Enhancing PHY Security of Cooperative Cognitive Radio Multicast Communications

Van-Dinh Nguyen, *Student Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, Oh-Soon Shin, *Member, IEEE*, Arumugam Nallanathan, *Fellow, IEEE*, and George K. Karagiannidis, *Fellow, IEEE*

***Abstract*—In this paper, we propose a cooperative approach to improve the security of both primary and secondary systems in cognitive radio multicast communications. During their access to the frequency spectrum licensed to the primary users, the secondary unlicensed users assist the primary system in fortifying security by sending a jamming noise to the eavesdroppers, while simultaneously protect themselves from eavesdropping. The main objective of this paper is to maximize the secrecy rate of the secondary system, while adhering to all individual primary users' secrecy rate constraints. In the case of active eavesdroppers and perfect channel state information (CSI) at the transceivers, the utility function of interest is nonconcave and the involved constraints are nonconvex, and thus, the optimal solutions are troublesome. To solve this problem, we propose an iterative algorithm to arrive at least to a local optimum of the original nonconvex problem. This algorithm is guaranteed to achieve a Karush–Kuhn–Tucker solution. Then, we extend the optimization approach to the case of passive eavesdroppers and imperfect CSI knowledge at the transceivers, where the constraints are transformed into a linear matrix inequality and convex constraints, in order to facilitate the optimal solution.**

***Index Terms*—Cognitive radio, convex optimization, interference, jamming noise, secrecy capacity, multicast transmission.**

Manuscript received January 21, 2017; revised July 7, 2017; accepted August 23, 2017. Date of publication September 1, 2017; date of current version December 22, 2017. This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No. NRF-2017R1A5A1015596), in part by Basic Science Research Program through the NRF funded by the Ministry of Education (No. 2017R1D1A1B03030436), and in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415/14/22 and by the U.K. Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/P019374/1. Part of this work was presented at the 2017 IEEE International Conference on Communications (ICC) [1]. The associate editor coordinating the review of this paper and approving it for publication was K. P. Subbalakshmi. *(Corresponding author: Oh-Soon Shin.)*

V.-D. Nguyen and O.-S. Shin are with the School of Electronic Engineering and the Department of ICMC Convergence Technology, Soongsil University, Seoul 06978, South Korea (e-mail: nguyenvandinh@ssu.ac.kr; osshin@ssu.ac.kr).

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, U.K. (e-mail: trung.q.duong@qub.ac.uk).

A. Nallanathan is with School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: nallanathan@ieee.org).

G. K. Karagiannidis is with the Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, 54 124 Thessaloniki, Greece (e-mail: geokarag@auth.gr).

Digital Object Identifier 10.1109/TCCN.2017.2748132

I. Introduction

TRADITIONALLY, a secrecy mechanism is applied at the higher layers of a communication system by using a secret key exchange between the source and the destination, such as the Diffie-Hellman key exchange [2]. However, the execution of key exchange algorithms over wireless networks may be vulnerable to eavesdropping attacks, due to the broadcasting nature of the wireless transmission media. As a result, research in information theory for wireless communication systems has focused on achieving secrecy, by using channel coding and signal processing techniques at the physical layer (PHY) [3], [4]. Specifically, the pioneering work [3] introduced PHY security via wiretap channels, by providing perfect secrecy that can be attained when the eavesdropper channel is a degraded version of the main source-to-destination channel.

Recently, PHY security for wireless communications has become an important research area. The underlying idea is to guarantee a positive secrecy rate of legitimate users by exploiting the random characteristics of wireless channel. In particular, Gopala *et al.* [5] proposed a low-complexity on/off power allocation strategy to attain secrecy under the assumption of full channel state information (CSI). The use of cooperative jamming noise (JN) was proposed in [6], where users who are prevented from transmitting according to a certain policy block the eavesdropper and thereby assist the remaining users. Anand and Chandramouli [7] analyzed the optimal location of an eavesdropper which results in zero secrecy capacity of all links, where the location is defined logically in terms of channel gains. From a quality-of-service (QoS) perspective, a secret transmit beamforming approach was considered in [8]–[10], in order to predetermine the signal-to-interference-plus-noise-ratio (SINR) target at the destination and/or at the eavesdropper. More recently, a jamming noise technique (a.k.a. artificial noise) was introduced, in order to improve the secrecy capacity by confusing the decoding capability of the eavesdroppers [11]–[17]. Furthermore, in [18], a new secure transmission was proposed in order to sustain the secrecy of the communication, by utilizing the available power to produce artificial noise for the eavesdropper. Zhou and McKay [19] considered the case of a passive eavesdropper with multi-antenna transmission, where the transmitter simultaneously transmits an information-bearing signal to the intended receiver and artificial noise to the eavesdropper. A joint information and jamming beamforming technique for a

full-duplex base station (BS) which secures both uplink and downlink transmission, was proposed in [20]. Finally, cooperation between the source and destination was proposed in [21], with the destination operating in the full-duplex mode, i.e., the destination receives information from the source and sends a jamming signal to the eavesdropper at the same time.

Being a critical issue, PHY security of cognitive radio networks (CRNs), which deal with specific security risks due to the broadcasting nature of radio signals, has not been well investigated until recently, e.g., [22]–[29]. More specifically, in [22]–[24], multi-antennas at the secondary transmitter were utilized to attain beamforming that maximizes the secrecy capacity of the secondary system, while adhering to the peak interference constraint at the primary receiver. In [25], cooperation between the secondary system and the primary system was proposed, in order to improve the secrecy capacity of the primary system. Furthermore, a simple case with single antenna at the eavesdropper was considered in [26] and [27]. Particularly, in [26], joint beamforming for information and jamming noise was proposed to protect both primary and secondary systems, with the secondary user acting as an amplify-and-forward relay to enhance the security of the primary system. A jamming beamforming technique was designed in [27], based on the nullspace of the legitimate channel, in order to protect the primary system by treating the signal from the secondary transmitter as interference. Zhu and Yao [28] considered a CRN model, where both primary user (PU) and secondary user (SU) send their confidential messages to intended receivers that are surrounded by a single eavesdropper. Besides, the capacity-equivocation region of cognitive interference channel was obtained in [30], where the primary receiver is treated as untrusted user (eavesdropper) who intends to eavesdrop the confidential message of the secondary system. Extensions of [30] were made in [31] and [32] by additionally considering the secrecy of the primary system.

In this paper, we consider the PHY security in cooperative cognitive radio multicast communications, where the eavesdroppers intend to wiretap data from both primary and secondary systems. We assume that the primary transmitter is equipped only with a single antenna, which implies that the primary transmitter cannot generate a jamming signal or design a beamforming vector to protect itself from the eavesdroppers. The secrecy capacity of the primary system is improved by implementing a cooperative framework between the primary and secondary systems. Specifically, the primary system allows the secondary system to share its spectrum, and in return the secondary system sends jamming noise to degrade the eavesdropper's channel, in order to protect the primary system. In the CRN multicast transmission model, we assume that there are one group of PUs and G groups of SUs, where all users in each group receives identical information from its transmitter, and furthermore, each group can be surrounded by multiple eavesdroppers. We note that the recent work in [28] is a special case of this paper, where only a single receiver and a single eavesdropper are assumed, which is well-known as unicast mode.

The aim of this paper is to design the optimal beamforming vectors that realize the PHY security and maximize the secrecy rate of the secondary system, while ensuring adherence to the individual secrecy rate constraints at each primary user. Specifically, the main contributions of this paper can be summarized as follows:

- For the perfect CSI case, we design a joint information and jamming signal at the secondary transmitter, where information is intended for secondary receivers and jamming noise is intended for eavesdroppers. The main objective is to maximize the secrecy rate of the secondary system, while satisfying the minimum secrecy rate requirement for each legitimate user of the primary system as well as the power constraint. We show that the equivalent problem can be converted to a single-layer optimization problem, which can be easily solved through convex quadratic programming.
- When the CSI of the channel from the secondary transmitter to the PUs is imperfect and only partial CSI of the eavesdroppers is available, we transform the non-linear constraints into a linear matrix inequality and convex constraints, based on a specific matrix inequality lemma. We show that the approximate optimization problem can be efficiently solved in a similar manner as the perfect CSI case.
- We propose an efficient method to find the approximate solution for optimal transmit beamforming, by providing the convexity of the original problem that is considered through the use of a convex approximation. The optimal solutions of transmit beamforming for the confidential information and jamming noise do not fix the transmit strategy. Importantly, we develop an iterative algorithm of low complexity for the computational solution of the considered optimization problem. The obtained solutions are proved to be at least local optimum, as satisfying the necessary optimal conditions.
- We provide extensive numerical results to justify the novelty of the proposed algorithm and compare its performance with the known solutions. In particular, the numerical results demonstrate fast convergence of the proposed algorithm and a significant improvement of the secrecy rate, compared with other known solutions. We should remark that our results are more general than in [28], which was considered under the assumptions of one eavesdropper and perfect CSI. In addition, the model in this paper is of practical interest in designing networks that are required to transmit the same data to a group of users, for example, in video broadcasting and various applications. Moreover, the considered problem in this paper is highly nonlinear and nonconvex function, thus it is more challenging to solve compared to SINR-based design in [28].

The rest of this paper is organized as follows. Section II describes the CRN multicast transmission model with multiple eavesdroppers and formulates the optimization problem. Section III derives optimal beamforming for information signal and jamming noise at the secondary transmitter under the assumption of perfect CSI, while Section IV extends the considered problem to the case of imperfect CSI and passive eavesdropper. Section V provides numerical results and discussions. Finally, the conclusions are drawn in Section VI. In order to make the rest of the paper easy to follow, the notations and symbols used in the paper are specified in Table I.

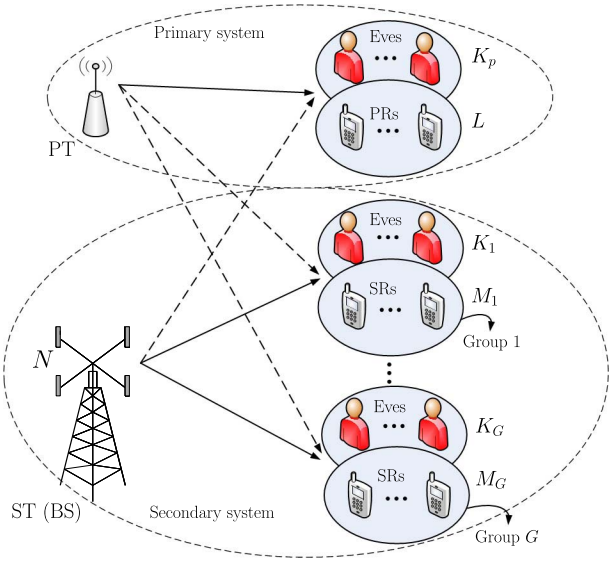


Fig. 1. A cooperative CRN multicast transmission model with multiple eavesdroppers.

TABLE I
NOTATIONS AND SYMBOLS

$\mathbf{X}^H$, $\mathbf{X}^T$ and $\mathrm{tr}(\mathbf{X})$	Hermitian transpose, normal transpose and trace of a matrix $\mathbf{X}$
$\|\cdot\|$ and $\|\cdot\|$	Euclidean norm of a matrix or vector and the magnitude of a complex scalar
$\mathbf{I}_N$	$N \times N$ identity matrix
$\mathbf{x} \sim \mathcal{CN}(\boldsymbol{\eta}, \boldsymbol{Z})$	Random vector following a complex circular Gaussian distribution with mean $\boldsymbol{\eta}$ and covariance matrix $\boldsymbol{Z}$
$\mathbb{E}[\cdot]$	Statistical expectation
$\mathbf{X} \succeq \mathbf{0}$	Positive semidefinite matrix
$\Re\{\cdot\}$	Real part of the argument
$\mathbf{h}_{m_g}$ and $\mathbf{f}_l$	Channels from ST to m_g-th SR and l-th PR
$\mathbf{g}_{k_g}$ and $\mathbf{f}_{k_p}$	Channels from ST to k_g-th Eve and k_p-th Eve
h_l and f_{m_g}	Channels from PT to l-th PR and m_g-th SR
g_{k_p} and f_{k_g}	Channels from PT to k_p-th Eve and k_g-th Eve
$\mathbf{w}_g$	Beamforming vector at ST intended to group $\mathcal{G}_g$
$\mathbf{u}$	Artificial noise vector with $\mathbf{u} \sim \mathcal{CN}(\mathbf{0}, \mathbf{U}\mathbf{U}^H)$
t_g	Maximum allowable rate for k_g-th Eve
z	Maximum allowable rate for k_p-th Eve
φ	Objective variable in maximizing secrecy rate of secondary system
α	Minimum SINR requirement for l-th PR
ϕ_g	Maximum received SINR for k_g-th Eve
β	Maximum received SINR for k_p-th Eve

II. System Model and Optimization Problem

A. System Model

We consider the PHY security of CRN multicast transmission with cooperation between a primary system and a secondary system. The primary system consists of one primary transmitter (PT) and L primary receivers (PRs), while the secondary system consists of one secondary transmitter (ST) and M secondary receivers (SRs), as illustrated in Fig. 1. The ST, which is a BS, is equipped with N antennas, whereas all other nodes are equipped with only one antenna.[1] The opportunistic spectrum access is improved by assigning the ST to send G information bearing signals $s_g, g = 1, \ldots, G$, where s_g is the information being sent to the g-th group with unit average power $\mathbb{E}\{|s_g|^2\} = 1$. We assume that each individual multicast group $\mathcal{G}_g$ in the secondary system consists of M_g secondary receivers. Specifically, the number of SRs in group $\mathcal{G}_g$ is denoted by $\mathcal{S}_g = \{1, \ldots, m_g, \ldots, M_g\}$. Then, the total number of SRs in the secondary system with multicast transmission is indeed $M = \sum_{g=1}^{G} M_g$. In the multicast transmission, all users within the same group will receive identical data from its transmitter. Regarding security, we assume that the eavesdroppers (Eves) potentially intend to wiretap and decode confidential messages from both primary and secondary systems [33]. We assume that each group $\mathcal{G}_g$ and the PRs are respectively wiretapped by a set of Eves such as $\mathcal{K}_{e,g} \triangleq \{1, \ldots, k_g, \ldots, K_g\}$, $\forall g$ and $\mathcal{K}_p \triangleq \{1, \ldots, k_p, \ldots, K_p\}$. This implies that at the same time, each legitimate user is wiretapped by a separate group of Eves.

