This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

Proactive Eavesdropping via Jamming in Full-duplex Multi-Antenna Systems: Beamforming Design and Antenna Selection

Farnaz Feizi, Mohammadali Mohammadi, *Member, IEEE,*
Zahra Mobini, *Member, IEEE*, and Chintha Tellambura, *Fellow, IEEE*

***Abstract*—This paper investigates the application of full-duplex (FD) multi-antenna transceivers in proactive eavesdropping systems. To this end, we jointly optimize the transmit and receive beamformers at the legitimate FD monitor to maximize the eavesdropping non-outage probability of the system. The resulting non-convex problem is solved using two-layer decomposition technique. The inner layer problem is formulated as a semidefinite relaxation problem, and the outer problem is solved by one-dimensional line search. We further propose sub-optimum beamforming designs, where the beamformers are obtained using zero-forcing, and maximum ratio transmission. To archive a low-complexity implementation, we study the antenna selection problem as an alternative for performance optimization. Particularly, based on the system's eavesdropping non-outage probability, several antenna selection schemes are proposed to choose single transmit and single receive antenna at the FD monitor. For each scheme, we derive closed-form expressions of the eavesdropping non-outage probability. Our findings reveal that proposed antenna selection schemes can achieve the performance close to that of the proposed optimum/sub-optimum beamforming design, but with much lower implementation complexity.**

***Index Terms*—Eavesdropping non-outage probability, proactive monitoring, full-duplex (FD), beamforming, antenna selection.**

I. Introduction

Due to the open nature of the wireless medium, wireless signals are exposed to be heard by both the authorized and unauthorized users. This can be a potential security hazard. In this context, physical-layer security techniques including jamming [2]–[4], artificial noise [5], and security-oriented beamforming [6] have been proposed to improve the secrecy performance. On the other hand, given the threats to public security, the need to monitor the activity of unauthorized wireless devices and systems has increased recently [7].

Thus, **proactive eavesdropping** has been considered as a new avenue of studies in the field of physical-layer security [7]. This new framework emphasizes on wireless surveillance, which aims to overhear and perceive communications among suspicious users who misuse communication resources for illegal activities [7]–[9]. In particular, for government agencies, proactive eavesdropping enables legal monitoring of communication links to detect abnormal behaviors of suspicious users, e.g., communications containing anti-security information [7]. Two effective approaches for legitimate information surveillance have been proposed in literature, namely, spoofing-relay-based proactive eavesdropping [8], [9] and proactive eavesdropping via jamming [10], [11]. In the spoofing-relay-based proactive eavesdropping, a full-duplex (FD) relay (monitor) eavesdrops the suspicious users as well as deceives them by changing the information transmission rate of the source node to enhance the eavesdropping performance. In the proactive eavesdropping via jamming approach, however, the legitimate monitor simultaneously eavesdrops and transmits jamming signals via either co-located or separately located eavesdropping and jamming antennas, to degrade the suspicious source-destination communication link. The co-located structures have drawn more attention, since they facilitate joint design of eavesdropping and jamming [11]. Therefore, FD transceivers play a key role in both approaches. Accordingly, thanks to significant progress in practical implementation of FD transceivers [12], [13], these approaches are expected to become operational.

A growing body of literature exists on the practical and theoretical aspects of legitimate surveillance approaches under various system setups, including relay systems [9], [14], [15], multi-antenna systems [16]–[20], unmanned aerial vehicle (UAV) assisted systems [21], [22], wireless powered communication systems [23], and intelligent reflecting surface enhanced wireless systems [24]. In particular, in [9] a proactive eavesdropping scheme with several FD spoofing relays and a cooperative jammer has been proposed, where spoofing relays not only intercept but also forward the manipulated information to control the data rate of the suspicious users in collaboration with the jammer. In [14] and [15], the authors studied wireless surveillance of a two-hop decode-and-forward and amplify-and-forward relaying communication system, respectively. In [16], the problem of average monitoring rate maximization for a suspicious source-destination pair, suspicious relay, and legitimate monitor system has been investigated. The performance of a multi-antenna FD monitor has been studied in [17], where joint design of jamming power and beamforming vector at the legitimate monitor has been considered. In [18], joint beamforming and jamming design for a millimeter wave information surveillance system has been investigated. Robust proactive monitoring via jamming scheme

F. Feizi, M. Mohammadi, and Z. Mobini are with the Faculty of Engineering, Shahrekord University, Shahrekord 115, Iran (email: F.feizi@stu.ac.ir, {m.a.mohammadi, z.mobini}@sku.ac.ir).

C. Tellambura is with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB T6G 2V4, Canada (e-mail: chintha@ece.ualberta.ca).

Part of this work has been presented at the 9th Int. Symp. Telecommun. (IST 2018), Tehran, Iran, Dec. 2018 [1].

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

has been studied in [19], where the worst-case probability of successful monitoring is maximized by designing the jamming interference beamforming. The authors in [20] characterized the achievable eavesdropping rate region of proactive eavesdropping over two suspicious communication links scenario, by optimizing the legitimate monitor's jamming transmit covariance matrix under the maximum transmit power constraint. A proactive eavesdropping scheme has been proposed in [21] where an FD monitor eavesdrops suspicious communication while sending the collected information to the UAV. In [22], the authors studied a wireless surveillance scenario where a ground legitimate monitor tries to decode the suspicious messages sent by a UAV-assisted suspicious transmitter. Legitimate eavesdropping in wireless-powered suspicious communication network has been investigated in [23], where optimal transmit power of the monitor for energy transfer and the optimal jamming transmit power of the jammer are derived to maximize the successful eavesdropping probability. An intelligent reflecting surface enabled legitimate monitoring system was proposed in [24], where monitor employs the passive reflection for constructive or destructive signal forwarding.

