IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 29, 2017, accepted May 29, 2017, date of publication June 6, 2017, date of current version June 27, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2712569

Probabilistic Robust Secure Beamforming in MISO Channels With Imperfect LCSI and Statistical ECSI

JING XU[1], SIWEN XU[1], AND CHONGBIN XU[2], (Member, IEEE)

[1]Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China
[2]Key Laboratory for Information Science of Electromagnetic Waves, Department of Communication Science and Engineering, Fudan University, Shanghai 200433, China

Corresponding author: Jing Xu (jing.xu@mail.xjtu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61431011.

ABSTRACT In this paper, we investigate the robust secure transmit beamformming design for multiple-input single-output wiretap channels overheard by multiple non-collaborating single-antenna eavesdroppers. Assuming that at the transmitter, the instantaneous legitimate receiver's channel state information (CSI) is imperfect and only the statistical eavesdroppers' CSI is known, we seek to maximize the target secrecy rate R with the total transmit power constraint and the secrecy outage probability constraint. The resulting outage-constrained secrecy rate maximization (O-SRM) is non-convex and difficult to solve. Thus, we develop an efficient algorithm to solve it and determine the robust secure beamforming design. Specifically speaking, we first prove that the original O-SRM problem can be solved by an equivalent outage-constrained power minimization problem (O-PMP), which is easy to perform semi-definite relaxation (SDR) and can be solved by semi-definite program (SDP) consequently. Second, we transform the non-convex secrecy rate outage constraints into deterministic ones by resorting to Bernstein-type inequality II. Finally, by solving the convex approximation of the O-PMP with different Rs and bisection search over R, we convert the original O-SRM problem into a sequence of solvable SDPs. Simulation results are provided to verify the secrecy-rate performance improvement of the proposed robust beamforming compared with the existing worst-case design proposed by Li and Ma and the simple non-robust maximum-ratio transmission.

INDEX TERMS Physical layer security, MISO wiretap channels, robust secure beamforming, semi-definite program.

I. INTRODUCTION

Physical-layer secure transmission techniques have received significant attention in wireless communications recently, since it can derive perfect security without using an encryption key in comparison to the conventional secret-key-based approach implemented in the application layer [1]–[7]. This property of physical-layer security is very attractive when key distribution or management is challenging in establishing secured communication links, e.g., in ad-hoc wireless networks [8], [9]. Moreover, from the perspective of offering high throughput and reliable communications, multiple-input multiple-output (MIMO) techniques have been extensively investigated in the last decade. In this context, dealing with virous MIMO scenarios, the research community pay much attention to exploiting the multi-antenna degrees of freedom, which could further enhance the information security of wireless transmission both fundamentally and practically [10]–[12].

From a viewpoint of transmission strategy optimization, the secrecy rate maximization (SRM) problem is found to be tractable in the multi-input single-output (MISO) wiretap channels [12], while it is challenging under the general MIMO case [13]. Therefore, this paper also focuses on the MISO scenario. In fact, there are considerable studies which address the transmit beamforming optimization in MISO wiretap channels for physical-layer security, see [14]–[23]) and the references therein. Generally speaking, it is difficult to have perfect eavesdroppers' CSI (ECSI) at the transmitter due to a lack of cooperation between the transmitters and the eavesdropper. Even in [24] and [25], the researchers study the secrecy transmit design when no information regarding the eavesdroppers is available at the transmitter.

However, when the eavesdroppers are part of the legitimate communication system, statistical eavesdroppers' CSI (ECSI) with certain accuracy is easier to obtain by the transmitter. Consequently, the beamforming design under the statistical ECSI assumption is addressed in [14]–[17].

Moreover, most of the transmit beamforming optimization in MISO wiretap channels are based on the acquisition of accurate instantaneous legitimate receivers' channel state information (LCSI) at the transmitter side, such as [14]–[20]. This assumption is much more challenging as the channel state information at the transmitter (CSIT) is destined to be in error due to channel estimation errors, channel mobility, limited feedback resources and delay [26]–[28]. Driven by this, many recent studies have addressed the robust beamforming against the imperfect CSIT for MISO wiretap channels [18]–[23]). Among them, [18]–[20] consider a case that the LCSI is quite accurate while the ECSI is imprecise due to the limited cooperation between the transmitter and the eavesdroppers. Additionally, [21]–[23] study the scenarios in which LCSI and ECSI are both imperfect. In this study, we investigate a more practical scenario below: i) **imperfect LCSI**: the transmitter only has some imprecise knowledge of instantaneous LCSI; ii) **and statistical ECSI**: the transmitter can obtain the distribution information of ECSI. Additionally, it is worth to point out that in [22], the robust secure beamforming strategies for MISO wiretap channels have been fully studied under various CSIT assumptions except the case we considered in this paper.

The existing robust approaches for MISO wiretap channels above could be roughly categorized into two classes, i.e., worst-case approach (e.g., [18], [19], [21], [23]) and outage based approach (e.g., [18], [20], [22]). It is noticed that the worst case approach is safe in the sense that the worst case performance is guaranteed, but it often leads to a very conservative design since those extreme conditions rarely occur. On the other hand, the chance constrained approach allows occasional violation of the constraints. Therefore, it is less restrictive and more practical. Thus, in this paper, we investigate the secrecy rate outage probability constrained robust beamforming for MISO wiretap channels where we assume the imperfect LCSI and statistical ECSI are available at the transmitter.

In this study, we show that the considered outage constrained secrecy rate maximization (O-SRM) problem can be solved in a convex and tractable fashion actually. Specifically, we first prove that the original O-SRM problem can be exactly solved by its equivalent variation: an outage constrained power minimization problem (O-PMP). Then, we conservatively change the probabilistic constraints into deterministic ones with using the Bernstein-type Inequlity II. Afterwards, by resorting to semi-definite relaxation (SDR) and bisection search method, we finally convert the original O-SRM problem into a sequence of solvable convex semi-definite programs (SDPs).

