Outage Constrained Secrecy Rate Maximization Design With SWIPT in MIMO-CR Systems

DOI:
10.1109/TVT.2017.2717495

Document Version
Accepted author manuscript

Outage Constrained Secrecy Rate Maximization Design with SWIPT in MIMO-CR Systems

Y. Yuan, *Student Member, IEEE*, and Zhiguo Ding, *Senior Member, IEEE*

***Abstract*—This paper investigates an outage-constrained secrecy rate maximization (OC-SRM) problem based on the statistical channel uncertainty assumption in an underlay multiple-input-multiple-output (MIMO) cognitive radio network (CRN) where the secondary transmitter (ST) provides simultaneous wireless information and power transfer (SWIPT) to receivers. Our objective is to design the transmit covariance matrix and artificial noise (AN)-aided covariance matrix through maximizing the secrecy rate of the secondary user while satisfying the given outage probability requirements. The designed problem is nonconvex and challenging. We employ the existing theory to reformulate the original problem to two equivalent subproblems by introducing auxiliary variables in order to overcome the difficulty arising from the Shannon capacity expression. The Bernstein-type inequality approach is resorted to conservatively approximate the probabilistic constraints. The merit of the transformation and conversion is that the tractable solutions of the original OC-SRM problem can be easily obtained through solving two convex conic subproblems alternately. Furthermore, we extend the proposed algorithm to solve full uncertainty model design. Numerical results demonstrate the efficacy of the proposed designs.**

***Index Terms*—SWIPT, Bernstein-type inequality, cognitive radio, secrecy capacity, MIMO wiretap channel.**

I. Introduction

Cognitive radio (CR) has been considered as a promising technique to enhance the usage of spectrum due to the openness spectrum and the limited interference of the primary system [1]. However, there exists a bottleneck for CR networks to provide a high date rate due to the energy-constrained devices. Based on the characteristics of radio frequency (RF) signal, simultaneous wireless information and power transfer (SWIPT) has been considered as a promising technique to extend lifetime of energy-constrained devices in CR networks [2]. However, there exists an unexpected security vulnerability of the desired information in CR networks since energy receivers (ERs) have high probability to successfully decode the desired information due to the better fading channels. In order to protect the successful delivery of the information, the security of CR with SWIPT should be carefully considered [3], [4]. In [3], Fang *et al.* investigated a secrecy problem for SWIPT with the artificial noise (AN)-aided precoding in a multiple-input multiple-output (MIMO)-CR broadcast scenario based on the perfect channel state information (CSI) assumption. In [4], the authors proposed a multiobjective optimization framework with SWIPT in order to design a resource allocation algorithm in the security multiple-input single-output (MISO)-CR networks where the idled secondary receivers (SUs) were considered as the potential eavesdroppers based on the imperfect CSI assumption. However, the secrecy rate maximization, which is achieved by AN-aided design based on statistical channel uncertainty assumption in MIMO-SWIPT, has not been considered under CR scenario in the literature.

In this paper, an outage-constrained design, which has the ability to guarantee the system performance in a delay-critical scenario compared with the perfect CSI design [5], [6] and worst-case design [7], is considered based on the assumption of statistical channel uncertainty model. An outage-constrained secrecy rate maximization (OC-SRM) problem is proposed to optimize the covariance matrix of the transmit signal and AN signal through satisfying probability requirements. Some similar OC-SRM problems have been studied in the traditional MISO-SWIPT system [8]-[11]. The authors in these papers considered the conservative approximation solutions to deal with the probabilistic constraints. However, the methods used to solve the secrecy rate function in MISO system cannot be applied to solve the same problems in MIMO system. Hence, in this paper, a more general and challenging OC-SRM problem is designed with SWIPT in MIMO-CR system. Due to the nonconvex and nonsmooth secrecy rate function and complicated probabilistic constraints, the proposed OC-SRM problem is more challenging to obtain the safe and tractable design. We transform the original OC-SRM problem into two equivalent subproblems by introducing auxiliary variables to solve the Shannon capacity expression in secrecy rate function based on the theory in [12]-[15]. To tackle the difficulty arising from probabilistic constraints in each subproblem, we consider a conservative approximation approach, namely Bernstein-type inequality (BTI) introduced in [8]-[11], to transform the probabilistic constraints into the safe and tractable forms. The tractable solution of the proposed OC-SRM problem can be obtained by alternately solving two convex conic subproblems. Finally, the effectiveness of the proposed algorithm is validated by simulation.

II. System Model

In this paper, we consider an underlay cognitive MIMO wiretap scenario, where a secondary transmitter (ST) with N_t antennas, a desired secondary information receiver (SIR) with N_d antennas, $(M \geq 1)$ secondary energy receivers (SER) with N_e antennas and $(K \geq 1)$ primary receivers (PU) with N_p antennas. The slow frequency-flat fading channel from the ST to the SIR, the kth PU and the mth SER are denoted by $\mathbf{G}_k \in \mathbb{C}^{N_t \times N_p}$ (PU), $\mathbf{H}_d \in \mathbb{C}^{N_t \times N_d}$ (SIR) and $\mathbf{H}_m \in \mathbb{C}^{N_t \times N_e}$ (SER), respectively. The received signals at the SIR, the kth

This work was supported by the UK EPSRC under grant number EP/L025272/1 and by H2020-MSCA-RISE-2015 under grant number 690750.

Y. Yuan and Z. Ding are with School of Computing and Communications, Lancaster University, Lancaster, LA1 4YW, U.K. e-mail: (y.yuan3@lancaster.ac.uk; z.ding@lancaster.ac.uk).