It should be mentioned that all the above mentioned works have not considered the impact of jamming on the quality of service (QoS) of other users who are legitimate (not suspicious) but are in the communication range of the monitor. In practice, a wireless network may also contain legitimate users who share the same spectrum with suspicious users, and thus their communications is likely to be degraded by the jamming signals. Therefore, we are motivated to study a wireless surveillance scenario where a legitimate monitor proactively eavesdrops a suspicious communication link and at the same time serves an unsuspicious user. Recent work in [25] investigated legitimate surveillance of a pair of suspicious users sharing the same spectrum with a pair of unsuspicious users. Specifically in [25], the problem of optimizing the jamming transmit power of the monitor for maximizing the successful eavesdropping probability was studied, under the constraint that the QoS of the unsuspicious users is not affected. Nevertheless, this problem has not been thoroughly investigated in the literature.

In this paper, unlike [17] that analyzed a multi-antenna legitimate surveillance system without any unsuspicious user, we study the performance of an FD multi-antenna surveillance system in presence of one unsuspicious downlink user. Particularly, in the downlink, a multi-antenna FD base station serves a scheduled downlink user, while at the same time acts as the legitimate monitor and tries to proactively eavesdrop suspicious transmissions between a pair of suspicious users. Moreover, the FD monitor acts as an interfere to the unauthorized destination and hence degrades the rate of the suspicious pair and enhances the successful eavesdropping probability. This multi-antenna setup allows for the enhancement of the surveillance performance with different beamforming designs and achieves spatial domain self-interference (SI) suppression at the monitor. The benefits of deploying multiple antennas at the FD monitor, however, come at the expense of additional computational complexity and radio frequency chains that scale up with antenna numbers [26]. To mitigate the growth of antenna numbers, antenna selection techniques offer an effective solution, which has low implementation complexity and performs close to traditional multi-antenna systems and is particularly relevant to systems with stricter computational/energy constraint. To the best of our knowledge, antenna selection has never been considered for multi-antenna FD surveillance systems, while this technique has been already investigated in the context of physical layer security [27], [28]. The main contributions of this work are:

- We formulate optimum transmit/receive beamforming design at the legitimate monitor and solve it using an efficient method. Our objective is to reduce the quality of the suspicious communication link, while guaranteeing a pre-defined QoS level at the unsuspicious downlink user. In order to reduce the computational complexity, we propose suboptimum beamforming schemes including maximal ratio transmission (MRT) and zero-forcing (ZF) at the legitimate monitor, to derive receive and transmit beamformers that cancel the SI effect and maximize the eavesdropping non-outage probability.
- We transform the complex non-convex beamforming optimization problem into a two-layer optimization problem. The inner layer problem is efficiently solved using semidefinite relaxation (SDR) and the outer problem is solved by one-dimensional line search.
- Several antenna selection schemes, including the optimal antenna selection scheme and four sub-optimal antenna selection schemes are proposed to maximize the eavesdropping non-outage probability. Specifically, a two-stage antenna selection is proposed that simultaneously ensures a QoS level at the downlink user and maximize the eavesdropping non-outage probability. The investigated antenna selection schemes are analyzed in terms of the eavesdropping non-outage probability and exact expressions are derived.
- Our findings reveal that proposed sub-optimal antenna selection schemes can achieve the performance close to that of the suboptimum beamforming designs. Moreover, when the number of receive antennas increases, the sub-optimal min-D max-E antenna selection scheme provides a better performance/implementation complexity trade-off than optimal antenna selection scheme, which its complexity is intensive when the number of antennas at the monitor becomes large.

The rest of the paper is organized as follows: Section II describes the network model. Section III and IV present the optimum/sub-optimum beamforming designs and antenna selection schemes, respectively, together with the system's eavesdropping non-outage probability analysis. Numerical results are presented in Section V, followed by conclusions in Section VI.

Notation: Bold upper-case letters denote matrices and bold lower-case letters denote vectors; The superscripts $(\cdot)^{\dagger}$ and $(\cdot)^{-1}$ stand for conjugate transpose and matrix inverse respectively; the trace of a matrix is denoted by $\text{tr}(\cdot)$; $\Pr(\cdot)$ denotes the probability; $\mathbb{E}\{X\}$, $f_X(\cdot)$ and $F_X(\cdot)$ denote the expectation, the probability density function (pdf), and

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

cumulative distribution function (cdf) of the random variable (RV) X, respectively; and $\mathcal{CN}(0,\sigma^2)$ denotes a zero-mean complex Gaussian RV with variance σ^2. We also use the notation $X \sim \chi^2_{2K}$ to denote a chi-square RV with $2K$ degrees-of-freedom (d.o.f.). $\mathrm{B}(\alpha,\beta)$ denotes the Beta function defined in [29, Eq. (8.380.1)]; $E_1(x) = \int_1^\infty \frac{e^{-xt}}{t}dt$ is the exponential-integral function of the first order [29, Eq. (8.211.1)]. $G^{mn}_{pq}\left(z \mid {a_1 \cdots a_p \atop b_1 \cdots b_q}\right)$ denotes the Meijer G-function [29, Eq. (9.301)].

II. System Model

We consider a legitimate surveillance system as shown in Fig. 1. An FD multi-antenna base station which acts as the legitimate monitor, denoted by E, tries to proactively eavesdrop the suspicious transmissions between a suspicious transmitter-receiver ($S-D$) pair, while simultaneously serving a scheduled downlink user U over the same frequency band. It is assumed that U, S, and D has single antenna each. E operates in FD mode, and hence, it is equipped with $\mathrm{N_R}$ receive antennas for eavesdropping and $\mathrm{N_T}$ transmit antennas for downlink transmission. As well, E utilizes the intended downlink signal for U to jam the suspicious receiver D.

