Secrecy Rate Maximization For Cooperative Overlay Cognitive Radio Networks with Artificial Noise

YuanYuan He†, Jamie Evans†, and Subhrakanti Dey‡
† Electrical and Computer Systems Engineering, Monash University, Melbourne, Australia
‡ Signals and Systems, Uppsala University, Uppsala, Sweden
e-mail: †{katrina.he, jamie.evans}@monash.edu, ‡Subhra.Dey@signal.uu.se

***Abstract*—We consider physical-layer security in a novel MISO cooperative overlay cognitive radio network (CRN) with a single eavesdropper. We aim to design an artificial noise (AN) aided secondary transmit strategy to maximize the joint achievable secrecy rate of both primary and secondary links, subject to a global secondary transmit power constraint and guaranteeing any transmission of secondary should at least not degrade the receive quality of primary network, under the assumption that global CSI is available. The resulting optimization problem is challenging to solve due to its non-convexity in general. A computationally efficient approximation methodology is proposed based on the semidefinite relaxation (SDR) technique and followed by a two-step alternating optimization algorithm for obtaining a local optimum for the corresponding SDR problem. This optimization algorithm consists of a one-dimensional line search and a non-convex optimization problem, which, however, through a novel reformulation, can be approximated as a convex semidefinite program (SDP). Analysis on the extension to multiple eavesdroppers scenario is also provided. Simulation results show that the proposed AN-aided joint secrecy rate maximization design (JSRMD) can significantly boost the secrecy performance over JSRMD without AN.**

***Index Terms*—Overlay Cognitive Radio, physical-layer security, amplify-and-forward relaying, artificial interference, semidefinite relaxation**

I. Introduction

Cognitive radio (CR) has been promoted as a promising technology to dramatically improve the efficiency of spectral utilization. The key idea of CR is to allow unlicensed/secondary users (SUs) to access the frequency spectrum originally licensed to primary users (PUs), as long as the transmission of SUs does not generate adverse impact on the PUs' performance. Here we consider the overlay paradigm of the cognitive radio network (CRN) [1], where the primary network leases part of its channel access time to SUs to simultaneously share the spectrum. In return, the SUs assign part of their power to cooperatively assist (relay) the PUs' transmission [1][2][3][4], in order to at least offset the harmful interference on the PUs caused by SUs' transmission [1]. As a result, by SUs' cooperative relaying, the achievable rate or reliability of the primary network can be significantly improved [2][3] or can be kept unchanged [4]; while the SUs gain opportunities to access the spectrum for their own data transmission.

To achieve secure communication, physical-layer security (PLS) approaches have been receiving growing attention recently [5]-[14]. The fundamental basis of PLS was proposed in the seminal work [5], which showed that it is possible to perfectly prevent eavesdroppers from overhearing/interpreting confidential messages purely by physical-layer transmit designs, without relying on traditional complex key encryption technqiues. An important performance measure for PLS is called the 'secrecy capacity', defined by [5] as the maximum achievable rate that can guarantee reliable communication while keeping eavesdroppers in complete ignorance. To achieve a positive secrecy rate, the channel condition of the legitimate receivers needs to be better than that of eavesdroppers [5][6], which, however, may not be always possible in practice. To overcome this limitation, multiple antennas based transmission techniques can be employed by leveraging spatial degree of freedom (DoF) to weaken the eavesdroppers' received signal quality substantially [7][8]. Another effective tool to enhance secrecy capacity is artificial noise (AN). In AN-aided systems, the transmitters allocate portion of their power to send artificially generated noise (jamming signal) to deliberately cause interference at the eavesdropper receivers. With known eavesdroppers' CSI (ECSI), the authors of [10][11] showed that generating spatially selective AN can gain a better secrecy rate than keeping AN isotropic (normally used when no ECSI is available). In addition, the role of inactive nodes acting as jamming helpers by transmitting AN to confuse the eavesdroppers has also been investigated in [9][12][14][21].

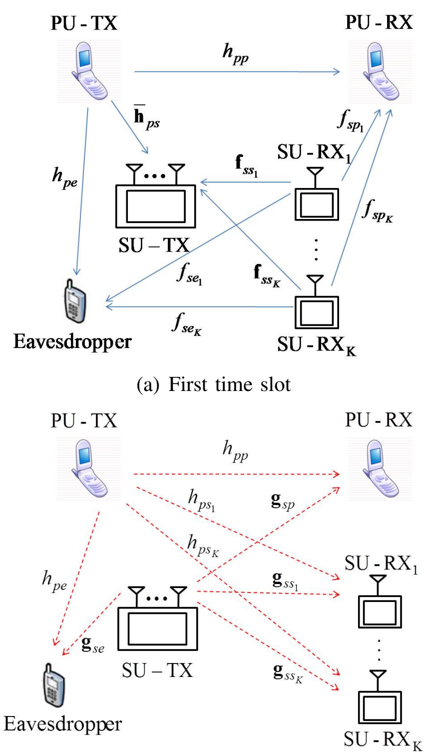
Secure transmission techniques have also been investigated in CRNs. In [15], the authors considered a secondary secrecy capacity maximization problem for a MISO undelay CRN, while, a primary secrecy rate maximization problem for a more general MISO underlay CRN was studied in [17]. In [16], the authors proposed an alternative implementation of the concept of spectrum leasing via cooperation, where, unlike the overlay CRN, SUs do not relay PUs' message but act as a helper to improve the primary secrecy rate. However, to the best of our knowledge, secrecy issues for cooperative-relaying-based overlay CRN have not yet been explored in the literature. This motivates the study presented in this paper.

We propose a novel secure MISO cooperative overlay CRN scheme with aid of AN in the presence of a single eavesdropper, where a single-antenna primary transmitter-receiver pair gives out half of its channel access time to share the spectrum with a multiple-antenna secondary transmitter (SU-TX) for delivering the secondary data to K single-antenna secondary receivers (SU-RXs), in exchange for secondary cooperation to relay primary's data using the amplify and forward (AF) scheme and protect the secrecy of both primary and secondary links. The key contributions of this paper are listed below: (1) Inspired by the non-CR secure networks [14][21], in order to confuse the eavesdroppers as much as possible, the proposed overlay scheme incorporates AN by letting both of SU-RXs and SU-TX alternately jam the eavesdropper in different phases of the AF scheme. More specifically, SU-RXs are employed as jamming helpers in the first time slot, while in the second time slot, apart from relaying primary data and transmitting secondary data, the SU-TX also assigns part of the total secondary transmit power to simultaneously send certain amount of spatially selective AN. (2) Unlike existing

978-1-4799-2003-7/14/$31.00 ©2014 IEEE

work on CRN security which only focused on improving either primary secrecy rate or secondary secrecy rate, we consider the scenario where both primary and secondary messages must be kept confidential from the eavesdroppers. (3) The proposed overlay scheme advocates joint design of secondary transmit beamforming for relaying primary information, transmit beamforming for secondary's own data, spatial AN covariance at the SU-TX, as well as transmit beamforming weights at SU-RXs, to maximize the joint achievable secrecy rate of both primary and secondary links, subject to a global secondary transmit power constraint and the constraint that any SU transmission should not degrade the received signal quality of the PU-RX, under the assumption that global CSI is available. (4) Our formulated optimization problem is non-convex in general. We propose a computationally efficient approximation algorithm based on a semidefinite relaxation (SDR) technique, where a local optimum of the associated SDR problem can be obtained by a two-step alternating optimization algorithm consisting of a one-dimensional line search and a non-convex optimization problem, which, however, can be approximated as a convex semidefinite program (SDP) via a novel reformulation and application of a "Sequential Parametric Convex Approximation Method". (5) An analysis on the extension to the multiple eavesdroppers scenario is also provided.