We aim to design multiple beamforming vectors at the ST, one for the JN and the other for its own information signal, to protect both primary and secondary systems. The transmit power at the PT is $P_p > 0$ and the data intended for the PRs is x_p with unit average power $\mathbb{E}\{|x_p|^2\} = 1$. Before transmission, the data of the SRs s_g in the group $\mathcal{G}_g$ is weighted to the $N \times 1$ beamforming vector $\mathbf{w}_g$, $\forall g$. Hence, the transmitted signals at the ST can be expressed through a vector $\mathbf{x}_s$ as

$$\mathbf{x}_s = \sum_{g=1}^{G} \mathbf{w}_g s_g + \mathbf{u} \tag{1}$$

where $\mathbf{u}$ is the artificial noise vector, whose elements are zero-mean complex Gaussian random variables with covariance matrix $\mathbf{U}\mathbf{U}^H$, such that $\mathbf{u} \sim \mathcal{CN}(\mathbf{0}, \mathbf{U}\mathbf{U}^H)$ with $\mathbf{U} \in \mathbb{C}^{N \times N}$. The artificial noise $\mathbf{u}$ is assumed to be unknown to all SRs, PRs, and Eves. For notational simplicity, we define $\mathbf{w} \triangleq [\mathbf{w}_1^T, \mathbf{w}_2^T, \ldots, \mathbf{w}_G^T]^T \in \mathbb{C}^{NG \times 1}$.

The corresponding SINR at the l-th PR for $l = 1, \ldots, L$ and the k_p-th Eve for $k_p = 1, \ldots, K_p$ are respectively given by

$$\Gamma_{p,l}(\mathbf{w}, \mathbf{U}) = \frac{P_p |h_l|^2}{\sum_{g=1}^{G} \left|\mathbf{f}_l^H \mathbf{w}_g\right|^2 + \left\|\mathbf{f}_l^H \mathbf{U}\right\|^2 + \sigma_l^2}, \tag{2}$$

$$\Gamma_{e,k_p}(\mathbf{w}, \mathbf{U}) = \frac{P_p \left|g_{k_p}\right|^2}{\sum_{g=1}^{G} \left|\mathbf{f}_{k_p}^H \mathbf{w}_g\right|^2 + \left\|\mathbf{f}_{k_p}^H \mathbf{U}\right\|^2 + \sigma_{k_p}^2} \tag{3}$$

where $h_l \in \mathbb{C}$, $g_{k_p} \in \mathbb{C}$, $\mathbf{f}_l \in \mathbb{C}^{N \times 1}$, and $\mathbf{f}_{k_p} \in \mathbb{C}^{N \times 1}$ are the respective baseband equivalent channels of the links PT $\rightarrow$ l-th PR, PT $\rightarrow$ k_p-th Eve, ST $\rightarrow$ l-th PR, and ST $\rightarrow$ k_p-th Eve. σ_l^2 and $\sigma_{k_p}^2$ are the variance of the additive white Gaussian noise (AWGN) at the l-th PR and k_p-th Eve, respectively.

The respective SINR at the m_g-th SR in the group $\mathcal{G}_g$ and the k_g-th Eve are given by

$$\Gamma_{s,m_g}(\mathbf{w}, \mathbf{U}) = \frac{\left|\mathbf{h}_{m_g}^H \mathbf{w}_g\right|^2}{\sum_{i=1, i \neq g}^{G} \left|\mathbf{h}_{m_g}^H \mathbf{w}_i\right|^2 + \left\|\mathbf{h}_{m_g}^H \mathbf{U}\right\|^2 + P_p \left|f_{m_g}\right|^2 + \sigma_{m_g}^2}, \tag{4}$$

$$\Gamma_{e,k_g}(\mathbf{w}, \mathbf{U}) = \frac{\left|\mathbf{g}_{k_g}^H \mathbf{w}_g\right|^2}{\sum_{i=1, i \neq g}^{G} \left|\mathbf{g}_{k_g}^H \mathbf{w}_i\right|^2 + \left\|\mathbf{g}_{k_g}^H \mathbf{U}\right\|^2 + P_p \left|f_{k_g}\right|^2 + \sigma_{k_g}^2} \tag{5}$$

[1] We note that the solution for multiple antennas at the PT is straightforward by following the same procedure presented in this paper since the resource allocation strategies at the ST and PT are independent.

where $\mathbf{h}_{m_g} \in \mathbb{C}^{N\times 1}$, $\mathbf{g}_{k_g} \in \mathbb{C}^{N\times 1}$, $f_{m_g} \in \mathbb{C}$, and $f_{k_g} \in \mathbb{C}$ are the corresponding baseband equivalent channels of the links ST $\rightarrow m_g$-th SR, ST $\rightarrow k_g$-th Eve, PT $\rightarrow m_g$-th SR, PT $\rightarrow k_g$-th Eve. $\sigma^2_{m_g}$ and $\sigma^2_{k_g}$ are the variance of AWGN at the m_g-th PR and k_g-th Eve, respectively. We further assume that all channels remain constant during a transmission block, yet change independently from one block to another. By using dirty-paper coding (DPC), the ST with encoding order from the group $\mathcal{G}_1$ to $\mathcal{G}_G$ enables the SRs in $\mathcal{S}_g$ to know the information signals intended for the SRs in $\mathcal{S}_{g'}, g' = 1, \ldots, g-1$ non-casually, so that it can be perfectly eliminated [34]. Hence, the SINR in (4) by DPC can be rewritten as

$$\Gamma^{\mathrm{DPC}}_{s,m_g}(\mathbf{w},\mathbf{U}) = \frac{\left|\mathbf{h}^H_{m_g}\mathbf{w}_g\right|^2}{\sum_{i>g}\left|\mathbf{h}^H_{m_g}\mathbf{w}_i\right|^2 + \left\|\mathbf{h}^H_{m_g}\mathbf{U}\right\|^2 + P_p\left|f_{m_g}\right|^2 + \sigma^2_{m_g}}.$$

It is clear that under the same beamformer/precoder $(\mathbf{w},\mathbf{U})$, $\Gamma^{\mathrm{DPC}}_{s,m_g}(\mathbf{w},\mathbf{U})$ is better than $\Gamma_{s,m_g}(\mathbf{w},\mathbf{U})$. However, DPC may be difficult to implement in practice due to its high computational complexity, and thus, we do not pursue it in this paper.

The channel of each legitimate user together with the respective Eves form a compound wiretap channel [35]. Therefore, the achievable secrecy rate for the l-th PR of the primary system, denoted by $C_{p,l}(\mathbf{w},\mathbf{U})$, can be expressed as [35], [36]

$$C_{p,l}(\mathbf{w},\mathbf{U}) = \left[\log_2\left(1+\Gamma_{p,l}(\mathbf{w},\mathbf{U})\right) - \max_{k_p\in\mathcal{K}_p}\log_2\left(1+\Gamma_{e,k_p}(\mathbf{w},\mathbf{U})\right)\right]^+ \quad (6)$$

where $[x]^+ = \max\{0,x\}$.

Similarly, the achievable secrecy rate for the m_g-th SR of the secondary system, denoted by $C_{s,m_g}(\mathbf{w},\mathbf{U})$, can be expressed as [35], [36]

$$C_{s,m_g}(\mathbf{w},\mathbf{U}) = \left[\log_2\left(1+\Gamma_{s,m_g}(\mathbf{w},\mathbf{U})\right) - \max_{k_g\in\mathcal{K}_{e,g}}\log_2\left(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})\right)\right]^+. \quad (7)$$

If $C_{p,l}(\mathbf{w},\mathbf{U})$ and $C_{s,m_g}(\mathbf{w},\mathbf{U})$ are above zero, the signal transmitted from the PT and ST are determined to be "undecodable" as is indicated in [6].

B. Optimization Problem Formulation

The objective of the system design is to maximize the minimum (max-min) secrecy rate of the secondary system while satisfying the minimum QoS requirements, such as the secrecy rate achievable for the primary system. Accordingly, the optimization problem can be mathematically formulated as

$$\mathbf{P.1}: \max_{\mathbf{w},\mathbf{U}} \min_{m_g\in\mathcal{S}_g, g\in\mathcal{G}} C_{s,m_g}(\mathbf{w},\mathbf{U}) \quad (8a)$$

$$\text{s.t.} \quad C_{p,l}(\mathbf{w},\mathbf{U}) \geq \bar{R}_{p,l},\ l\in\mathcal{L} \quad (8b)$$

$$\sum_{g=1}^{G}\left\|\mathbf{w}_g\right\|^2 + \|\mathbf{U}\|^2 \leq P_s \quad (8c)$$

where $\mathcal{L} \triangleq \{1,\ldots,L\}$ and $\mathcal{G} \triangleq \{1,\ldots,G\}$. In (8b), $\bar{R}_{p,l} > 0$ are the minimum secrecy rate requirement for each legitimate user of the primary system. This implies that the QoS for each PR can be different and flexible. In (8c), P_s is the transmit power budget at the ST.

Remark 1: There are two other performance metrics of interest involved in the considered system. In particular, one is to maximize the secrecy rate of the primary system subject to the secrecy rate threshold of secondary system and the transmit power budget at the ST, while the other is to minimize the total transmit power at the ST subject to the secrecy rate threshold of both systems. However, the optimal solution for (8) is also applicable to those cases that will be presented shortly.

The recent works in [20], [28], [37], and [38] often introduce new variables to relax the optimization problem as

$$\widetilde{\mathbf{W}}_g = \mathbf{w}_g\mathbf{w}_g^H, \forall g \quad (9)$$

which must satisfy the rank-one constraint, i.e., $\mathrm{rank}(\widetilde{\mathbf{W}}_g) = 1, \forall g$. Then, they use semi-definite program (SDP) relaxation to solve the optimization problem by constructing an equivalent problem. In which, the optimal solution involves the dual variables of the relaxed problem. Unfortunately, some numerical solvers may not exhibit the optimal solution of dual variables, and then the construction of primal variables may not be possible. In what follows, we will solve (8) via a convex quadratic program and thus the rank-one constraints are automatically satisfied.

III. Theoretical Benchmark With Perfect CSI

We first consider the case for which the instantaneous CSI of all channels is available at the transceivers. In particular, the CSI of all channels in both systems can be obtained through feedback from the legitimate receivers to the legitimate transmitters. After CSI acquisition, we assume that only M SRs and L PRs are scheduled to be concurrently served. Herein, the remaining users (unscheduled users) are not necessarily malicious, but they could be untrusted users. Thus, the unscheduled users are treated as potential eavesdroppers, but with perfectly known CSI at the transmitters. These assumptions are consistent with several previous works on information theoretic analysis and optimization for the similar kind of problem, [5], [6], [12], [20], [21], for instance.[2]

A. Optimal Solution

We note that finding an optimal solution for (8) is challenging due to the nonconcavity of the objective function and nonconvexity of the feasible set. In this section, we propose an iterative algorithm that arrives a local optimum of the considered optimization problem. As the first step, we convert (8) to another equivalent form as

$$\underset{\mathbf{w},\mathbf{U},\boldsymbol{t},z}{\text{maximize}} \min_{m_g\in\mathcal{S}_g, g\in\mathcal{G}}\left\{\log_2\left(1+\Gamma_{s,m_g}(\mathbf{w},\mathbf{U})\right) - t_g\right\} \quad (10a)$$

[2]Though this assumption is quite ideal, however, the performance with assumption of perfect CSI is still of practical importance since it plays as a benchmark how the CRN system may achieve in more realistic conditions [24], [27]–[29].

$$\text{s.t.} \quad \log_2\big(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})\big) \le t_g,\ k_g \in \mathcal{K}_{e,g}, g \in \mathcal{G} \quad (10b)$$
$$\log_2\big(1+\Gamma_{p,l}(\mathbf{w},\mathbf{U})\big) - z \ge \bar{R}_{p,l},\ l \in \mathcal{L} \quad (10c)$$
$$\log_2\big(1+\Gamma_{e,k_p}(\mathbf{w},\mathbf{U})\big) \le z,\ k_p \in \mathcal{K}_p \quad (10d)$$
$$(8c) \quad (10e)$$

where $\boldsymbol{t} \triangleq \{t_g\}$ and z are the maximum allowable rates for Eves to wiretap the information signals from the ST and the PT, respectively. Even after the above transformations, problem (10) is still nonconvex and difficult to solve due to nonconcavity of the objective function. Toward a tractable form, let us rewrite (10) equivalently as

$$\underset{\mathbf{w},\mathbf{U},\boldsymbol{t},z,\varphi}{\text{maximize}} \quad \varphi \quad (11a)$$
$$\text{s.t.} \quad \log_2\big(1+\Gamma_{s,m_g}(\mathbf{w},\mathbf{U})\big) - t_g \ge \varphi, m_g \in \mathcal{S}_g, g \in \mathcal{G} \quad (11b)$$
$$\log_2\big(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})\big) \le t_g,\ k_g \in \mathcal{K}_{e,g}, g \in \mathcal{G} \quad (11c)$$
$$\log_2\big(1+\Gamma_{p,l}(\mathbf{w},\mathbf{U})\big) - z \ge \bar{R}_{p,l},\ l \in \mathcal{L} \quad (11d)$$
$$\log_2\big(1+\Gamma_{e,k_p}(\mathbf{w},\mathbf{U})\big) \le z,\ k_p \in \mathcal{K}_p \quad (11e)$$
$$(8c) \quad (11f)$$

where φ is newly introduced variable to maximize the secrecy rate of the secondary system. The equivalence between (10) and (11) can be easily confirmed by justifying that the constraints in (11b) must hold with equality at optimum. Observe that the objective function is monotonic in its argument, therefore, we now only deal with the nonconvex constraints (11b)-(11e). Toward this end, we provide the following result.[3]

Lemma 1: For the secondary system, the inner convex approximations of nonconvex constraints (11b) and (11c) are given by:

$$\mathcal{F}_{m_g}^{(n)}(\mathbf{w},\mathbf{U}) \ge (\varphi + t_g)\ln 2, \quad (12)$$
$$\mathcal{F}_{k_g}^{(n)}(\mathbf{w},\mathbf{U}) \le t_g \ln 2 \quad (13)$$

where $\mathcal{F}_{m_g}^{(n)}(\mathbf{w},\mathbf{U})$ and $\mathcal{F}_{k_g}^{(n)}(\mathbf{w},\mathbf{U})$ are a lower bounding concave function for $\log_2(1+\Gamma_{s,m_g}(\mathbf{w},\mathbf{U}))$ and an upper bounding convex function for $\log_2(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U}))$, which are concretized by (57) and (60) in Appendix A, respectively.