PU and the mth SER may be written as

$$\mathbf{y}_d = \mathbf{H}_d^H \mathbf{x} + \mathbf{n}_d, \tag{1}$$

$$\mathbf{y}_k = \mathbf{G}_k^H \mathbf{x} + \mathbf{n}_k, k \in K, \tag{2}$$

$$\mathbf{y}_m = \mathbf{H}_m^H \mathbf{x} + \mathbf{n}_m, m \in M, \tag{3}$$

respectively, where $\mathbf{n}_d \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}), \mathbf{n}_k \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{n}_m \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ denote i.i.d. standard complex Gaussian noise; $\mathbf{x} \in \mathbb{C}^{N_t}$ is the transmit signal of ST, which can be formed as $\mathbf{x} = \mathbf{s}+\mathbf{v}$, where $\mathbf{s} \in \mathbb{C}^{N_t}$ denotes the coded confidential signal, the distribution of which follows $\mathcal{CN}(\mathbf{0}, \mathbf{Q})$ with the transmit covariance $\mathbf{Q} \succeq \mathbf{0}$ and $\mathbf{v} \sim \mathcal{CN}(\mathbf{0}, \mathbf{V})$ is AN-aided signal with the covariance $\mathbf{V} \succeq \mathbf{0}$ to enhance physical layer security [9]. We assume that all SERs are linear models rather than practical nonlinear models in [16]. Thus, the harvested energy at the mth SU-ER is given by $E_m = \xi_m \mathrm{Tr}(\mathbf{H}_m^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_m, m \in M$, where $\xi \in (0, 1]$ is the energy conversion efficiency. Since all SERs are potential eavesdroppers, the achievable secrecy rate of SIR can be expressed by [17]-[19]

$$R_s = \min_{m \in M} \; \{C_d(\mathbf{Q}, \mathbf{V}) - C_m(\mathbf{Q}, \mathbf{V})\}, \tag{4}$$

where $C_d(\mathbf{Q}, \mathbf{V}) = \log|\mathbf{I} + (\mathbf{H}_d^H \mathbf{V} \mathbf{H}_d + \mathbf{I})^{-1} \mathbf{H}_d^H \mathbf{Q} \mathbf{H}_d|$ and $C_m(\mathbf{Q}, \mathbf{V}) = \log|\mathbf{I} + (\mathbf{H}_m^H \mathbf{V} \mathbf{H}_m + \sigma_e^2 \mathbf{I})^{-1} \mathbf{H}_m^H \mathbf{Q} \mathbf{H}_m|$ are the mutual information of the SIR and the mth SER, respectively. Since the secondary system and the primary system share the same spectrum resource in the underlay CRN, we need consider interference power at the kth PU from ST as $I_k = \mathrm{Tr}(\mathbf{G}_k^H(\mathbf{Q}+\mathbf{V})\mathbf{G}_k), k \in K$.

III. Robust secure communication design

In this section, we propose the OC-SRM problem under the imperfect CSI assumption since there exist the channel estimation and quantization errors in practical scenarios.

A. Channel Uncertainty Models

In this subsection, we introduce two models of statistical channel uncertainty in the following.

1) Partial Channel Uncertainty (PCU): We first consider a particular channel uncertainty scenario, where ST has the perfect CSI of SIR and the imperfect CSI of all SERs and PUs. Accordingly, the actual channels of the mth SER and the kth PU can be respectively modeled as

$$\mathbf{H}_m = \widehat{\mathbf{H}}_m + \triangle\mathbf{H}_m, m \in M, \quad \mathbf{G}_k = \widehat{\mathbf{G}}_k + \triangle\mathbf{G}_k, k \in K, \tag{5}$$

where $\widehat{\mathbf{H}}_m$ and $\widehat{\mathbf{G}}_k$ are the estimated channel matrixes; $\mathrm{vec}(\triangle\mathbf{H}_m) \sim \mathcal{CN}(0, \mathbf{C}_m)$ and $\mathrm{vec}(\triangle\mathbf{G}_k) \sim \mathcal{CN}(0, \mathbf{D}_k)$ denote the corresponding statistical errors, where $\mathbf{C}_m$ and $\mathbf{D}_k$ are the positive semidefinite matrixes.

2) Full Channel Uncertainty (FCU): Next, we consider a general uncertainty case, in which ST has the imperfect CSI of all receivers. Thus, the actual channel of SIR is determined as

$$\mathbf{H}_d = \widehat{\mathbf{H}}_d + \triangle\mathbf{E}_d, \tag{6}$$

where $\widehat{\mathbf{H}}_d$ is the estimated CSI and corresponding error satisfies the complex Gaussian distribution, $\mathrm{vec}(\triangle\mathbf{E}_d) \sim \mathcal{CN}(0, \mathbf{Z}_d)$, where $\mathbf{Z}_d$ is a positive semidefinite matrix. Based on the above uncertainty models, the OC-SRM problem can be expressed as

$$\max_{\mathbf{Q}, \mathbf{V}, R} \quad R \tag{7a}$$

$$s.t. \;\; \Pr\{\min_{m \in M}\{C_d(\mathbf{Q}, \mathbf{V}) - C_m(\mathbf{Q}, \mathbf{V})\} \geq R\} \geq 1-\rho, \forall_m, \tag{7b}$$

$$\Pr\{\min \xi \mathrm{Tr}(\mathbf{H}_m^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_m) \geq \eta_m\} \geq 1-\rho_m, \forall_m, \tag{7c}$$

$$\Pr\{\mathrm{Tr}(\mathbf{G}_k^H(\mathbf{Q}+\mathbf{V})\mathbf{G}_k) \leq \Gamma_k\} \geq 1-\rho_k, \forall_k, \tag{7d}$$

$$\mathrm{Tr}(\mathbf{Q}+\mathbf{V}) \leq P, \mathbf{Q} \succeq \mathbf{0}, \mathbf{V} \succeq \mathbf{0}, \tag{7e}$$

where η_m is the harvested energy target at the mth SER; Γ_k denotes tolerable interference power at the kth PU; P is the power budget at the ST; $\rho \in (0, 1]$, $\rho_m \in (0, 1]$ and $\rho_k \in (0, 1]$ indicate the maximum allowable outage probabilities associated with the secrecy rate of SIR, harvested energy of the mth SER and received interference power of the kth PU.

