Multiple Amplify-and-Forward Full-Duplex Relays for Legitimate Eavesdropping

Jihwan Moon, Hoon Lee, Changick Song, *Member*, *IEEE*, and Inkyu Lee, *Fellow*, *IEEE*

***Abstract*—In this paper, we consider a legitimate proactive eavesdropping scenario where a central monitor tries to intercept the information exchanged between a pair of suspicious entities through amplify-and-forward full-duplex relays and a cooperative jammer. Specifically, the eavesdropping relays simultaneously listen to the suspicious transmitter and forward the eavesdropped information to the central monitor. At the same time, the jammer broadcasts the jamming signal to maintain the suspicious data rate below the channel capacity of the central monitor so that the eavesdropped information can be successfully decoded by the central monitor. In this system, we jointly design the relay precoders at the eavesdropping relays and the transmit covariance matrix at the jammer to maximize the eavesdropping rate by a two-layer semi-definite relaxation approach. Simulation results verify the efficiency of our proposed solution and show considerable performance gains over conventional schemes.**

I. Introduction

Due to the intrinsic broadcast nature of wireless communications, guaranteeing the confidentiality of the transmitted information has always been a major challenge. Particularly, the upcoming 5th generation (5G) wireless networks are aiming at supporting massive connections of devices for the Internet of Things (IoT), which leads to great attention on the protection of private data. In response to this, a great number of approaches to ensure physical layer security have been proposed for various types of systems ranging from a basic wiretap cofiguration in [1] to MIMO wiretap channels [2], relay-aided networks [3] [4], and energy harvesting systems [5] [6]. These conventional physical layer security studies view eavesdroppers as unauthorized users, and accordingly, most designs have been carried out in a way that the transmitted information is indecipherable to the eavesdroppers.

Recently, legitimate *proactive eavesdropping*, which completely shifts the conventional paradigm of secure communications, has started to garner a lot of interest (see [7] and the references therein). A main purpose of this new framework is to monitor or intervene suspicious users who are deemed to misuse communications systems for illegal activities.

The work of J. Moon, H. Lee and I. Lee was supported by National Research Foundation (NRF) funded by the Ministry of Science, ICT & Future Planning (MSIP) of Korea Government under Grant 2017R1A2B3012316. The work of C. Song was supported by the National Research Foundation of Korea through the Korea Government under Grant 2015R1C1A1A02036927.

J. Moon, H. Lee, and I. Lee are with the School of Electrical Engineering, Korea University, Seoul, Korea (e-mail: {anschino, ihun1, inkyu}@korea.ac.kr).

C. Song is with the Dept. of Information and Communications Eng., Korea National University of Transportation, Chungju, Korea (e-mail: c.song@ut.ac.kr).

In [8] and [9], the authors proposed an eavesdropping system in which a full-duplex (FD) legitimate monitor intercepts information from a suspicious pair by proactively adjusting the suspicious data rate through simultaneous jamming. For this system, it is important to keep the suspicious communications rate less than the eavesdropping channel capacity so that the legitimate monitor can successfully decode the intercepted information from an information theoretic perspective. Hence, the authors coined a term *eavesdropping rate* to indicate the suspicious communications rate satisfying such a condition and evaluated the system performance based on that. The authors of [10] extended this system to a variety of general multi-antenna full-duplex monitors and obtained both optimal and suboptimal solutions that minimize the eavesdropping outage probability.

All the aforementioned works assumed the legitimate monitor to have a direct link from eavesdropping targets. However, it is more natural for the monitor to operate out of the targets' sight where the direct link signal may not exist. One way to address such an issue is to deploy undetectable small sized relay nodes between the central monitor and the eavesdropping targets, but this has not been thoroughly studied yet in literature. Recent works in [11]–[13] examined amplify-and-forward (AF) and decode-and-forward (DF) suspicious relay networks in the proactive eavesdropping paradigm, but it should be noted that the relays in these works were on the suspicious side, and not for legitimate eavesdropping.

In this paper, we consider a proactive eavesdropping scenario where a central monitor is intentionally located far away from suspicious users to stay undetected. Without having a direct eavesdropping link, we propose a new system which makes use of intermediate eavesdropping relays and a cooperative jammer to facilitate eavesdropping. Specifically, the eavesdropping relays that operate in an AF FD mode simultaneously listen to the suspicious transmitter and forward the eavesdropped information to the central monitor. At the same time, the jammer broadcasts the jamming signals to maintain the suspicious data rate below the channel capacity of the central monitor. In this system, we present a solution for the relay precoders at the eavesdropping relays and the transmit covariance matrix at the jammer so as to maximize the eavesdropping rate by utilizing a two-layer semi-definite relaxation (SDR) method. Also, unlike the existing literatures [8] and [9], we take the effects of the residual self-interference (SI) and a non-negligible relay processing delay into consideration. Simulation results verify that our proposed schemes

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

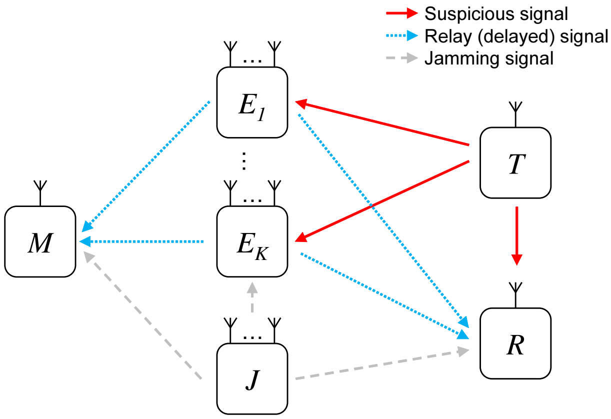

Fig. 1. Schematic diagram

outperform other conventional methods.

The rest of this paper is organized as follows: The proposed system model and the problem formulation are described in Section II. Then, an SDR-based solution for eavesdropping rate maximization is discussed in Section III. Numerical results are provided in Section IV, and Section V concludes the paper.