Similarly for the primary system, the nonconvex constraints (11d) and (11e) are innerly approximated by the following convex constraints:

$$\mathcal{P}_{l}^{(n)}(\mathbf{w},\mathbf{U}) \ge (z + \bar{R}_{p,l})\ln 2, \quad (14)$$
$$\mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U}) \le z \ln 2 \quad (15)$$

where $\mathcal{P}_{l}^{(n)}(\mathbf{w},\mathbf{U})$ and $\mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U})$ are a lower bounding concave function for $\log_2(1+\Gamma_{p,l}(\mathbf{w},\mathbf{U}))$ and an upper bounding convex function for $\log_2(1+\Gamma_{e,k_p}(\mathbf{w},\mathbf{U}))$, which are also concretized by (64) and (65) in Appendix A, respectively.

Proof: See Appendix A. ∎

It is noteworthy that the following equalities hold at the optimum, i.e., $(\mathbf{w}^{(n+1)},\mathbf{U}^{(n+1)}) = (\mathbf{w}^{(n)},\mathbf{U}^{(n)})$:

$$\mathcal{F}_{m_g}^{(n)}(\mathbf{w}^{(n)},\mathbf{U}^{(n)}) = \log_2\Big(1+\Gamma_{s,m_g}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big), \quad (16)$$

[3]Hereafter, suppose the value of $(\mathbf{w},\mathbf{U})$ at the $(n+1)$-th iteration in an iterative algorithm presented shortly is denoted by $(\mathbf{w}^{(n)},\mathbf{U}^{(n)})$.

Algorithm 1 An Iterative Algorithm to Solve (8)

Initialization: Set $n := 0$ and solve (22) to generate an initial feasible point $\big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\big)$

1: **repeat**
2: Solve (20) to obtain the optimal solution: $\big(\mathbf{w}^*,\mathbf{U}^*\big)$.
3: Update $\mathbf{w}^{(n+1)} := \mathbf{w}^*$ and $\mathbf{U}^{(n+1)} := \mathbf{U}^*$.
4: Set $n := n+1$.
5: **until** Convergence or maximum required number of iterations

$$\mathcal{F}_{k_g}^{(n)}(\mathbf{w}^{(n)},\mathbf{U}^{(n)}) = \log_2\Big(1+\Gamma_{e,k_g}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big), \quad (17)$$
$$\mathcal{P}_{l}^{(n)}(\mathbf{w}^{(n)},\mathbf{U}^{(n)}) = \log_2\Big(1+\Gamma_{p,l}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big), \quad (18)$$
$$\mathcal{P}_{k_p}^{(n)}(\mathbf{w}^{(n)},\mathbf{U}^{(n)}) = \log_2\Big(1+\Gamma_{e,k_p}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big). \quad (19)$$

In summary, at the $(n+1)$-th iteration of the proposed method, we solve the following convex problem

$$\underset{\mathbf{w},\mathbf{U},\boldsymbol{t},z,\varphi}{\text{maximize}} \quad \varphi \quad (20a)$$
$$\text{s.t.} \quad \mathcal{F}_{m_g}^{(n)}(\mathbf{w},\mathbf{U}) \ge (\varphi + t_g)\ln 2,\ m_g \in \mathcal{S}_g, g \in \mathcal{G} \quad (20b)$$
$$\mathcal{F}_{k_g}^{(n)}(\mathbf{w},\mathbf{U}) \le t_g \ln 2,\ k_g \in \mathcal{K}_{e,g}, g \in \mathcal{G} \quad (20c)$$
$$\mathcal{P}_{l}^{(n)}(\mathbf{w},\mathbf{U}) \ge (z + \bar{R}_{p,l})\ln 2,\ l \in \mathcal{L} \quad (20d)$$
$$\mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U}) \le z \ln 2,\ k_p \in \mathcal{K}_p \quad (20e)$$
$$(8c). \quad (20f)$$

An iterative algorithm for solving (20) requires an initial feasible point of (11) to start, i.e., the constraints (11d)-(11f) are satisfied. Therefore, we solve the following nonconvex optimization problem

$$\max_{\mathbf{w},\mathbf{U},z} \ \min_{l\in\mathcal{L}} \ \big\{\log_2\big(1+\Gamma_{p,l}(\mathbf{w},\mathbf{U})\big) - z - \bar{R}_{p,l}\big\} \quad (21a)$$
$$\text{s.t.} \quad \log_2\big(1+\Gamma_{e,k_p}(\mathbf{w},\mathbf{U})\big) \le z,\ k_p \in \mathcal{K}_p \quad (21b)$$
$$(8c). \quad (21c)$$

We first generate a feasible point $(\mathbf{w}^{(0)},\mathbf{U}^{(0)})$ to satisfy (21c) and then solve the following convex approximation problem at the n-th iteration

$$\max_{\mathbf{w},\mathbf{U},z} \ \min_{l\in\mathcal{L}} \ \Big\{\mathcal{P}_{l}^{(n)}(\mathbf{w},\mathbf{U}) - (z + \bar{R}_{p,l})\ln 2\Big\} \quad (22a)$$
$$\text{s.t.} \quad \mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U}) \le z \ln 2,\ k_p \in \mathcal{K}_p \quad (22b)$$
$$(8c) \quad (22c)$$

and output a feasible point of (11) when

$$\min_{l\in\mathcal{L}} \ \Big\{\mathcal{P}_{l}^{(n)}(\mathbf{w},\mathbf{U}) - \big(z + \bar{R}_{p,l}\big)\ln 2\Big\} \ge 0. \quad (23)$$

We numerically observe that it requires no more than 3 iterations to satisfy (23) in all cases. After solving (20), we update $(\mathbf{w}^{(n)},\mathbf{U}^{(n)})$ for the next iteration until convergence or maximum required number of iterations. Algorithm 1 outlines the proposed iterative method for solving (8).

B. Proof of Convergence and Complexity Analysis

The convergence result of Algorithm 1 is stated in the following proposition.

Proposition 1: Algorithm 1 produces a sequence $\{(\mathbf{w}^{(n)}, \mathbf{U}^{(n)})\}$ of improved points of (8), which converges to a Karush-Kuhn-Tucker (KKT) point.

Proof: See Appendix B. ∎

Complexity Analysis: We note that the proposed iterative algorithm requires solving only simple convex quadratic constraints at each iteration. We now provide the complexity analysis of Algorithm 1. Specifically, in each iteration of Algorithm 1, the per-iteration computational complexity of solving (20) is $O(n^2\tilde{n}^{2.5}+\tilde{n}^{3.5})$, where $n = N(G+N)+G+2$ is scalar real variables and $\tilde{n} = \sum_{g=1}^{G}(M_g+K_g)+K_p+L+1$ is quadratic and linear constraints [39].

IV. Optimal Solution With Realistic Scenario

A. CSI Model

In this section, we extend the optimization approach of the last section to a realistic scenario, where the instantaneous CSI between ST and PRs is imperfectly known and Eves are passive devices. Specifically, the primary and secondary systems may not cooperate completely in reality, and therefore the channels $\mathbf{f}_l, \forall l$ will be difficult to obtain perfectly. For instance, the PRs may be inactive for a long period of the secondary data transmission time. Then, the CSI of the PRs can be only obtained at the ST when the PRs is in active mode with the PT. As a result, the CSI of PRs at the ST may be outdated when the secondary system performs the transmit strategy. Hence, the CSI of the link between the ST and PRs is modeled as [11]

$$\begin{aligned} &\mathbf{f}_l = \hat{\mathbf{f}}_l + \Delta\mathbf{f}_l,\ \forall l \\ &\Omega_l \triangleq \left\{\Delta\mathbf{f}_l \in \mathbb{C}^{N\times 1} : \Delta\mathbf{f}_l^H \Delta\mathbf{f}_l \le \delta_l^2\right\} \end{aligned} \tag{24}$$

where $\hat{\mathbf{f}}_l$ is the channel estimate of the l-th PR available at the ST, and $\Delta\mathbf{f}_l$ represents the associated CSI error. In particular, we assume a time division duplex system with slowly time-varying channels. At the beginning of each time slot, the legitimate users (PRs, SRs) report their channel gains to the ST. The downlink CSI of the ST-to-legitimate users are obtained by measuring the uplink pilot based on some estimation methods, such as minimum-mean-square-error (MMSE). However, the detailed method to estimate these CSIs is beyond the scope of this paper. For notational simplicity, we define Ω_l by a set of all possible CSI errors associated with the l-th PR. In addition, we assume that $\Delta\mathbf{f}_l$ are deterministic and bounded, and therefore δ_l represents the size of the uncertainty region of the estimated CSI for the l-th PR.

In addition, a passive Eve does not allow legitimate users to instantaneously obtain its CSI [11], [19], [27], which can be justified as the following two reasons. First, to wiretap the confidential messages from both systems, the eavesdroppers require to become as a part of the communication system, i.e., knowing the channel in the downlink. Second, to wiretap a downlink channel without being removed from the system, an eavesdropper has to protect its visibility from the ST without exposing its CSI, for example, not responding its calls (like a passive user). For the passive Eves, we further assume that the entries of g_{k_p}, $\mathbf{f}_{k_p}$, $\forall k_p$, f_{k_g}, and $\mathbf{g}_{k_g}$, $\forall k_g$, follow independent and identically distributed (i.i.d.) Rayleigh fading, and that the instantaneous CSI of these wiretap channels is not available at ST. These assumptions of passive Eves are commonly used in [11], [17], [19], and [27]. Meanwhile, the channels $\mathbf{h}_{m_g}, \forall m, g$, are assumed to be perfectly known since the SRs are active users in the secondary system.

B. Optimization Problem Formulation

Based on the above setting and similar to (11), the optimization problem **P.1** can be reformulated as

$$\mathbf{P.2}\text{: } \underset{\mathbf{w},\mathbf{U},\boldsymbol{t},z,\varphi}{\text{maximize}} \quad \varphi \tag{25a}$$

$$\text{s.t.} \quad \log_2\big(1+\Gamma_{s,m_g}(\mathbf{w},\mathbf{U})\big) - t_g \ge \varphi, m_g \in \mathcal{S}_g, g \in \mathcal{G} \tag{25b}$$

$$\max_{\mathbf{g}_{k_g}, f_{k_g}} \log_2\big(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})\big) \le t_g, k_g \in \mathcal{K}_{e,g}, g \in \mathcal{G} \tag{25c}$$

$$\min_{\Delta\mathbf{f}_l \in \Omega_l} \log_2\big(1+\Gamma_{p,l}(\mathbf{w},\mathbf{U})\big) - z \ge \bar{R}_{p,l},\ l \in \mathcal{L} \tag{25d}$$

$$\max_{\mathbf{g}_{k_p}, f_{k_p}} \log_2\big(1+\Gamma_{e,k_p}(\mathbf{w},\mathbf{U})\big) \le z,\ k_p \in \mathcal{K}_p \tag{25e}$$

$$(8c) \tag{25f}$$

where $\boldsymbol{t} \triangleq \{t_g\}$ and z are the maximum allowable rates for Eves in decoding the information signals from the ST and the PT, respectively, which were defined in (10); φ is objective variable to maximize the secrecy rate of the secondary system, which was also defined in (11). Observe that (25b) is well presented in (12). It is now clear that the difficulty in solving (25) is due to (25c)-(25e) since the remaining constraints are convex and approximate convex. Instead of this, we can find a sub-optimal solution of (25) as follows

$$\underset{\mathbf{w},\mathbf{U},\boldsymbol{t},z,\varphi,\boldsymbol{\phi},\boldsymbol{\alpha},\beta}{\text{maximize}} \quad \varphi \tag{26a}$$

$$\text{s.t.} \quad \log_2\big(1+\phi_g\big) \le t_g,\ g \in \mathcal{G} \tag{26b}$$

$$\Pr\left(\max_{k_g \in \mathcal{K}_{e,g}} \Gamma_{e,k_g}(\mathbf{w},\mathbf{U}) \le \phi_g\right) \ge \epsilon_g,\ g \in \mathcal{G} \tag{26c}$$

$$\log_2(1+\alpha_l) - z \ge \bar{R}_{p,l},\ l \in \mathcal{L} \tag{26d}$$

$$\min_{\Delta\mathbf{f}_l \in \Omega_l} \Gamma_{p,l}(\mathbf{w},\mathbf{U}) \ge \alpha_l,\ l \in \mathcal{L} \tag{26e}$$

$$\log_2(1+\beta) \le z \tag{26f}$$

$$\Pr\left(\max_{k_p \in \mathcal{K}_p} \Gamma_{e,k_p}(\mathbf{w},\mathbf{U}) \le \beta\right) \ge \tilde{\epsilon} \tag{26g}$$

$$(8c),\ (25b) \tag{26h}$$

where $\boldsymbol{\phi} = \{\phi_g\}$, $\boldsymbol{\alpha} = \{\alpha_l\}$, and β are newly introduced variables. Constraint (26e) is imposed to ensure that for a given CSI error set Ω_l, the minimum received SINR at the l-th PR is larger than or equal to a minimum SINR requirement α_l. According to (26c) and (26g), the probabilities that the maximum received SINR at the k_g-th passive Eve and at the k_p-th passive Eve are less than or equal to $\phi_g > 0$ and $\beta > 0$ are ensured to be greater than ϵ_g and $\tilde{\epsilon}$, respectively. To ensure secure communications of the primary system (secondary system), it is required for $\tilde{\epsilon}$ (ϵ_g) to be large enough (close to 1).