B. Robust SRM Problem under PCU

Problem (7) is non-convex and computationally intractable due to the Shannon capacity expression in secrecy rate function and the outage probability constraints (7b)-(7d) [20]. We consider to replace $\{C_d - C_m\}$ in outage secrecy function (7b) by an easy-to-handle function, which also satisfies the probabilistic requirement. First, we need to rewrite C_d and $C_{e,m}$ based on the concept of log function

$$C_d = \log|\mathbf{H}_d^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_d + \mathbf{I}| - \log|\mathbf{H}_d^H \mathbf{V} \mathbf{H}_d + \mathbf{I}|, \tag{8}$$

$$C_m = \log|\mathbf{H}_m^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_m + \mathbf{I}| - \log|\mathbf{H}_m^H \mathbf{V} \mathbf{H}_m + \mathbf{I}|. \tag{9}$$

Then, we consider to use following lemma in order to solve log det function in (8) and (9) efficiently

Lemma 1: [12]: Let's define a positive matrix $\mathbf{E} \succ \mathbf{0}$, $\mathbf{E} \in \mathbb{C}^{N \times N}$ with integer N, there exist a function, $v(\mathbf{S}, \mathbf{E}) = -\mathrm{Tr}(\mathbf{SE}) + \ln|\mathbf{S}| + N$, satisfies the following equation

$$\ln|\mathbf{E}^{-1}| = \max_{\mathbf{S} \in \mathbb{C}^{N \times N}, \mathbf{S} \succeq \mathbf{0}} \quad v(\mathbf{S}, \mathbf{E}) \tag{10}$$

By invoking Lemma 1, the second term of (8) and the first term of (9) can be rewritten as follows, respectively

$$-\log|(\mathbf{H}_d^H \mathbf{V} \mathbf{H}_d + \mathbf{I})^{-1}| = \min_{\mathbf{S}_d \succeq \mathbf{0}} \mathrm{Tr}(\mathbf{S}_d(\mathbf{H}_d^H \mathbf{V} \mathbf{H}_d + \mathbf{I})) - \ln|\mathbf{S}_d| - N_d \tag{11}$$

$$-\log|(\mathbf{H}_m^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_m + \mathbf{I})^{-1}| = \min_{\mathbf{S}_m \succeq \mathbf{0}} \mathrm{Tr}(\mathbf{S}_m(\mathbf{H}_m^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_m + \mathbf{I})) - \ln|\mathbf{S}_m| - N_e. \tag{12}$$

The authors in [13]-[15] give the following expression to approximate the mutual information at low signa-to-noise ratio (SNR) for MIMO channel

$$\log|\mathbf{I} + \frac{1}{\sigma^2}\mathbf{H}\mathbf{Q}\mathbf{H}^H| = \frac{1}{\sigma^2}\mathrm{Tr}\{\mathbf{H}\mathbf{Q}\mathbf{H}^H\} + \mathcal{O}(\frac{1}{\sigma^2}\|\mathbf{H}\mathbf{Q}\mathbf{H}^H\|). \tag{13}$$

Based on Lemma 1 and low SNR approximation, the secrecy rate outage constraint (7b) can be reformulated as

$$\begin{aligned}\Pr\{&\mathrm{Tr}(\mathbf{H}_d^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_d) - \mathrm{Tr}(\mathbf{S}_d(\mathbf{H}_d^H \mathbf{V} \mathbf{H}_d + \mathbf{I})) + \ln|\mathbf{S}_d| + N_d \\ &- \mathrm{Tr}(\mathbf{S}_m(\mathbf{H}_m^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_m + \mathbf{I})) + \ln|\mathbf{S}_m| + N_e + \mathrm{Tr}(\mathbf{H}_m^H \mathbf{V} \mathbf{H}_m) \\ &- R \geq 0\} \geq 1-\rho.\end{aligned} \tag{14}$$

Next, we need to solve the new challenge: probabilistic constraints, in (7c), (7d) and (14). Since $\mathbf{e}_m = \mathrm{vec}(\triangle\mathbf{H}_m)$ and $\mathbf{e}_k = \mathrm{vec}(\triangle\mathbf{G}_k)$, we can define $\mathbf{e}_m \sim \mathcal{CN}(0, \mathbf{C}_m)$ and $\mathbf{e}_k \sim \mathcal{CN}(0, \mathbf{D}_k)$. Then, we have the following transformation

$$\mathbf{e}_m = \mathbf{C}_m^{\frac{1}{2}} \mathbf{v}_m, \quad \mathbf{e}_k = \mathbf{D}_k^{\frac{1}{2}} \mathbf{x}_k, \tag{15}$$

where $\mathbf{v}_m \sim \mathcal{CN}(0, \mathbf{I}_{N_t \times N_e})$ and $\mathbf{x}_k \sim \mathcal{CN}(0, \mathbf{I}_{N_t \times N_p})$. By substituting the uncertainty channel models into the outage constraints in (7) and invoking the identity function $\mathrm{Tr}(\mathbf{A}^H \mathbf{BCD}) = \mathrm{vec}(\mathbf{A})^H(\mathbf{D}^T \otimes \mathbf{B})\mathrm{vec}(\mathbf{C})$, we can express secrecy outage constraint (14) as

$$\begin{aligned}\Pr\{&\mathbf{v}_m^H \mathbf{C}_m^{\frac{1}{2}} \mathbf{\Theta}_m \mathbf{C}_m^{\frac{1}{2}} \mathbf{v}_m + 2\Re(\mathbf{v}_m^H \mathbf{C}_m^{\frac{1}{2}} \mathbf{\Theta}_m \mathbf{h}_m) + \widehat{\mathbf{h}}_m^H \mathbf{\Theta}_m \widehat{\mathbf{h}}_m \leq c_m\} \\ &\geq 1-\rho.\end{aligned} \tag{16}$$