Notations: We use $\mathbb{R}$ and $\mathbb{C}$ as sets of real and complex numbers, respectively, and $|\cdot|$ and $\mathbb{E}[\cdot]$ stand for the absolute value and the expectation operation, respectively. $\|\mathbf{X}\|$, $\mathbf{X}^{\mathbf{H}}$, $\mathbf{X}^{\dagger}$, $\mathrm{tr}(\mathbf{X})$, $\mathrm{vec}(\mathbf{X})$ and $\mathrm{rank}(\mathbf{X})$ are the Frobenius norm, Hermitian, conjugate, trace, vectorization and rank of a matrix $\mathbf{X}$, respectively. We define $\mathbf{I_d}$ as a $d \times d$ identity matrix, and $\mathrm{diag}(\mathbf{X_1}, ..., \mathbf{X_D})$ represents a block-wise diagonalization of matrices $\mathbf{X_1}, ..., \mathbf{X_D}$. The operation $\otimes$ denotes Kronecker product, and $\mathbf{X} \succeq \mathbf{0}$ means that $\mathbf{X}$ is positive semi-definite. $\mathcal{CN}(\mathbf{m}, \mathbf{\Omega})$ indicates a circularly symmetric complex Gaussian distribution with mean vector $\mathbf{m}$ and covariance matrix $\mathbf{\Omega}$. For some real x and y, $\max\{x, y\}$ outputs the larger value of x and y.

II. System Model

Fig. 1 depicts our proposed system where a far located central monitor having a single antenna tries to proactively eavesdrop the information exchanged between a suspicious transmitter and a receiver with the aid of intermediate multi-antenna eavesdropping relays and a cooperative multi-antenna jammer. Throughout the paper, T, R, E_k, J and M indicate the suspicious transmitter, the suspicious receiver, the k-th eavesdropping relay, the jammer, and the central monitor, respectively.

We assume that each of the suspicious pair is equipped with a single antenna, and they employ an adaptive transmission policy in which its data rate is adjusted based on the effective channel condition at the receiver [8]–[13]. It is also assumed that a direct eavesdropping link between the central monitor and the suspicious transmitter does not exist due to the strong path loss. The multiple AF FD eavesdropping relays then simultaneously listen to the suspicious transmitter and forward the eavesdropped information to the central monitor. We denote N_{T,E_k} and N_{R,E_k} as the number of transmit and receive antennas, respectively, at the k-th eavesdropping relay. In the meantime, the jammer with $N_{T,J}$ transmit antennas broadcasts jamming signals to retain the suspicious data rate below the channel capacity of the central monitor for successful decoding at the central monitor.

We denote h_{XY}, $\mathbf{h}_{\mathsf{XY}}$ and $\mathbf{H}_{\mathsf{XY}}$ as the complex channel coefficient, the channel vector and the channel matrix, respectively, from node X to Y where $\mathsf{X}, \mathsf{Y} \in \{T, R, E_k, \forall k, J, M\}$. We assume that all the channel variables are subject to channel reciprocity and undergo quasi-static flat fading such that they remain constant for a block of $N \gg 1$ suspicious symbol transmissions. In addition, global channel state information (CSI) is assumed available at the the central monitor, the eavesdropping relays and the jammer, while the suspicious pair are unconscious of being eavesdropped and have knowledge of their mutual CSI only [9]–[12].

At time instant n for $n = 1, ..., N$, the received signal at the k-th eavesdropping relay is given by

$$\begin{aligned}\mathbf{y_{E_k}[n]} =& \mathbf{h_{TE_k}} \mathbf{x_T[n]} + \underbrace{\tilde{\mathbf{H}}_{E_k E_k} \mathbf{x_{E_k}[n]}}_{\text{SI}} + \underbrace{\sum_{\ell \neq k} \mathbf{H_{E_\ell E_k}} \mathbf{x_{E_\ell}[n]}}_{\text{IRI}} \\ &+ \underbrace{\mathbf{H_{JE_k}} \mathbf{x_J[n]}}_{\text{Jamming signal}} + \mathbf{z_{E_k}[n]}, \qquad (1)\end{aligned}$$

where $x_T[n] \sim \mathcal{CN}(0, P_T)$, $\mathbf{x_{E_k}[n]} \in \mathbb{C}^{\mathbf{N_{T,E_k}} \times 1}$ and $\mathbf{x_J[n]} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q_J})$ are the transmitted signals from the suspicious transmitter, the k-th eavesdropping relay, and the jammer, respectively, with $\mathbf{Q_J} \in \mathbb{C}^{\mathbf{N_{T,J}} \times \mathbf{N_{T,J}}}$ being the transmit covariance matrix of the jammer. $\tilde{\mathbf{H}}_{E_k E_k}$ indicates the residual SI channel matrix at the k-th eavesdropping relay, whose element independently follows $\mathcal{CN}(0, \sigma^2_{\mathrm{SI},k})$ [14], and $\mathbf{z_{E_k}[n]} \sim \mathcal{CN}(\mathbf{0}, \sigma^2_{\mathbf{E_k}} \mathbf{I_{N_{R,E_k}}})$ represents the noise vector for the k-th eavesdropping relay.

In this work, we take into account a non-negligible relay processing delay τ [15]. We particularly assume $\tau \geq T_{\mathrm{sym}}$ where T_{sym} is the symbol period of the suspicious transmitter. Then, the transmitted signal $\mathbf{x_{E_k}[n]}$ at the k-th eavesdropping relay can be expressed as $\mathbf{x_{E_k}[n]} = \mathbf{G_{E_k}} \mathbf{y_{E_k}[n - \tau]}$ where $\mathbf{G_{E_k}}$ equals the relay precoder for the k-th eavesdropping relay. It is worth pointing out that since the suspicious receiver is unaware of the eavesdropping relays, the delayed signals $\mathbf{x_{E_k}[n]}$ only act as interference to the receiver.

Consequently, the received signals $y_M[n]$ and $y_R[n]$ at the central monitor and the suspicious receiver are written as (2) and (3), respectively, at the top of the next page where $z_M[n] \sim \mathcal{CN}(0, \sigma^2_M)$ and $z_R[n] \sim \mathcal{CN}(0, \sigma^2_R)$ stand for the noise at each corresponding node.