A. Transmission Protocol

Assume that the suspicious source S transmits information signal x_s to its paired receiver D with transmit power P_s. The overheard signal at E can be written as

$$y_e = \sqrt{P_s}\mathbf{w}_r^\dagger \mathbf{h}_{se} x_s + \sqrt{P_e}\mathbf{w}_r^\dagger \mathbf{H}_{\mathsf{SI}} \mathbf{w}_t x_c + \mathbf{w}_r^\dagger \mathbf{n}_e, \quad (1)$$

where P_e is the transmit power of E, $\mathbf{w}_r \in \mathbb{C}^{\mathrm{N_R}\times 1}$ denotes the receive beamforming vector at the legitimate monitor with $\mathbb{E}\left\{\|\mathbf{w}_r\|^2\right\} = 1$, and $\mathbf{h}_{se} \in \mathbb{C}^{\mathrm{N_R}\times 1}$ is the channel vector between the S and E. Similar to [30], we model the elements of the SI channel $\mathbf{H}_{\mathsf{SI}} \in \mathbb{C}^{\mathrm{N_R}\times \mathrm{N_T}}$ as independent identically distributed (i.i.d) $\mathcal{CN}(0,\lambda_{\mathsf{SI}})$. Moreover, $\mathbf{w}_t \in \mathbb{C}^{\mathrm{N_T}\times 1}$ denotes the transmit beamformer at E with $\mathbb{E}\left\{\|\mathbf{w}_t\|^2\right\} = 1$, and x_c is the information signal intended for U, which is also used for jamming. Finally, $\mathbf{n}_e \sim \mathcal{CN}(0,\sigma_e^2\mathbf{I})$ is the zero-mean additive Gaussian noise (AWGN) at E. According to (1), the signal-to-interference-plus-noise ratio (SINR) at the legitimate monitor is

$$\mathrm{SINR_E} = \frac{P_s|\mathbf{w}_r^\dagger \mathbf{h}_{se}|^2}{P_e|\mathbf{w}_r^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2 + \sigma_e^2}. \quad (2)$$

Furthermore, the received signal at D is given by

$$y_d = \sqrt{P_s}h_{sd}x_s + \sqrt{P_e}\mathbf{h}_{ed}^\dagger \mathbf{w}_t x_c + n_d, \quad (3)$$

where h_{sd} denotes the channel coefficient between S and D, $\mathbf{h}_{ed} \in \mathbb{C}^{\mathrm{N_T}\times 1}$ is the channel vector corresponding to E-D link, and $n_d \sim \mathcal{CN}(0,\sigma_d^2)$ denotes the AWGN at D. Accordingly, the SINR at D is given by

$$\mathrm{SINR_D} = \frac{P_s|h_{sd}|^2}{P_e|\mathbf{h}_{ed}^\dagger \mathbf{w}_t|^2 + \sigma_d^2}. \quad (4)$$

Finally, the received signal at U can be expressed as

$$y_u = \sqrt{P_e}\mathbf{h}_{eu}^\dagger \mathbf{w}_t x_c + \sqrt{P_s}h_{su}x_s + n_u, \quad (5)$$

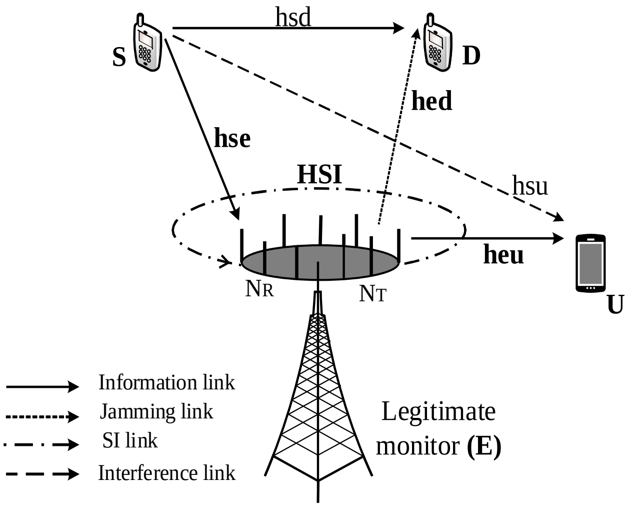


Fig. 1: FD proactive monitoring network.

where $\mathbf{h}_{eu} \in \mathbb{C}^{\mathrm{N_T}\times 1}$ is the channel vector between E and U, h_{su} denotes the channel coefficient between S and U, and $n_u \sim \mathcal{CN}(0,\sigma_u^2)$ is the AWGN at U. The received SINR at U can be obtained as

$$\mathrm{SINR_U} = \frac{P_e|\mathbf{h}_{eu}^\dagger \mathbf{w}_t|^2}{P_s|h_{su}|^2 + \sigma_u^2}. \quad (6)$$

The channel coefficient h_{sd} corresponding to the S-D link is assumed as i.i.d. complex Gaussian RV with zero-mean and variance λ_{sd}. Moreover, the entries of $\mathbf{h}_{se}$, $\mathbf{h}_{ed}$, and $\mathbf{h}_{eu}$ are i.i.d. zero mean complex Gaussian RVs with variance λ_{se}, λ_{ed}, and λ_{eu}, respectively.

By considering the eavesdropping non-outage probability as the performance metric, denoted as $\mathbb{E}\{X\}$, we evaluate the performance of various beamforming designs and antenna selection schemes at the legitimate monitor. The indicator function X in $\mathbb{E}\{X\}$ denotes the event of successful eavesdropping at the legitimate monitor, given by [10]

$$X = \begin{cases} 1 & \text{if } \mathrm{SINR_E} \geq \mathrm{SINR_D}, \\ 0 & \text{otherwise}, \end{cases} \quad (7)$$

where $X=1$ and $X=0$ indicate eavesdropping non-outage and outage events, respectively. In other words, to achieve a reliable detection at suspicious receiver, S varies its transmission rate according to $\mathrm{SINR_D}$. Hence, if $\mathrm{SINR_E} \geq \mathrm{SINR_D}$, the legitimate monitor, E, can also reliably decode the information intended to D. On the other hand, if $\mathrm{SINR_E} < \mathrm{SINR_D}$, legitimate monitor, E, is unable to decode this information without any error [17]. The eavesdropping non-outage probability is mathematically represented by

$$\mathbb{E}\{X\} = \Pr\left(\mathrm{SINR_E} \geq \mathrm{SINR_D}\right). \quad (8)$$

From (2) and (4) it is clear that $\mathbb{E}\{X\}$ depends on the receive and transmit beamformer at the legitimate monitor. Moreover, from (6) , the received SINR at the downlink user is a function of transmit beamformer.