The rest of this paper is organized as follows. Section II introduces the system model and problem formulation. The proposed robust secure beamforming design is illustrated in detail in Section III. Simulation results are then provided in Section IV, and conclusions are drawn in Section V.

Notations: The uppercase (lower) boldface letter represents a matrix (vector), and italics denote scalars. The conjugate transpose and trace operator are denoted by $(\cdot)^H$ and $Tr(\cdot)$, respectively. $\mathbb{C}^{M\times N}$ stands for an M-by-N dimensional complex matrix set. $\|\cdot\|$ is the Euclidean norm of vector and the Frobenius norm of matrix. $\mathcal{CN}(\mathbf{x},\mathbf{Q})$ stands for a circularly symmetric complex Gaussian random vector where $\mathbf{x}$ is the mean and $\mathbf{Q}$ is the covariance matrix. I and $\log_2$ are respectively identity matrix and the logarithm of basis two. $[\cdot]^+$ denotes $\max\{0,\cdot\}$. $diag\{\cdot\}$ represents a diagonal matrix. $\lambda_{max}(A)$ and $\mathbf{u}_{max}(A)$ respectively denote the maximum eigenvalue of matrix A and the corresponding eigenvector.

II. SYSTEM MODEL AND PROBLEM FORMULATION

In this section, we first describe the considered system model and CSI uncertainty scenario, then formulate the considered outage constrained secrecy rate maximization (O-SRM) problem.

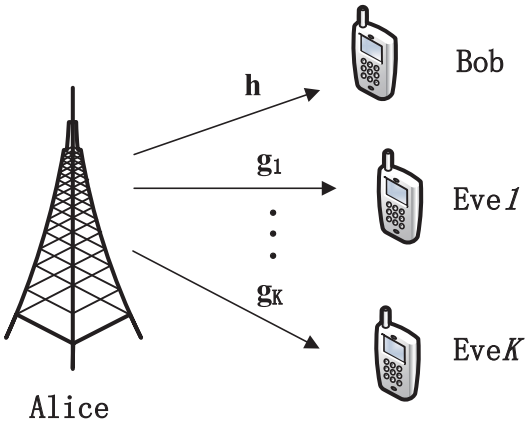


FIGURE 1. Considered MISO wiretap channels.

A. SYSTEM MODEL

The considered Gaussian MISO wiretap channels are illustrated in Fig. 1, in which there are a transmitter with N_t transmit antennas, and a legitimate receiver and K eavesdroppers, each with a single antenna. To clearly and succinctly describe the system model we discussed, the transmitter, legitimate receiver and the kth eavesdropper are respectively referred as Alice, Bob and Eve k, $k\in\mathcal{K}=\{1,\cdots,K\}$. In this model, Alice sends confidential message to Bob, and this transmission is overheard by multiple non-collaborating single-antenna eavesdroppers. Consequently, the received signals at Bob and the kth Eve are respectively represented as

$$\begin{aligned} y_b &= h^H w s + n_b, \\ y_{e,k} &= g_k^H w s + n_k, \quad \forall k\in\mathcal{K} \end{aligned} \tag{1}$$

where w is the transmit beamforming vector to be optimized and s is the symbol intended to Bob, $E\{|s|^2\}=1$; $\mathbf{h}\in\mathbb{C}^{N_t\times 1}$

and $\mathbf{g}_k \in \mathbb{C}^{N_t \times 1}$ are respectively the flat fading channel vectors to Bob and to the kth Eve; Without loss of generality, $n_b \sim \mathcal{CN}(0, 1)$ and $n_k \sim \mathcal{CN}(0, 1)$ are complex additive white Gaussian noise vectors.

B. CSIT UNCERTAINTY ASSUMPTION

We assume that Alice has imperfect LCSI and statistical ECSI, which corresponds to the scenario where Bob is active user in the wireless system and Eves are part of the legitimate communication system. To be specific, Bob and the kth Eve's channel can be respectively modeled as

$$\begin{aligned} h &= \hat{h} + \Delta h, \\ g_k &\sim \mathcal{CN}\left(0, \alpha_{e,k}^2 I\right), \forall k \in \mathcal{K} \end{aligned} \tag{2}$$

where $\hat{\mathbf{h}} \in \mathbb{C}^{N_t \times 1}$ is the estimated h which is known to Alice; The corresponding CSI error is Δh, following the distribution $\Delta h \sim \mathcal{CN}\left(0, \sigma_b^2 I\right)$; $\alpha_{e,k}^2$ is the coefficient of the kth Eve's covariance matrix, which is a known parameter at Alice.

C. OUTAGE-CONSTRAINED SECRECY RATE MAXIMIZATION

The instantaneous secrecy rate [20] is calculated as

$$R_s = \left[\log_2(1 + \left\|h^H w\right\|^2) - \max_{k \in \mathcal{K}} \log_2(1 + \left\|g_k^H w\right\|^2)\right]^+. \tag{3}$$

As we know, a widely employed criteria for designing the transmit strategy is to maximize the achievable secrecy rate, subject to a total power constraint [18]. However, this optimization is relatively conservative in practice since many applications in wireless communication system are able to tolerate occasional events of outage under the condition of not significantly affecting users' quality of service [20]. Much more importantly, limited CSIT assumption of imperfect LCSI and statistical ECSI makes it more difficult to design the robust secure beamforming which ensures a given rate target all the time. Therefore, it is more interesting to solve the modified optimization below:

$$\begin{aligned} R^\star(P) = \max_{w} \; & R \\ s.t. \; & \Pr\left(S_k(\mathbf{w}) \geq R\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}, \\ & \|w\|^2 \leq P \end{aligned} \tag{4}$$

where

$$S_k(\mathbf{w}) = \log_2(1 + \left\|h^H w\right\|^2) - \log_2(1 + \left\|g_k^H w\right\|^2) \tag{5}$$

and R is theate; P is the given average transmit power of Alice; $p_k \in (0, 1]$ is the maximum tolerable secrecy outage probability for the kth Eve.