We further assume that the jamming interference $\mathbf{H_{JE_k}} \mathbf{x_J[n]}$ and $\mathbf{h^T_{MJ}} \mathbf{x_J[n]}$ in the received signals (1) and (2) of the eavesdropping relays and the central monitor, respectively, are completely removed by performing cooperative jamming. This strategy can be achieved by sharing the jamming signals among the central moitors, the eavesdropping relays and the jammer in prior [6].

$$y_M[n] = \sum_{k=1}^{K} \mathbf{h}_{\mathbf{ME_k}}^{\mathbf{T}} \mathbf{G}_{\mathbf{E_k}} \Big(\underbrace{\mathbf{h}_{\mathbf{TE_k}} \mathbf{x}_{\mathbf{T}}[\mathbf{n}-\tau]}_{\text{Desired signal}} + \tilde{\mathbf{H}}_{\mathbf{E_k E_k}} \mathbf{x}_{\mathbf{E_k}}[\mathbf{n}-\tau] + \sum_{\ell \neq \mathbf{k}} \mathbf{H}_{\mathbf{E_\ell E_k}} \mathbf{x}_{\mathbf{E_\ell}}[\mathbf{n}-\tau] + \mathbf{H}_{\mathbf{JE_k}} \mathbf{x}_{\mathbf{J}}[\mathbf{n}-\tau] + \mathbf{z}_{\mathbf{E_k}}[\mathbf{n}-\tau] \Big) + \mathbf{h}_{\mathbf{MJ}}^{\mathbf{T}} \mathbf{x}_{\mathbf{J}}[\mathbf{n}] + \mathbf{z}_{\mathbf{M}}[\mathbf{n}], \tag{2}$$

$$y_R[n] = \underbrace{h_{TR} x_T[n]}_{\text{Desired signal}} + \sum_{k=1}^{K} \mathbf{h}_{\mathbf{RE_k}}^{\mathbf{T}} \mathbf{G}_{\mathbf{E_k}} \Big(\underbrace{\mathbf{h}_{\mathbf{TE_k}} \mathbf{x}_{\mathbf{T}}[\mathbf{n}-\tau]}_{\text{Delayed interference}} + \tilde{\mathbf{H}}_{\mathbf{E_k E_k}} \mathbf{x}_{\mathbf{E_k}}[\mathbf{n}-\tau] + \sum_{\ell \neq \mathbf{k}} \mathbf{H}_{\mathbf{E_\ell E_k}} \mathbf{x}_{\mathbf{E_\ell}}[\mathbf{n}-\tau] + \mathbf{H}_{\mathbf{JE_k}} \mathbf{x}_{\mathbf{J}}[\mathbf{n}-\tau] + \mathbf{z}_{\mathbf{E_k}}[\mathbf{n}-\tau] \Big) + \mathbf{h}_{\mathbf{RJ}}^{\mathbf{T}} \mathbf{x}_{\mathbf{J}}[\mathbf{n}] + \mathbf{z}_{\mathbf{R}}[\mathbf{n}], \tag{3}$$

Defining the signal-to-interference-plus-noise ratio (SINR) at node X as $\gamma_{\mathsf{X}}\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right)$ and the system bandwidth as W, the eavesdropping rate $r_{\mathrm{e}}\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right)$ is given by $W \log_2\left(1 + \gamma_R\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right)\right)$ if $\gamma_M\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right) \geq \gamma_R\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right)$ and 0 otherwise [8] [9]. Then, we have the following eavesdropping rate maximization problem:

$$\text{(P):} \quad \max_{\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}} \; r_{\mathrm{e}}\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right) \tag{4a}$$

$$\text{s.t.} \quad \gamma_M\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right) \geq \bar{\gamma}_M, \tag{4b}$$

$$\mathbb{E}\left[\left|\mathbf{x}_{\mathbf{E_k}}[\mathbf{n}]\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right)\right|^2\right] \leq \bar{P}_{E_k}, \; \forall k, \tag{4c}$$

$$\mathrm{tr}\left(\mathbf{Q}_{\mathbf{J}}\right) \leq \bar{P}_J. \tag{4d}$$

The goal of (P) is to obtain the optimal relay precoders $\left\{\mathbf{G}_{\mathbf{E_k}}\right\}$ for the eavesdropping relays and the optimal transmit covariance matrix $\mathbf{Q}_{\mathbf{J}}$ for the jammer to achieve the maximum eavesdropping rate $r_{\mathrm{e}}\left(\left\{\mathbf{G}_{\mathbf{E_k}}\right\}, \mathbf{Q}_{\mathbf{J}}\right)$. At the same time, we want to guarantee a certain minimum SINR $\bar{\gamma}_M$ for the central monitor to reliably decode and extract meaningful eavesdropped information in (4b), while not exceeding the maximum power budget $\bar{P}_{E_k}$ at the k-th eavesdropping relay in (4c) and $\bar{P}_J$ at the jammer in (4d). In the subsequent sections, we provide a solution for (P) by utilizing a two-layer SDR approach.

III. SDR-based Optimization for (P)

It has been shown that one of the most challenging aspects of multiple FD relays is how to handle inter-relay interference (IRI) and SI induced by the FD operation [16]. In order to tackle this problem, we apply the block-diagonalization (BD) approach [17] to suppress those interferences and formulate a more tractable SDR problem.

To this end, let us define $\bar{\mathbf{H}}_{E_k} \triangleq \left[\mathbf{H}_{\mathbf{E_k E_1}}^{\mathbf{H}} \; \cdots \; \mathbf{H}_{\mathbf{E_k E_K}}^{\mathbf{H}}\right]^H$ for $k = 1, ..., K$. Then, provided that $N_{T,E_k} > \sum_{\ell=1}^{K} N_{R,E_\ell}$, the singular value decomposition (SVD) of $\bar{\mathbf{H}}_{E_k}$ is expressed as $\bar{\mathbf{H}}_{E_k} = \bar{\mathbf{U}}_{E_k} \bar{\mathbf{S}}_{E_k} \left[\bar{\mathbf{V}}_{E_k,1} \; \bar{\mathbf{V}}_{E_k,0}\right]^H$ where $\bar{\mathbf{V}}_{E_k,0} \in \mathbb{C}^{N_{T,E_k} \times \theta_{E_k,0}}$ with $\theta_{E_k,0} \triangleq N_{T,E_k} - \sum_{\ell=1}^{K} N_{R,E_\ell}$ spans the nullspace of $\bar{\mathbf{H}}_{E_k}$.