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

III. Joint Receive/Transmit Beamforming Design

In this section, for the described FD surveillance system, we jointly optimize the transmit beamformer, $\mathbf{w}_t$, and receive beamformer, $\mathbf{w}_r$, that maximize the eavesdropping non-outage probability given a pre-defined QoS level at the downlink user. Moreover, we present two sub-optimal low-complexity ZF-based beamforming designs.

In order to characterize the fundamental information-theoretic performance limits of proactive eavesdropping over suspicious link, we assume that E has the perfect CSI of all links [10], [18], [20]. In practice, the legitimate monitor can overhear the pilot signals sent by suspicious transmitter and suspicious receiver to acquire the CSI of $\mathbf{h}_{se}$ and $\mathbf{h}_{ed}$, respectively. On the other hand, it can obtain the CSI of h_{sd} by eavesdropping the feedback channels of suspicious transmitter-receiver pair [20].

A. Optimum Beamforming Design

In this subsection, we propose a joint design of transmit and receive beamformer at the legitimate monitor, subject to individual SINR constraints at the downlink user, given by γ_{th}. Accordingly, the beamforming design problem is formulated as

$$\max_{\mathbf{w}_r,\mathbf{w}_t} \quad \mathbb{E}\{X\} \tag{9a}$$

$$\text{s.t} \quad \text{SINR}_{\text{U}} \geq \gamma_{\text{th}}, \tag{9b}$$

$$\|\mathbf{w}_t\| = \|\mathbf{w}_r\| = 1. \tag{9c}$$

By using (4), (2) and (8) the optimization problem (9) can be expressed as

$$\max_{\mathbf{w}_r,\mathbf{w}_t} \ \Pr\!\left(\frac{P_s|\mathbf{w}_r^\dagger \mathbf{h}_{se}|^2}{P_e|\mathbf{w}_r^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma_e^2} \geq \frac{P_s|h_{sd}|^2}{P_e|\mathbf{h}_{ed}^\dagger \mathbf{w}_t|^2+\sigma_d^2}\right) \tag{10a}$$

$$\text{s.t} \quad \frac{P_e|\mathbf{h}_{eu}^\dagger \mathbf{w}_t|^2}{P_s|h_{su}|^2+\sigma_u^2} \geq \gamma_{\text{th}}, \tag{10b}$$

$$\|\mathbf{w}_t\| = \|\mathbf{w}_r\| = 1. \tag{10c}$$

The objective function of (10) can be rewritten as [17]

$$\begin{aligned} \min_{\mathbf{w}_r,\mathbf{w}_t} \quad & \frac{|h_{sd}|^2}{P_e|\mathbf{h}_{ed}^\dagger \mathbf{w}_t|^2+\sigma_d^2} - \frac{|\mathbf{w}_r^\dagger \mathbf{h}_{se}|^2}{P_e|\mathbf{w}_r^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma_e^2} \\ \text{s.t} \quad & \frac{P_e|\mathbf{h}_{eu}^\dagger \mathbf{w}_t|^2}{P_s|h_{su}|^2+\sigma_u^2} \geq \gamma_{\text{th}}, \\ & \|\mathbf{w}_t\| = \|\mathbf{w}_r\| = 1. \end{aligned} \tag{11a}$$

The problem in (11) is non-convex, and thus for which the globally optimal solution is difficult to be obtained efficiently in general. Fortunately, by inspecting the objective function, we find out that only the second term, i.e., $\frac{|\mathbf{w}_r^\dagger \mathbf{h}_{se}|^2}{P_e|\mathbf{w}_r^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma_e^2}$, depends on the $\mathbf{w}_r$. Therefore, for a given $\mathbf{w}_t$, the optimum $\mathbf{w}_r$ is the solution of

$$\max_{\|\mathbf{w}_r\|=1} \quad \frac{|\mathbf{w}_r^\dagger \mathbf{h}_{se}|^2}{P_e|\mathbf{w}_r^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2+\sigma_e^2}. \tag{12}$$

Since (12) is a generalized Rayleigh ratio problem [31], the optimum receive beamformer can be obtained in closed-form as $\mathbf{w}_r^* = \frac{\left(\rho_e \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t\mathbf{w}_t^\dagger \mathbf{H}_{\mathsf{SI}}^\dagger + \mathbf{I}_{N_{\text{R}}}\right)^{-1}\mathbf{h}_{se}}{\|\left(\rho_e \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t\mathbf{w}_t^\dagger \mathbf{H}_{\mathsf{SI}}^\dagger + \mathbf{I}_{N_{\text{R}}}\right)^{-1}\mathbf{h}_{se}\|}$, where $\rho_e = \frac{P_e}{\sigma_e^2}$. Accordingly, by substituting $\mathbf{w}_r^*$ into (11), the optimization problem (11) can be written as

$$\min_{\|\mathbf{w}_t\|=1} \quad \frac{\frac{1}{\mu_1}|h_{sd}|^2}{1+\frac{P_e}{\sigma_d^2}|\mathbf{h}_{ed}^\dagger \mathbf{w}_t|^2} + \frac{\rho_e|\mathbf{h}_{se}^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t|^2}{1+\rho_e \mathbf{w}_t^\dagger \mathbf{H}_{\mathsf{SI}}^\dagger \mathbf{H}_{\mathsf{SI}}\mathbf{w}_t} \tag{13a}$$