where $\widehat{\mathbf{h}}_m = \mathrm{vec}(\widehat{\mathbf{H}}_m)$, $\mathbf{\Theta}_m = (\mathbf{S}_m^T \otimes (\mathbf{Q}+\mathbf{V}) - \mathbf{I}_{N_t} \otimes \mathbf{V})$ and $c_m = \mathrm{Tr}(\mathbf{H}_d^H(\mathbf{Q}+\mathbf{V})\mathbf{H}_d) - \mathrm{Tr}(\mathbf{S}_d(\mathbf{H}_d^H \mathbf{V} \mathbf{H}_d + \mathbf{I})) + \ln|\mathbf{S}_d| + N_d - \mathrm{Tr}(\mathbf{S}_m) + \ln|\mathbf{S}_m| + N_e - R$. The harvested energy outage constraint (7c) can be reformulated as

$$\Pr\{\mathbf{v}_m^H \mathbf{C}_m^{\frac{1}{2}} \mathbf{\Xi} \mathbf{C}_m^{\frac{1}{2}} \mathbf{v}_m + 2\Re(\mathbf{v}_m^H \mathbf{C}_m^{\frac{1}{2}} \mathbf{\Xi} \widehat{\mathbf{h}}_m) + \widehat{\mathbf{h}}_m^H \mathbf{\Xi} \widehat{\mathbf{h}}_m \geq \frac{\eta_m}{\xi}\} \geq 1-\rho_m, \tag{17}$$

where $\mathbf{\Xi}=\mathbf{I}_{N_t}^T\otimes(\mathbf{Q}+\mathbf{V})$. Similarly, we transform the interference temperature outage constraint (7d) into the following form

$$\Pr\{\mathbf{x}_k^H\mathbf{D}_k^{\frac{1}{2}}\mathbf{\Phi}\mathbf{D}_k^{\frac{1}{2}}\mathbf{x}_k+2\Re(\mathbf{x}_k^H\mathbf{D}_k^{\frac{1}{2}}\mathbf{\Phi}\widehat{\mathbf{g}}_k)+\widehat{\mathbf{g}}_k^H\mathbf{\Phi}\widehat{\mathbf{g}}_k\le\Gamma_k\}\ge1-\rho_k, \quad (18)$$

where $\widehat{\mathbf{g}}_k=\mathrm{vec}(\widehat{\mathbf{G}}_k)$ and $\mathbf{\Phi}=\mathbf{I}_{N_t\times N_p}^T\otimes(\mathbf{Q}+\mathbf{V})$.

The above transformation still cannot provide a convex approximation of the original problem due to the intractable outage constraints in (16)-(18). In order to convert the intractable outage constraints into tractable deterministic constraints, we consider to employ the BTI approach, which can provide a conservative approximation of the outage constraint based on large deviation inequalities for complex Gaussian quadratic vector functions.

Lemma 2: (*BTI*) [11], [21]: Consider the following outage constraint

$$f(\mathbf{A},\mathbf{u},c)\Leftrightarrow\Pr\{\mathbf{x}^H\mathbf{A}\mathbf{x}+2\mathrm{Re}\{\mathbf{x}^H\mathbf{u}\}+c\ge0\}\ge1-\rho, \quad (19)$$

where $\mathbf{A}\in\mathbb{C}^{N\times N}$ is a complex Hermitian matrix, $\mathbf{a}\in\mathbb{C}^{N\times1}$, $\mathbf{x}\sim\mathcal{CN}(\mathbf{0},\mathbf{I})$ and fixed $\rho\in(0,1]$. With any slack variables λ and μ, the outage constraint can be equivalently transformed into the following three inequalities

$$\begin{cases}\mathrm{Tr}(\mathbf{A})-\sqrt{-2\ln(\rho)}\lambda+\ln(\rho)\mu+c\ge0,\\ \left\|\begin{bmatrix}\mathrm{vec}(\mathbf{A})\\ \sqrt{2}\mathbf{u}\end{bmatrix}\right\|\le\lambda,\\ \mu\mathbf{I}_N+\mathbf{A}\succeq\mathbf{0},\quad \mu\ge0.\end{cases} \quad (20)$$

By involving Lemma 2, the convex approximation of the secrecy outage constraint in (16) can be reformulated into the following inequalities:

$$\begin{cases}\mathrm{Tr}(\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Theta}_m\mathbf{C}_m^{\frac{1}{2}})+\sqrt{-2\ln(\rho)}\lambda_m-\ln(\rho)\mu_m+\widehat{\mathbf{h}}_m^H\mathbf{\Theta}_m\widehat{\mathbf{h}}_m-c_m\le0,\\ \left\|\begin{bmatrix}\mathrm{vec}(\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Theta}_m\mathbf{C}_m^{\frac{1}{2}})\\ \sqrt{2}\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Theta}_m\mathbf{h}_m\end{bmatrix}\right\|\le\lambda_m,\\ \mu_m\mathbf{I}_{N_t\times N_e}-\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Theta}_m\mathbf{C}_m^{\frac{1}{2}}\succeq\mathbf{0},\quad \mu_m\ge0,\quad\forall m,\end{cases} \quad (21)$$

and that of the energy outage constraint in (17) can be represented by

$$\begin{cases}\mathrm{Tr}(\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Xi}\mathbf{C}_m^{\frac{1}{2}})-\sqrt{-2\ln(\rho_m)}\alpha_m+\ln(\rho_m)\beta_m+\widehat{\mathbf{h}}_m^H\mathbf{\Xi}\widehat{\mathbf{h}}_m-\frac{\eta_m}{\xi}\ge0,\\ \left\|\begin{bmatrix}\mathrm{vec}(\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Xi}\mathbf{C}_m^{\frac{1}{2}})\\ \sqrt{2}\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Xi}\widehat{\mathbf{h}}_m\end{bmatrix}\right\|\le\alpha_m,\\ \beta_m\mathbf{I}_{N_t\times N_e}+\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Xi}\mathbf{C}_m^{\frac{1}{2}}\succeq\mathbf{0},\quad\beta_m\ge0,\quad\forall m.\end{cases} \quad (22)$$