C. Proposed Solution

We are now in position to expose the hidden convexity of constraints (26c), (26e), and (26g). Since $\mathbf{U}$ does not require

a rank-constraint matrix, we introduce $\widetilde{\mathbf{U}} \triangleq \mathbf{U}\mathbf{U}^H$ to facilitate the optimization problem. Let us handle the constraint (26e) first by rewriting it as

$$\max_{\Delta\mathbf{f}_l\in\Omega_l} \sum_{g=1}^{G} \left|\mathbf{f}_l^H\mathbf{w}_g\right|^2 + \mathrm{tr}\left(\mathbf{f}_l^H\widetilde{\mathbf{U}}\mathbf{f}_l\right) + \sigma_l^2 \le \frac{P_p|h_l|^2}{\alpha_l}, l \in \mathcal{L}. \quad (27)$$

For arbitrary l-th PR, (27) can be shaped to take the following equivalent form

$$\sum_{g=1}^{G} \mu_{l,g} + \tilde{\mu}_l + \sigma_l^2 \le \frac{P_p|h_l|^2}{\alpha_l}, l \in \mathcal{L} \quad (28)$$

$$\max_{\Delta\mathbf{f}_l\in\Omega_l} \left|\mathbf{f}_l^H\mathbf{w}_g\right|^2 \le \mu_{l,g}, l \in \mathcal{L}, g \in \mathcal{G} \quad (29)$$

$$\max_{\Delta\mathbf{f}_l\in\Omega_l} \mathrm{tr}\left(\mathbf{f}_l^H\widetilde{\mathbf{U}}\mathbf{f}_l\right) \le \tilde{\mu}_l, l \in \mathcal{L} \quad (30)$$

where $\boldsymbol{\mu}_l = \{\mu_{l,g}\}$ and $\tilde{\boldsymbol{\mu}} = \{\tilde{\mu}_l\}$ are new variables. Note that both sides of (28) are convex, so it is iteratively replaced by the following linear constraint

$$\sum_{g=1}^{G} \mu_{l,g} + \tilde{\mu}_l + \sigma_l^2 \le \frac{2P_p|h_l|^2}{\alpha_l^{(n)}} - \frac{P_p|h_l|^2}{\left(\alpha_l^{(n)}\right)^2}\alpha_l, l \in \mathcal{L}. \quad (31)$$

To make the tractable form of (29) and (30), we first transform these constraints into a matrix inequality based on the following lemma.

Lemma 2 (S-Procedure [40]): Let $f_m(\mathbf{x}) = \mathbf{x}^H\mathbf{A}_m\mathbf{x} + 2\mathrm{Re}\{\mathbf{b}_m^H\mathbf{x}\} + c_m$, where $m = \{1, 2\}$, $\mathbf{A}_m \in \mathbb{H}^N$, $\mathbf{b}_m \in \mathbb{C}^{N\times 1}$ and $c_m \in \mathbb{R}$. Then there exists a $\hat{\mathbf{x}}$ such that $f_z(\hat{\mathbf{x}}) < 0$ satisfies: $f_1(\mathbf{x}) \le 0 \Rightarrow f_2(\mathbf{x}) \le 0$ if and only if there exists $\omega \ge 0$ such that

$$\omega\begin{bmatrix}\mathbf{A}_1 & \mathbf{b}_1\\ \mathbf{b}_1^H & c_1\end{bmatrix} - \begin{bmatrix}\mathbf{A}_2 & \mathbf{b}_2\\ \mathbf{b}_2^H & c_2\end{bmatrix} \succeq \mathbf{0}. \quad (32)$$

Substituting $\mathbf{f}_l = \hat{\mathbf{f}}_l + \Delta\mathbf{f}_l, \forall l$ into (29) and applying Lemma 2, then

$$\begin{aligned} & \Delta\mathbf{f}_l^H\Delta\mathbf{f}_l - \delta_l^2 \le 0 \\ \Rightarrow\ (29):\ & \Delta\mathbf{f}_l^H\mathbf{w}_g\mathbf{w}_g^H\Delta\mathbf{f}_l + 2\Re\left\{\hat{\mathbf{f}}_l^H\mathbf{w}_g\mathbf{w}_g^H\Delta\mathbf{f}_l\right\} \\ & + \hat{\mathbf{f}}_l^H\mathbf{w}_g\mathbf{w}_g^H\hat{\mathbf{f}}_l - \mu_{l,g} \le 0 \end{aligned} \quad (33)$$

holds if and only if there exists $\boldsymbol{\omega}_l = \{\omega_{l,g} \ge 0\}$, $\forall l$, so that the following matrix inequality constraint holds

$$\begin{bmatrix}\omega_{l,g}\mathbf{I}_N - \mathbf{w}_g\mathbf{w}_g^H & -\mathbf{w}_g\mathbf{w}_g^H\hat{\mathbf{f}}_l \\ -\hat{\mathbf{f}}_l^H\mathbf{w}_g\mathbf{w}_g^H & -\hat{\mathbf{f}}_l^H\mathbf{w}_g\mathbf{w}_g^H\hat{\mathbf{f}}_l - \omega_{l,g}\delta_l^2 + \mu_{l,g}\end{bmatrix} \succeq \mathbf{0}. \quad (34)$$

However, (34) is still not in a tractable form. At this point, we apply the application of Schur's complement lemma [41, eq. (7.2.6)] to obtain the following linear matrix inequality (LMI)

$$\exists\omega_{l,g} \ge 0 : \mathbf{C}_{l,g}(\mathbf{w}_g, \mu_{l,g}, \omega_{l,g}) \triangleq \begin{bmatrix} 1 & \mathbf{w}_g^H & -\mathbf{w}_g^H\hat{\mathbf{f}}_l \\ \mathbf{w}_g & \omega_{l,g}\mathbf{I}_N & \\ -\hat{\mathbf{f}}_l^H\mathbf{w}_g & & -\omega_{l,g}\delta_l^2 + \mu_{l,g}\end{bmatrix} \succeq \mathbf{0},\ g \in \mathcal{G}, l \in \mathcal{L}. \quad (35)$$

It is also worth noting that constraint (35) now includes only a finite number of constraints.

Analogously, with $\tilde{\boldsymbol{\omega}} = \{\tilde{\omega}_l \ge 0\}$, constraint (30) admits the following representation

$$\exists\tilde{\omega}_l \ge 0 : \tilde{\mathbf{C}}_l(\widetilde{\mathbf{U}}, \tilde{\mu}_l, \tilde{\omega}_l) \triangleq \begin{bmatrix}\tilde{\omega}_l\mathbf{I}_N - \widetilde{\mathbf{U}} & -\widetilde{\mathbf{U}}\hat{\mathbf{f}}_l \\ -\hat{\mathbf{f}}_l^H\widetilde{\mathbf{U}} & -\hat{\mathbf{f}}_l^H\widetilde{\mathbf{U}}\hat{\mathbf{f}}_l - \tilde{\omega}_l\delta_l^2 + \tilde{\mu}_l\end{bmatrix} \succeq \mathbf{0},\ l \in \mathcal{L}. \quad (36)$$

To deal with the nonconvex constraints given in (26g) and (26c), we provide the following two lemmas.

Lemma 3: For the primary system, constraint (26g) is transformed to a new constraint as

$$\lambda_{\min}\left(\sum\nolimits_{g=1}^{G} \mathbf{w}_g\mathbf{w}_g^H + \widetilde{\mathbf{U}}\right) \ge \tilde{\xi}(\beta) \quad (37)$$

where $\tilde{\xi}(\beta) \triangleq (\exp(-\frac{\beta}{NP_p}\sigma_{k_p}^2)/(1-\tilde{\epsilon}^{1/K_p})^{1/N} - 1)\frac{P_p}{\beta}$.

Proof: See Appendix C. ∎

In Lemma 3, the claim is clearly true in the trivial case of $\beta \to \infty$, i.e., the primary system is inactive, which leads to $\sum_{g=1}^{G}\mathbf{w}_g\mathbf{w}_g^H + \widetilde{\mathbf{U}} \succeq \mathbf{0}$. This is always true and thus confirms our analysis. Next, we rewrite (37) equivalently in the form of

$$2\ln\eta + \beta\frac{\sigma_{k_p}^2}{NP_p} \ge 0 \quad (38)$$

$$\left(\eta^2/(1-\tilde{\epsilon}^{1/K_p})^{1/N} - 1\right)P_p \le \beta\theta \quad (39)$$

$$\lambda_{\min}\left(\sum\nolimits_{g=1}^{G} \mathbf{w}_g\mathbf{w}_g^H + \widetilde{\mathbf{U}}\right) \ge \theta \quad (40)$$

where θ and η are newly introduced variables. Since the constraints (38) and (39) are convex, and we now focus on the remaining nonconvex constraint. In (40), we note that both $\sum_{g=1}^{G}\mathbf{w}_g\mathbf{w}_g^H$ and $\widetilde{\mathbf{U}}$ are Hermitian matrices. In addition, the eigenvalues of a Hermitian matrix $\mathbf{Q}$ are real and satisfy $\mathrm{tr}(\mathbf{x}^H\mathbf{Q}^H\mathbf{x}) \ge \lambda\|\mathbf{x}\|^2$ for any given vector $\mathbf{x}$ if and only if $\lambda_{\min}(\mathbf{Q}) \ge \lambda$. Since $\lambda_{\min}(\mathbf{w}_g\mathbf{w}_g^H) = 0$ for all g, the lower bound of left side of (40) is given by

$$\lambda_{\min}\left(\sum\nolimits_{g=1}^{G} \mathbf{w}_g\mathbf{w}_g^H + \widetilde{\mathbf{U}}\right) \ge \lambda_{\min}(\widetilde{\mathbf{U}}). \quad (41)$$

The implication of (41) is that the ST will degrade the eavesdropper's channel by transmitting jamming noise rather than the desired signals. From (40), it follows that

$$\lambda_{\min}(\widetilde{\mathbf{U}}) \ge \theta \Leftrightarrow \widetilde{\mathbf{U}} \succeq \mathbf{I}_N\theta. \quad (42)$$

Lemma 4: For the secondary system, constraint (26c) is transformed to a new constraint as

$$\frac{\left\|\mathbf{w}_g\right\|^2}{\phi_g} \le \xi_g + \sum_{i=1,i\ne g}^{G} \|\mathbf{w}_i\|^2 + \lambda_{\min}\left(\widetilde{\mathbf{U}}\right),\ g \in \mathcal{G} \quad (43)$$

where $\xi_g \triangleq [\exp(\frac{\sigma_{k_g}^2}{NP_p})\epsilon_g^{-1/NK_g} - 1]P_p$.

Proof: See Appendix D. ∎

The formulation in (43) can be further shaped to take the following convex constraints

$$\begin{aligned} \frac{\left\|\mathbf{w}_g\right\|^2}{\phi_g} \le \xi_g + & \sum_{i=1,i\ne g}^{G} 2\Re\{(\mathbf{w}_i^{(n)})^H\mathbf{w}_i\} \\ & - \sum_{i=1,i\ne g}^{G} \left\|\mathbf{w}_i^{(n)}\right\|^2 + \vartheta,\ g \in \mathcal{G} \end{aligned} \quad (44)$$

$$\lambda_{\min}(\widetilde{\mathbf{U}}) \ge \vartheta \Leftrightarrow \widetilde{\mathbf{U}} \succeq \mathbf{I}_N\vartheta \quad (45)$$

where ϑ is newly introduced variable.

Algorithm 2 An Iterative Algorithm to Solve (25)

Initialization: Set $n := 0$ and solve (47) to generate an initial feasible point $\left(\mathbf{w}^{(n)}, \widetilde{\mathbf{U}}^{(n)}, \boldsymbol{\alpha}^{(n)}\right)$

1: **repeat**
2: Solve (46) to obtain the optimal solution: $\left(\mathbf{w}^*, \widetilde{\mathbf{U}}^*, \boldsymbol{\alpha}^*\right)$.
3: Update $\mathbf{w}^{(n+1)} := \mathbf{w}^*$, $\widetilde{\mathbf{U}}^{(n+1)} := \widetilde{\mathbf{U}}^*$, and $\boldsymbol{\alpha}^{(n+1)} := \boldsymbol{\alpha}^*$.
4: Set $n := n + 1$.
5: **until** Convergence or maximum required number of iterations

Remark 2: We note that the new constraints in (37) and (43) are not equivalent to (26g) and (26c). Specifically, the optimal solutions for the former are also feasible for the latter, respectively, but not vice versa due to the inequalities in (76) and (81), and thus this leads to a lower bound of the system performance.

Remark 3: In this paper, the wiretap channels are modeled as i.i.d. Rayleigh random variables. Nevertheless, a different continuous channel distribution does not affect the type of constraints in (37) and (43). In other words, the proposed convex approximation is still applicable to any continuous channel distribution thanks to widespread applications of inner approximation method [42]. Therefore, our study is valid without loss of generality.