Based on this BD, we can form the k-th relay precoder $\mathbf{G}_{\mathbf{E_k}}$ as $\mathbf{G}_{\mathbf{E_k}} = \bar{\mathbf{V}}_{\mathbf{E_k},\mathbf{0}} \bar{\mathbf{G}}_{\mathbf{E_k}}$ to simultaneously achieve $\bar{\mathbf{H}}_{E_k} \mathbf{G}_{\mathbf{E_k}} = \mathbf{0}$, $\forall k$ where $\bar{\mathbf{G}}_{E_k} \in \mathbb{C}^{\theta_{E_k,0} \times N_{R,E_k}}$ is now the optimization variable of interest. The SINRs γ_M and γ_R are then given as

$$\gamma_M\left(\left\{\bar{\mathbf{G}}_{E_k}\right\}\right) = \frac{P_T \left|\sum_{k=1}^{K} \bar{\mathbf{h}}_{ME_k}^H \bar{\mathbf{G}}_{E_k} \mathbf{h}_{\mathbf{TE_k}}\right|^2}{\sum_{k=1}^{K} \sigma_{E_k}^2 \bar{\mathbf{h}}_{ME_k}^H \bar{\mathbf{G}}_{E_k} \bar{\mathbf{G}}_{E_k}^H \bar{\mathbf{h}}_{ME_k} + \sigma_M^2},$$

$$\gamma_R\left(\left\{\bar{\mathbf{G}}_{E_k}\right\}, \mathbf{Q}_{\mathbf{J}}\right) = \frac{P_T \left|h_{TR}\right|^2}{\bar{z}_R + \sigma_R^2},$$

where $\bar{\mathbf{h}}_{ME_k} \triangleq \bar{\mathbf{V}}_{E_k,0}^H \mathbf{h}_{\mathbf{ME_k}}^{\dagger}$, $\bar{\mathbf{h}}_{RE_k} \triangleq \bar{\mathbf{V}}_{E_k,0}^H \mathbf{h}_{\mathbf{RE_k}}^{\dagger}$ and $\bar{z}_R \triangleq P_T \left|\sum_{k=1}^{K} \bar{\mathbf{h}}_{RE_k}^H \bar{\mathbf{G}}_{E_k} \mathbf{h}_{\mathbf{TE_k}}\right|^2 + \sum_{k=1}^{K} \sigma_{E_k}^2 \bar{\mathbf{h}}_{RE_k}^H \bar{\mathbf{G}}_{E_k} \bar{\mathbf{G}}_{E_k}^H \bar{\mathbf{h}}_{RE_k} + \mathbf{h}_{\mathbf{RJ}}^{\mathbf{H}} \mathbf{Q}_{\mathbf{J}} \mathbf{h}_{\mathbf{RJ}}$.

Accordingly, we can rewrite the original problem (P) as

$$\begin{aligned} \text{(P1):} \quad & \max_{\left\{\bar{\mathbf{G}}_{E_k}\right\}, \mathbf{Q}_{\mathbf{J}}} \; \gamma_R\left(\left\{\bar{\mathbf{G}}_{E_k}\right\}, \mathbf{Q}_{\mathbf{J}}\right) \\ & \text{s.t.} \quad \gamma_M\left(\left\{\bar{\mathbf{G}}_{E_k}\right\}\right) \geq \gamma_R\left(\left\{\bar{\mathbf{G}}_{E_k}\right\}, \mathbf{Q}_{\mathbf{J}}\right), \\ & \qquad \gamma_M\left(\left\{\bar{\mathbf{G}}_{E_k}\right\}\right) \geq \bar{\gamma}_M, \\ & \qquad \mathrm{tr}\left(\bar{\mathbf{G}}_{E_k}\left(P_T \mathbf{h}_{\mathbf{TE_k}} \mathbf{h}_{\mathbf{TE_k}}^{\mathbf{H}} + \sigma_{\mathbf{E_k}}^{\mathbf{2}} \mathbf{I}_{\mathbf{N_{R,E_k}}}\right) \bar{\mathbf{G}}_{E_k}^H\right) \\ & \qquad \quad \leq \bar{P}_{E_k}, \; \forall k, \\ & \qquad \mathrm{tr}\left(\mathbf{Q}_{\mathbf{J}}\right) \leq \bar{P}_J. \end{aligned}$$

To further simplify the problem, we concatenate the effective relay precoders $\left\{\bar{\mathbf{G}}_{E_k}\right\}$ as $\bar{\mathbf{g}} \triangleq \left[\mathrm{vec}\left(\bar{\mathbf{G}}_{E_1}\right)^H \; \cdots \; \mathrm{vec}\left(\bar{\mathbf{G}}_{E_K}\right)^H\right]^H$ and define $\bar{\mathbf{G}} \triangleq \bar{\mathbf{g}} \bar{\mathbf{g}}^H$. Then, we can derive the following equivalent expressions of the summations in (P1) as [18]

$$\left|\sum_{k=1}^{K} \bar{\mathbf{h}}_{RE_k}^H \bar{\mathbf{G}}_{E_k} \mathbf{h}_{\mathbf{TE_k}}\right|^2 = \mathrm{tr}\left(\mathbf{B_1} \bar{\mathbf{G}}\right),$$

$$\left|\sum_{k=1}^{K} \bar{\mathbf{h}}_{ME_k}^H \bar{\mathbf{G}}_{E_k} \mathbf{h}_{\mathbf{TE_k}}\right|^2 = \mathrm{tr}\left(\mathbf{B_2} \bar{\mathbf{G}}\right),$$

$$\sum_{k=1}^{K} \sigma_{E_k}^2 \bar{\mathbf{h}}_{RE_k}^H \bar{\mathbf{G}}_{E_k} \bar{\mathbf{G}}_{E_k}^H \bar{\mathbf{h}}_{RE_k} = \mathrm{tr}\left(\mathbf{B_3} \bar{\mathbf{G}}\right),$$