The outage-constrained secrecy rate maximization (O-SRM) problem in (4) tries to maximize the secrecy rate target while guaranteeing the secrecy rate outage probability smaller than certain given threshold and satisfying the total power constraint. In [22], the O-SRM problem formulation is first established but for different CSIT uncertainty scenarios. In this study, we seek to solve the O-SRM problem (4) with assuming the imperfect LCSI and statistical ECSI.

III. PROPOSED ROBUST BEAMFORMING DESIGN

In this section, we will describe the proposed approach to solving the O-SRM problem (4) which takes P as a parameter to derive the maximum value of the achievable target secrecy rate $R^\star(P)$. Obviously, the O-SRM problem (4) is non-convex and difficult to solve efficiently. To make it tractable, we will seek to decompose (4) into a sequence of semi-definite programs (SDPs) (one for each target rate $R > 0$) which are convex and tractable.

A. TRANSFORM THE ORIGINAL PROBLEM WITH BISECTION SEARCH

First of all, we consider the following lemma.

Lemma 1: If the optimal objective value of the O-SRM problem (4), $R^\star(P) > 0$, the function

$$\gamma_k(P) \triangleq S_k(P\mathbf{w}) = \log_2\left(\frac{1 + Ph^H w w^H h}{1 + Pg_k^H w w^H g_k}\right) \tag{6}$$

is monotonically increasing with the power P increasing. Moreover, the value of $R^\star(P)$ is monotonically increasing with the power P increasing.

Proof: A detailed proof is present in Appendix A. ■

Afterwards, by utilizing Lemma 1, we transform the original O-SRM problem (4) into an equivalent optimization problem as described in Theorem 1.

Theorem 1: In the case of $R^\star(P) > 0$, the following outage-constrained power minimization problem (O-PMP)

$$\begin{aligned} \min_{w} \; & \mathbf{w}^H \mathbf{w} \\ s.t. \; & \Pr\left(S_k(\mathbf{w}) \geq R^\star(P)\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K} \end{aligned} \tag{7}$$

exactly solves the O-SRM problem (4) in the sense that the optimal solution of (7) is also that of (4), and vice verse. Besides, with $\mathbf{w}^\star$ denoting the corresponding optimal solution to (4) and (7), we have $\mathbf{w}^{\star H}\mathbf{w}^\star = P$.

Proof: Please see Appendix B for the proof. ■

According to Theorem 1, the discussed O-SRM problem (4) can be solved equivalently by handling (7). Additionally, the benefit for considering the O-PMP (7) is twofold: i) The O-PMP (7) tries to satisfy a probabilistic outage constraint (in which the target achievable secrecy rate is given) and to minimize the average transmit power. Therefore, this optimization itself is interesting and practically meaningful; ii) In comparison of the original O-SRM problem (4), the O-PMP (7) is easier to perform semi-definite relaxation (SDR) and derive solvable convex semi-definite programs (SDPs).

Next, by combining Lemma 1 and Theorem 1, we figure out the main idea of our proposed algorithm for robust beamforming design in this work. Specifically speaking, to derive $R^\star(P)$ and the corresponding beamforming vector $\mathbf{w}^\star$, we can transform the original O-SRM problem (4) into a sequence of O-PMP as follows:

$$\begin{aligned} \min_{w} \; & \mathbf{w}^H \mathbf{w} \\ s.t. \; & \Pr\left(S_k(\mathbf{w}) \geq R)\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K} \end{aligned} \tag{8}$$

with different given target secrecy rate Rs. According to Lemma 1, $R^\star(P)$ is monotonically increasing with respect to P. Then, by solving (8) with different R and using a bisection search over R, $R^\star(P)$ and the corresponding $\mathbf{w}^\star$ can be obtained finally. Here, let us describe the proposed method briefly. At the initialization stage, we set the termination parameter $\varepsilon > 0$, the initial lower bound R_l and the upper bound R_u ($R^\star(P) \in [R_l, R_u]$). Then, a loop begins with $R_{mid} = \frac{R_l+R_u}{2}$ being the target secrecy rate. If (8) is infeasible, update R_u with R_{mid}; otherwise, solve (8) and check if $\|\mathbf{w}\|^2 < P$. If it is satisfied, update R_l with R_{mid}; otherwise, update R_u with R_{mid}. When $R_u - R_l \le \varepsilon$, this loop will end and return $\mathbf{w}$ as the desired $\mathbf{w}^\star$.

Next, we focus on how to solve a sequences of O-PMPs (8) in a tractable convex fashion.

B. REPLACE THE OUTAGE CONSTRAINTS CONSERVATIVELY

Since the probabilistic constraints in (8) usually have no closed-form expressions and are seldom convex [29], we conservatively transform the considered probabilistic constraints into a deterministic form in this subsection.

By plugging $W \triangleq ww^H$ into (8), we obtain the specific form of those non-convex stochastic outage constraints as

$$\begin{aligned}\Pr\Bigg(&\begin{bmatrix}\Delta h\\ g_k\end{bmatrix}^H diag\left\{W, -2^R W\right\}\begin{bmatrix}\Delta h\\ g_k\end{bmatrix}\\ &+2Re\left\{\begin{bmatrix}\Delta h\\ g_k\end{bmatrix}^H diag\left\{W, -2^R W\right\}\begin{bmatrix}\hat{h}\\ 0\end{bmatrix}\right\}\\ &+\begin{bmatrix}\hat{h}\\ 0\end{bmatrix}^H diag\left\{W, -2^R W\right\}\begin{bmatrix}\hat{h}\\ 0\end{bmatrix}\ge 2^R-1\Bigg)\ge 1-p_k\end{aligned} \tag{9}$$

for $\forall k \in \mathcal{K}$.