$$\text{s.t} \quad \text{tr}\left(\mathbf{h}_{eu}^\dagger \mathbf{w}_t \mathbf{w}_t^\dagger \mathbf{h}_{eu}\right) \geq \varphi, \tag{13b}$$

where $\varphi = \frac{\gamma_{\text{th}}}{P_e}\left(P_s|h_{su}|^2+\sigma_u^2\right)$ and $\mu_1 = \frac{\sigma_d^2}{\sigma_e^2}$. The problem (13) is still a non-convex optimization problem due to the complex objective function. In order to circumvent this issue, similar to [17], we first introduce slack variable $t = 1+\frac{P_e}{\sigma_d^2}|\mathbf{h}_{ed}^\dagger \mathbf{w}_t|^2$. Then, applying the SDR technique to relax the quadratic terms of the beamformers in the objective function and constraints, the original problem is reformulated as follows:

$$\min_{\mathbf{W},t} \quad \frac{|h_{sd}|^2}{\mu_1 t} + \frac{\rho_e \ \text{tr}\left(\mathbf{W}\mathbf{H}_{\mathsf{SI}}^\dagger \mathbf{h}_{se}\mathbf{h}_{se}^\dagger \mathbf{H}_{\mathsf{SI}}\right)}{1+\rho_e \ \text{tr}\left(\mathbf{W}\mathbf{H}_{\mathsf{SI}}^\dagger \mathbf{H}_{\mathsf{SI}}\right)}, \tag{14a}$$

$$\text{s.t} \quad t = 1+\frac{P_e}{\sigma_d^2}\ \text{tr}\left(\mathbf{W}\mathbf{h}_{ed}\mathbf{h}_{ed}^\dagger\right), \tag{14b}$$

$$\text{tr}\left(\mathbf{W}\mathbf{h}_{eu}\mathbf{h}_{eu}^\dagger\right) \geq \varphi, \tag{14c}$$

$$\text{tr}\left(\mathbf{W}\right) = 1, \tag{14d}$$

$$\mathbf{W} \succeq 0, \tag{14e}$$

where $\mathbf{W} \triangleq \mathbf{w}_t\mathbf{w}_t^\dagger$. Problem (14) is still non-convex in objective function and constraints (14b) and (14d). However, by reformulating (14) into a two-layer problem, the problem can be solved [17], [32]. In particular, for the inner layer problem, we first drop the rank-one constraint, and then solve problem (14) for a given t. In order to solve the resulting quasi-convex fractional semidefinite programming (SDP), since the denominator of the fractional SDP is always positive, we use the Charnes and Cooper's transformation to convert fractional SDP into an equivalent SDP [33]. To this end, we define the transformed variable $\mathbf{Z} = s\mathbf{W}$, where $s > 0$ complies with $s+\rho_e \ \text{tr}\left(\mathbf{Z}\mathbf{H}_{\mathsf{SI}}^\dagger \mathbf{H}_{\mathsf{SI}}\right) = 1$. Therefore, by multiplying by the numerator and the denominator of the objective function in (14) with s, the inner problem is transformed into

$$f(t) = \min_{\mathbf{Z}\succeq 0, s>0} \quad \rho_e \ \text{tr}\left(\mathbf{Z}\mathbf{H}_{\mathsf{SI}}^\dagger \mathbf{h}_{se}\mathbf{h}_{se}^\dagger \mathbf{H}_{\mathsf{SI}}\right), \tag{15a}$$

$$\text{s.t} \quad s+\rho_e \ \text{tr}\left(\mathbf{Z}\mathbf{H}_{\mathsf{SI}}^\dagger \mathbf{H}_{\mathsf{SI}}\right) = 1, \tag{15b}$$

$$s(t-1) = \frac{P_e}{\sigma_d^2}\ \text{tr}\left(\mathbf{Z}\mathbf{h}_{ed}\mathbf{h}_{ed}^\dagger\right), \tag{15c}$$

$$\text{tr}\left(\mathbf{Z}\mathbf{h}_{eu}\mathbf{h}_{eu}^\dagger\right) \geq s\varphi, \tag{15d}$$

$$\text{tr}\left(\mathbf{Z}\right) = s, \tag{15e}$$

where $f(t)$ is the optimal value of problem (15). For given t, by dropping the non-convex constraint (15e), the optimization problem (15) becomes convex problem and thus can be solved by using CVX software. We notice that by applying Shapiro-Barvinok-Pataki rank reduction result[1], it can be shown that rank-one optimum solution of $\mathbf{Z}$ exists for the SDR problem (15).

We now consider the outer layer problem, which is formu-

[1] It is well-know from [34] that the real-valued or complex-valued nonseparable SDP has the optimal solution $\mathbf{X}^*$ satisfying $\text{rank}(X^*)(\text{rank}(X^*)+1) \leq 2m$ where m is the number of linear constraints. In case of complex-valued nonseparable SDP, the rank bound can be improved to $\text{rank}(X^*)^2 \leq m$ [35, Theorem 3.2].

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1 The proposed optimization scheme

```
Step 1: Initialize $t$:
        Define a fine grid of $t$, where $t \in [1, 1+\frac{P_e}{\sigma_d^2}\|\mathbf{h}_{ed}^\dagger\|^2)$
    and set $t = 1$.
Step 2:
    while $t \le 1+\frac{P_e}{\sigma_d^2}\|\mathbf{h}_{ed}^\dagger\|^2$ do
        Obtain $\mathbf{Z}$ and $f(t)$ by solving (15). Save $f(t)$ for given $t$.
        Take another $t$ from its grid.
    end while
Step 3: Solve (16) over $t$ and take the minimum $f(t)$ as
    optimal solution.
Step 4: Solve (15) with the optimal $f(t)$ and obtain $\mathbf{Z}^*$ and
    $s^*$.
Step 5: Obtain optimal $\mathbf{W}^* = s^*\mathbf{Z}^*$.
Step 6: Take $\mathbf{w}_t$ as the eigenvector corresponding to non-
    zero eigenvalue of $\mathbf{W}^*$.
```