With the above discussions, the approximate convex problem solved at the $(n+1)$-th iteration of the proposed design is given by

$$\underset{\substack{\mathbf{w},\widetilde{\mathbf{U}}\succeq\mathbf{0},\boldsymbol{t},z,\varphi,\boldsymbol{\phi},\boldsymbol{\alpha},\\ \beta,\boldsymbol{\mu}_l,\tilde{\boldsymbol{\mu}},\boldsymbol{\omega}_l,\tilde{\boldsymbol{\omega}},\theta,\eta,\vartheta}}{\text{maximize}} \quad \varphi \tag{46a}$$

$$\text{s.t.} \quad \mathcal{F}_{m_g}^{(n)}(\mathbf{w},\widetilde{\mathbf{U}}) \geq (\varphi + t_g)\ln 2,\ m_g \in \mathcal{S}_g, g \in \mathcal{G} \tag{46b}$$

$$\sum\nolimits_{g=1}^{G} \|\mathbf{w}_g\|^2 + \text{tr}(\widetilde{\mathbf{U}}) \leq P_s \tag{46c}$$

$$\text{(26b), (26d), (26f), (31), (35),}$$
$$\text{(36), (38), (39), (42), (44), (45).} \tag{46d}$$

To find an initial feasible point to (25), we solve the following convex optimization problem

$$\max_{\substack{\mathbf{w},\widetilde{\mathbf{U}}\succeq\mathbf{0},z,\boldsymbol{\alpha},\beta,\\ \boldsymbol{\mu}_l,\tilde{\boldsymbol{\mu}},\boldsymbol{\omega}_l,\tilde{\boldsymbol{\omega}},\theta,\eta}} \min_{l\in\mathcal{L}} \left\{\log_2(1+\alpha_l) - z - \bar{R}_{p,l}\right\} \tag{47a}$$

$$\text{s.t.} \quad \text{(26f), (31), (35), (36), (38), (39), (42), (46c)} \tag{47b}$$

and stop at reaching

$$\min_{l\in\mathcal{L}} \left\{\log_2(1+\alpha_l) - z - \bar{R}_{p,l}\right\} \geq 0. \tag{48}$$

The proposed iterative method is outlined in Algorithm 2. In a similar manner to Proposition 1, we can show that Algorithm 2 yields a nondecreasing sequence of objective due to updating the involved variables after each iteration.

Complexity Analysis: The optimization problem in (46) involves GL LMI constraints of size $N+2$, L LMI constraints of size $N+1$, and 2 LMI constraints of size N. Since the major complexity of solving (46) comes from LMI constraints, we ignore the complexity of the constraints of lower sizes and they will not affect the complexity order of the whole problem. As a result, in each iteration of Algorithm 2, the worst-case computational complexity for solving the generic convex problem in (46) using interior point methods is given by $O(n\sqrt{GL(N+2)+L(N+1)+2N}[GL(N+2)^3 + L(N+1)^3 + 2N^3 + nGL(N+2)^2 + nL(N+1)^2 + 2nN^2 + n^2])$, where $n = G(L+3) + N(N+G) + 2L + 6$ [39].

V. Numerical Results and Discussions

In this section, we use simulations to evaluate the performance of the proposed approach. The number of groups of SUs is set to $G = 2$, each of which consists of two SR users, i.e., $M_g = 2$, $\forall g$. The number of PRs is set to $L = 2$, and each group of SUs and PUs is surrounded by two Eves, i.e., $K_p = K_g = 2$. All channel entries are assumed to be i.i.d. complex Gaussian random variables with $\mathcal{CN}(0,1)$, and the background thermal noise at each user is generated as i.i.d. complex Gaussian random variables with zero means and unit variance. The transmit power at the PT is fixed to $P_p = 20$ dBm. For simplicity, we further assume that the minimum secrecy rate requirement for all PUs are the same, i.e., $\bar{R}_{p,l} = \bar{R}_p, \forall l$. For the imperfect CSI of the PU channels, we define the normalized channel estimation errors as $\bar{\delta}_l^2 = \delta_l^2/\|\mathbf{f}_l\|^2 = 5\%$, $\forall l$. To guarantee secure communications, we choose $\tilde{\epsilon} = 0.99$ and $\epsilon_g = 0.99$, $\forall g$ for the passive Eves. The results obtained in this paper are referred to as the proposed optimal scheme. We also compare the performance of the proposed scheme with the known solutions, namely, the "No JN scheme" [23], [24] and "Partial ZF (zero-forcing) scheme" [22]. In the "No JN scheme," the optimal solution can be obtained by setting $\mathbf{U}$ to $\mathbf{0}$. In the "Partial ZF scheme," we consider the null space approach at the ST. First of all, the JN is transmitted to all Eves and to avoid interfering with both PUs and SUs as

$$\mathbf{U}^H\mathbf{f}_l = 0, \forall l \quad \text{and} \quad \mathbf{U}^H\mathbf{h}_{m_g} = 0, \forall m_g, g. \tag{49}$$

In a CRN, the primary system should have higher priority, and thus the transmitted information at the ST should not generate interferences to the PUs as

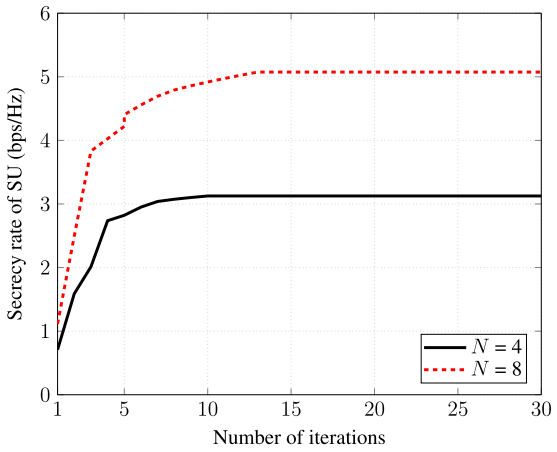
$$\mathbf{w}_g^H\mathbf{f}_l = 0, \forall l, g. \tag{50}$$

To simplify the problem, we enforce the information transmitted at the ST so that it should not introduce interference to other groups as

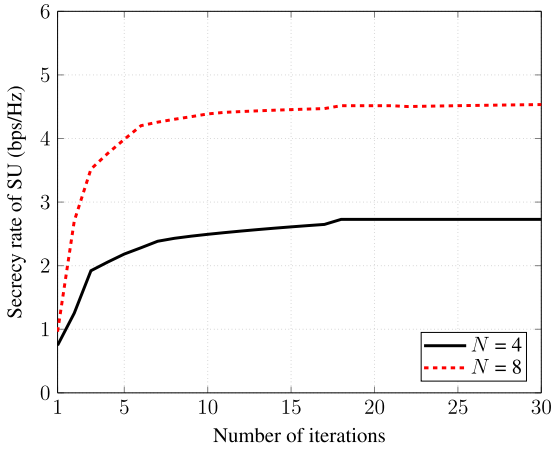
$$\mathbf{w}_g^H\mathbf{h}_{m_i} = 0, \forall i \neq g. \tag{51}$$

It is evident that $\Gamma_{p,l} = \frac{P_p|h_l|^2}{\sigma_l^2}, \forall l$, does not depend on $\mathbf{w}_g$ and $\mathbf{U}$. So, we utilize (49), (50), and (51) into **P1** to obtain the optimal solution for "Partial ZF scheme." To solve convex problems we use the SDPT3 as the internal solver [43] in MATLAB environment. The results of the secrecy rate are shown by averaging over 1,000 simulation trials.

Fig. 2 illustrates the typical convergence behavior of the proposed Algorithm 1 and Algorithm 2 as a function of the number of iterations with different numbers of antennas at the ST for Algorithm 1 in Fig. 2(a) and for Algorithm 2 in



(a) Convergence results of Algorithm 1 for different numbers of antennas at the ST.



(b) Convergence results of Algorithm 2 for different numbers of antennas at the ST.

Fig. 2. Convergence results of Algorithm 1 and 2 for different numbers of antennas at the ST over one random channel realization with $\bar{R}_p = 2$ bps/Hz and $P_s = 15$ dBm.

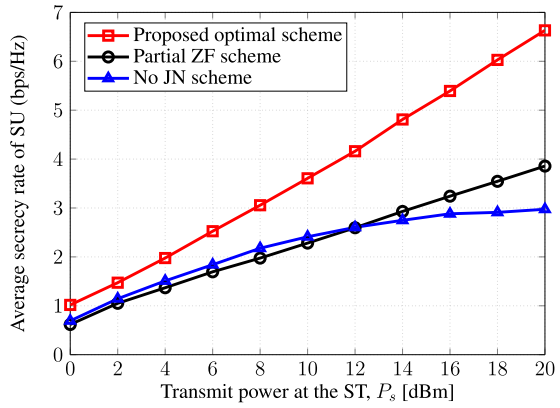


Fig. 3. Average secrecy rate of the secondary system vs. the transmit power at the ST with perfect CSI, where $\bar{R}_p = 2$ bps/Hz and $N = 8$.

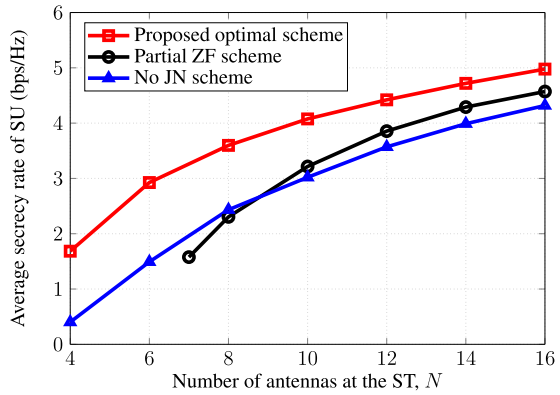


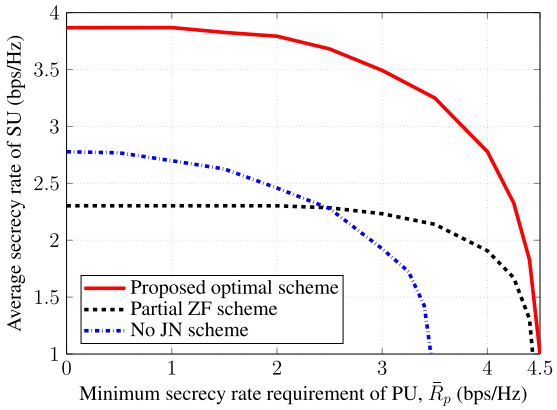
Fig. 4. Average secrecy rate of the secondary system vs. the number of transmit antennas at the ST with perfect CSI, where $\bar{R}_p = 2$ bps/Hz and $P_s = 10$ dBm.

Fig. 2(b). As seen, the objective values of both algorithms increase rapidly within the first 10 iterations and stabilize after a few more iterations, and its convergence rate is slightly sensitive to the problem size, i.e., as N increases. The convergence results also confirm that all optimization variables are accounted to find a better solution for the next iteration, i.e., the secrecy rates of SUs monotonically increasing. In addition, Fig. 2 shows that at least 90% of secrecy rate is obtained when the proposed algorithms reach to 10 iterations.

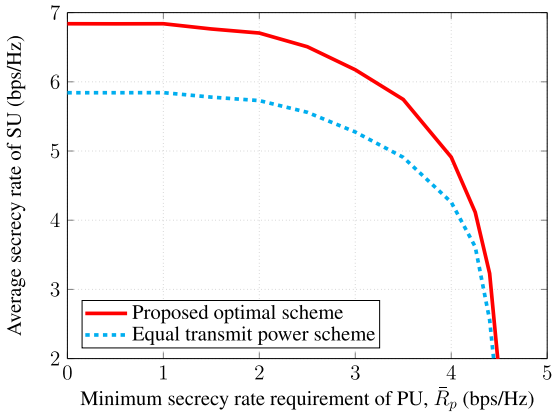
Fig. 3 plots the average secrecy rate of secondary system versus the transmit power at the ST. As can be seen, the proposed optimal scheme greatly improves the secrecy rate of the "Partial ZF scheme" and "No JN scheme," especially in high power regime. The performance gain is thus achieved as a result of more intelligent interference management than that of other schemes for primary users and Eves. Another interesting observation is that the "No JN scheme" outperforms the "Partial ZF scheme" in low power regime ($P_s \leq 12$ dBm), but it tends to saturate when the transmit power becomes high. This is mainly due to the fact that, in high power regime, the ST needs to scale down the transmit power to maintain the secrecy rate of the primary system, which results in a loss of the secrecy rate of secondary system. Moreover, the simulation results in Fig. 3 further confirm that incorporating information and JN beamforming is a powerful means to transmit with full power.

In Fig. 4, we study the secrecy rate of secondary system as a function of the number of transmit antennas at the ST, N. The results show that the achievable secrecy rate increases as the number of transmit antennas increases in all schemes, since more degrees of freedom are added to the ST. The proposed optimal scheme still achieves a better performance than other schemes in all the range of N. We note that the optimal solution for the "Partial ZF scheme" is infeasible when $N < 7$ because for the "Partial ZF scheme," interference among legitimate users cannot be completely canceled out with insufficient number of transmit antennas. As expected, the gap between the proposed scheme and "Partial ZF scheme" is reduced as a result of providing more degrees of freedom.

The average secrecy rate of the secondary system is investigated as a function of the minimum secrecy rate requirement of primary system, $\bar{R}_p$, in Fig. 5(a) for different schemes and in Fig. 5(b) for different power sharing. As can be seen from Fig. 5(a), the secondary system achieves a higher secrecy rate with the proposed optimal scheme than with other schemes. Notably, the performance of "No JN scheme" is degraded



(a) Average secrecy rate of the secondary system for different schemes, where P_s = 10 dBm.



(b) Average secrecy rate of the secondary system for different power sharing, where P_s = 20 dBm

Fig. 5. Average secrecy rate of the secondary system vs. the minimum secrecy rate requirement of the primary system, (a) for different schemes and (b) for different power sharing with perfect CSI, where $N = 8$.