Since $\Delta h \sim \mathcal{CN}\left(0, \sigma_b^2 I\right)$ and $g_k \sim \mathcal{CN}\left(0, \alpha_{e,k}^2 I\right)$ in this study, we recall that the Berstein-type inequality bounds the probability of quadratic forms of Gaussian variables involving matrices. To be more specific, the Bernstein-type inequality II [29] is stated below:

$$\begin{aligned}\Pr\Big(x^H Ax+2Re\left\{x^H a\right\}\le Tr\,(A)-\sqrt{2\sigma}\sqrt{\|vecA\|^2+2\|a\|^2}\\ -\sigma s^-(A)\Big)\le\exp(-\sigma)\end{aligned} \tag{10}$$

for any $\sigma \ge 0$ where $A \in \mathbb{C}^{N\times N}$, is a complex Hermitian matrix, $a \in \mathbb{C}^{N\times 1}$, and $x \sim \mathcal{CN}(0, I)$. Here $s^-(A) = \max\left(\lambda_{max}(-A), 0\right)$.

Similar to the idea in [29], we can derive safe tractable approximation (or convex restriction) of the original secrecy outage constraints (9) by resorting to Bernstein-type inequality II. In order to utilize the it more conveniently, we first rewrite the probabilistic constraints (9) as a similar form of Bernstein-type inequality II. Let us respectively rewrite the LCSI error and ECSI as

$$\Delta h = \mathbf{E}_b^{1/2} x_h,\ g_k = \mathbf{E}_{e,k}^{1/2} x_{e,k}, \forall k \in \mathcal{K}$$

where $x_h \sim \mathcal{CN}(0, I)$, $x_{e,k} \sim \mathcal{CN}(0, I)$. Furthermore, we define $\tilde{x}_k \triangleq \left[x_h^H,\ x_{e,k}^H\right]^H$, then the outage constraint (9) can be expressed in another way as

$$\Pr\left(\tilde{x}_k^H A_k \tilde{x}_k + 2Re\left\{\tilde{x}_k^H a_k\right\} \le c_k\right) \le p_k \tag{11}$$

where

$$A_k \triangleq diag\left\{\left(E_b^{1/2} W E_b^{1/2}\right),\ -2^R\left(E_{e,k}^{1/2} W E_{e,k}^{1/2}\right)\right\},$$
$$a_k \triangleq diag\left\{\left(E_b^{1/2} W\right), 0\right\}\left[\hat{h}^H, 0\right]^H,\ c_k \triangleq 2^R - 1 - \hat{h}^H W \hat{h}.$$

Afterwards, we set $\sigma_k = -\ln(p_k)$ and combine (10) and (11). Consequently, the original chance constraint in (4) is conservatively replaced with the following deterministic one:

$$c_k \le Tr\,(A_k) - \sqrt{2\sigma_k}\sqrt{\|vecA_k\|^2 + 2\|a_k\|^2} - \sigma_k s^-(A_k). \tag{12}$$

If (12) is true, then the original chance constraint in (8) (or (9), (11)) must hold true.

C. DERIVE SOLVABLE CONVEX PROBLEMS BY SDR

By substituting its outage constraints for the deterministic constraints in (12), we conservatively transform (8) into

$$\begin{aligned}\min_W\quad & Tr\,(W)\\ & Tr\,(A_k) - \sqrt{2\sigma_k}\mu_k - \sigma_k \upsilon_k - c_k \ge 0,\ \forall k \in \mathcal{K},\\ & \left\|\begin{matrix}vec\,(A_k)\\ \sqrt{2}a_k\end{matrix}\right\| \le \mu_k,\ \forall k \in \mathcal{K},\\ & \upsilon_k I + A_k \succeq 0,\quad \upsilon_k \ge 0,\ \forall k \in \mathcal{K},\ W \succeq 0,\\ & rank(W) = 1\end{aligned} \tag{13}$$

where μ_k, υ_k are slack variables.

Then, we utilize semi-definite relaxation (SDR) approach and drop the rank constraint. Thus, (13) is transformed into the following convex semi-definite program (SDP):

$$\begin{aligned}\min_W\quad & Tr\,(W)\\ & Tr\,(A_k) - \sqrt{2\sigma_k}\mu_k - \sigma_k \upsilon_k - c_k \ge 0,\ \forall k \in \mathcal{K},\\ & \left\|\begin{matrix}vec\,(A_k)\\ \sqrt{2}a_k\end{matrix}\right\| \le \mu_k,\ \forall k \in \mathcal{K},\\ & \upsilon_k I + A_k \succeq 0,\ \upsilon_k \ge 0,\quad \forall k \in \mathcal{K},\ W \succeq 0\end{aligned} \tag{14}$$

whose optimal solution $W^\star$ can be efficiently obtained by mathematical tools CVX [30].

Thus far, by solving (14), the convex approximation of (8), we can derive a good feasible solution to (8) in a tractable convex fashion after employing the above restriction-relax procedure.

However, due to the rank relaxation, there is no guarantee that the resulting $W^\star$ is of rank one. If $\text{rank}(W^\star) = 1$, the rank-one solution of (14) definitely satisfies the outage constraints in (8), and can be a good feasible solution of (8). Otherwise, when $W^\star$ does not meet rank-one condition, we should utilize the approximation method to obtain a feasible

solution to (13). Here, we follow the intuitively reasonable heuristics and take $\lambda_{max}(\mathbf{W}^\star)\mathbf{u}_{max}(\mathbf{W}^\star)$ as the approximation of the optimal beamforming vector [31]. Moreover, in this case, we can not guarantee that this rank-one approximation solution also satisfies the outage constraints in (8). Therefore, when $\text{rank}(W^\star) \neq 1$, we should plug the rank-one approximation solution into the outage constraints of (8) and check their feasibility. If the outage constraints of (8) are satisfied, this rank-one approximation solution is still a good feasible solution of (8); otherwise, (8) is not solved through its convex approximation (14). Afterwards, we should update the given target secrecy rate R with a smaller one when we continue the proposed bisection search over R.