Due to the similarly transformation of the previous function, the outage constraint (18) can be recast into

$$\begin{cases}\mathrm{Tr}(\mathbf{D}_k^{\frac{1}{2}}\mathbf{\Phi}\mathbf{D}_k^{\frac{1}{2}})+\sqrt{-2\ln(\rho_k)}\nu_k-\ln(\rho_k)\omega_k+\widehat{\mathbf{g}}_k^H\mathbf{\Phi}\widehat{\mathbf{g}}_k-\Gamma_k\le0,\\ \left\|\begin{bmatrix}\mathrm{vec}(\mathbf{D}_k^{\frac{1}{2}}\mathbf{\Phi}\mathbf{D}_k^{\frac{1}{2}})\\ \sqrt{2}\mathbf{C}_m^{\frac{1}{2}}\mathbf{\Xi}\widehat{\mathbf{g}}_k\end{bmatrix}\right\|\le\nu_k,\\ \omega_k\mathbf{I}_{N_t\times N_p}-\mathbf{D}_k^{\frac{1}{2}}\mathbf{\Phi}\mathbf{D}_k^{\frac{1}{2}}\succeq\mathbf{0},\quad\omega_k\ge0,\quad\forall k.\end{cases} \quad (23)$$

It is worth to note that the outage constraints of the original problem (7) have been convert into the tractable deterministic forms based on the above three transformations. The new problem (7) is still not jointly convex for all variables after replacing (7b)-(7d) by (21)-(23). In order to overcome this challenge, we proposed an alternating optimization (AO) algorithm. Then, the secrecy rate maximization problem (7) can be solved by fixing $\mathbf{S}_s$ and $\mathbf{S}_m$

$$\begin{aligned}\max_{\mathbf{Q},\mathbf{V},R,\lambda_m,\mu_m,\alpha_m,\beta_m,\nu_k,\omega_k}\quad & R\\ s.t.\quad & (21)-(23),(7e).\end{aligned} \quad (24)$$

Algorithm 1: AO Algorithm for (7) in PCU

1) **Initialize:** Set $n=1,\varepsilon>0,\mathbf{S}_d^0=\mathbf{I},\mathbf{S}_m^0=\mathbf{I},m=1,\ldots,M$;
2) **Repeat:**
   a) Solving (24) with fixed $\mathbf{S}_d=\mathbf{S}_d^{l-1}$ and $\mathbf{S}_m=\mathbf{S}_m^{l-1}$ to obtain $(\mathbf{Q}^{l-1},\mathbf{V}^{l-1},R^{l-1})$;
   b) Solving (25) with fixed $\mathbf{Q}=\mathbf{Q}^{l-1}$ and $\mathbf{V}=\mathbf{V}^{l-1}$ to get $(\mathbf{S}_d^l,\mathbf{S}_m^l,R^l)$;
   c) $l=l+1$;
3) **Until** $|R^l-R^{l-1}|\le\varepsilon$
4) Output $(\mathbf{Q}^l,\mathbf{V}^l,R^l)$.

Assuming $\mathbf{Q}$ and $\mathbf{V}$ are the optimal solutions to problem (24), $\mathbf{S}_s$ and $\mathbf{S}_m$ can be optimized by fixing $\mathbf{Q}$ and $\mathbf{V}$ as follows:

$$\begin{aligned}\max_{\mathbf{S}_s,\mathbf{S}_m,R,\lambda_m,\mu_m}\quad & R\\ s.t.\quad & (21),\mathbf{S}_s\succeq\mathbf{0},\mathbf{S}_m\succeq\mathbf{0}.\end{aligned} \quad (25)$$

We summarize the AO algorithm in algorithm 1. Subproblem (24) and (25) can be efficiently solved by using CVX tool box [22]. It is notable that the optimal solutions generated at the $l-1$st iteration are also the feasible values at the lth iteration. For this reason, the proposed AO algorithm generates a nondecreasing sequence of the secrecy rate. In addition, the smaller tolerance ε is, the more iterative steps are need. Hence, the time of solving the proposed algorithm can be roughly estimated as the time of solving the two subproblems multiplies the number of iterations.

C. Robust SRM Problem under FCU

In this subsection, we consider to investigate the robust secrecy rate maximization based on the FCU model. The proposed method used to solve the problems of the PCU model can be employed to the FCU model. Since $\mathbf{e}_d=\mathrm{vec}(\triangle\mathbf{E}_d)$, the distribution of $\mathbf{e}_d$ is $\mathbf{e}_d\sim\mathcal{CN}(0,\mathbf{U}_d)$. With a standard complex Gaussian random vector $\mathbf{z}_d$, we have

$$\mathbf{e}_d=\mathbf{U}_d^{\frac{1}{2}}\mathbf{v}_d, \quad (26)$$

where $\mathbf{v}_d\sim\mathcal{CN}(0,\mathbf{I}_{N_t\times N_d})$. By substituting the channel errors (15) and (26) into (14), the secrecy outage constraint under FCU model can be expressed as