lated as

$$\min_{t} \quad \frac{|h_{sd}|^2}{\mu_1}\frac{1}{t} + f(t) \qquad \text{s.t} \quad t_{min} \le t \le t_{max}, \tag{16}$$

where t_{min} and t_{max} are the upper and lower bounds of slack variable t, respectively. The solution to problem (16) can be readily obtained by one-dimensional line search over t. It can be readily checked that $t_{min} = 1$ and t_{max} is the maximum eigenvalue of matrix $\mathbf{I}_{\mathrm{N_T}} + \frac{P_e}{\sigma_d^2}\mathbf{h}_{ed}\mathbf{h}_{ed}^\dagger$, i.e., $t_{max} = 1 + \frac{P_e}{\sigma_d^2}\|\mathbf{h}_{ed}^\dagger\|^2$. To this end, by solving the SDP problem (15) with the optimal $f(t)$, obtained from one-dimensional line search, we can obtain the optimal design variable $\mathbf{W}^*$.

The proposed optimum beamforming design is outlined in**Algorithm 1.**

The complexity of solving the SDR problem (15) is $O(N_{\mathrm{T}}^{4.5})$ [36]. Moreover, since one-dimensional optimization along t is required, problem (15) needs to be solved N times, where N is the number of quantization point on t. Therefore, the total running time is $O(NN_{\mathrm{T}}^{4.5})$.

B. ZF/MRT Beamforming Design

The optimum beamforming design requires SDP that has a high computational complexity. Therefore, herein, two low-complexity sub-optimum ZF/MRT beamforming designs, namely RZF-I and RZF-II beamforming, are designed for the legitimate monitor to take advantage of the available multiple receive antennas to completely mitigate SI. To ensure feasibility, we need to deploy at least two receive antennas at the monitor, i.e., $\mathrm{N_R} > 1$. We consider two different maximization problems to obtain the $\mathbf{w}_r$ and $\mathbf{w}_t$.

1) RZF-I Beamforming: In this scheme, $\mathbf{w}_t$ is set according to the MRT principle to degrade the received SINR at the suspicious receiver, $\mathrm{SINR_D}$. With $\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}} = \frac{\mathbf{h}_{ed}}{\|\mathbf{h}_{ed}\|}$, the optimal beamforming vector $\mathbf{w}_r$, which maximizes eavesdropping non-outage probability, is the solution of

$$\max_{\|\mathbf{w}_r\|=1} |\mathbf{w}_r^\dagger\mathbf{h}_{se}|^2, \qquad \text{s.t} \quad \mathbf{w}_r^\dagger\mathbf{H}_{\mathsf{SI}}\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}} = 0. \tag{17}$$

Using projection matrix theory and following similar steps as in [37], the receive beamformer which satisfies the condition in (17), is given by

$$\mathbf{w}_{r,\mathsf{I}}^{\mathsf{ZF}} = \frac{\Xi^\perp\mathbf{h}_{ed}}{\|\Xi^\perp\mathbf{h}_{ed}\|}. \tag{18}$$

where $\Xi^\perp = I_{\mathrm{N_R}} - \frac{\mathbf{H}_{\mathsf{SI}}\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}}(\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}})^\dagger\mathbf{H}_{\mathsf{SI}}^\dagger}{\|\mathbf{H}_{\mathsf{SI}}\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}}\|^2}$ is the projection idempotent matrix with rank $(\mathrm{N_R} - 1)$. We note that matrix $\Xi^\perp$ can be expressed as [37]

$$\Xi^\perp = \mathbf{\Phi}^\dagger\mathsf{diag}\,(\mathbf{0}, \mathbf{1}, \cdots, \mathbf{1})\,\mathbf{\Phi}, \tag{19}$$

where $\mathbf{\Phi}$ is a unitary matrix. Therefore, using $\mathbf{w}_{r,\mathsf{I}}^{\mathsf{ZF}}$, the objective function in (17) can be expressed as

$$\begin{aligned} |(\mathbf{w}_{r,\mathsf{I}}^{\mathsf{ZF}})^\dagger\mathbf{h}_{se}|^2 &= \mathbf{h}_{se}^\dagger\Xi^\perp\mathbf{h}_{se} \\ &= \hat{\mathbf{h}}_{se}^\dagger\mathsf{diag}\,(0, 1, \cdots, 1)\,\hat{\mathbf{h}}_{se} \\ &= \|\tilde{\mathbf{h}}_{se}\|^2, \end{aligned} \tag{20}$$

where $\hat{\mathbf{h}}_{se} = \mathbf{\Phi}\mathbf{h}_{se}$ and $\tilde{\mathbf{h}}_{se}$ is a $(\mathrm{N_R}-1)\times 1$ vector, consisting of the $(\mathrm{N_R} - 1)$ last element of $\hat{\mathbf{h}}_{se}$.

2) RZF-II Beamforming: In RZF-II scheme, the QoS requirement of the downlink user is taken into consideration and $\mathbf{w}_{t,\mathsf{II}}$ is designed such that $\mathrm{SINR_U}$ is maximized. Therefore, we set $\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}} = \frac{\mathbf{h}_{eu}}{\|\mathbf{h}_{eu}\|}$. Moreover, the optimal receive beamformer $\mathbf{w}_r$ which maximizes eavesdropping non-outage probability as

$$\max_{\|\mathbf{w}_r\|=1} |\mathbf{w}_r^\dagger\mathbf{h}_{se}|^2, \qquad \text{s.t} \quad \mathbf{w}_r^\dagger\mathbf{H}_{\mathsf{SI}}\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}} = 0. \tag{21}$$

Similar to the RZF-I scheme, the receive weight vector $\mathbf{w}_r$ can be written as

$$\mathbf{w}_{r,\mathsf{II}}^{\mathsf{ZF}} = \frac{\Delta^\perp\mathbf{h}_{se}}{\|\Delta^\perp\mathbf{h}_{se}\|}. \tag{22}$$

where $\Delta^\perp = I_{\mathrm{N_R}} - \frac{\mathbf{H}_{\mathsf{SI}}\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}}(\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}})^\dagger\mathbf{H}_{\mathsf{SI}}^\dagger}{\|\mathbf{H}_{\mathsf{SI}}\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}}\|^2}$ is the projection idempotent matrix with rank $(\mathrm{N_R} - 1)$.