Up to present, how to derive the proposed robust beamforming design has been introduced thoroughly. We can summarize the detailed procedure in Algorithm 1 below.

Algorithm 1 The Proposed Robust Secure Beamforming

Initialization: Set accuracy tolerance $\varepsilon > 0$ and the initial bounds R_l and R_u which ensure $R^\star(P) \in [R_l, R_u]$;
While $R_u - R_l > \varepsilon$
Set $R_{mid} = \frac{R_l + R_u}{2}$ as the given target secrecy rate;
If (14) is infeasible
  $R_u = R_{mid}$;
else
  Solve (14) to get $\mathbf{W}^\star$ and $\mathbf{w} = \lambda_{max}(\mathbf{W}^\star)\mathbf{u}_{max}(\mathbf{W}^\star)$;
  If The outage constraints in (8) are satisfied
    If $\|\mathbf{w}\|^2 \leq P$
      $R_l = R_{mid}$;
      $\mathbf{w}^\star = \mathbf{w}$, a feasible rank-one solution to (4);
    else $R_u = R_{mid}$;
    end
  else $R_u = R_{mid}$;
  end
end
end
Return $\mathbf{w}^\star$.

IV. SIMULATION RESULTS

In this section, the simulation results are provided to illustrate the secrecy rate performance of the proposed probabilistic robust secure beamforming design compared with other existing methods: the worst-case robust design proposed in [21] (Problem (34)) and the simple non-robust secure beamforming design developed in [21] (Problem (16)). The worst-case design in [21] seeks the maximal secrecy rate and guarantees perfect secrecy for any admissible CSI uncertainties, including the worst case. This design transforms the original non-convex SRM problem into a convex one and solves it by convex optimization software. The non-robust design beamforming design developed in [21] focuses on solving the SRM problem under the premise of perfect LCSI and perfect ECSI.

The simulation results to be presented are based on the following settings: the number of transmit antennas at Alice is $N_t = 4$; the estimate value of LCSI $\hat{h}$ is presumed; without loss of generality, the maximum tolerable secrecy outage probability for the kth Eve p_k and the coefficient of the kth Eve's covariance matrix $\alpha_{e,k}^2$ are the same among different eavesdroppers; regarding the imperfect LCSI effects, we define the channel uncertainty ratio of LCSI as $\alpha_b \triangleq \sigma_b^2/\|\hat{h}\|$; in addition, each point in the figures is averaged over 10000 random channel realizations.

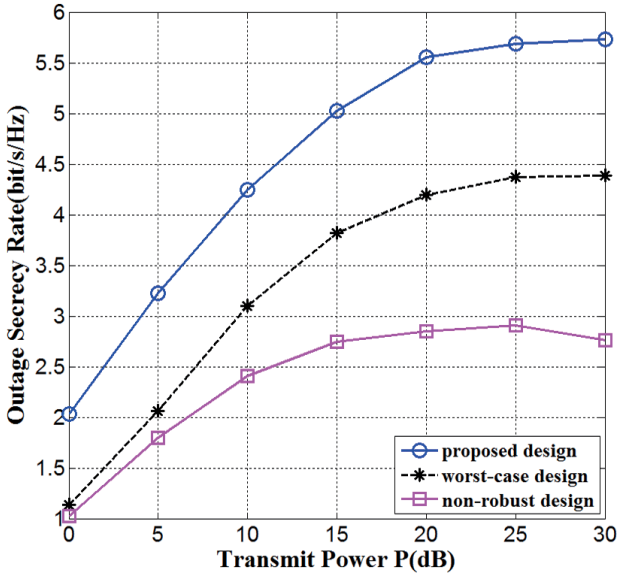


FIGURE 2. Outage secrecy rate versus transmit power P for various designs with $\alpha_b = 0.01$, $\alpha_{e,k}^2 = 0.1$.

In Fig. 2, we evaluate the outage secrecy rate versus the transmit power P for various designs with $\alpha_b = 0.01$, $\alpha_{e,k}^2 = 0.1$. The bounds of target secrecy rate are set as $R_l = 0$ (bits/s/Hz) and $R_u = 10$ (bits/s/Hz). As expected, the proposed outage-constrained robust beamforming design achieves the best outage secrecy rate performance compared with other two related designs in Fig. 2. Specifically speaking, it can be observed that at the outage secrecy rate of 2.5 (bits/s/Hz), the proposed design not only shows nearly 5 dB power gain over the worst-case robust design (Problem (34) in [21]), but also achieves about 10 dB power gain over the non-robust design (Problem (16) in [21]).

Fig. 3 depicts the empirical cumulative distribution function (CDF) of the achieved secrecy rate for different designs, with the target rate $R = 3$ (bits/s/Hz), $p_k = 0.1$, $\alpha_b = 0.01$ and $\alpha_{e,k}^2 = 0.01$. It is clearly displayed that both the proposed probabilistic robust secure beamforming and the worst-case secure design always meet the outage constraints ($p_k = 0.1$), while the non-robust design does not satisfy those outage constraints all the time: about 50% of the rates are below the target rate $R = 3$ (bits/s/Hz). This is due to the fact that the non-robust design does not take channel uncertainties into consideration. Besides, as we know, the conservative worst-case robust beamforming, guarantees the worst-case secrecy performance although the extreme conditions rarely occur in practice. Consequently, the proposed probabilistic design is expected to yield better secrecy rate performance. In this