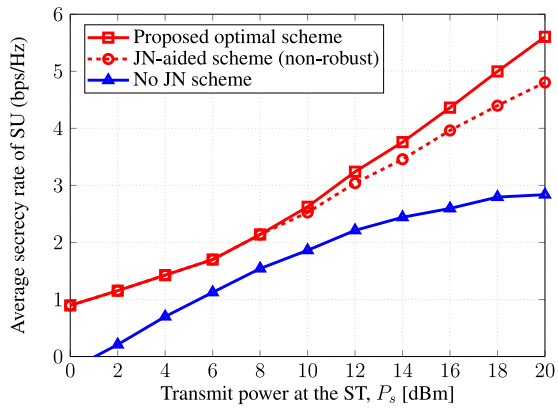
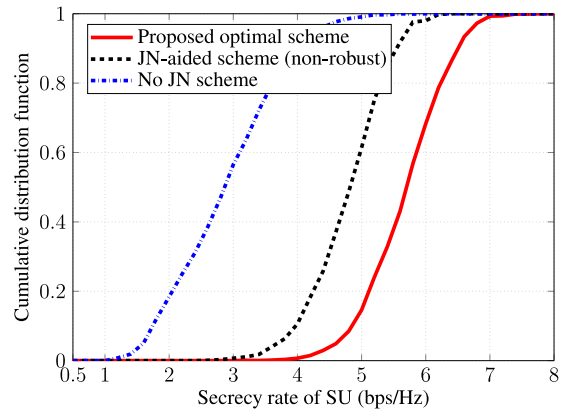
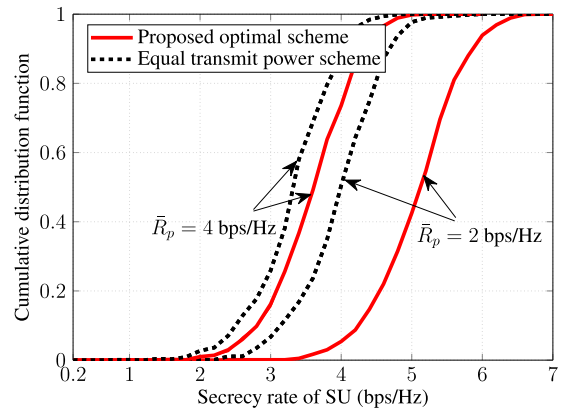


Fig. 6. Average secrecy rate of the secondary system vs. the transmit power at the ST with realistic scenario, where $\bar{R}_p = 1$ bps/Hz and $N = 8$.



(a) CDF of the secrecy rate of the secondary system for different schemes, where $\bar{R}_p$ = 1 bps/Hz.



(b) CDF of the secrecy rate of the secondary system for different power sharing.

Fig. 7. CDF of secrecy rate of the secondary system, the probability that the secrecy rate will take a value less than or equal to a given secrecy rate threshold, (a) for different schemes and (b) for different power sharing with realistic scenario, where $N = 8$ and $P_s = 20$ dBm.

significant as $\bar{R}_p$ increases. The main reason for such a case is that, the ST is required to cause less interference to the PRs and transmit high interference to degrade the Eves' channels, which results in a significant loss of the secondary system's secrecy rate. The secrecy rate of the "Partial ZF scheme" is nearly unchanged when $\bar{R}_p$ increases and approaches that of the proposed optimal scheme for high $\bar{R}_p$, since the ST does not cause any interference to the PRs. In Fig. 5(b), we plot the average secrecy rate of the secondary system for the proposed optimal scheme under different assumption of sharing equally the resources, i.e., transmit power at the ST. Particularly, the information and JN beamforming are assumed to share 50% of the power resource, i.e., $\sum_{g=1}^{G} \|\mathbf{w}_g\|^2 \leq P_s/2$ and $\|\mathbf{U}\|^2 \leq P_s/2$. As seen, the proposed joint information and JN beamforming offers better performance compared to that of the equal transmit power scheme. However, the gap between the schemes diminishes for high secrecy rate of the primary system. The reason for this is two-fold: 1) For small $\bar{R}_p$, a small portion of JN already fulfills the QoS requirement of PU, and there is no need to further waste power budget on JN; 2) For extremely stringent QoS requirement of PU, JN becomes crucial and so it is reasonable to allocate a significant part of the power budget to JN (i.e., nearly a half as shown in Fig. 5(b)) to meet the QoS requirement. From both Figs. 5(a) and 5(b), for high $\bar{R}_p$, the secondary system lacks degree of freedom for leveraging multiuser diversity.

We now turn our attention to illustrate the robustness of the proposed design in realistic scenario. We also compare

the performance of the proposed robust design to that of non-robust secrecy rate. For the non-robust secrecy rate design, we use the presumed CSIs as $\hat{\mathbf{f}}_l,\ \forall l$ rather than the true ones, to perform the transmit design (as presented in Section IV), which then evaluates the resultant secrecy rate. Fig. 6 depicts the secrecy rate as a function of the transmit power at the ST. As can be observed that the secrecy rate of non-robust design is sensitive to the CSI uncertainties for high P_s. In particular, when $P_s \geq 8$ dBm, the non-robust design exhibits the degradation in terms of the secrecy rate that tends to worsen as P_s increases. Moreover, the proposed optimal design achieves the best secrecy rate performance, compared to other designs.

Finally, we generate cumulative distribution functions (CDFs) of the secrecy rate of the secondary system in Fig. 7(a) for different schemes and in Fig. 7(b) for different power sharing. It is obvious in both CDFs that on account for a larger feasible set, the proposed optimal scheme can promise a bigger secrecy rate as expected. For instance, the proposed optimal scheme attains 0.8 bps/Hz and 2.8 bps/Hz of the achievable secrecy rate higher than the non-robust scheme and "No JN scheme," respectively, for approximately 60% of the simulated trials in Fig. 7(a). For large $\bar{R}_p$, the gap between the proposed design and non-robust design is reduced as in Fig. 7(b) due to a decrease in the available multiuser diversity gain.

VI. Conclusion

In this paper, we have considered PHY security for both primary and secondary systems in the presence of multiple secondary receiver groups and multiple primary receivers. The secondary system has been proposed to assist the primary system by sending jamming noise to degrade the decoding capability of the eavesdroppers. The main objective is to maximize the secrecy rate of the secondary system, while the secondary transmitter is constrained not only by the power budget, but also by the individual minimum secrecy rate requirements of the primary users. We have proposed iterative algorithms to solve the optimization problems. The idea of the proposed method is to approximate the nonconvex problem by a convex formulation in each iteration. We have proved that our iterative algorithms are guaranteed to monotonically converge to at least local optima of the original nonconvex design problems. We have carried out simulations to evaluate the advantages of the proposed design. It has been shown that for a given initial feasible point, the proposed iterative algorithms are guaranteed to always converge to an optimal solution.

Appendix A
Proof of Lemma 1

The following inequalities play an important role in our developments:

$$\ln\left(1+\frac{|x|^2}{y}\right) \geq \ln\left(1+\frac{\left|x^{(n)}\right|^2}{y^{(n)}}\right) - \frac{\left|x^{(n)}\right|^2}{y^{(n)}} + 2\frac{\Re\left\{(x^{(n)})^* x\right\}}{y^{(n)}} - \frac{\left|x^{(n)}\right|^2(|x|^2+y)}{y^{(n)}(y^{(n)}+\left|x^{(n)}\right|^2)},\ \forall x\in\mathbb{C}, y>0, \quad (52)$$

$$\frac{|x|^2}{y} \geq 2\frac{(x^{(n)})^* x}{y^{(n)}} - \frac{\left|x^{(n)}\right|^2}{(y^{(n)})^2}y,\ \ \forall x\in\mathbb{C}, y>0, \quad (53)$$

$$\ln(1+x) \leq \ln\left(1+x^{(n)}\right) + \frac{(x-x^{(n)})}{(1+x^{(n)})},\ \ \forall x\geq 0 \quad (54)$$

where (52) and (53) follow from the convexity of functions $\ln(1+|x|^2/y)$ and $|x|^2/y$ [44], [45], respectively; while (54) is a result of the concavity of function $\ln(1+x)$.

Let us treat the nonconvex constraint (11b) first. As the first step, (4) is equivalently rewritten by

$$\Gamma_{s,m_g}(\mathbf{w},\mathbf{U}) = \frac{\left|\mathbf{h}_{m_g}^H\mathbf{w}_g\right|^2}{\chi_{s,m_g}(\mathbf{w},\mathbf{U})} \quad (55)$$

where

$$\chi_{s,m_g}(\mathbf{w},\mathbf{U}) = \sum_{i=1,i\neq g}^{G}\left|\mathbf{h}_{m_g}^H\mathbf{w}_i\right|^2 + \left\|\mathbf{h}_{m_g}^H\mathbf{U}\right\|^2 + P_p|f_{m_g}|^2 + \sigma_{m_g}^2.$$

From (55), it follows that

$$\ln\left(1+\frac{|\mathbf{h}_{m_g}^H\mathbf{w}_g|^2}{\chi_{s,m_g}(\mathbf{w},\mathbf{U})}\right) = -\ln\left(1-\frac{|\mathbf{h}_{m_g}^H\mathbf{w}_g|^2}{\chi_{s,m_g}(\mathbf{w},\mathbf{U})+|\mathbf{h}_{m_g}^H\mathbf{w}_g|^2}\right). \quad (56)$$

From the fact that $0 \leq \frac{|\mathbf{h}_{m_g}^H\mathbf{w}_g|^2}{\chi_{s,m_g}(\mathbf{w},\mathbf{U})+|\mathbf{h}_{m_g}^H\mathbf{w}_g|^2} \triangleq \Theta(\mathbf{w},\mathbf{U}) < 1$, the function $-\ln(1-\Theta(\mathbf{w},\mathbf{U}))$ is jointly convex w.r.t. the involved variables [40], which is useful for developing an approximate solution for (56). In particular, at feasible point $\left(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\right)$, applying (52) yields

$$\begin{aligned}
&-\ln\left(1-\frac{\left|\mathbf{h}_{m_g}^H\mathbf{w}_g\right|^2}{\chi_{s,m_g}(\mathbf{w},\mathbf{U})+\left|\mathbf{h}_{m_g}^H\mathbf{w}_g\right|^2}\right)\\
&\quad\geq -\ln\left(1-\frac{\left|\mathbf{h}_{m_g}^H\mathbf{w}_g^{(n)}\right|^2}{\chi_{s,m_g}(\mathbf{w}^{(n)},\mathbf{U}^{(n)})+\left|\mathbf{h}_{m_g}^H\mathbf{w}_g^{(n)}\right|^2}\right)\\
&\qquad-\Gamma_{s,m_g}\left(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\right)+2\frac{\Re\left\{\left(\mathbf{w}_g^{(n)}\right)^H\mathbf{h}_{m_g}\mathbf{h}_{m_g}^H\mathbf{w}_g\right\}}{\chi_{s,m_g}(\mathbf{w}^{(n)},\mathbf{U}^{(n)})}\\
&\qquad-\frac{\Gamma_{s,m_g}\left(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\right)\left(\chi_{s,m_g}(\mathbf{w},\mathbf{U})+\left|\mathbf{h}_{m_g}^H\mathbf{w}_g\right|^2\right)}{\chi_{s,m_g}(\mathbf{w}^{(n)},\mathbf{U}^{(n)})+|\mathbf{h}_{m_g}^H\mathbf{w}_g^{(n)}|^2}\\
&\quad\coloneqq \mathcal{F}_{m_g}^{(n)}(\mathbf{w},\mathbf{U}).
\end{aligned} \quad (57)$$

Note that $\mathcal{F}_{m_g}^{(n)}(\mathbf{w},\mathbf{U})$ is concave and is global lower bound of $-\ln(1-\Theta(\mathbf{w},\mathbf{U}))$. It implies that we can iteratively replace $-\ln(1-\Theta(\mathbf{w},\mathbf{U}))$ by $\mathcal{F}_{m_g}^{(n)}(\mathbf{w},\mathbf{U})$ to achieve a convex approximation of (11b) [42]. Hence, by substituting (55), (56), and (57) into (11b), we

provide (12). To handling the constraint (11c), we equivalently rewrite $\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})$ as

$$\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})=\frac{\left|\mathbf{g}_{k_g}^H\mathbf{w}_g\right|^2}{\chi_{e,k_g}(\mathbf{w},\mathbf{U})} \tag{58}$$

where

$$\chi_{e,k_g}(\mathbf{w},\mathbf{U})=\sum_{i=1,i\neq g}^{G}\left|\mathbf{g}_{k_g}^H\mathbf{w}_i\right|^2+\left\|\mathbf{g}_{k_g}^H\mathbf{U}\right\|^2+P_p|f_{k_g}|^2+\sigma_{k_g}^2.$$

The constraint (11c) requires a tight upper bound of $\log_2\big(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})\big)$. Applying (54) yields

$$\begin{aligned}\ln\big(1+\Gamma_{e,k_g}(\mathbf{w},\mathbf{U})\big)\leq{}&\log_2\Big(1+\Gamma_{e,k_g}\big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\big)\Big)\\&+\Big(1+\Gamma_{e,k_g}\big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\big)\Big)^{-1}\\&\times\left(\frac{|\mathbf{g}_{k_g}^H\mathbf{w}_g|^2}{\chi_{e,k_g}(\mathbf{w},\mathbf{U})}-\Gamma_{e,k_g}\big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\big)\right).\end{aligned} \tag{59}$$