C. Performance Analysis

Here, we study the eavesdropping non-outage probability performance of the RZF-I and RZF-II beamforming designs. We further characterize the outage probability of the downlink user. Derivation of the eavesdropping non-outage probability of the optimum beamforming design is difficult. Thus, we have resorted to simulations for evaluating the eavesdropping non-outage probability of the optimum beamforming design in Section V.

1) Eavesdropping Non-outage Probability: By substituting $\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}}$ and $\mathbf{w}_{r,\mathsf{I}}^{\mathsf{ZF}}$ into (4) and (2), the received SINRs at the legitimate monitor and suspicious receiver with the RZF-I

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

beamforming design can be expressed as

$$\mathrm{SINR}_{\mathrm{D}}^{\mathrm{I}} = \frac{P_s|h_{sd}|^2}{P_e\|\mathbf{h}_{ed}\|^2 + \sigma_d^2}, \tag{23a}$$

$$\mathrm{SINR}_{\mathrm{E}}^{\mathrm{I}} = \rho_s\|\tilde{\mathbf{h}}_{se}\|^2, \tag{23b}$$

respectively, where $\rho_s = \frac{P_s}{\sigma_e^2}$. Moreover, by invoking (2) and (4) and using $\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}}$ and $\mathbf{w}_{r,\mathsf{II}}^{\mathsf{ZF}}$, the received SINRs at the legitimate monitor and suspicious receiver with the RZF-II beamforming design can be expressed as

$$\mathrm{SINR}_{\mathrm{D}}^{\mathrm{II}} = \frac{P_s|h_{sd}|^2}{P_e\frac{|\mathbf{h}_{ed}^\dagger\mathbf{h}_{eu}|^2}{\|\mathbf{h}_{eu}\|^2} + \sigma_d^2}, \tag{24a}$$

$$\mathrm{SINR}_{\mathrm{E}}^{\mathrm{II}} = \rho_s\|\tilde{\mathbf{h}}_{se}\|^2, \tag{24b}$$

respectively. By invoking (8), the eavesdropping non-outage probability of the proposed sub-optimum beamforming designs can be written as

$$\begin{aligned}\mathbb{E}\{X^{\mathrm{i}}\} &= \Pr\left(\frac{P_s}{\sigma_e^2}\|\tilde{\mathbf{h}}_{se}\|^2 \geq \frac{P_s|h_{sd}|^2}{P_e|\mathbf{h}_{ed}^\dagger\mathbf{w}_t|^2 + \sigma_d^2}\right)\\ &= 1 - \int_0^\infty F_Y(w)f_W(w)dw,\end{aligned} \tag{25}$$

where $\mathrm{i} \in \{\mathrm{I},\mathrm{II}\}$, $Y = \|\tilde{\mathbf{h}}_{se}\|^2$, and $W = \frac{|h_{sd}|^2}{\rho_e|\mathbf{h}_{ed}^\dagger\mathbf{w}_t|^2+\mu_1}$. We now present the eavesdropping non-outage probability of the proposed sub-optimum designs.

Proposition 1. *The exact eavesdropping non-outage probability of the RZF-I and RZF-II beamforming design can be respectively derived as*

$$\begin{aligned}\mathbb{E}\{X^I\} =& \frac{1}{\Gamma(\mathrm{N_T})}\sum_{j=0}^{\mathrm{N_R}-2}\sum_{k=0}^{\mathrm{N_T}-1}\frac{\binom{\mathrm{N_T}}{k}}{(k+1)\Gamma(j+1)}\\ &\times\left(\frac{\mathrm{N_T}\mu_1}{\lambda_{ed}\rho_e}\right)^{\mathrm{N_T}-k-1}\left(\frac{\lambda_{sd}\mathrm{N_T}}{\lambda_{ed}\lambda_{se}\rho_e}\right)^j\\ &\times G_{01}^{10}\left(\left(\frac{\mu_1}{\lambda_{sd}} + \frac{1}{\lambda_{se}}\right)\frac{\lambda_{sd}\mathrm{N_T}}{\lambda_{ed}\rho_e}\,\middle|\,\begin{matrix}-j\\ k-j+1,1\end{matrix}\right)\end{aligned} \tag{26a}$$

$$\begin{aligned}\mathbb{E}\{X^{II}\} =& \frac{e^{\frac{\mu_1}{\rho_e\lambda_{ed}}}}{\lambda_{sd}}\sum_{j=0}^{\mathrm{N_R}-2}\frac{1}{\Gamma(j+1)}\left(\frac{\lambda_{sd}}{\rho_e\lambda_{ed}\lambda_{se}}\right)^j\\ &\times\left(G_{12}^{21}\left(\frac{\lambda_{sd}}{\rho_e\lambda_{ed}\lambda_{se}}\,\middle|\,\begin{matrix}-j\\ 1-j,1\end{matrix}\right) +\right.\\ &\left.\mu_1\left(\frac{\lambda_{sd}}{\rho_e\lambda_{ed}}\right)G_{12}^{21}\left(\frac{\lambda_{sd}}{\rho_e\lambda_{ed}\lambda_{se}}\,\middle|\,\begin{matrix}-j\\ -j,1\end{matrix}\right)\right).\end{aligned} \tag{26b}$$