$$\sum_{k=1}^{K} \sigma_{E_k}^2 \bar{\mathbf{h}}_{ME_k}^H \bar{\mathbf{G}}_{E_k} \bar{\mathbf{G}}_{E_k}^H \bar{\mathbf{h}}_{ME_k} = \mathrm{tr}\left(\mathbf{B_4} \bar{\mathbf{G}}\right),$$

$$\mathrm{tr}\left(\bar{\mathbf{G}}_{E_k}\left(P_T \mathbf{h}_{\mathbf{TE_k}} \mathbf{h}_{\mathbf{TE_k}}^{\mathbf{H}} + \sigma_{\mathbf{E_k}}^{\mathbf{2}} \mathbf{I}_{\mathbf{N_{R,E_k}}}\right) \bar{\mathbf{G}}_{E_k}^H\right) = \mathrm{tr}\left(\mathbf{B}_{\mathbf{5},\mathbf{E_k}} \bar{\mathbf{G}}\right),$$

$$\mathbf{B_1} \triangleq \left[\mathbf{h^T_{TE_1}} \otimes \mathbf{\bar{h}^H_{RE_1}} \ \cdots \ \mathbf{h^T_{TE_K}} \otimes \mathbf{\bar{h}^H_{RE_K}}\right]^{\mathbf{H}} \left[\mathbf{h^T_{TE_1}} \otimes \mathbf{\bar{h}^H_{RE_1}} \ \cdots \ \mathbf{h^T_{TE_K}} \otimes \mathbf{\bar{h}^H_{RE_K}}\right], \tag{6}$$

$$\mathbf{B_2} \triangleq \left[\mathbf{h^T_{TE_1}} \otimes \mathbf{\bar{h}^H_{ME_1}} \ \cdots \ \mathbf{h^T_{TE_K}} \otimes \mathbf{\bar{h}^H_{ME_K}}\right]^{\mathbf{H}} \left[\mathbf{h^T_{TE_1}} \otimes \mathbf{\bar{h}^H_{ME_1}} \ \cdots \ \mathbf{h^T_{TE_K}} \otimes \mathbf{\bar{h}^H_{ME_K}}\right], \tag{7}$$

$$\mathbf{B_3} \triangleq \text{diag}\left(\sigma^2_{\mathbf{E_1}}\left(\mathbf{I_{N_{R,E_1}}} \otimes \mathbf{\bar{h}_{RE_1}\bar{h}^H_{RE_1}}\right), \ \cdots, \ \sigma^2_{\mathbf{E_1}}\left(\mathbf{I_{N_{R,E_K}}} \otimes \mathbf{\bar{h}_{RE_K}\bar{h}^H_{RE_K}}\right)\right), \tag{8}$$

$$\mathbf{B_4} \triangleq \text{diag}\left(\sigma^2_{\mathbf{E_1}}\left(\mathbf{I_{N_{R,E_1}}} \otimes \mathbf{\bar{h}_{ME_1}\bar{h}^H_{ME_1}}\right), \ \cdots, \ \sigma^2_{\mathbf{E_1}}\left(\mathbf{I_{N_{R,E_K}}} \otimes \mathbf{\bar{h}_{ME_K}\bar{h}^H_{ME_K}}\right)\right), \tag{9}$$

$$\mathbf{B_{5,E_k}} \triangleq \mathbf{E^H_{E_k}}\left(\left(\mathbf{P_T h_{TE_k} h^H_{TE_k}} + \sigma^2_{\mathbf{E_k}}\mathbf{I_{N_{R,E_k}}}\right)^{\mathbf{T}} \otimes \mathbf{I}_{\theta_{\mathbf{E_k},0}}\right)\mathbf{E_{E_k}}, \tag{10}$$

where the constants are defined by (6)-(10) with $\mathbf{E_{E_k}} \triangleq \left[\mathbf{0} \ \cdots \ \mathbf{I}_{\theta_{E_k,0}\mathbf{N}_{R,E_k}} \ \cdots \ \mathbf{0}\right]$. Here the identity matrix spans from the $\left(\sum_{j=1}^{k-1}\theta_{E_j,0}N_{R,E_j}+1\right)$-th to the $\sum_{j=1}^{k}\theta_{E_j,0}N_{R,E_j}$-th column.

(P1) also reveals that $\mathbf{Q_J}$ can be designed independent of $\left\{\mathbf{\bar{G}}_{E_k}\right\}$ since it only affects the amount of jamming interference $\mathbf{h^H_{RJ}Q_J h_{RJ}}$ at the suspicious receiver. In fact, the maximum jamming to the suspicious receiver subject to $\text{tr}\left(\mathbf{Q_J}\right) \le \bar{P}_J$ is easily obtained by the maximal ratio transmission (MRT) with $\mathbf{Q}_{\mathbf{J},\max} = \mathbf{\bar{P}_J}\frac{\mathbf{h_{RJ}h^H_{RJ}}}{\|\mathbf{h_{RJ}}\|^2}$ [19], and all the other interference $0 \le \mathbf{h^H_{RJ}Q_J h_{RJ}} \le \mathbf{\bar{P}_J}\|\mathbf{h_{RJ}}\|^{\mathbf{2}}$ can be represented by simply adjusting the transmit power P_J of $\mathbf{Q_J} = \mathbf{P_J}\frac{\mathbf{h_{RJ}h^H_{RJ}}}{\|\mathbf{h_{RJ}}\|^2}$ for $0 \le P_J \le \bar{P}_J$ where $\text{tr}\left(\mathbf{Q_J}\right) = P_J$.

