. 57, no. 3, pp. 1141–1150, Mar. 2009.

M. C. Grant and S. P. Boyd, *The CVX Users’ Guide* (Release 2.1) CVX Research, Inc., 2015.

C. Shen, T. H. Chang, K. Y. Wang, and Z. Qiu, “Distributed robust multicell coordinated beamforming with imperfect CSI: An ADMM approach,” *IEEE Trans. Signal Process.*, vol. 60, no. 6, pp. 2988-3003, Jun. 2012.

K. C. Ho, K. C. Tan, and A. Nehorai, “Estimating directions of arrival of completely and incompletely polarized signals with electromagnetic vector sensors,” *IEEE Trans. Signal Process.*, vol. 47, no. 10, pp. 2845–2852, Oct. 1999.