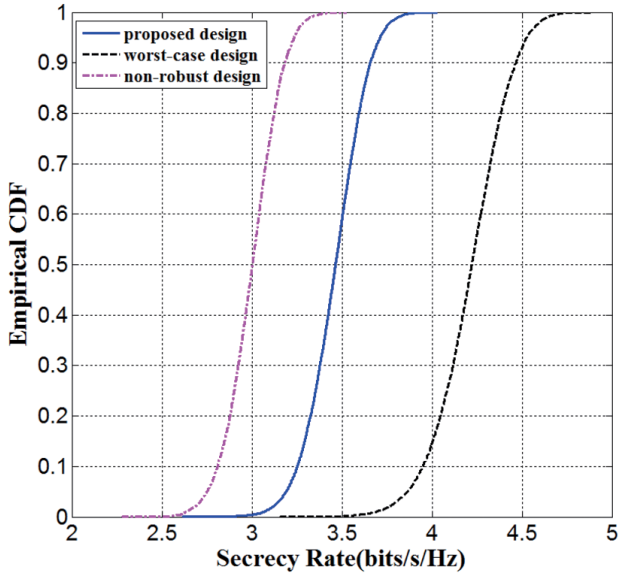


FIGURE 3. The Empirical CDF of secrecy rate with the target rate $R = 3$ (bits/s/Hz), $p_k = 0.1$, $\alpha_b = 0.01$ and $\alpha_{e,k}^2 = 0.01$.

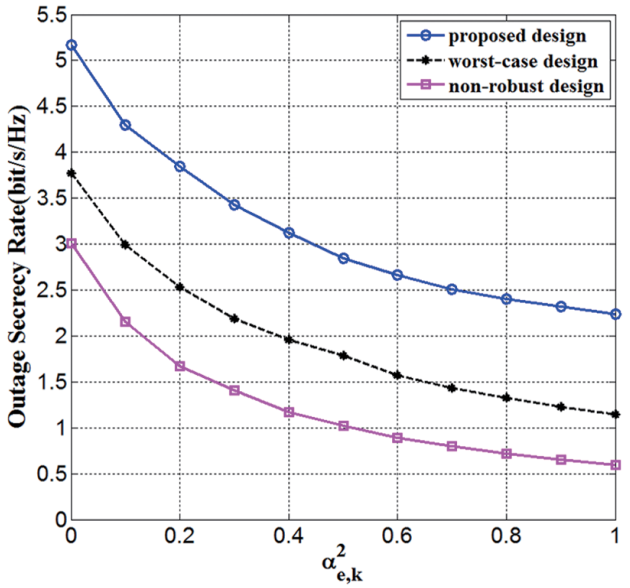


FIGURE 5. Outage secrecy rate versus $\alpha_{e,k}^2$ (the parameter for ECSI's statistical distribution) with $\alpha_b = 0.01$ and $P = 10$dB.

regard, the empirical CDF curves in Fig. 3 confirms that our proposed design achieves a better overall secrecy rate performance since it is less conservative than the conservative worst-case robust beamforming design. This phenomenon is also consistent with the power reduction of the proposed chance-constrained robust secure beamforming, which has been noticed in Fig. 2. Therefore, both Fig. 2 and Fig. 3 confirm the benefit of chance-constrained robust design proposed in this paper in comparison of worst-case robust design.

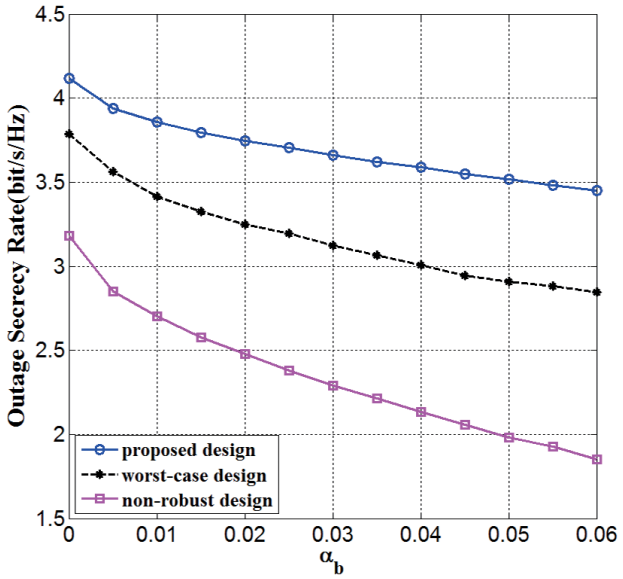


FIGURE 4. Outage secrecy rate versus LCSI's uncertainty ratio α_b with $\alpha_{e,k}^2 = 0.01$ and $P = 5$dB.

Fig. 4 presents the outage secrecy rate versus the channel uncertainty ratio of LCSI α_b with fixed $\alpha_{e,k}^2 = 0.01$ and $P = 5$dB. It is observed from Fig. 4 that the secrecy rate decreases as LCSI error ratio α_b grows. However, the outage secrecy rate of the proposed chance-constrained robust beamforming design is more stable, which also demonstrates the robustness improvement of our proposed design. Fig. 5 plots outage secrecy rate versus the coefficient of the kth Eve's covariance matrix $\alpha_{e,k}^2$ with fixed $\alpha_b = 0.01$ and $P = 10$dB. Not surprising, the proposed robust design again yields better secrecy rate than the other two designs.

V. CONCLUSION

In this paper, we have studied the robust secure beamforming design for MISO wiretap channels. Assuming that the imperfect LCSI and statistical ECSI are available at the transmitter, we establish an optimization problem which maximizes the secrecy rate under the total transmit power constraint and the secrecy rate outage probability constraint. By using bisection search, the Bernstein-type inequality II and SDR approach, the original non-convex optimization is recast as a sequence of SDPs. Finally, simulation results demonstrate the superiority of the proposed beamforming design in comparison of some other existing approaches.