We therefore rewrite (P1) as

$$\text{(P1.1):} \max_{\mathbf{\bar{G}},P_J} \frac{P_T\left|h_{TR}\right|^2}{\text{tr}\left(\left(P_T\mathbf{B_1}+\mathbf{B_3}\right)\mathbf{\bar{G}}\right)+P_J\left\|\mathbf{h_{RJ}}\right\|^2+\sigma^2_R} \tag{11a}$$

$$\text{s.t.} \ \frac{P_T\text{tr}\left(\mathbf{B_2\bar{G}}\right)}{\text{tr}\left(\mathbf{B_4\bar{G}}\right)+\sigma^2_M} \ge \frac{P_T\left|h_{TR}\right|^2}{\text{tr}\left(\left(P_T\mathbf{B_1}+\mathbf{B_3}\right)\mathbf{\bar{G}}\right)+P_J\left\|\mathbf{h_{RJ}}\right\|^2+\sigma^2_R}, \tag{11b}$$

$$\frac{P_T\text{tr}\left(\mathbf{B_2\bar{G}}\right)}{\text{tr}\left(\mathbf{B_4\bar{G}}\right)+\sigma^2_M} \ge \bar{\gamma}_M, \tag{11c}$$

$$P_J \le \bar{P}_J, \ \text{tr}\left(\mathbf{B_{5,E_k}\bar{G}}\right) \le \bar{P}_{E_k}, \ \forall k, \tag{11d}$$

$$\text{rank}\left(\mathbf{\bar{G}}\right) \le 1, \ \mathbf{\bar{G}} \succeq \mathbf{0}. \tag{11e}$$

(P1.1) is still difficult to handle since (11b) and the rank-one constraint induce non-convexity issues. We thus first relax the rank-one constraint, and apply the two-layer optimization procedure with a new auxiliary variable $\alpha > 0$ as

$$\begin{aligned}\text{(P1.2):} \max_{\alpha,\mathbf{\bar{G}},P_J} \ & \alpha,\\ \text{s.t.} \ & P_T\left|h_{TR}\right|^2 = \alpha P_T\text{tr}\left(\mathbf{B_1\bar{G}}\right)+\alpha\text{tr}\left(\mathbf{B_3\bar{G}}\right)\\ & \qquad +\alpha P_J\left\|\mathbf{h_{RJ}}\right\|^2+\alpha\sigma^2_R,\\ & P_T\text{tr}\left(\mathbf{B_2\bar{G}}\right) \ge \max\left\{\alpha,\bar{\gamma}_M\right\}\left(\text{tr}\left(\mathbf{B_4\bar{G}}\right)+\sigma^2_M\right),\\ & \mathbf{\bar{G}} \succeq \mathbf{0}, \ \mathbf{P_J} \le \mathbf{\bar{P}_J}, \ \text{tr}\left(\mathbf{B_{5,E_k}\bar{G}}\right) \le \mathbf{\bar{P}_{E_k}}, \ \forall \mathbf{k}.\end{aligned}$$

In a similar manner, we search for an optimal α_{opt} through a one-dimensional search method in the outer layer, and for a fixed α, we solve the following SDR inner problem:

$$\text{(P1.3):} \min_{\mathbf{\bar{G}},P_J} \ \text{tr}\left(\mathbf{\bar{G}}\right)$$

$$\text{s.t.} \ P_T\left|h_{TR}\right|^2 = \alpha P_T\text{tr}\left(\mathbf{B_1\bar{G}}\right)+\alpha\text{tr}\left(\mathbf{B_3\bar{G}}\right) + \alpha P_J\left\|\mathbf{h_{RJ}}\right\|^2+\alpha\sigma^2_R, \tag{13a}$$

$$P_T\text{tr}\left(\mathbf{B_2\bar{G}}\right) \ge \max\left\{\alpha,\bar{\gamma}_M\right\}\left(\text{tr}\left(\mathbf{B_4\bar{G}}\right)+\sigma^2_M\right), \tag{13b}$$

$$\mathbf{\bar{G}} \succeq \mathbf{0}, \ \mathbf{P_J} \le \mathbf{\bar{P}_J}, \ \text{tr}\left(\mathbf{B_{5,E_k}\bar{G}}\right) \le \mathbf{\bar{P}_{E_k}}, \ \forall \mathbf{k}. \tag{13c}$$

Since (P1.3) is convex, it can be readily solved via existing softwares such as CVX [20]. Nevertheless, if the rank of the optimal solution $\mathbf{\bar{G}}_{\text{opt}}$ at α_{opt} is greater than one, then α_{opt} is only an upper bound of the original problem (P1). In this case, approximation techniques such as randomization or SVD should be proceeded to obtain a rank-one suboptimal solution [21].

A. Baseline scheme: Nullification on the suspicious receiver

We have seen that interference induced by the eavesdropping relays with a relay processing delay $\tau \ge T_{\text{sym}}$ brings about an adverse effect on the SINR of the suspicious receiver, which eventually lowers the eavesdropping rate. Hence, additional zero-forcing on the suspicious receiver may be considered for $N_{T,E_k} > 1+\sum_{\ell=1}^{K}N_{R,E_\ell}$ with $\mathbf{G_{E_k}} = \mathbf{\tilde{V}_{E_k,0}\tilde{G}_{E_k}}$, where $\mathbf{\tilde{V}}_{E_k,0} \in \mathbb{C}^{N_{T,E_k}\times\tilde{\theta}_{E_k,0}}$ and $\tilde{\theta}_{E_k,0} \triangleq N_{T,E_k} - \left(1+\sum_{\ell=1}^{K}N_{R,E_\ell}\right)$ spans the nullspace of $\mathbf{\tilde{H}}_{E_k} \triangleq \left[\mathbf{h^\dagger_{RE_k}} \ \mathbf{H^H_{E_kE_1}} \ \cdots \ \mathbf{H^H_{E_kE_k}} \ \cdots \ \mathbf{H^H_{E_kE_K}}\right]^H$ through SVD.