II. System Model and Problem Formulation



(a) First time slot

(b) Second time slot

Fig. 1. System model of AN-aided cooperative overlay CRN

We consider a CRN consisting of a PU-TX, a PU-RX, a SU-TX, K SU-RXs ($K \geq 2$) and an eavesdropper, where the SU-TX is equipped with M transmit antennas ($M > K$) and all other terminals have a single antenna, and each node operates in a half-duplex mode. To allow for efficient spectrum sharing between PUs and SUs, a cooperative overlay CRN paradigm with a two-phase transmission scheme is considered as illustrated in Fig.1, where the PUs lease half of its time slot to the SU to transmit its own data via the spectrum band owned by the PU. In exchange, SU-TX has to employ part of its power to relay the PU-TX's message to at least offset the resulting interference to PU-RX and while also preventing the eavesdropper from decoding the messages from both PU-TX and SU-TX by transmitting AN. More specifically, (1) in the first time slot, the PU-TX transmits its signal to the PU-RX, and the SU-TX listens to the primary transmission and obtains the primary signal. Since SU-RXs are normally inactive in the first time slot, here they are employed as temporary jamming helpers to further confuse the eavesdropper [12]. (2) In the second time slot, in addition to the PU-TX's transmission, the SU-TX relays the primary signal and simultaneously transmits its own data and AN.

All channels involved are assumed to be independent and identically distributed (i.i.d.) and undergo quasi-static flat fading. The channel coefficients from PU-TX to PU-RX, PU-TX to the eavesdropper, PU-TX to the i^{th} SU-RXs (represented as SU-RX$_i$, $\forall i = 1, \ldots, K$), SU-RX$_i$ to PU-RX, and SU-RX$_i$ to the eavesdropper, are denoted by the complex scalars $h_{pp}, h_{pe}, h_{ps_i}, f_{sp_i}$ and f_{se_i}, respectively. The $1 \times M$ complex channel vectors from the PU-TX to the SU-TX, and SU-RX$_i$ to the SU-TX are represented by $\bar{\mathbf{h}}_{ps}$ and $\mathbf{f}_{ss_i}, i = 1, \ldots, K$, respectively. Let $\mathbf{g}_{sp} \in \mathbb{C}^{M \times 1}$, $\mathbf{g}_{ss_i} \in \mathbb{C}^{M \times 1}, \forall i = 1, \ldots, K$, and $\mathbf{g}_{se} \in \mathbb{C}^{M \times 1}$ indicate the complex channel vectors from SU-TX to PU-RX, SU-TX to SU-RX$_i$, $\forall i = 1, \ldots, K$, and SU-TX to the eavesdropper, respectively. Thus, the received signals at the PU-RX, the eavesdropper and the SU-TX in the first time slot, are given, respectively, as,

$$
\begin{aligned}
y_{p,1} &= \sqrt{P_p} h_{pp} s_p + \sum_{i=1}^{K} f_{sp_i} \phi_i \bar{z} + n_p, \\
y_{e,1} &= \sqrt{P_p} h_{pe} s_p + \sum_{i=1}^{K} f_{se_i} \phi_i \bar{z} + n_e, \\
\mathbf{y}_{ST} &= \sqrt{P_p} \bar{\mathbf{h}}_{ps}^{\mathcal{H}} s_p + \sum_{i=1}^{K} \mathbf{f}_{ss_i}^{\mathcal{H}} \phi_i \bar{z} + \mathbf{n}_{ST},
\end{aligned} \tag{1}
$$

where ${}^{\mathcal{H}}$ denotes the Hermitian transpose; s_p denotes the primary transmit symbol with $E[|s_p|^2] = 1$; P_p is the transmit power of PU-TX; $\bar{z} \sim \mathcal{CN}(0, 1)$, is a common jamming signal transmitted by each SU-RXs with complex weights $\phi_1, \ldots, \phi_K$, respectively [13][22], to confuse the eavesdroppers in the first time slot. N_p, n_e and $\mathbf{n}_{ST}$ denote the additive white noise at the PU-RX, the eavesdropper and the SU-TX, respectively, and are modelled as $n_p \sim \mathcal{CN}(0, \sigma^2)$, $n_e \sim \mathcal{CN}(0, \sigma^2)$ and $\mathbf{n}_{ST} \sim \mathcal{CN}(0, \sigma^2 \mathrm{I}_M)$. Since the received primary signal at the SU-TX is contaminated by jamming signals from SU-RXs, a pre-filtering weight vector $\mathbf{u} \in \mathbb{C}^{M \times 1}$ is applied to the received signal $\mathbf{y}_{ST}$ at the SU-TX to null out these undesirable jamming signals, resulting in the recovered primary signal $y_{st} = \mathbf{u}^{\mathcal{H}} \mathbf{y}_{ST} = \sqrt{P_p} \mathbf{u}^{\mathcal{H}} \bar{\mathbf{h}}_{ps}^{\mathcal{H}} s_p + \mathbf{u}^{\mathcal{H}} \mathbf{n}_{ST}$, where $\mathbf{u}$ can be chosen to be $\mathbf{u} = \underset{\mathbf{u}}{\text{argmax}} \ |\mathbf{u}^{\mathcal{H}} \bar{\mathbf{h}}_{ps}^{\mathcal{H}}|^2$, subject to $\mathbf{u}^{\mathcal{H}} \mathbf{f}_{ss_i}^{\mathcal{H}} = 0 \ \forall i = 1, \ldots, K$; and $|\mathbf{u}|^2 = 1$. Let $\bar{\mathbf{F}}_{ss} \in \mathbb{C}^{M \times K} \triangleq [\mathbf{f}_{ss_1}^{\mathcal{H}}, \ldots, \mathbf{f}_{ss_K}^{\mathcal{H}}]$. Then according to [13], the optimal solution for $\mathbf{u}$ is given by $\mathbf{u} = \frac{(\mathbf{I}_M - \bar{\mathbf{F}}_{ss}(\bar{\mathbf{F}}_{ss}^{\mathcal{H}} \bar{\mathbf{F}}_{ss})^{-1} \bar{\mathbf{F}}_{ss}^{\mathcal{H}}) \bar{\mathbf{h}}_{ps}^{\mathcal{H}}}{||(\mathbf{I}_M - \bar{\mathbf{F}}_{ss}(\bar{\mathbf{F}}_{ss}^{\mathcal{H}} \bar{\mathbf{F}}_{ss})^{-1} \bar{\mathbf{F}}_{ss}^{\mathcal{H}}) \bar{\mathbf{h}}_{ps}^{\mathcal{H}}||}$. Note that if SU-RXs are inactive in the first time slot, then $\mathbf{u}$ reduces to $\mathbf{u} = \frac{\bar{\mathbf{h}}_{ps}^{\mathcal{H}}}{||\bar{\mathbf{h}}_{ps}^{\mathcal{H}}||}$.