Although the right-hand side of (59) is still nonconvex, it can be further convexified by

$$\begin{aligned}\mathcal{F}_{k_g}^{(n)}(\mathbf{w},\mathbf{U})\coloneqq{}&\log_2\Big(1+\Gamma_{e,k_g}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big)\\&+\Big(1+\Gamma_{e,k_g}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big)^{-1}\\&\times\left(\frac{|\mathbf{g}_{k_g}^H\mathbf{w}_g|^2}{\Phi_{k_g}^{(n)}(\mathbf{w},\mathbf{U})}-\Gamma_{e,k_g}\big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\big)\right)\end{aligned} \tag{60}$$

where $\Phi_{k_g}^{(n)}(\mathbf{w},\mathbf{U})$ is the first-order approximation of $\chi_{e,k_g}(\mathbf{w},\mathbf{U})$ around the point $(\mathbf{w}^{(n)},\mathbf{U}^{(n)})$ by using (53), which is given by

$$\begin{aligned}\Phi_{k_g}^{(n)}(\mathbf{w},\mathbf{U})\triangleq{}&\sum_{i=1,i\neq g}^{G}2\Re\left\{\Big(\mathbf{w}_i^{(n)}\Big)^H\mathbf{g}_{k_g}\mathbf{g}_{k_g}^H\mathbf{w}_i\right\}\\&-\sum_{i=1,i\neq g}^{G}\left|\mathbf{g}_{k_g}^H\mathbf{w}_i^{(n)}\right|^2+2\Re\left\{\mathbf{g}_{k_g}^H\mathbf{U}^{(n)}\mathbf{U}^H\mathbf{g}_{k_g}\right\}\\&-\left\|\mathbf{g}_{k_g}^H\mathbf{U}^{(n)}\right\|^2+P_p|f_{k_g}|^2+\sigma_{k_g}^2.\end{aligned}$$

The constraint (11c) is then approximated by the following convex constraint

$$\mathcal{F}_{k_g}^{(n)}(\mathbf{w},\mathbf{U})\leq t_g\ln 2. \tag{61}$$

In a similar manner, at feasible point $(\mathbf{w}^{(n)},\mathbf{U}^{(n)})$, the nonconvex constraints (11d) and (11e) are approximated by the following convex constraints

$$\mathcal{P}_l^{(n)}(\mathbf{w},\mathbf{U})\geq\big(z+\bar{R}_{p,l}\big)\ln 2, \tag{62}$$

$$\mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U})\leq z\ln 2 \tag{63}$$

where $\mathcal{P}_l^{(n)}(\mathbf{w},\mathbf{U})$ and $\mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U})$ are respectively given by

$$\begin{aligned}\mathcal{P}_l^{(n)}(\mathbf{w},\mathbf{U})\coloneqq{}&\ln\Big(1+\Gamma_{p,l}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big)+\Gamma_{p,l}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\\&-\Gamma_{p,l}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\frac{\big(\chi_{p,l}(\mathbf{w},\mathbf{U})+P_p|h_l|^2\big)}{\chi_{p,l}(\mathbf{w}^{(n)},\mathbf{U}^{(n)})+P_p|h_l|^2},\end{aligned} \tag{64}$$

$$\begin{aligned}\mathcal{P}_{k_p}^{(n)}(\mathbf{w},\mathbf{U})\coloneqq{}&\ln\Big(1+\Gamma_{e,k_p}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\Big)\\&+\Big(1+\Gamma_{e,k_p}(\mathbf{w}^{(n)},\mathbf{U}^{(n)})\Big)^{-1}\\&\times\left(\frac{P_p|g_{k_p}|^2}{\Phi_{k_p}^{(n)}(\mathbf{w},\mathbf{U})}-\Gamma_{e,k_p}(\mathbf{w}^{(n)},\mathbf{U}^{(n)})\right),\end{aligned} \tag{65}$$

with

$$\begin{aligned}\Phi_{k_p}^{(n)}(\mathbf{w},\mathbf{U})={}&\sum_{g=1}^{G}2\Re\left\{(\mathbf{w}_g^{(n)})^H\mathbf{f}_{k_p}\mathbf{f}_{k_p}^H\mathbf{w}_g\right\}-\sum_{g=1}^{G}|\mathbf{f}_{k_p}^H\mathbf{w}_g^{(n)}|^2\\&+2\Re\left\{\mathbf{f}_{k_p}^H\mathbf{U}^{(n)}\mathbf{U}^H\mathbf{f}_{k_p}\right\}-\left\|\mathbf{f}_{k_p}^H\mathbf{U}^{(n)}\right\|^2+\sigma_{k_p}^2,\\\chi_{p,l}(\mathbf{w},\mathbf{U})={}&\sum_{g=1}^{G}|\mathbf{f}_l^H\mathbf{w}_g|^2+\|\mathbf{f}_l^H\mathbf{U}\|^2+\sigma_l^2,\\\chi_{e,k_p}(\mathbf{w},\mathbf{U})={}&\sum_{g=1}^{G}\left|\mathbf{f}_{k_p}^H\mathbf{w}_g\right|^2+\left\|\mathbf{f}_{k_p}^H\mathbf{U}\right\|^2+\sigma_{k_p}^2.\end{aligned}$$

Appendix B
Proof of Proposition 1

Let $\varphi(\mathbf{w},\mathbf{U})$ and $\varphi^{(n)}(\mathbf{w},\mathbf{U})$ denote the objective of (11) and (20), respectively. We have

$$\varphi(\mathbf{w},\mathbf{U})\geq\varphi^{(n)}(\mathbf{w},\mathbf{U}),\quad\text{(thanks to (57))} \tag{66}$$

and

$$\varphi\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)=\varphi^{(n)}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big),\quad\text{(thanks to (16))}. \tag{67}$$

Let $(\mathbf{w}^{(n+1)},\mathbf{U}^{(n+1)})$ and $(\mathbf{w}^{(n)},\mathbf{U}^{(n)})$ be the optimal solution and feasible point of (20), respectively. It follows that

$$\begin{aligned}\varphi\Big(\mathbf{w}^{(n+1)},\mathbf{U}^{(n+1)}\Big)&\geq\varphi^{(n)}\Big(\mathbf{w}^{(n+1)},\mathbf{U}^{(n+1)}\Big)\\&\geq\varphi^{(n)}\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big)\\&=\varphi\Big(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\Big).\end{aligned} \tag{68}$$

It shows that $(\mathbf{w}^{(n+1)},\mathbf{U}^{(n+1)})$ is a better point to (20) than $(\mathbf{w}^{(n)},\mathbf{U}^{(n)})$ in the scene of improving the objective value. Furthermore, the sequence $\{\varphi^{(n)}\}$ is bounded above due to the power constraint in (8c). Let $(\bar{\mathbf{w}},\bar{\mathbf{U}})$ be a saddle point of (20), by Cauchy's theorem, there is a convergent subsequence $\{(\mathbf{w}^{(n_\kappa)},\mathbf{U}^{(n_\kappa)})\}$ satisfying

$$\lim_{\kappa\to+\infty}\Big[\varphi\Big(\mathbf{w}^{(n_\kappa)},\mathbf{U}^{(n_\kappa)}\Big)-\varphi\big(\bar{\mathbf{w}},\bar{\mathbf{U}}\big)\Big]=0. \tag{69}$$

For every n there is κ such that $n_\kappa \le n \le n_{\kappa+1}$. From (68) and (69), it is true that

$$\begin{aligned}0 &= \lim_{\kappa\to+\infty}\left[\varphi\left(\mathbf{w}^{(n_\kappa)},\mathbf{U}^{(n_\kappa)}\right)-\varphi\left(\bar{\mathbf{w}},\bar{\mathbf{U}}\right)\right]\\ &\le \lim_{n\to+\infty}\left[\varphi\left(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\right)-\varphi\left(\bar{\mathbf{w}},\bar{\mathbf{U}}\right)\right]\\ &\le \lim_{\kappa\to+\infty}\left[\varphi\left(\mathbf{w}^{(n_{\kappa+1})},\mathbf{U}^{(n_{\kappa+1})}\right)-\varphi\left(\bar{\mathbf{w}},\bar{\mathbf{U}}\right)\right]\\ &= 0\end{aligned} \tag{70}$$

which leads to $\lim_{n\to+\infty}\varphi(\mathbf{w}^{(n)},\mathbf{U}^{(n)}) = \varphi(\bar{\mathbf{w}},\bar{\mathbf{U}})$. In other words, Algorithm 1 will stop when the following termination condition is met, i.e.,

$$\left|\left(\varphi\left(\mathbf{w}^{(n)},\mathbf{U}^{(n)}\right)-\varphi\left(\bar{\mathbf{w}},\bar{\mathbf{U}}\right)\right)/\varphi\left(\bar{\mathbf{w}},\bar{\mathbf{U}}\right)\right| \le \epsilon \tag{71}$$

where ϵ is a given accuracy. Following the same arguments as those in [42, Th. 1], we can prove that each accumulation point $(\bar{\mathbf{w}},\bar{\mathbf{U}})$ of the sequence $\{(\mathbf{w}^{(n)},\mathbf{U}^{(n)})\}$ is a KKT-point of (8). Proposition 1 is thus proved.

Appendix C
Proof of Lemma 3

Since the channels are modeled as i.i.d. Rayleigh random variables, the constraint in (26g) can be rewritten for each k_p link as

$$\Pr\left(\frac{P_p|g_{k_p}|^2}{\sum_{g=1}^{G}\mathrm{tr}(\mathbf{F}_{k_p}\widetilde{\mathbf{W}}_g)+\mathrm{tr}(\mathbf{F}_{k_p}\widetilde{\mathbf{U}})+\sigma_{k_p}^2}\le\beta\right)\ge\tilde{\epsilon} \tag{72}$$

$$\Leftrightarrow \Pr\left(\frac{P_p}{\beta}|g_{k_p}|^2\le\mathrm{tr}\left(\mathbf{F}_{k_p}\left(\sum_{g=1}^{G}\widetilde{\mathbf{W}}_g+\widetilde{\mathbf{U}}\right)\right)+\sigma_{k_p}^2\right)\ge\tilde{\epsilon} \tag{73}$$

where $\mathbf{F}_{k_p}\triangleq\mathbf{f}_{k_p}\mathbf{f}_{k_p}^H$ and $\widetilde{\mathbf{W}}_g\triangleq\mathbf{w}_g\mathbf{w}_g^H$. It is very difficult to calculate the distribution of $\mathrm{tr}\left(\mathbf{F}_{k_p}\left(\sum_{g=1}^{G}\widetilde{\mathbf{W}}_g+\widetilde{\mathbf{U}}\right)\right)$ directly. Instead of this, we consider its lower bound. For notational simplicity, let us define $\mathbf{A}=\sum_{g=1}^{G}\widetilde{\mathbf{W}}_g+\widetilde{\mathbf{U}}$. In [46],

$$\sum_{i=1}^{N}\lambda_i(\mathbf{F}_{k_p})\lambda_{N-i+1}(\mathbf{A})\le\mathrm{tr}(\mathbf{F}_{k_p}\mathbf{A}) \tag{74}$$

is shown for $N\times N$ Hermitian matrices $\mathbf{F}_{k_p}$ and $\mathbf{A}$, where $\lambda_i(\mathbf{X})$ denotes the i-th eigenvalue of matrix $\mathbf{X}\in\mathbb{H}^{N\times N}$, and its magnitude is sorted as $\lambda_{\max}(\mathbf{X})=\lambda_1(\mathbf{X})\ge\lambda_2(\mathbf{X})\ge\cdots\ge\lambda_N(\mathbf{X})=\lambda_{\min}(\mathbf{X})$. Since $\mathbf{F}_{k_p}$ is a rank-one positive semidefinite matrix, (74) can be written as

$$\begin{aligned}\mathrm{tr}(\mathbf{F}_{k_p}\mathbf{A}) &\ge \lambda_1(\mathbf{F}_{k_p})\lambda_N(\mathbf{A})\\ &= \lambda_{\max}(\mathbf{F}_{k_p})\lambda_{\min}(\mathbf{A})\\ &= \mathrm{tr}(\mathbf{F}_{k_p})\lambda_{\min}(\mathbf{A}).\end{aligned} \tag{75}$$

Substituting (75) into (73), we get

$$\begin{aligned}&\Pr\left(\frac{P_p}{\beta}|g_{k_p}|^2\le\mathrm{tr}\left(\mathbf{F}_{k_p}\left(\sum_{g=1}^{G}\widetilde{\mathbf{W}}_g+\widetilde{\mathbf{U}}\right)\right)+\sigma_{k_p}^2\right)\\ &\quad\ge\Pr\left(\frac{P_p}{\beta}|g_{k_p}|^2\le\mathrm{tr}(\mathbf{F}_{k_p})\lambda_{\min}(\mathbf{A})+\sigma_{k_p}^2\right)\ge\tilde{\epsilon}.\end{aligned} \tag{76}$$

Let $x=\mathrm{tr}(\mathbf{F}_{k_p})=\mathrm{tr}(|\mathbf{f}_{k_g}|^2)$. Then, x follows a chi-squared distribution since $|\mathbf{f}_{k_g}|^2$ is a sum of squares of N independent Gaussian random variables. Correspondingly, the probability density function (PDF) of x is given as $f_X(x)=\frac{e^{-x}x^{N-1}}{\Gamma(N)}$. Let $y=\frac{P_p}{\beta}|g_{k_p}|^2$, and it then follows an exponential distribution with the PDF as $f_Y(y)=\frac{\beta}{P_p}e^{-\frac{\beta}{P_p}y}$. Therefore, the probability in (76) is obtained as

$$\begin{aligned}&\Pr\left(y\le x\lambda_{\min}(\mathbf{A})+\sigma_{k_p}^2\right)\ge\tilde{\epsilon}\\ &\quad\Leftrightarrow\int_0^{\infty}\int_0^{x\lambda_{\min}(\mathbf{A})+\sigma_{k_p}^2}f_X(x)f_Y(y)dydx\ge\tilde{\epsilon}\\ &\quad\Leftrightarrow\int_0^{\infty}\left(1-\exp\left(-\frac{\beta}{P_p}(x\lambda_{\min}(\mathbf{A})+\sigma_{k_p}^2)\right)\right)f_X(x)dx\ge\tilde{\epsilon}\\ &\quad\overset{(a)}{\Leftrightarrow}1-\exp\left(-\frac{\beta}{P_p}\sigma_{k_p}^2\right)\left[\frac{\beta}{P_p}\lambda_{\min}(\mathbf{A})+1\right]^{-N}\ge\tilde{\epsilon}\end{aligned} \tag{77}$$

where (a) is obtained using [47, eq. (3.351.3)]. Next, the constraint in (26g) for K_p links is given as

$$\begin{aligned}&(26g)\Leftrightarrow\\ &\quad\prod_{k_p=1}^{K_p}\Pr\left(\frac{P_p|g_{k_p}|^2}{\sum_{g=1}^{G}\mathrm{tr}(\mathbf{F}_{k_p}\widetilde{\mathbf{W}}_g)+\mathrm{tr}(\mathbf{F}_{k_p}\widetilde{\mathbf{U}})+\sigma_{k_p}^2}\le\beta\right)\ge\tilde{\epsilon}\\ &\quad\overset{(b)}{\Leftrightarrow}1-\exp\left(-\frac{\beta}{P_p}\sigma_{k_p}^2\right)\left[\frac{\beta}{P_p}\lambda_{\min}(\mathbf{A})+1\right]^{-N}\ge\tilde{\epsilon}^{1/K_p}\\ &\quad\Leftrightarrow\lambda_{\min}(\mathbf{A})\ge\left[\exp\left(-\frac{\beta}{NP_p}\sigma_{k_p}^2\right)/(1-\tilde{\epsilon}^{1/K_p})^{1/N}-1\right]\frac{P_p}{\beta}\end{aligned} \tag{78}$$

where (b) is obtained by combining (77) since the channels of K_p passive Eves are independent and modeled as i.i.d. random variables.