$$\Pr\Bigg\{\begin{bmatrix}\mathbf{v}_d^H & \mathbf{v}_m^H\end{bmatrix}\begin{bmatrix}\mathbf{U}_d^{\frac{1}{2}}\boldsymbol{\varpi}_d\mathbf{U}_d^{\frac{1}{2}} & \mathbf{0}\\ \mathbf{0} & \mathbf{C}_m^{\frac{1}{2}}\mathbf{\Psi}_m\mathbf{C}_m^{\frac{1}{2}}\end{bmatrix}\begin{bmatrix}\mathbf{v}_d^H & \mathbf{v}_m^H\end{bmatrix}^H$$
$$+2\Re\left(\begin{bmatrix}\mathbf{v}_d^H & \mathbf{v}_m^H\end{bmatrix}\begin{bmatrix}\mathbf{U}_d^{\frac{1}{2}}\boldsymbol{\varpi}_d & \mathbf{0}\\ \mathbf{0} & \mathbf{C}_m^{\frac{1}{2}}\mathbf{\Psi}_m\end{bmatrix}\begin{bmatrix}\widehat{\mathbf{h}}_d^H & \widehat{\mathbf{h}}_m^H\end{bmatrix}^H\right)$$
$$+\begin{bmatrix}\widehat{\mathbf{h}}_d^H & \widehat{\mathbf{h}}_m^H\end{bmatrix}\begin{bmatrix}\boldsymbol{\varpi}_d & \mathbf{0}\\ \mathbf{0} & \mathbf{\Psi}_m\end{bmatrix}\begin{bmatrix}\widehat{\mathbf{h}}_d^H & \widehat{\mathbf{h}}_m^H\end{bmatrix}^H-c_m\le0\Bigg\}\ge1-\rho, \quad (27)$$

where $\widehat{\mathbf{h}}_d=\mathrm{vec}(\widehat{\mathbf{H}}_d)$, $\boldsymbol{\varpi}_d=\mathbf{S}_d^T\otimes\mathbf{V}-\mathbf{I}_{N_t}\otimes(\mathbf{Q}+\mathbf{V})$, $\mathbf{\Psi}_m=\mathbf{S}_m^T\otimes(\mathbf{Q}+\mathbf{V})-\mathbf{I}_{N_t}\otimes\mathbf{V}$ and $c_m=-\mathrm{Tr}(\mathbf{S}_s)+\ln|\mathbf{S}_d|+N_d-\mathrm{Tr}(\mathbf{S}_m)+\ln|\mathbf{S}_m|-N_e-R$. In order to involve Lemma 2 to transform secrecy outage constraint (27) into more tractable form, we set

$$\begin{cases}\mathbf{v}_{d,m}=\begin{bmatrix}\mathbf{v}_d^H & \mathbf{v}_m^H\end{bmatrix}^H\\ \mathbf{A}_{d,m}=\begin{bmatrix}\mathbf{U}_d^{\frac{1}{2}}\boldsymbol{\varpi}_d\mathbf{U}_d^{\frac{1}{2}} & \mathbf{0}\\ \mathbf{0} & \mathbf{C}_m^{\frac{1}{2}}\mathbf{\Psi}_m\mathbf{C}_m^{\frac{1}{2}}\end{bmatrix}\\ \mathbf{B}_{d,m}=\begin{bmatrix}\mathbf{U}_d^{\frac{1}{2}}\boldsymbol{\varpi}_d & \mathbf{0}\\ \mathbf{0} & \mathbf{C}_m^{\frac{1}{2}}\mathbf{\Psi}_m\end{bmatrix}\begin{bmatrix}\widehat{\mathbf{h}}_d^H & \widehat{\mathbf{h}}_m^H\end{bmatrix}^H\\ \sigma_{d,m}=\begin{bmatrix}\widehat{\mathbf{h}}_d^H & \widehat{\mathbf{h}}_m^H\end{bmatrix}\begin{bmatrix}\boldsymbol{\varpi}_d & \mathbf{0}\\ \mathbf{0} & \mathbf{\Psi}_m\end{bmatrix}\begin{bmatrix}\widehat{\mathbf{h}}_d^H & \widehat{\mathbf{h}}_m^H\end{bmatrix}^H-c_m\end{cases}$$

to simplify (27) as

$$\Pr\{\mathbf{v}_{d,m}^H\mathbf{A}_{d,m}\mathbf{v}_{d,m}+2\Re(\mathbf{v}_{d,m}^H\mathbf{B}_{d,m})+\sigma_{d,m}\leq 0\}\geq 1-\rho, \quad (28)$$

which has the similar form with (19). By applying Lemma 2, the secrecy outage constraint (27) can be equivalently represented by the following three inequalities

$$\begin{cases} \mathrm{Tr}(\mathbf{A}_{d,m})+\sqrt{-2\ln(\rho)}\theta_{d,m}-\ln(\rho)\delta_{d,m}+\sigma_{d,m}\leq 0, \\ \left\|\begin{bmatrix}\mathrm{vec}(\mathbf{A}_{d,m})\\ \sqrt{2}\mathbf{B}_{d,m}\end{bmatrix}\right\|\leq\theta_{d,m}, \\ \delta_{d,m}\mathbf{I}_{N_t\times N_e}-\mathbf{A}_{d,m}\succeq\mathbf{0}, \quad \delta_{d,m}\geq 0. \end{cases} \quad (29)$$

The harvested energy and interference outage constraints based on FCU model are same as that of PCU model. Hence, the OC-SRM problem based on FCU is reformulated by

$$\begin{aligned} &\max_{\mathbf{Q},\mathbf{V},\mathbf{S}_d,\mathbf{S}_m,R,\delta_{d,m},\theta_{d,m},\alpha_m,\beta_m,\nu_k,\omega_k} \quad R \\ &\quad s.t. \quad (22),(23),(29),(7e). \end{aligned} \quad (30)$$