In the second time slot, an amplify-and-forward (AF) scheme is employed at the SU-TX for relaying the primary signal.

Similar to [3], the SU-TX first normalizes the received primary signal y_{st} by scaling it with the normalization factor $c_p = \frac{1}{\sqrt{\mathbf{u}^{\mathcal{H}}(P_p\overline{\mathbf{h}}_{ps}^{\mathcal{H}}\overline{\mathbf{h}}_{ps}+\sigma^2\mathbf{I}_M)\mathbf{u}}}$, so that $s_p' = c_p y_{st} = c_p\sqrt{P_p}\mathbf{u}^{\mathcal{H}}\overline{\mathbf{h}}_{ps}^{\mathcal{H}}s_p + c_p\mathbf{u}^{\mathcal{H}}\mathbf{n}_{ST}$ satisfies $E[|s_p'|^2] = 1$. Then it concurrently transmits both the primary stream s_p' re-encoded with a beamforming vector $\mathbf{w} \in \mathbb{C}^{M\times 1}$ and the secondary's own data stream $\{s_{s_1}, \ldots, s_{s_K}\}$, where s_{s_i} is the transmit symbol intended for SU-RX$_i$ and $E[|s_{s_i}|^2] = 1$, precoded by a beamforming vector $\mathbf{v}_i \in \mathbb{C}^{M\times 1}$, $i = 1, \ldots, K$ [3] [4]. Meanwhile, in order to confuse the eavesdropper, SU-TX also emits a jamming vector (AN) [10][14]. Thus, the resulting transmit signal vector ($M \times 1$) at the SU-TX is given by $\mathbf{x} = \mathbf{w}s_p' + \sum_{i=1}^K \mathbf{v}_i s_{s_i} + \mathbf{z}$, where $\mathbf{z} \in \mathbb{C}^{M\times 1} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_z)$ is the AN with covariance $\mathbf{Q}_z = E[\mathbf{z}\mathbf{z}^{\mathcal{H}}]$. And the transmit power of SU-TX can be expressed as $|\mathbf{w}|^2 + \sum_{i=1}^K |\mathbf{v}_i|^2 + \text{Tr}(\mathbf{Q}_z)$. Accordingly, in this subslot, the signals received at the PU-RX, the eavesdropper and each SU-RXs from both PU-TX and SU-TX, can thus be written as,

$$
\begin{aligned}
y_{p,2} =& \sqrt{P_p}\left(h_{pp} + q\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}\right)s_p + c_p\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}\mathbf{u}^{\mathcal{H}}\mathbf{n}_{ST} \\
&+ \sum_{i=1}^K \mathbf{g}_{sp}^{\mathcal{H}}\mathbf{v}_i s_{s_i} + \mathbf{g}_{sp}^{\mathcal{H}}\mathbf{z} + n_p, \\
y_{e,2} =& \sqrt{P_p}\left(h_{pe} + q\mathbf{g}_{se}^{\mathcal{H}}\mathbf{w}\right)s_p + c_p\mathbf{g}_{se}^{\mathcal{H}}\mathbf{w}\mathbf{u}^{\mathcal{H}}\mathbf{n}_{ST} \\
&+ \sum_{i=1}^K \mathbf{g}_{se}^{\mathcal{H}}\mathbf{v}_i s_{s_i} + \mathbf{g}_{se}^{\mathcal{H}}\mathbf{z} + n_e, \\
y_{s_i} =& \sqrt{P_p}\left(h_{ps_i} + q\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}\right)s_p + c_p\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}\mathbf{u}^{\mathcal{H}}\mathbf{n}_{ST} \\
&+ \mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{v}_i s_{s_i} + \sum_{j=1, j\neq i}^K \mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{v}_j s_{s_j} + \mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{z} + n_{s_i}, \\
& \qquad i = 1, \ldots, K \qquad (2)
\end{aligned}
$$

where $q = c_p\mathbf{u}^{\mathcal{H}}\overline{\mathbf{h}}_{ps}^{\mathcal{H}}$ and $n_{s_i} \sim \mathcal{CN}(0, \sigma^2)$ is the additive white Gaussian noise at the SU-RX$_i$, $i = 1, \ldots, K$.

Let $\boldsymbol{\phi}^{\mathcal{H}} \in \mathbb{C}^{1\times K} \triangleq \{\phi_1, \ldots, \phi_K\}$, $\mathbf{f}_{sp} \in \mathbb{C}^{K\times 1} \triangleq \{f_{sp_1}, \ldots, f_{sp_K}\}^T$ and $\mathbf{f}_{se} \in \mathbb{C}^{K\times 1} \triangleq \{f_{se_1}, \ldots, f_{se_K}\}^T$. All the SU-RXs, PU-RX and eavesdropper only decode their desirable signals and treat the remaining interference as noise. The eavesdropper is interested in both the primary and secondary signals. Then based on (1) and (2), the achievable rate at the PU-RX and the eavesdropper are correspondingly given as [20][21][3],

$$
\begin{aligned}
R_p =& \frac{1}{2}\log\left(1 + \frac{P_p|h_{pp}|^2}{\sigma^2 + |\boldsymbol{\phi}^{\mathcal{H}}\mathbf{f}_{sp}|^2}\right. \\
&\left. + \frac{P_p|h_{pp} + q\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2}{\sigma^2(1 + c_p^2|\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2) + \sum_{i=1}^K |\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{v}_i|^2 + \mathbf{g}_{sp}^{\mathcal{H}}\mathbf{Q}_z\mathbf{g}_{sp}}\right), \\
R_e =& \frac{1}{2}\log\left(1 + \frac{P_p|h_{pe}|^2}{\sigma^2 + |\boldsymbol{\phi}^{\mathcal{H}}\mathbf{f}_{se}|^2}\right. \\
&\left. + \frac{P_p|h_{pe} + q\mathbf{g}_{se}^{\mathcal{H}}\mathbf{w}|^2 + \sum_{i=1}^K |\mathbf{g}_{se}^{\mathcal{H}}\mathbf{v}_i|^2}{\sigma^2(1 + c_p^2|\mathbf{g}_{se}^{\mathcal{H}}\mathbf{w}|^2) + \mathbf{g}_{se}^{\mathcal{H}}\mathbf{Q}_z\mathbf{g}_{se}}\right) \qquad (3)
\end{aligned}
$$

where the scalar factor $\frac{1}{2}$ is added due to the two-phase transmission process. The sum rate of secondary network is given by

$$
R_s^{\text{sum}} = \sum_{i=1}^K \frac{1}{2}\log\left(1 + \frac{|\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{v}_i|^2}{Y(\mathbf{w}) + \sum_{j\neq i}^K |\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{v}_j|^2 + \mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{Q}_z\mathbf{g}_{ss_i}}\right), \qquad (4)
$$

where $Y(\mathbf{w}) \triangleq \sigma^2(1 + c_p^2|\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}|^2) + P_p|h_{ps_i} + q\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}|^2$.