Appendix

A. PROOF OF LEMMA 1

Since $\log(\cdot)$ is a monotone increasing function, let us first consider the following function

$$f_k(P) \triangleq \frac{1 + Ph^H ww^H h}{1 + Pg_k^H ww^H g_k}. \tag{15}$$

Because the optimal secrecy rate is above 0, we have $\log_2(1 + \|h^H w\|^2) - \log_2(1 + \|g_k^H w\|^2) > 0, \ \forall k \in \mathcal{K}$. Then it is easy to derive

$$h^H ww^H h > g_k^H ww^H g_k.$$

Thus we obtain

$$f_k'(P) = \frac{h^H w w^H h - g_k^H w w^H g_k}{(1 + P g_k^H w w^H g_k)^2} > 0. \tag{16}$$

Therefore, it is verified that the function $f_k(P)$ is strictly increasing with respect to P for the considered case of $S_k(\mathbf{w}) > 0$.

Furthermore, we can assert that $\gamma_k(P) \triangleq S_k(P\mathbf{w}) = \log_2(f_k(P))$ is monotonically increasing with the power P growing in the case of $S_k(P\mathbf{w}) > 0$.

Next, we discuss an equivalent variation of the O-SRM problem (4), presented as follows:

$$\begin{aligned} R^\star(P) = \max_{w} \; & R \\ s.t. \; & \Pr\left(S_k(P\mathbf{w}) \geq R\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}, \\ & \|w\|^2 \leq 1. \end{aligned} \tag{17}$$

According to (17), as $\gamma_k(P) \triangleq S_k(P\mathbf{w})$ is monotonically increasing with the power P growing in the case of $S_k(P\mathbf{w}) > 0$, it is easy to conclude that $R^\star(P)$ is monotonically increasing with the power P increasing.

Up to present, the proof of Lemma 1 is completed.

B. PROOF OF THEOREM 1

This proof is divided into three steps: First, we prove that the optimal solution to (4) satisfies $\mathbf{w}_1^H \mathbf{w}_1 = P$; Second, we prove that the optimal solution to (4) is also an optimal solution to (7); Third, we prove the converse. Without loss of generality, let $\mathbf{w}_1$ be an optimal solution of (4), and $\mathbf{w}_2$ be an optimal solution of (7) in the following proof.

1) $\mathbf{w}_1^H \mathbf{w}_1 = P$

Since $\mathbf{w}_1^H \mathbf{w}_1 \leq P$, if we suppose $\mathbf{w}_1^H \mathbf{w}_1 \neq P$, then $\mathbf{w}_1^H \mathbf{w}_1 < P$. From $\mathbf{w}_1^H \mathbf{w}_1 < P$, we can construct another point

$$\breve{\mathbf{w}}_1 = P_1 \mathbf{w}_1 \text{ with } P_1 > 1 \text{ such that } \breve{\mathbf{w}}_1^H \breve{\mathbf{w}}_1 = P.$$

From Lemma 1, $\gamma_k(P) \triangleq S_k(P\mathbf{w})$ is monotonically increasing with P increasing. Hence $S_k(\breve{\mathbf{w}}_1) = S_k(P_1\mathbf{w}_1) > S_k(\mathbf{w}_1)$. Without loss of generality, let

$$S_k(\breve{\mathbf{w}}_1) = S_k(\mathbf{w}_1) + S_{1,k} \text{ with } S_{1,k} > 0.$$

Now consider

$$\begin{aligned} &\Pr\left(S_k(\mathbf{w}_1) \geq R^\star(P)\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K} \\ &\Rightarrow \Pr\left(S_k(\mathbf{w}_1) + S_{1,k} \geq R^\star(P) + S_{1,k}\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}, \\ &\quad \text{i.e.,} \;\; \Pr\left(S_k(\breve{\mathbf{w}}_1) \geq R^\star(P) + S_{1,k}\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}. \end{aligned}$$

This means not only $\breve{\mathbf{w}}_1$ is feasible to (4), but also can achieve a higher objective value than $\mathbf{w}_1$ in (4). This contradicts the optimality of $R^\star(P)$ in (4). Therefore, we can conclude that $\mathbf{w}_1^H \mathbf{w}_1 = P$ should be right.

2) $\mathbf{w}_1$ IS ALSO AN OPTIMAL SOLUTION OF (7)

Suppose $\mathbf{w}_1$ is optimal to (4), but not optimal to (7). Obviously, $\mathbf{w}_1$ is feasible to (7). Then, the following relation holds:

$$\mathbf{w}_2^H \mathbf{w}_2 < \mathbf{w}_1^H \mathbf{w}_1 = P.$$

From $\mathbf{w}_2^H \mathbf{w}_2 < P$, we can construct another point

$$\breve{\mathbf{w}}_2 = P_2 \mathbf{w}_2 \text{ with } P_2 > 1 \text{ such that } \breve{\mathbf{w}}_2^H \breve{\mathbf{w}}_2 = P.$$

Moreover, according to Lemma 1, $\gamma_k(P) \triangleq S_k(P\mathbf{w})$ is monotonically increasing with P increasing. Hence $S_k(\breve{\mathbf{w}}_2) = S_k(P_2\mathbf{w}_2) > S_k(\mathbf{w}_2)$. Without loss of generality, let

$$S_k(\breve{\mathbf{w}}_2) = S_k(\mathbf{w}_2) + S_{2,k} \text{ with } S_{2,k} > 0.$$

Now consider

$$\begin{aligned} &\Pr\left(S_k(\mathbf{w}_2) \geq R^\star(P)\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K} \\ &\Rightarrow \Pr\left(S_k(\mathbf{w}_2) + S_{2,k} \geq R^\star(P) + S_{2,k}\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}, \\ &\quad \text{i.e.,} \;\; \Pr\left(S_k(\breve{\mathbf{w}}_2) \geq R^\star(P) + S_{2,k}\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}. \end{aligned}$$

This means not only $\breve{\mathbf{w}}_2$ is feasible to (4), but also can achieve a higher objective value than $\mathbf{w}_1$ in (4). This contradicts the optimality of $R^\star(P)$ in (4). Therefore, we can conclude that $\mathbf{w}_1$ should be an optimal solution of (7).