Then, from [18] and utilizing the MRT beamforming structure $\mathbf{Q_J} = \mathbf{P_J}\frac{\mathbf{h_{RJ}h^H_{RJ}}}{\|\mathbf{h_{RJ}}\|^2}$ with $0 \le P_J \le \bar{P}_J$, we can easily transform (P1) into

$$\begin{aligned}\text{(P1.4):} \max_{\mathbf{\tilde{G}},P_J} \ & \frac{P_T\left|h_{TR}\right|^2}{P_J\left\|\mathbf{h_{RJ}}\right\|^2+\sigma^2_R}\\ \text{s.t.} \ & \frac{P_T\text{tr}\left(\mathbf{\tilde{B}_2\tilde{G}}\right)}{\text{tr}\left(\mathbf{\tilde{B}_4\tilde{G}}\right)+\sigma^2_M} \ge \max\left\{\frac{P_T\left|h_{TR}\right|^2}{P_J\left\|\mathbf{h_{RJ}}\right\|^2+\sigma^2_R},\bar{\gamma}_M\right\},\\ & P_J \le \bar{P}_J, \ \text{tr}\left(\mathbf{\tilde{B}}_{5,E_k}\mathbf{\tilde{G}}\right) \le \bar{P}_{E_k}, \ \forall k,\\ & \text{rank}\left(\mathbf{\tilde{G}}\right) \le 1, \ \mathbf{\tilde{G}} \succeq \mathbf{0},\end{aligned}$$

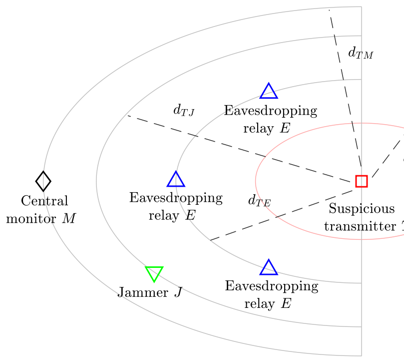

Fig. 2. Node placement of a central monitor, eavesdropping relays, a jammer and suspicious communications users

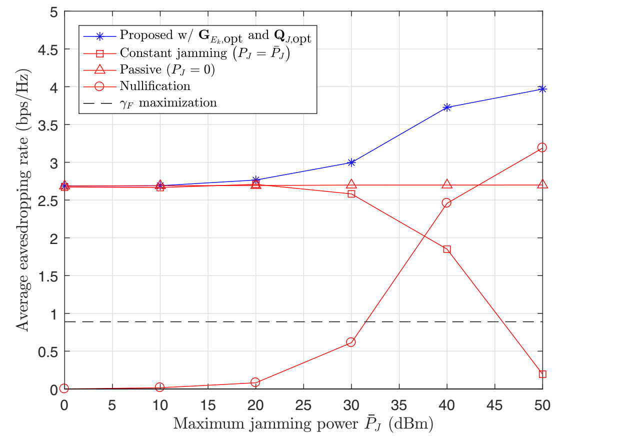

Fig. 3. Average eavesdropping rate as a function of $\bar{P}_J$ with multiple eavesdropping relays

where $\tilde{\mathbf{B}}_2$, $\tilde{\mathbf{B}}_4$ and $\tilde{\mathbf{E}}_{E_k}$ are essentially the same as the previous $\mathbf{B_2}$, $\mathbf{B_4}$ and $\mathbf{E_{E_k}}$ except that $\bar{\mathbf{h}}_{ME_k}$ and $\theta_{E_k,0}$ are now replaced by $\tilde{\mathbf{h}}_{ME_k} \triangleq \tilde{\mathbf{V}}^H_{E_k,0}\mathbf{h}^\dagger_{\mathbf{ME_k}}$ and $\tilde{\theta}_{E_k,0}$, respectively. From the result of this additional nullification, the eavesdropping relays are now fully occupied by forwarding information, while it is only the jammer that controls the suspicious data rate. Also, unlike (P1.1), the two-layer optimization approach for (P1.4) always yields a rank-one optimal solution, and its proof is omitted for brevity.

IV. Simulation Results

In this section, we provide numerical performance of the proactive eavesdropping system with the AF FD eavesdropping relays and the cooperative jammer in the presence of suspicious communications users. We adopt the channel model $|\mathbf{H_{XY}}|^2 = 10^{-3}d_{\mathsf{XY}}^{-\beta}\,|\mathsf{H}_{\mathsf{XY}}|^2$, $\forall \mathsf{X},\mathsf{Y} \in \{T, R, E_k, \forall k, J, M\}$, where β is the path loss exponent, and d_{XY} represents the distance between X and Y as in [22]. We assume that each element of the small-scale channel matrix H_{XY} follows an independent Rayleigh distribution with $\beta = 3.5$.

The suspicious receiver is randomly placed with a fixed distance d_{TR} from the suspicious transmitter. Also, the central monitor, the k-th eavesdropping relays, and the jammer are randomly located from the suspicious transmitter with distance d_{TM}, d_{TE_k} and d_{TJ}, respectively, within a half circle area as depicted in Fig. 2. The bandwidth is set to $W = 20$ MHz, and the transmit power at the suspicious transmitter is fixed as 23 dBm. The minimum required SINR at the central monitor is $\bar{\gamma}_M = 0$ dB, and the maximum transmit power for the eavesdropping relays and the jammer equal $\bar{P}_{E_k} = 33$ dBm, $\forall k$, and $\bar{P}_J = 33$ dBm, respectively. We also assume that the residual SI power after both analog and digital SIC is $\sigma^2_{\mathrm{SI},k} = -100$ dB [23], while all additive white Gaussian noise power values are set to -170 dBm/Hz.

We compare our proposed system with the baseline scheme discussed in Section III-A, named by "Nullification", where zero-forcing is applied on the suspicious receiver, and with "γ_M maximization" where the channel capacity γ_M of the central monitor is maximized without taking into consideration any interference effects on the suspicious users. In addition, "Passive" and "Constant jamming" schemes indicate that only the relay precoders $\{\mathbf{G_{E_k}}\}$ are optimized with $P_J = 0$ and $P_J = \bar{P}_J$, respectively.

We first evaluate the performance with $K = 3$, $N_{R,E_k} = 1$, $N_{T,E_k} = KN_{R,E_k} + 2$ and $N_{T,J} = 5$. Fig. 3 presents the average eavesdropping rate as a function of the maximum jamming power $\bar{P}_J$ when $d_{TR} = 20$ m, $d_{TE_k} = 150$ m, $\forall k$, $d_{TJ} = 150$ m and $d_{TM} = 620$ m. As $\bar{P}_J$ increases, the proposed optimal power allocation scheme outperforms other compared ones. For instance, there are 38%, 47% and 69% performance gains over the passive, the constant jamming and the nullification schemes, respectively, at $P_J = 40$ dBm. Meanwhile, it is shown that the constant jamming scheme becomes inefficient as $\bar{P}_J$ grows, since it unnecessarily decreases the suspicious data rate, that is, the eavesdropping rate. Therefore, the figure underlines not only the necessity of the jammer but also the importance of power allocation in enhancing the eavesdropping rate. We can also notice that the eavesdropping performance of "Nullification" rapidly increases with $\bar{P}_J$. This is because only the jammer controls γ_R to fulfill the successful eavesdropping channel condition $\gamma_M \geq \gamma_R$. Thus, as more jamming power is allowed, the capability of the jammer to adjust γ_R improves without the aid of extra interference from the relays. In addition, merely maximizing the channel capacity γ_M of the central monitor without consideration of interference to the suspicious receiver ends up with poor eavesdropping performance.