Therefore, the secrecy rate maximization problem for our overlay CRN can be formulated as,

$$
\begin{aligned}
\underset{\mathbf{w}, \{\mathbf{v}_i\}_{i=1}^K, \mathbf{Q}_z \succeq 0, \boldsymbol{\phi}}{\text{maximize}} \quad & R_{\text{secrecy}} = [R_p + R_s^{\text{sum}} - R_e]^+ \\
\text{subject to} \quad & \frac{P_p|h_{pp}|^2}{\sigma^2} \leq \frac{P_p|h_{pp}|^2}{\sigma^2 + |\boldsymbol{\phi}^{\mathcal{H}}\mathbf{f}_{sp}|^2}, \qquad (5a)
\end{aligned}
$$

$$
\frac{P_p|h_{pp}|^2}{\sigma^2} \leq \frac{P_p|h_{pp} + q\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2}{\sigma^2(1 + c_p^2|\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2) + \sum_{i=1}^K |\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{v}_i|^2 + \mathbf{g}_{sp}^{\mathcal{H}}\mathbf{Q}_z\mathbf{g}_{sp}}, \qquad (5b)
$$

$$
|\mathbf{w}|^2 + \sum_{i=1}^K |\mathbf{v}_i|^2 + \text{Tr}(\mathbf{Q}_z) + |\boldsymbol{\phi}|^2 \leq P_s. \qquad (5c)
$$

Note that the secrecy rate must be non-negative, otherwise the secondary network will not transmit. Constraints (5a) and (5b) guarantee that at each time slot, the transmission of secondary network should at least not degrade the received SINR at the PU-RX. (5c) is the global secondary transmit power constraint and P_s is the maximum transmit power of the secondary network. Obviously, constraint (5a) can be written as $|\boldsymbol{\phi}^{\mathcal{H}}\mathbf{f}_{sp}|^2 = 0$, which implies zero jamming interference at the PU-TX in the first time slot. Problem (5) is nonconvex in general and thus it is very difficult to find its globally optimal solution. However, (5) can be rewritten as a nonconvex quadratic optimization problem and the semidefinite relaxation (SDR) technique [23] can be applied to obtain a computationally efficient approximate algorithm for solving Problem (5).

III. An SDR-based Approach for the overlay CRN Secrecy Rate Maximization Problem

Let $\mathbf{G}_{ss_i} = \mathbf{g}_{ss_i}\mathbf{g}_{ss_i}^{\mathcal{H}}, \forall i = 1, \ldots, K$, $\mathbf{G}_{se} = \mathbf{g}_{se}\mathbf{g}_{se}^{\mathcal{H}}$, $\mathbf{G}_{sp} = \mathbf{g}_{sp}\mathbf{g}_{sp}^{\mathcal{H}}$, and $\overline{\mathbf{w}}^{\mathcal{H}} = [\mathbf{w}^{\mathcal{H}}, 1]$, then $|h_{pp} + q\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2$, $|h_{ps_i} + q\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}|^2$ and $|h_{pp} + q\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2$ can be expressed as,

$$
\begin{aligned}
|h_{pp} + q\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2 &= \overline{\mathbf{w}}^{\mathcal{H}}\begin{bmatrix} q^2\mathbf{G}_{sp} & qh_{pp}\mathbf{g}_{sp} \\ qh_{pp}^{\mathcal{H}}\mathbf{g}_{sp}^{\mathcal{H}} & |h_{pp}|^2 \end{bmatrix}\overline{\mathbf{w}} \\
&\triangleq \overline{\mathbf{w}}^{\mathcal{H}}\mathbf{A}_p\overline{\mathbf{w}} \\
|h_{ps_i} + q\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}|^2 &= \overline{\mathbf{w}}^{\mathcal{H}}\begin{bmatrix} q^2\mathbf{G}_{ss_i} & qh_{ps_i}\mathbf{g}_{ss_i} \\ qh_{ps_i}^{\mathcal{H}}\mathbf{g}_{ss_i}^{\mathcal{H}} & |h_{ps_i}|^2 \end{bmatrix}\overline{\mathbf{w}} \\
&\triangleq \overline{\mathbf{w}}^{\mathcal{H}}\mathbf{A}_{s_i}\overline{\mathbf{w}} \\
|h_{pe} + q\mathbf{g}_{se}^{\mathcal{H}}\mathbf{w}|^2 &= \overline{\mathbf{w}}^{\mathcal{H}}\begin{bmatrix} q^2\mathbf{G}_{se} & qh_{pe}\mathbf{g}_{se} \\ qh_{pe}^{\mathcal{H}}\mathbf{g}_{se}^{\mathcal{H}} & |h_{pe}|^2 \end{bmatrix}\overline{\mathbf{w}} \\
&\triangleq \overline{\mathbf{w}}^{\mathcal{H}}\mathbf{A}_e\overline{\mathbf{w}} \qquad (6)
\end{aligned}
$$

Similarly, let $\mathbf{B}_p \triangleq \begin{bmatrix} c_p^2\mathbf{G}_{sp} & 0 \\ 0 & 1 \end{bmatrix}$, $\mathbf{B}_{s_i} \triangleq \begin{bmatrix} c_p^2\mathbf{G}_{ss_i} & 0 \\ 0 & 1 \end{bmatrix}$ and $\mathbf{B}_e \triangleq \begin{bmatrix} c_p^2\mathbf{G}_{se} & 0 \\ 0 & 1 \end{bmatrix}$, then, we can obtain $(1 + c_p^2|\mathbf{g}_{sp}^{\mathcal{H}}\mathbf{w}|^2) = \overline{\mathbf{w}}^{\mathcal{H}}\mathbf{B}_p\overline{\mathbf{w}}$, $(1 + c_p^2|\mathbf{g}_{ss_i}^{\mathcal{H}}\mathbf{w}|^2) = \overline{\mathbf{w}}^{\mathcal{H}}\mathbf{B}_{s_i}\overline{\mathbf{w}}$ and $(1 + c_p^2|\mathbf{g}_{se}^{\mathcal{H}}\mathbf{w}|^2) = \overline{\mathbf{w}}^{\mathcal{H}}\mathbf{B}_e\overline{\mathbf{w}}$. Let $\mathbf{F}_{se} = \mathbf{f}_{se}\mathbf{f}_{se}^{\mathcal{H}}$, $\mathbf{F}_{sp} = \mathbf{f}_{sp}\mathbf{f}_{sp}^{\mathcal{H}}$, $\overline{\mathbf{W}} = \overline{\mathbf{w}}\overline{\mathbf{w}}^{\mathcal{H}}$, $\mathbf{V}_i = \mathbf{v}_i\mathbf{v}_i^{\mathcal{H}}, \forall i = 1, \ldots, K$, and $\boldsymbol{\Phi} = \boldsymbol{\phi}\boldsymbol{\phi}^{\mathcal{H}}$. By applying $\mathbf{x}^{\mathcal{H}}\mathbf{A}\overline{\mathbf{x}} = Tr(\mathbf{A}\mathbf{x}\mathbf{x}^{\mathcal{H}})$, R_{secrecy} can be equivalently written as (7) (shown on the top of the next page), where $a = 1 + \frac{P_p|h_{pp}|^2}{\sigma^2}$, and Problem (5) can be equivalently formulated as the following rank-constrained optimization problem:

$$
\begin{aligned}
\underset{\overline{\mathbf{W}}, \{\mathbf{V}_i\}_{i=1}^K, \mathbf{Q}_z, \boldsymbol{\Phi}}{\text{maximize}} \quad & R_{\text{secrecy}} \\
\text{subject to} \quad & Tr(\mathbf{F}_{sp}\boldsymbol{\Phi}) = 0; \qquad (8a)
\end{aligned}
$$

$$R_{\text{secrecy}} = \frac{1}{2}\Bigg[\log\left(a + \frac{P_pTr(\mathbf{A}_p\overline{\mathbf{W}})}{\sigma^2 Tr(\mathbf{B}_p\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{G}_{sp}\mathbf{V}_i) + Tr(\mathbf{G}_{sp}\mathbf{Q}_z)}\right) + \sum_{i=1}^{K}\log\left(1 + \frac{Tr(\mathbf{G}_{ss_i}\mathbf{V}_i)}{\sigma^2 Tr(\mathbf{B}_{s_i}\overline{\mathbf{W}}) + P_pTr(\mathbf{A}_{s_i}\overline{\mathbf{W}}) + \sum_{j\neq i}^{K} Tr(\mathbf{G}_{ss_i}\mathbf{V}_j) + Tr(\mathbf{G}_{ss_i}\mathbf{Q}_z)}\right) - \log\left(1 + \frac{P_p|h_{pe}|^2}{\sigma^2 + Tr(\mathbf{F}_{se}\mathbf{\Phi})} + \frac{P_pTr(\mathbf{A}_e\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{G}_{se}\mathbf{V}_i)}{\sigma^2 Tr(\mathbf{B}_e\overline{\mathbf{W}}) + Tr(\mathbf{G}_{se}\mathbf{Q}_z)}\right)\Bigg]^+ \tag{7}$$

$$\frac{P_pTr(\mathbf{A}_p\overline{\mathbf{W}})}{\sigma^2 Tr(\mathbf{B}_p\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{G}_{sp}\mathbf{V}_i) + Tr(\mathbf{G}_{sp}\mathbf{Q}_z)} \geq \frac{P_p|h_{pp}|^2}{\sigma^2}; \tag{8b}$$

$$Tr(\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{V}_i) + \text{Tr}(\mathbf{Q}_z) + Tr(\mathbf{\Phi}) \leq P_s + 1; \tag{8c}$$

$$Tr\left(\begin{bmatrix}\mathbf{0}_{M\times M} & \mathbf{0}_{M\times 1}\\ \mathbf{0}_{1\times M} & 1\end{bmatrix}\overline{\mathbf{W}}\right) = 1; \tag{8d}$$

$$\text{Rank}(\overline{\mathbf{W}}) \leq 1;\quad \text{Rank}(\mathbf{V}_i) \leq 1,\ \forall i;\quad \text{Rank}(\mathbf{\Phi}) \leq 1; \tag{8e}$$

$$\overline{\mathbf{W}} \succeq 0, \mathbf{V}_i \succeq 0, \forall i = 1,\ldots,K,\ \mathbf{Q}_z \succeq 0,\ \mathbf{\Phi} \succeq 0. \tag{8f}$$

By relaxing (neglecting) the non-convex rank one constraints (8e), Problem (8) reduces to,

$$\underset{\overline{\mathbf{W}},\{\mathbf{V}_i\}_{i=1}^K,\mathbf{Q}_z,\mathbf{\Phi}}{\text{maximize}} \quad R_{\text{secrecy}} \qquad \text{subject to} \quad (8a)-(8d);(8f). \tag{9}$$

which is known as an SDR of Problem (5), and is generally an approximation (upper bound) to Problem (5).

Remark 1: If the optimal $\overline{\mathbf{W}}, \{\mathbf{V}_i\}_{i=1}^K$ and $\mathbf{\Phi}$ of the SDR-based (Problem (9)) are of rank-one or zero, the solution to the SDR problem is also optimal to the original Problem (5) and thus the beamforming vectors $\mathbf{w}, \{\mathbf{v}_i\}_{i=1}^K$ and ϕ for Problem (5) can be obtained via conducting an eigenvalue decomposition on $\overline{\mathbf{W}}, \{\mathbf{V}_i\}_{i=1}^K$ and $\mathbf{\Phi}$ respectively. Otherwise, some other rank-one decomposition-based approximation approaches, such as the Gaussian randomization technique (see [23][10] for more details), can be applied to turn the SDR solution into an approximate solution for the original Problem (5).

In the following, we will focus on solving the SDR Problem (9). At this point, Problem (9) is still hard to solve due to the non-convexity of the objective function. However, we find that by letting $\varsigma \triangleq 1 + \frac{P_p|h_{pe}|^2}{\sigma^2 + Tr(\mathbf{F}_{se}\mathbf{\Phi})}$ be fixed, Problem (9) can be approximately reformulated as a convex optimization problem. Motivated by this, the alternating optimization algorithm (AOA) can be employed to obtain a locally optimal solution for Problem (9).

More specifically, we first write Problem (9) as:

$$\underset{\varsigma}{\text{maximize}} \quad \Omega(\varsigma) \qquad \text{subject to} \quad \varsigma_{\min} < \varsigma \leq 1 + \frac{P_p|h_{pe}|^2}{\sigma^2}. \tag{10}$$

where $\varsigma_{\min} = 1 + \frac{P_p|h_{pe}|^2}{\sigma^2 + |\phi^{\mathcal{H}}\mathbf{f}_{se}|^2_{\max}}$ with $|\phi^{\mathcal{H}}\mathbf{f}_{se}|^2_{\max} = \left(\frac{\sqrt{P_s}\mathbf{f}_{se}^{\mathcal{H}}(\mathbf{I}_K - \mathbf{f}_{sp}(\mathbf{f}_{sp}^{\mathcal{H}}\mathbf{f}_{sp})^{-1}\mathbf{f}_{sp}^{\mathcal{H}})\mathbf{f}_{se}}{||(\mathbf{I}_K - \mathbf{f}_{sp}(\mathbf{f}_{sp}^{\mathcal{H}}\mathbf{f}_{sp})^{-1}\mathbf{f}_{sp}^{\mathcal{H}})\mathbf{f}_{se}||}\right)^2$ and

$$\Omega(\varsigma) \triangleq \max_{\overline{\mathbf{W}},\{\mathbf{V}_i\}_{i=1}^K,\mathbf{Q}_z,\mathbf{\Phi}} \quad R_{\text{secrecy}}\big|_{1+\frac{P_p|h_{pe}|^2}{\sigma^2+Tr(\mathbf{F}_{se}\mathbf{\Phi})}=\varsigma} \qquad \text{subject to} \quad 1 + \frac{P_p|h_{pe}|^2}{\sigma^2 + Tr(\mathbf{F}_{se}\mathbf{\Phi})} \leq \varsigma \quad (8a)-(8d);(8f). \tag{11}$$