Appendix D
Proof of Lemma 4

The constraint in (26c) can be rewritten for each k_g link as

$$\Pr\left(P_p\phi_g|f_{k_g}|^2\ge\mathrm{tr}\left(\mathbf{G}_{k_g}\left(\widetilde{\mathbf{W}}_g-\phi_g\sum_{i=1,i\ne g}^{G}\widetilde{\mathbf{W}}_i-\phi_g\widetilde{\mathbf{U}}\right)\right)-\sigma_{k_g}^2\phi_g\right)\ge\epsilon_g \tag{79}$$

where $\mathbf{G}_{k_g}\triangleq\mathbf{g}_{k_g}\mathbf{g}_{k_g}^H$ for all k_g. For any given $N\times N$ Hermitian matrix $\mathbf{B}$, it follows from [46] that

$$\begin{aligned}\mathrm{tr}(\mathbf{G}_{k_g}\mathbf{B}) &\le \sum_{i=1}^{N}\lambda_i(\mathbf{G}_{k_g})\lambda_i(\mathbf{B})\\ &= \lambda_{\max}(\mathbf{G}_{k_g})\lambda_{\max}(\mathbf{B})\\ &= \mathrm{tr}(\mathbf{G}_{k_g})\lambda_{\max}(\mathbf{B}).\end{aligned} \tag{80}$$

Substituting (75) and (80) into (79), we have

$$\Pr\left(P_p\phi_g|f_{k_g}|^2\ge\mathrm{tr}\left(\mathbf{G}_{k_g}\left(\widetilde{\mathbf{W}}_g-\phi_g\sum_{i=1,i\ne g}^{G}\widetilde{\mathbf{W}}_i-\phi_g\widetilde{\mathbf{U}}\right)\right)-\sigma_{k_g}^2\phi_g\right)$$

$$\geq \Pr\left(P_p\phi_g|f_{k_g}|^2 \geq \mathrm{tr}(\mathbf{G}_{k_g})\left[\left\|\mathbf{w}_g\right\|^2 - \phi_g\sum_{i=1,i\neq g}^{G}\|\mathbf{w}_i\|^2 - \phi_g\lambda_{\min}(\widetilde{\mathbf{U}})\right] - \sigma_{k_g}^2\phi_g\right) \geq \epsilon_g. \tag{81}$$

Following similar steps to the proof of Lemma 3, we can obtain

$$\begin{aligned}
&\frac{\left\|\mathbf{w}_g\right\|^2}{\phi_g} - \sum_{i=1,i\neq g}^{G}\|\mathbf{w}_i\|^2 - \lambda_{\min}(\widetilde{\mathbf{U}}) \\
&\qquad \leq \left[\exp\left(\frac{\sigma_{k_g}^2}{NP_p}\right)\epsilon_g^{-1/NK_g} - 1\right]P_p \\
\Leftrightarrow\ &\frac{\left\|\mathbf{w}_g\right\|^2}{\phi_g} \leq \left[\exp\left(\frac{\sigma_{k_g}^2}{NP_p}\right)\epsilon_g^{-1/NK_g} - 1\right]P_p \\
&\qquad + \sum_{i=1,i\neq g}^{G}\|\mathbf{w}_i\|^2 + \lambda_{\min}(\widetilde{\mathbf{U}})
\end{aligned} \tag{82}$$

which completes the proof.

REFERENCES

[1] V.-D. Nguyen, T. Q. Duong, O.-S. Shin, A. Nallanathan, and G. K. Karagiannidis, "Robust beamforming for secrecy rate in cooperative cognitive radio multicast communications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[4] S. K. L.-Y. Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[6] E. Tekin and A. Yener, "The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, Jun. 2008.

[7] S. Anand and R. Chandramouli, "On the location of an eavesdropper in multiterminal networks," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 1, pp. 148–157, Mar. 2010.

[8] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Oct. 2009, pp. 1134–1141.

[9] A. Mukherjee and A. L. 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.

[10] 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.

[11] 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.

[12] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[13] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[14] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[15] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[16] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 1–6.

[17] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170–2181, Apr. 2016.

[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.

[20] 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. 24, pp. 6391–6401, Dec. 2014.

[21] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.

[22] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2609–2633, Nov. 2016.

[23] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication in multiantenna cognitive radio networks with imperfect channel state information," *IEEE Trans. Signal Process.*, vol. 59, no. 4, pp. 1683–1693, Apr. 2011.

[24] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[25] F. Gabry *et al.*, "Cooperation for secure broadcasting in cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Ottawa, ON, Canada, Jun. 2012, pp. 5613–5618.

[26] Y. Y. He, J. Evans, and S. Dey, "Secrecy rate maximization for cooperative overlay cognitive radio networks with artificial noise," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 1663–1668.

[27] V.-D. Nguyen, T. M. Hoang, and O.-S. Shin, "Secrecy capacity of the primary system in a cognitive radio network," *IEEE Trans. Veh. Technol.*, vol. 64, no. 8, pp. 3834–3843, Aug. 2015.

[28] F. Zhu and M. Yao, "Improving physical-layer security for CRNs using SINR-based cooperative beamforming," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1835–1841, Mar. 2016.

[29] V.-D. Nguyen, T. Q. Duong, and O.-S. Shin, "Physical layer security for primary system: A symbiotic approach in cooperative cognitive radio networks," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[30] Y. Liang, A. Somekh-Baruch, H. V. Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, Feb. 2009.

[31] H. G. Bafghi, S. Salimi, B. Seyfe, and M. R. Aref, "Cognitive interference channel with two confidential messages," in *Proc. Int. Symp. Inf. Theory Appl. (ISITA)*, Taichung, Taiwan, Oct. 2010, pp. 952–956.

[32] R. K. Farsani and R. Ebrahimpour, "Capacity theorems for the cognitive radio channel with confidential messages," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, Jun. 2014, pp. 1416–1420.

[33] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

[34] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[35] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–12, Oct. 2009.

[36] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[37] 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.

[38] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4599–4615, Aug. 2014.

[39] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization* (MPS-SIAM Series on Optimization). Philadelphia, PA, USA: SIAM, 2001.
[40] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2007.
[41] A. Ben-Tal, L. E. Ghaoui, and A. Nemirovski, *Robust Optimization*. Princeton, NJ, USA: Princeton Univ. Press, 2009.
[42] B. R. Marks and G. P. Wright, "A general inner approximation algorithm for nonconvex mathematical programs," *Oper. Res.*, vol. 26, no. 4, pp. 681–683, Jul./Aug. 1978.
[43] K. C. Toh, M. J. Todd, and R. H. Tütüncü, "SDPT3—A MATLAB software package for semidefinite programming, version 1.3," *Optim. Methods Softw.*, vol. 11, nos. 1–4, pp. 545–581, Jan. 1999.
[44] H. Tuy, *Convex Analysis and Global Optimization*. Dordrecht, The Netherlands: Kluwer Acad., 2001.
[45] V.-D. Nguyen, T. Q. Duong, H. D. Tuan, O.-S. Shin, and H. V. Poor, "Spectral and energy efficiencies in full-duplex wireless information and power transfer," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2220–2233, May 2017.
[46] J. B. Lasserre, "A trace inequality for matrix product," *IEEE Trans. Autom. Control*, vol. 40, no. 8, pp. 1500–1501, Aug. 1995.
[47] I. S. Gradshteyn and I. M. Ryzhik, *Tables of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic Press, 2007.

Van-Dinh Nguyen (S'14) received the B.S. degree in telecommunications from the Ho Chi Minh City University of Technology (Bach Khoa University), Vietnam, in 2012 and the M.S. degree in electronic engineering from Soongsil University, Seoul, South Korea, in 2015, where he is currently pursuing the Ph.D. degree in electronic engineering. He was a visiting student with Queen's University Belfast, U.K. in 2015, for two months and in 2016, for a month. His research interests include wireless communications, physical layer security, cognitive radio, and nonorthogonal multiple access.

Trung Q. Duong (S'05–M'12–SM'13) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden, in 2012. Since 2013, he has been with Queen's University Belfast, U.K., as a Lecturer (Assistant Professor). He has authored or co-authored over 270 technical papers published in scientific journals (145 articles) and presented at international conferences (125 papers). His current research interests include small-cell networks, ultradense networks, physical layer security, energy-harvesting communications, and massive MIMO.

He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON COMMUNICATIONS, and the *IET Communications*, and a Senior Editor for the IEEE COMMUNICATIONS LETTERS. He was a recipient of the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, the IEEE International Conference on Communications (ICC) 2014, the IEEE Global Communications Conference (GLOBECOM) 2016, and the Prestigious Royal Academy of Engineering Research Fellowship from 2016 to 2021.

Oh-Soon Shin (S'00–M'10) received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, South Korea, in 1998, 2000, and 2004, respectively. From 2004 to 2005, he was with the Division of Engineering and Applied Sciences, Harvard University, MA, USA, as a Post-Doctoral Fellow. From 2006 to 2007, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. In 2007, he joined the School of Electronic Engineering, Soongsil University, Seoul, where he is currently an Associate Professor. His research interests include communication theory, wireless communication systems, and signal processing for communication.

Arumugam Nallanathan (S'97–M'00–SM'05–F'17) has been a Professor of wireless communications with the School of Electronic Engineering and Computer Science, Queen Mary University of London since 2017. He was with the Department of Informatics, King's College London from 2007 to 2017, where he was a Professor of wireless communications from 2013 to 2017. He was an Assistant Professor with the Department of Electrical and Computer Engineering, National University of Singapore from 2000 to 2007. His research interests include 5G wireless networks, Internet of Things, and molecular communications. He published over 350 technical papers in scientific journals and international conferences. He was a co-recipient of the Best Paper Award presented at the IEEE International Conference on Communications 2016 (ICC 2016) and IEEE International Conference on Ultra-Wideband 2007 (ICUWB 2007). He is an IEEE Distinguished Lecturer. He has been selected as a Web of Science (ISI) Highly Cited Researcher in 2016.

He was a recipient of the IEEE Communications Society SPCE Outstanding Service Award 2012 and IEEE Communications Society RCC Outstanding Service Award 2014. He is an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS and the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. He was an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2006 to 2011, the IEEE WIRELESS COMMUNICATIONS LETTERS and the IEEE SIGNAL PROCESSING LETTERS. He served as the Chair for the Signal Processing and Communication Electronics Technical Committee of IEEE Communications Society and a Technical Program Chair and a member of Technical Program Committees in numerous IEEE conferences.

George K. Karagiannidis (M'96–SM'03–F'14) was born in Pithagorion, Samos Island, Greece. He received the University Diploma and Ph.D. degrees in electrical and computer engineering from the University of Patras, in 1987 and 1999, respectively. From 2000 to 2004, he was a Senior Researcher with the Institute for Space Applications and Remote Sensing, National Observatory of Athens, Greece. In 2004, he joined the Faculty of Aristotle University of Thessaloniki, Greece, where he is currently a Professor with the Electrical and Computer Engineering Department and the Director of Digital Telecommunications Systems and Networks Laboratory. He is also a Honorary Professor with South West Jiaotong University, Chengdu, China.

His research interests are in the broad area of digital communications systems and signal processing, with emphasis on wireless communications, optical wireless communications, wireless power transfer and applications, molecular and nanoscale communications, stochastic processes in biology and wireless security. He has authored or co-authored over 400 technical papers published in scientific journals and presented at international conferences. He has also authored the Greek edition of a book entitled *Telecommunications Systems* and co-authored the book entitled *Advanced Optical Wireless Communications Systems* (Cambridge Publications, 2012).

Dr. Karagiannidis has been involved as a general chair, a technical program chair, and a technical program committee member in several IEEE and non-IEEE conferences. In the past, he was an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS, a Senior Editor of the IEEE COMMUNICATIONS LETTERS, an Editor of the *EURASIP Journal of Wireless Communications and Networks* and several times Guest Editor in the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. From 2012 to 2015, he was the Editor-in Chief of the IEEE COMMUNICATIONS LETTERS.

He was a recipient of the 2015 and 2016 Thomson Reuters HighlyCited Researcher Award and one of the highlycited authors across all areas of electrical engineering.