3) $\mathbf{w}_2$ IS ALSO AN OPTIMAL SOLUTION OF (4)

Because $\mathbf{w}_2$ is optimal to (7), we have

$$\Pr\left(S_k(\mathbf{w}_2) \geq R^\star(P)\right) \geq 1 - p_k, \quad \forall k \in \mathcal{K}. \tag{18}$$

In addition, since $\mathbf{w}_1^H \mathbf{w}_1 = P$ and $\mathbf{w}_1$ should be the optimal solution of (7), it is easy to derive that $\mathbf{w}_2^H \mathbf{w}_2 = \mathbf{w}_1^H \mathbf{w}_1 = P$. Thus, it is obvious that $\mathbf{w}_2$ is feasible to (4).

Next, we suppose $\mathbf{w}_2$ is feasible but not optimal to (4). This implies

$$\max\left\{R \;\middle|\; \Pr\left(S_k(\mathbf{w}_2) \geq R\right) \geq 1 - p_k, \forall k \in \mathcal{K}\right\} < R^\star(P).$$

However, this contradicts (18). Therefore, we can conclude that $\mathbf{w}_2$ should be an optimal solution to (4).

Thus far, we have completed the proof of Theorem 1.

REFERENCES

[1] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[2] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Interference assisted secret communication," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 3153–3167, May 2011.

[3] Q. Xu, P. Ren, H. Song, and Q. Du, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations," *IEEE Access*, vol. 4, pp. 2840–2853, Jun. 2016.

[4] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

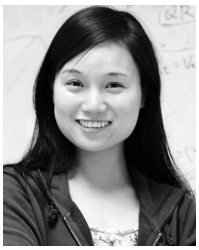
[5] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Secure cooperative transmission against jamming-aided eavesdropper for ARQ based wireless networks," *IEEE Access*, vol. 5, pp. 3763–3776, Mar. 2017.

[6] D. Wang, P. Ren, J. Cheng, Q. Du, Y. Wang, and L. Sun, "Secure transmission for mixed FSO-RF relay networks with physical-layer key encryption and wiretap coding," *Opt. Exp.*, vol. 25, no. 9, pp. 10078–10089, 2017.

[7] D. Wang, P. Ren, Q. Du, Y. Wang, and L. Sun, "Reciprocally-benefited secure transmission for spectrum sensing-based cognitive radio sensor networks," *Sensors*, vol. 16, no. 12, pp. 1–21, Nov. 2016, doi: 10.3390/s16121998.

[8] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[9] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.
[10] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1833–1847, May 2015.
[11] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for mimo wiretap channels using alternating optimization," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1727, Sep. 2013.
[12] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[13] S. Loyka and C. D. Charalambous, "Optimal signaling for secure communications over Gaussian MIMO wiretap channels," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7207–7215, Dec. 2016.
[14] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for MISO wiretap channels under secrecy outage constraint," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 18–21, Jan. 2015.
[15] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *Proc. Statist. Signal Process. Workshop (SSP)*, 2012, pp. 389–392.
[16] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.
[17] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.
[18] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.
[19] J. Huang and A. Lee Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2011.
[20] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[21] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Trans. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.
[22] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, Oct. 2013.
[23] J. Li and A. P. Petropulu, "Explicit solution of worst-case secrecy rate for MISO wiretap channels with spherical uncertainty," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3892–3895, Jul. 2011.
[24] A. Mukherjee and A. Lee Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[25] M. Pei, J. Wei, K.-K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544–549, Feb. 2012.
[26] F. Gao, T. Cui, and A. Nallanathan, "On channel estimation and optimal training design for amplify and forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1907–1916, May 2008.
[27] T. Cui, F. Gao, T. Ho, and A. Nallanathan, "Distributed space–time coding for two-way wireless relay networks," *IEEE Trans. Signal Process.*, vol. 57, no. 2, pp. 658–671, Feb. 2009.
[28] F. Gao, R. Zhang, and Y.-C. Liang, "Optimal channel estimation and training design for two-way relay networks," *IEEE Trans. Commun.*, vol. 57, no. 10, pp. 3024–3033, Oct. 2009.
[29] K.-Y. Wang, A. M.-C. So, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Outage constrained robust transmit optimization for multiuser MISO downlinks: Tractable approximations by conic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 21, pp. 5690–5705, Nov. 2011.
[30] M. Grant and S. Boyd. (Jun. 2009). *CVX: MATLAB Software for Disciplined Convex Programming*. [Online]. Available: http://cvxr.com/cvx/
[31] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20–34, May 2010.



JING XU received the B.S. and Ph.D. degrees in information and communications engineering from Xi'an Jiaotong University, Xi'an, China, in 2005 and 2011, respectively. Since 2011, she has been with the Department of Information and Communications Engineering, Xi'an Jiaotong University, as an Assistant Professor. Her current research interests include cooperative communications, wireless physical layer security, cognitive radio, and multiple-input multiple-output systems.

SIWEN XU received the B.Eng. degree in electronic and information engineering from the China University of Geosciences, Wuhan, China, in 2015. She is currently pursuing the M.Eng. degree with Xi'an Jiaotong University. Her research interests include wireless communications and physical layer security.

CHONGBIN XU (M'16) received the B.S. degree in information engineering from Xi'an Jiaotong University in 2005 and the Ph.D. degree in information and communication engineering from Tsinghua University in 2012. Since 2014, he has been with the Department of Communication Science and Engineering, Fudan University, China. His research interests are in the areas of signal processing and communication theory, including linear precoding, iterative detection, and random access techniques.