Note that the lower bound of ς in Problem (10) is obtained by allocating all of P_s to the SU-RXs for sending jamming signals in the first time slot, which results in no transmission on SU-TX (i.e., $\mathbf{W} = \mathbf{0}, \mathbf{V}_i = \mathbf{0}, \forall i, \mathbf{Q}_z = \mathbf{0}$). Thus, in that case, the secrecy rate maximization problem (5) becomes, $\underset{\phi}{\text{maximize}}\ |\phi^{\mathcal{H}}\mathbf{f}_{se}|^2$, subject to $|\phi^{\mathcal{H}}\mathbf{f}_{sp}|^2 = 0$ and $|\phi|^2 = P_s$, which leads to the above value of $\varsigma_{\min}$.

Then, starting with an arbitrary initial value of ς, the following two steps are iteratively applied until convergence:

Step 1: With a fixed value of ς, find a locally optimal $\overline{\mathbf{W}}, \{\mathbf{V}_i\}_{i=1}^K, \mathbf{Q}_z, \mathbf{\Phi}$ by solving the Problem (11).

Step 2: With the resulting $\overline{\mathbf{W}}, \{\mathbf{V}_i\}_{i=1}^K, \mathbf{Q}_z, \mathbf{\Phi}$, update the optimal ς by solving Problem (10).

This two-step AOA algorithm is guaranteed to converge, since the secrecy rate is non-decreasing at each iteration.

Problem (10) in **Step 2** is a single-variable optimization problem and can be easily solved by a one-dimensional line search method. Thus the main difficulty of implementing the above AOA algorithm is how to solve the non-convex optimization problem (11) in **Step 1**. To overcome this difficulty, we will first reformulate Problem (11) into a DC programming problem, which can then be approximated into a convex optimization problem, such that a local optimum of Problem (11) can be obtained.

By introducing a set of auxiliary variables, $\Gamma_0,\ldots,\Gamma_{K+1}, F_0,\ldots,F_{K+1}$, Problem (11) can be equivalently expressed as,

$$\underset{\overline{\mathbf{W}},\{\mathbf{V}_i\}_{i=1}^K,\mathbf{Q}_z,\mathbf{\Phi},\{\Gamma_j\},\{F_j\}}{\text{maximize}} \quad \frac{1}{2}\left[\sum_{i=0}^{K+1}\log(\Gamma_j) - \sum_{i=0}^{K+1}\log(F_j)\right]^+$$

subject to

$$P_p|h_{pe}|^2 \leq (\varsigma - 1)(\sigma^2 + Tr(\mathbf{F}_{se}\mathbf{\Phi})); \tag{12a}$$

$$a\left(\sigma^2 Tr(\mathbf{B}_p\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{G}_{sp}\mathbf{V}_i) + Tr(\mathbf{G}_{sp}\mathbf{Q}_z)\right) + P_pTr(\mathbf{A}_p\overline{\mathbf{W}}) \geq \Gamma_0; \tag{12b}$$

$$\sigma^2 Tr(\mathbf{B}_p\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{G}_{sp}\mathbf{V}_i) + Tr(\mathbf{G}_{sp}\mathbf{Q}_z) \leq F_0; \tag{12c}$$

$$\sigma^2 Tr(\mathbf{B}_{s_i}\overline{\mathbf{W}}) + P_pTr(\mathbf{A}_{s_i}\overline{\mathbf{W}}) + \sum_{j\neq i}^{K} Tr(\mathbf{G}_{ss_i}\mathbf{V}_j) + Tr(\mathbf{G}_{ss_i}\mathbf{Q}_z) + Tr(\mathbf{G}_{ss_i}\mathbf{V}_i) \geq \Gamma_i,\ \forall i = 1,\ldots,K; \tag{12d}$$

$$\sigma^2 Tr(\mathbf{B}_{s_i}\overline{\mathbf{W}}) + P_pTr(\mathbf{A}_{s_i}\overline{\mathbf{W}}) + \sum_{j\neq i}^{K} Tr(\mathbf{G}_{ss_i}\mathbf{V}_j) + Tr(\mathbf{G}_{ss_i}\mathbf{Q}_z) \leq F_i, \quad \forall i = 1,\ldots,K; \tag{12e}$$

$$\sigma^2 Tr(\mathbf{B}_e\overline{\mathbf{W}}) + Tr(\mathbf{G}_{se}\mathbf{Q}_z) \geq \Gamma_{K+1}; \tag{12f}$$

$$\varsigma\left(\sigma^2 Tr(\mathbf{B}_e\overline{\mathbf{W}}) + Tr(\mathbf{G}_{se}\mathbf{Q}_z)\right) + P_p Tr(\mathbf{A}_e\overline{\mathbf{W}})$$
$$+\sum_{i=1}^{K} Tr(\mathbf{G}_{se}\mathbf{V}_i) \leq F_{K+1}; \tag{12g}$$
$$Tr(\mathbf{F}_{sp}\mathbf{\Phi}) = 0; \tag{12h}$$
$$\frac{|h_{pp}|^2}{\sigma^2}\left(\sigma^2 Tr(\mathbf{B}_p\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{G}_{sp}\mathbf{V}_i) + Tr(\mathbf{G}_{sp}\mathbf{Q}_z)\right)$$
$$\leq Tr(\mathbf{A}_p\overline{\mathbf{W}}); \tag{12i}$$
$$Tr(\overline{\mathbf{W}}) + \sum_{i=1}^{K} Tr(\mathbf{V}_i) + \mathrm{Tr}(\mathbf{Q}_z) + Tr(\mathbf{\Phi}) \leq P_s + 1; \tag{12j}$$
$$Tr\left(\begin{bmatrix}\mathbf{0}_{M\times M} & \mathbf{0}_{M\times 1}\\ \mathbf{0}_{1\times M} & 1\end{bmatrix}\overline{\mathbf{W}}\right) = 1; \tag{12k}$$
$$\overline{\mathbf{W}} \succeq 0,\quad \mathbf{V}_i \succeq 0,\quad \forall i = 1,\ldots,K,\ \mathbf{Q}_z \succeq 0,\ \mathbf{\Phi} \succeq 0. \tag{12l}$$