Fig. 4 compares the average eavesdropping rate for different numbers of the eavesdropping relays K with $d_{TR} = 20$ m, $d_{TE_k} = 200$ m, $\forall k$, $d_{TJ} = 130$ m and $d_{TM} = 620$ m. Note that the performance difference between our proposed scheme and the conventional "γ_M maximization" and "Nullification" becomes more pronounced as the number of eavesdropping relays increases. This implies that with more eavesdropping relays, the impact of the optimized relay precoder and jam-

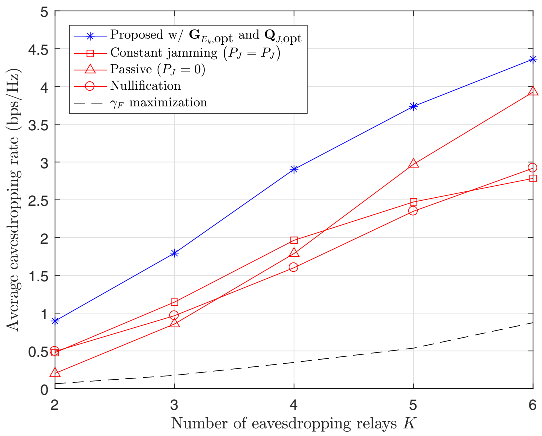

Fig. 4. Average eavesdropping rate as a function of K

ming power becomes significant.

V. Conclusion

In this work, we have proposed a proactive eavesdropping scheme where a distant central monitor eavesdrops the information exchanged between a suspicious pair through AF FD relays and a cooperative jammer. We have utilized the two-layer SDR approach to optimize the relay precoders at the eavesdropping relays and the transmit covariance matrix of the jammer. The simulation results have verified that our proposed solutions outperform other conventional schemes.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, October 1975.

[2] H. Lee, C. Song, J. Moon, and I. Lee, "Precoder designs for MIMO Gaussian multiple access wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 8563 – 8568, September 2017.

[3] Q. Li, W.-K. Ma, and D. Han, "Sum secrecy rate maximization for full-duplex two-way relay networks using Alamouti-based rank-two beamforming," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, pp. 1359–1374, December 2016.

[4] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, "Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 2537–2551, April 2016.

[5] Z. Zhu, Z. Chu, Z. Wang, and I. Lee, "Outage constrained robust beamforming for secure broadcasting systems with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 7610–7620, November 2016.

[6] J. Moon, H. Lee, C. Song, and I. Lee, "Secrecy performance optimization for wireless powered communication networks with an energy harvesting jammer," *IEEE Transactions on Communications*, vol. 65, pp. 764–774, February 2017.

[7] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: a new wireless security paradigm," *IEEE Wireless Communications*, vol. 24, pp. 152–159, August 2017.

[8] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Wireless Communications Letters*, vol. 5, pp. 80–83, February 2016.

[9] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 2790–2806, May 2017.

[10] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: design and performance analysis," *IEEE Transactions on Wireless Communications*, vol. 16, pp. 4585–4599, July 2017.

[11] G. Ma, J. Xu, L. Duan, and R. Zhang, "Wireless surveillance of two-hop communications," *[Online] Available on: https://arxiv.org/abs/1704.07629*.

[12] X. Jiang, H. Lin, C. Zhong, X. Chen, and Z. Zhang, "Proactive eavesdropping in relaying systems," *IEEE Signal Processing Letters*, vol. 24, pp. 917–921, June 2017.

[13] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," *accepted for IEEE Signal Processing Letters*.

[14] D. Nguyen, L.-N. Tran, P. Pirinen, and M. Latva-aho, "Precoding for full duplex multiuser MIMO systems: spectral and energy efficiency maximization," *IEEE Transactions on Signal Processing*, vol. 61, pp. 4038–4050, August 2013.

[15] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Transactions on Signal Processing*, vol. 59, pp. 5983–5993, December 2011.

[16] X. Xu, X. Chen, M. Zhao, S. Zhou, C.-Y. Chi, and J. Wang, "Power-efficient distributed beamforming for full-duplex MIMO relaying networks," *IEEE Transactions on Vehicular Technology*, vol. 66, pp. 1087–1103, February 2017.

[17] H. Sung, S.-R. Lee, and I. Lee, "Generalized channel inversion methods for multiuser MIMO systems," *IEEE Transactions on Communications*, vol. 57, pp. 3489–3499, November 2009.

[18] H. Lütkepohl, *Handbook of matrices*. John Wiley & Sons, Inc., July 1996.

[19] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," *IEEE Transactions on Wirless Communications*, vol. 12, pp. 1989–2001, May 2013.

[20] M. Grant and S. Boyd, *CVX: Matlab Software for Disciplined Convex Programming, version 2.1*. http://cvxr.com/cvx, March 2014.

[21] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite Relaxation of Quadratic Optimization Problems," *IEEE Signal Processing Magazine*, vol. 27, pp. 20–34, May 2010.

[22] H. Xing, K.-K. Wong, A. Nallanathan, and R. Zhang, "Wireless powered cooperative jamming for secrecy multi-AF relaying networks," *IEEE Transactions on Wireless Communications*, vol. 15, pp. 7971–7984, December 2016.

[23] C. Zhang, L. Laughlin, M. A. Beach, K. A. Morris, and J. L. Haine, "A self-interference cancellation testbed for full-duplex transceiver prototyping," *in Proc. IEEE International Conference on Communications and Electronics (ICCE)*, pp. 457–461, September 2016.