After replacing the outage constraints (7b)-(7d) with their tractable deterministic constraints (29), (22) and (23), the approximated optimization problem based on FCU model is still nonconvex w.r.t. all the variables jointly. With the similar AO algorithm proposed in PCU model, problem (30) first can be solved by CVX tool box [22] based on the fixed $\mathbf{S}_s$ and $\mathbf{S}_m$ to obtain the optimal $\mathbf{Q}^*$ and $\mathbf{V}^*$. Then, we set $\mathbf{Q}=\mathbf{Q}^*$ and $\mathbf{V}=\mathbf{V}^*$ to optimize the following problem to obtain the optimal $\mathbf{S}_s^*$ and $\mathbf{S}_m^*$,

$$\begin{aligned} &\max_{\mathbf{S}_d,\mathbf{S}_m,R,\delta_{d,m},\theta_{d,m}} \quad R \\ &\quad s.t. \quad (29),\mathbf{S}_d\succeq\mathbf{0},\mathbf{S}_m\succeq\mathbf{0}. \end{aligned} \quad (31)$$

Since the AO algorithm of the FCU model and that of the PCU model are similar, as shown in Algorithm 1, we omit the summary of the AO algorithm of the FCU model, which generates a nondecreasing sequence of the secrecy rate.

IV. Numerical Results

In this section, we provide numerical results to illustrate the secrecy performance of the proposed algorithm based on the two channel uncertainty models in a MIMO-CR system. To accomplish the simulation, we consider the following parameter settings: $N_t=6$, $N_d=N_e=N_p=2$, EH receiver $M=2$, PU receiver $K=2$, outage probability $\rho_s=\rho_m=\rho_k=\rho,\forall_m,\forall_k$,harvested energy target $\eta_m=-4dB,\forall_m$, energy conversion efficiency $\xi_m=0.8,\forall_m$, accuracy tolerance of the proposed algorithm $\varepsilon=0.001,\mathbf{C}_m=\mathbf{D}_k=\mathbf{U}_d=\sigma^2\mathbf{I},\forall_m,\forall_k$; the distribution of all randomly generated channels satisfies $\mathcal{CN}(0,1)$. Over 500 estimated channel realizations are randomly generated to achieve the average accurate results. The remain parameters are specifically given in each figure.

We compare the proposed design against the worst case design method and non-robust method. In order to have a fair comparison between the proposed design method and the worst case design method, the error bound used in the worst case design can be expressed by $\varepsilon=\sqrt{\frac{\sigma^2F_{2M}^{-1}(1-\rho)}{2}}$ based on the theory in [9]-[11], where $F_{2M}^{-1}(\cdot)$ denotes the inverse cumulative distribution function (CDF) of the Chi-square distribution with $2M$ degrees of freedom.

Fig. 1 represents the secrecy rate performance of the various schemes versus the transmit power with the different outage tolerance ρ of 1% and 10%. The secrecy rates of all methods increase with the increase of the transmit power. Moreover, Fig.1 indicates that there is remarkable enhancement in the system secrecy rate using the proposed Berntein-type method compared with those methods of the worst-case and the non-robust. The non-robust method performs the worst, due to its inconsideration of the channel uncertainties. The secrecy rate of the stricter outage tolerance ($\rho=0.01$) is higher than that of the relaxed outage tolerance ($\rho=0.1$). Fig. 2 shows the secrecy rate performance of the three methods versus different error variance σ^2 based on the PCU model. The secrecy rates of all methods decrease along with the increase of the error variance. It can be observed that the proposed design method has the higher secrecy rate than other two methods. Also, the performance gap between the proposed design method and the worst-case method as well as the non-robust method becomes larger when the error variance σ^2 is bigger. Moreover, this figure indicates that when the interference power tolerance of primary user is increased from $I=-2(dB)$ to $I=5(dB)$, all design methods can lead to high secrecy rate. The results in Fig. 3 indicate that the secrecy rate levels of all design methods increase as the transmit power becomes large, meanwhile the proposed Berntein-type method is also better than other two methods based on the PCU model. The performance gap between the perfect CSI method and the proposed method based on the PCU model (see Fig. 1) is larger than the two methods based on the FCU model (see Fig. 3) under the same simulation setting. This is because that system needs more power to overcome channel estimation and quantization errors for all channels. The results in Fig. 4 indicate that the degradation trend of the secrecy rate of all methods based on the FCU model is similar with that of the PCU model. The proposed Berntein-type method based on the FCU model also outperforms the other two methods under any interference power tolerance.

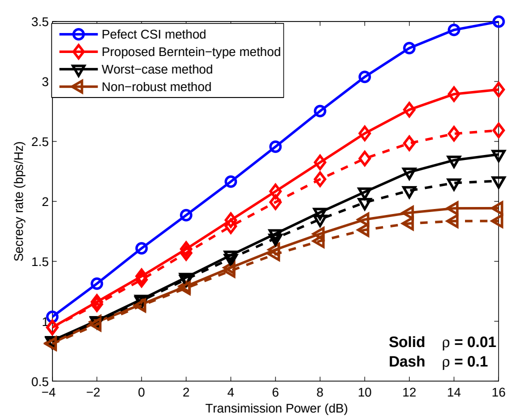

Fig. 1. The secrecy rate of the different methods versus the transmit power for different outage probability ρ based on the PCU model with $I=-2dB,\sigma^2=0.005$.

V. Conclusion

This paper investigates an outage-constrained secrecy rate maximization (OC-SRM) problem for a MIMO-CR downlink network with SWIPT based on the two channel uncertainty models. In order to handle this non-convex problem, we resort a safe approximation method to deal with the log det function and employ Berntein-type inequality approach to convert the outage constraints into the deterministic forms. After the

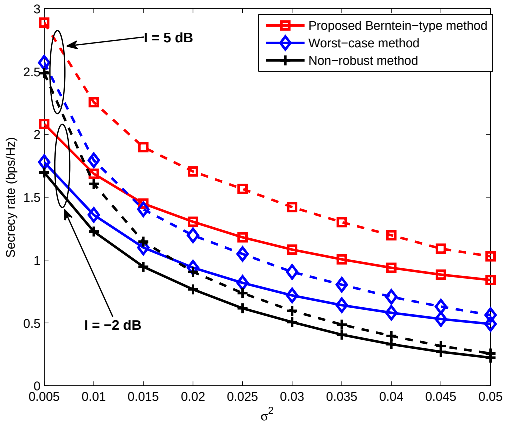

Fig. 2. The secrecy rate versus error variance σ^2 for the different interference power based on the PCU model with $\rho = 0.01,\ P = 6dB$.