Problem (12) is a DC programming problem. We introduce another auxiliary variable t and rewrite Problem (12) equivalently as,

$$\begin{aligned}\underset{\overline{\mathbf{W}},\{\mathbf{V}_i\}_{i=1}^K,\mathbf{Q}_z,\mathbf{\Phi},\{\Gamma_j\},\{F_j\},t}{\text{maximize}}\quad & \frac{1}{2}\left[\sum_{i=0}^{K+1}\log(\Gamma_j) - t\right]^+\\ \text{subject to}\quad & \sum_{i=0}^{K+1}\log(F_j) \leq t;\\ & (12a) - (12l).\end{aligned} \tag{13}$$

So far, Problem (13) is still nonconvex due to the non-convexity of the constraint $\sum_{i=0}^{K+1}\log(F_j) \leq t$. However, the Sequential Parametric Convex Approximation Method (SPCA), proposed in [18][19], can be applied here to find at least a locally optimal solution for Problem (13). The idea is to replace the non-convex function $\log(F_j)$ by its first-order taylor series expansion at a given point Fc_j (a linear approximation based upper bound), namely,

$$\log(F_j) \approx \log(Fc_j) + \frac{1}{Fc_j}(F_j - Fc_j). \tag{14}$$

So that Problem (13) approximately becomes a convex optimization problem as below:

$$\begin{aligned}\underset{\overline{\mathbf{W}},\{\mathbf{V}_i\},\mathbf{Q}_z,\mathbf{\Phi},\{\Gamma_j\},\{F_j\},t}{\text{maximize}}\quad & \frac{1}{2}\left[\sum_{i=0}^{K+1}\log(\Gamma_j) - t\right]^+\\ \text{subject to}\quad & \sum_{i=0}^{K+1}\left[\log(Fc_j) + \frac{1}{Fc_j}(F_j - Fc_j)\right] \leq t;\\ & (12a) - (12l).\end{aligned} \tag{15}$$

which is a convex SDP and can be solved efficiently via interior points methods using CVX. Thus the SPCA algorithm, with guaranteed convergence [18][19] to at least a local optimum of Problem (13) (which is equivalent to Problem (11)), can be formally summarized as below:

SPCA Algorithm
Initialize $n = 1$ and $\mathbf{F}_c^{(0)} = \{Fc_0^{(0)}, \ldots, Fc_{K+1}^{(0)}\}$;
Repeat
(1) Find the optimal $\mathbf{W}^{(n)}, \{\mathbf{V}_i^{(n)}\}_{i=1}^K, \mathbf{Q}_z^{(n)}, \mathbf{\Phi}$, $\{\Gamma_j^{(n)}\}_{j=0}^{K+1}, \{F_j^{(n)}\}_{j=0}^{K+1}, t^{(n)}$ by solving Problem (15) using CVX, with given $Fc_j = Fc_j^{(n-1)}, \forall j$;
(2) Update $\mathbf{F}_c^{(n)} = \{F_0^{(n)}, \ldots, F_{K+1}^{(n)}\}$;
(3) n=n+1;
Until convergence.

IV. Extension to the Multiple Eavesdroppers Scenario

In this section, we will consider the overlay CRN secrecy communication problem in the presence of L eavesdroppers ($L \geq 2$). The eavesdroppers are assumed to individually overhear the communication without any collusion. Let $f_{se_{il}}, \forall i = 1\ldots,K,\ \forall l = 1,\ldots,L$ represent the complex channel coefficient from the SU-RX$_i$ to the l^{th} eavesdropper, in the first time slot. The channel from PU-TX to the l^{th} eavesdropper are denoted by the complex scalars $h_{pe_l}, l = 1,\ldots,L$, and $\mathbf{g}_{se_l} \in \mathbb{C}^{M\times 1}, \forall l = 1,\ldots,L$ indicate the complex channel vectors from the SU-TX to the l^{th} eavesdropper. Then, let $\mathbf{f}_{se_l} \in \mathbb{C}^{K\times 1} \triangleq \{f_{se_{1l}},\ldots,f_{se_{Kl}}\}^T,\ \forall l$, the achievable rate at each eavesdroppers is given as, for $\forall l = 1,\ldots,L$,

$$\begin{aligned}R_{e_l} =& \frac{1}{2}\log\left(1 + \frac{P_p|h_{pe_l}|^2}{\sigma^2 + |\phi^{\mathcal{H}}\mathbf{f}_{se_l}|^2}\right.\\ &\left. + \frac{P_p|h_{pe_l} + q\mathbf{g}_{se_l}^{\mathcal{H}}\mathbf{w}|^2 + \sum_{i=1}^K|\mathbf{g}_{se_l}^{\mathcal{H}}\mathbf{v}_i|^2}{\sigma^2(1 + c_p^2|\mathbf{g}_{se_l}^{\mathcal{H}}\mathbf{w}|^2) + \mathbf{g}_{se_l}^{\mathcal{H}}\mathbf{Q}_z\mathbf{g}_{se_l}}\right)\end{aligned} \tag{16}$$

In this case, the secrecy rate maximization problem for the overlay CRN with multiple eavesdroppers, can be formulated as

$$\begin{aligned}\underset{\mathbf{w},\{\mathbf{v}_i\}_{i=1}^K,\mathbf{Q}_z\succeq 0,\phi}{\text{maximize}}\quad & R_{\text{secrecy}} = \left[R_p + R_s^{\text{sum}} - \max_l R_{e_l}\right]^+\\ \text{subject to}\quad & (5a) - (5c).\end{aligned} \tag{17}$$

The Problem (17) can be written as,

$$\min_{l\in\{1,\ldots,L\}} R^*_{\text{secrecy}_l} \tag{18}$$

where

$$\begin{aligned}R^*_{\text{secrecy}_l} \triangleq \underset{\mathbf{w},\{\mathbf{v}_i\}_{i=1}^K,\mathbf{Q}_z\succeq 0,\phi}{\text{maximize}}\quad & [R_p + R_s^{\text{sum}} - R_{e_l}]^+\\ \text{subject to}\quad & (5a) - (5c).\end{aligned} \tag{19}$$

This implies that Problem (17) can be decomposed into L independent subproblems, where the l^{th} subproblem (19) corresponds to finding the maximum secrecy rate to the l^{th} eavesdropper. The algorithm proposed in Section III for solving Problem (5) for the single eavesdropper case can be directly applied, and followed by picking the solution that gives the minimum value of $R^*_{\text{secrecy}_l}$.

V. Numerical Results

In this section, we will evaluate the joint secrecy rate performance of our AN-aided cooperative overlay CRN obtained by the proposed SDR-based approximation algorithm (termed as the "AN-aided joint secrecy rate maximization design (JSRMD)"") via numerical simulations. All the channels involved are assumed to be independent and undergoing identical Rayleigh fading, i.e., each channel follows an complex Gaussian distribution with zero mean and unit variance. The number of transmit antennas at SU-TX is $M = 3$ and the number of SU-RXs is $K = 2$. The constant primary transmit power P_p is set to be 0 dB.

Fig.2 illustrates the secrecy rate performance of the proposed AN-aided JSRMD algorithm versus the secondary transmit power P_s for a single eavesdropper case, and compares these results with the corresponding secrecy rate performance of JSRMD without any help of AN, i.e., the No-AN JSRMD case. The striking observation from Fig.2 is that the proposed AN-aid JSRMD provides a significant performance improvement over No-AN JSRMD. The performance gain of AN-

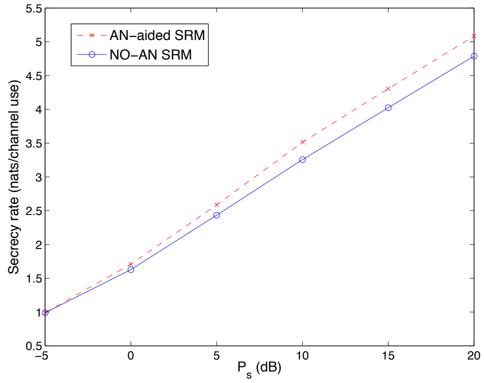


Fig. 2. Secrecy rates versus the secondary transmit power for one eavesdropper case

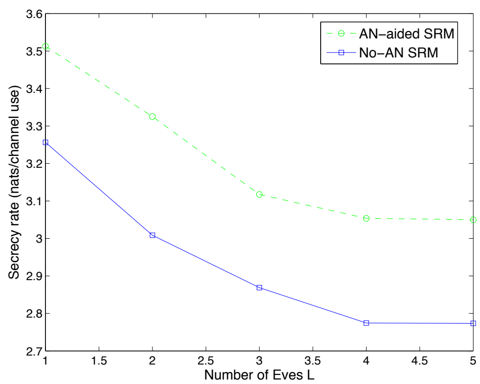


Fig. 3. Secrecy rates versus the number of eavesdroppers with $P_s = 10$ dB

aided JSRMD is not very obvious when P_s is small (e.g. when $P_s \leq 0$ dB), since not much spare power could be used for generating AN. But with increasing P_s, the benefit of AN becomes more and more pronounced. For example, the performance gap between the AN-aided JSRMD and No-AN JSRMD at $P_s = 5$ dB and $P_s = 15$ dB are approximately 0.1536 nats/channel use and 0.2811 nats/channel use respectively. This is very encouraging since it shows that AN can significantly enhance the security of our overlay CRN even for a single eavesdropper case.

Fig.3 displays the secrecy rate performance versus the number of eavesdroppers with $P_s = 10$ dB for the proposed AN-aid JSRMD and No-AN JSRMD, respectively. It can be seen from Fig.3 that, for any of these two curves, the secrecy rate performance decreases as number of eavesdroppers K increases, as expected. We also observe from Fig.3 that the proposed AN-aid JSRMD yields a superior performance than No-AN JSRMD, even for the $K = 5$ eavesdroppers case. This further confirms the benefit of using AN in our overlay CRN.

VI. Conclusions and Extensions

This paper has considered an AN-aided joint secrecy rate (for both primary and secondary links) maximization problem for a novel MISO cooperative overlay cognitive radio network (CRN) with a single eavesdropper, subject to a global secondary transmit power constraint and a guarantee of improvement or no degradation at the least of the primary network's performance, under the assumption of global CSI knowledge. Our formulated optimization problem is nonconvex and hard to solve in general. We dealt with this difficulty by resorting to the semidefinite relaxation (SDR) technique, so that a computationally efficient algorithm for obtaining a local optimum for the corresponding SDR problem can be developed. An extension to the multiple eavesdroppers scenario was also discussed. Simulation results illustrated that the proposed scheme can significantly enhance the secrecy performance of our overlay CRN. Future work will involve extending these results to the case of imperfect or completely unknown CSI for the eavesdroppers.

References

[1] A. Goldsmith, S.A. Jafar, I. Maric, and S. Srinivasa, ”Breaking spectrum gridlock with cognitive radios: an information theoretic perspective,” *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894-914, May 2009.

[2] S. Hua, H. Liu, M. Wu and S. S. Panwar, “Exploiting MIMO antennas in cooperative cognitive radio networks,” in *Proc. IEEE INFOCOM 2011*, Shanghai, China, Apri. 2011, pp. 2714-2722.

[3] R. Manna, R. H. Y. Louie, Y. Li and B. Vucetic, “Cooperative Spectrum Sharing in Cognitive Radio Networks With Multiple Antennas,” *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5509-5522, Nov. 2011.

[4] L. Li, F. A. Khan, M. Pesavento and T. Ratnarajah, “Power Allocation and Beamforming in Overlay Cognitive Radio Systems,” in *Proc. IEEE 73rd Vehicular Technology Conf. (VTC Spring)*, Budapest, Hungary, May 2011, pp. 1-5.

[5] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[6] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[7] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961-4972, Aug. 2011.

[8] S. Shafiee and S. Ulukus, “Achievable rates in Gaussian MISO channels with secrecy constraints,” in *Proc. IEEE International Symposium on Inf. Theory (ISIT 2007)*, Nice, France, Jun. 2007, pp. 2466-2470.

[9] 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.

[10] W. Liao, T. Chang, W. Ma and C. 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] J. Huang and A. L. Swindlehurst, ”Cooperative jamming for secure communications in MIMO relay networks” *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[13] L. Dong, Z. Han, A. P. Petropulu and H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[14] 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.

[15] Y. Pei, Y. 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 , Apri. 2010.

[16] K. Lee, O. Simeone, C. Chae and J. Kang, “Spectrum Leasing via Cooperation for Enhanced Physical-Layer Secrecy,” in *Proc. IEEE International Conf. on Communi.(ICC 2011)*, Kyoto, Japan, Jun. 2011, pp. 1-5.

[17] T. Kwon, V. W.S. Wong, and R. Schober, “Secure MISO cognitive radio system with perfect and imperfect CSI,” in *Proc. IEEE Globecom 2012*, Anaheim, CA, USA, Dec 2012, pp. 1254-1259.

[18] A. Beck, A. Ben-Tal and L. Tetruashvili, “A sequential parametric convex approximation method with applications to nonconvex truss topology design problems,” *Journal of Global Optimization*, vol. 47, no. 1, pp. 29-51, May 2010.

[19] A. Khabbazibasmenj, F. Roemer, S. A. Vorobyov and M. Haardt, ”Sum-Rate Maximization in Two-Way AF MIMO Relaying: Polynomial Time Solutions to a Class of DC Programming Problems,” *IEEE Trans. Signal Process.*, vol. 60, no. 10, pp. 5478-5493, Oct. 2012.

[20] L. Lai and H. El Gamal, ”The relayeavesdropper channel: cooperation for secrecy,” *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[21] T.T. Kim and H.V. Poor, ”On the secure degrees of freedom of relaying with half-duplex feedback,” *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 291-302, Jan. 2011.

[22] G. Zheng, L. Choo and K. Wong, ”Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relays,” *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317-1322, Mar. 2011.

[23] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, “Semidefinite relaxation of quadratic optimization problems,” *IEEE Trans. Signal Process. Mag.*, vol. 27, no. 3, pp. 20-34, May 2010.