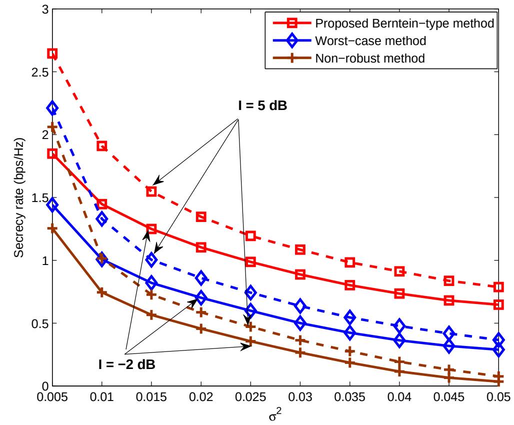

Fig. 4. The secrecy rate versus error variance σ^2 for the different interference power based on the FCU model with $\rho = 0.01,\ P = 6dB$.

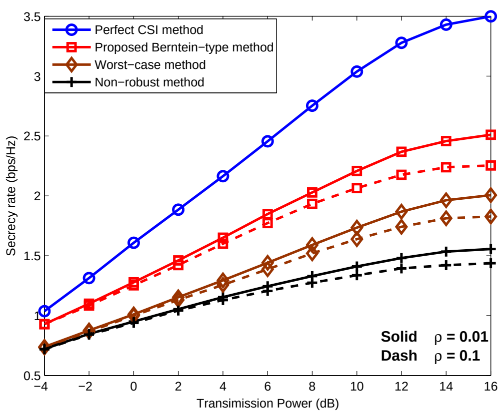

Fig. 3. The secrecy rate of the different methods versus the transmit power for different outage probability ρ based on the FCU model with $I = -2dB, \sigma^2 = 0.005$.

conservative approximation, the original problem has been transformed to a tractable problem, which can be computed alternately by solving two convex subproblems. Simulation results show that the proposed safe design scheme outperforms worst-case scheme and non-robust scheme.

REFERENCES

[1] Y.-C. Liang, K.-C. Chen, G. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Trans. Veh. Technol.*, vol. 60, no. 7, pp. 3386-3407, Sep. 2011.

[2] I. Krikidis et al., "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Commun. Mag.*, vol. 52, no.11, pp. 104-110, Nov. 2014.

[3] B. Fang, Z. Qian, W. Zhong, and W. Shao, "AN-Aided Secrecy Precoding for SWIPT in Cognitive MIMO Broadcast Channels," *IEEE Commun. Lett.*, vol. 19, no. 9, pp. 1632-1635, Sep 2015.

[4] D. W. K. Ng, E. S. Lo, and R. Schober, "Multi-objective resource allocation for secure communication in cognitive radio networks with wireless information and power transfer," *IEEE Trans. Veh, Technol.*, vol. 65, no. 5, pp. 3166-3184, May 2016.

[5] J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, and H. Zhu, "Large system secrecy rate analysis for SWIPT MIMO wiretap channels," *IEEE Trans. Inf. Forensics and Secur.*, vol. 11, no. 1, pp. 74-85, Jan. 2016.

[6] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with MISO beamforming," *IEEE Trans. Signal Process.*, vol. 62, no. 7, pp. 1850-1863, Apr. 2014.

[7] S. Wang and B. Wang, "Robust Secure Transmit Design in MIMO Channels with Simultaneous Wireless Information and Power Transfer," *IEEE signal Processing Letters*, vol. 22, no. 11, pp. 2147-2151, Nov. 2015.

[8] M. R. A. Khandaker, K.-K. Wong, Y. Y. Zhang and Z. B. Zheng, "Probabilistically Robust SWIPT for Secrecy MISOME Systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 211-226, Jan. 2017.

[9] 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, 2013.

[10] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multi-antenna eavesdroppers, *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283-297, Jan. 2016.

[11] 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. 2014.

[12] J. Jose, N. Prasad, M. Khojastepour, and S. Rangarajan, "On robust weighted-sum rate maximization in MIMO interference networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 1C6, Kyoto, Japan, Jun. 5C9, 2011.

[13] S. Verdú, "Spectral efficiency in the wideband regime," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1319-1343, Jun. 2002.

[14] J. H. Wang and D. P. Palomar, "Worst-Case Robust MIMO Transmission With Imperfect Channel Knowledge," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3086-3100, April. 2009.

[15] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a MIMO secrecy channel with a multiple-antenna eavesdropper," *IEEE Trans. Veh, Technol.*, vol. 63, no.4, pp,1678–1690, May 2014.

[16] E. Boshkovska, D. W. K. Ng, N. Zlatanov and R. Schober, "Practical Non-Linear Energy Harvesting Model and Resource Allocation for SWIPT Systems," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2082-2085, Dec. 2015.

[17] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4-5, pp. 355-580, 2008.

[18] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359-368, Feb 2012.

[19] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725-1729, June 2011.

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

[21] I. Bechar, "A Bernstein-type inequality for stochastic processs of quadratic forms of Gaussian variables," 2009 [Online]. Available: http://arxiv.org/abs/0909.3595

[22] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 1.21. Apr. 2011 [Online]. Available: http://cvxr.com/cvx/