Proof: See Appendix A. ■

2) Downlink User Outage Probability: The outage probability of the downlink user is defined as the probability that the instantaneous SINR at U falls below a predefined threshold, γ_{th}, i.e.,

$$P_{\mathsf{out}}^{\mathsf{i}} = \Pr(\mathrm{SINR}_{\mathrm{U}}^{\mathsf{i}} \leqslant \gamma_{\mathrm{th}}) = F_{\mathrm{SINR}_{\mathrm{U}}^{i}}(\gamma_{\mathrm{th}}), \quad \mathrm{i} \in \{\mathrm{I},\mathrm{II}\}. \tag{27}$$

By substituting $\mathbf{w}_{t,\mathsf{I}}^{\mathsf{MRT}}$ and $\mathbf{w}_{t,\mathsf{II}}^{\mathsf{MRT}}$ into (6), the received SINRs at the downlink user with RZF-I and RZF-II beamforming design can be expressed as

$$\mathrm{SINR}_{\mathrm{U}}^{\mathrm{I}} = \frac{P_e\frac{|\mathbf{h}_{eu}^\dagger\mathbf{h}_{ed}|^2}{\|\mathbf{h}_{ed}\|^2}}{P_s|h_{su}|^2 + \sigma_u^2}, \tag{28a}$$

$$\mathrm{SINR}_{\mathrm{U}}^{\mathrm{II}} = \frac{P_e\|\mathbf{h}_{eu}\|^2}{P_s|h_{su}|^2 + \sigma_u^2}, \tag{28b}$$

respectively.

Proposition 2. *The exact outage probability of the downlink user with RZF-I and RZF-II beamforming design can be respectively expressed as*

$$P_{\mathrm{out}}^{\mathrm{I}} = 1 - \frac{e^{-\frac{\gamma_{\mathrm{th}}\sigma_u^2}{\lambda_{eu}P_e}}}{1 + \frac{P_s\lambda_{se}\gamma_{\mathrm{th}}}{P_e\lambda_{eu}}}, \tag{29a}$$

$$\begin{aligned}P_{\mathrm{out}}^{\mathrm{II}} =& 1 - \sum_{m=0}^{\mathrm{N_T}-1}\sum_{k=0}^{m}\binom{m}{k}\left(\frac{\gamma_{\mathrm{th}}\sigma_u^2}{\lambda_{su}\lambda_{eu}P_e}\right)^m\left(\frac{P_s}{\sigma_u^2}\right)^k\\ &\times\frac{\Gamma(k+1)e^{-\frac{\gamma_{\mathrm{th}}\sigma_u^2}{\lambda_{eu}P_e}}}{\Gamma(m+1)\left(\frac{1}{\lambda_{se}} + \frac{P_s\gamma_{\mathrm{th}}}{P_e\lambda_{eu}}\right)^{k+1}}.\end{aligned} \tag{29b}$$

Proof: The proof is straightforward and thus omitted. ■

We will consider next the problem of antenna selection in full-duplex proactive monitoring system. Before proceeding to this topic, it must be noted that multi-antenna systems suffer from high signal processing complexity and hardware cost. This is due to the fact that multi-antenna terminals require multiple radio frequency chains, consisting of amplifiers, mixers and analog to digital convertors, which typically require significant system implementation costs [26]. On the other hand, beamforming schemes normally impose high computational load to the system. In this context, antenna selection schemes with low implementation complexity have been proposed as a practical alternative in the literature to maintain system performance at a certain required level.

IV. Antenna Selection

We now consider antenna selection for the considered FD multi-antenna proactive system. Antenna selection is proposed as an alternative to the performance optimization developed earlier and is particularly relevant to systems with stricter computational/energy constraints. Antenna selection in FD systems is a complicated and hard problem as compared to that in HD systems widely studied in the current literature. This is because the backward and forward channels at the FD nodes are coupled through the SI link [30], [38], [39]. Therefore, antenna selection at the transmit or receive side cannot be performed independently of each other as is the case for HD systems. The coupling introduces new mathematical challenges for performance analysis since the involved RVs of various links now become correlated.

In the considered system, we assume that the legitimate monitor selects one single antenna out of $\mathrm{N_R}$ available antennas, i.e., i-th antenna, to receive and one single transmit antenna out of $\mathrm{N_T}$ available antennas, i.e. j-th antenna, to transmit signals. The channel between the j-th transmit and i-th receive antenna from terminal X to terminal Y, is denoted by $h_{XY}^{ji} \sim \mathcal{CN}(0,\lambda_{XY})$ where $X \in \{s,e\}$ and $Y \in \{e,d\}$.

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

Moreover, h_{SI}^{ji} denotes the SI link between the j-th transmit and i-th receive antenna at the FD legitimate monitor.

With antenna selection, the SINR at suspicious receiver, D, and legitimate monitor, E, can be respectively expressed as

$$\mathrm{SINR_D} = \frac{P_s|h_{sd}|^2}{P_e|h_{ed}^j|^2 + \sigma_d^2}, \tag{30a}$$

$$\mathrm{SINR_E} = \frac{P_s|h_{se}^i|^2}{P_e|h_{SI}^{ji}|^2 + \sigma_e^2}. \tag{30b}$$

A. Antenna Selection Schemes

In this subsection, with the aim of maximizing the eavesdropping non-outage probability, we propose four antenna selection schemes, which jointly select single receive and one single transmit antenna at the legitimate monitor.

1) Optimal AS Scheme: The optimal AS scheme maximizes the eavesdropping non-outage probability of the system, which is mathematically expressed as

$$\begin{aligned} i^*, j^* &= \underset{1\le i\le \mathrm{N_R},\ 1\le j\le \mathrm{N_T}}{\arg\max} \ \Pr\left(\frac{P_s|h_{se}^i|^2}{P_e|h_{SI}^{ji}|^2+\sigma_e^2} \ge \frac{P_s|h_{sd}|^2}{P_e|h_{ed}^j|^2+\sigma_d^2}\right) \\ &= \underset{1\le i\le \mathrm{N_R},\ 1\le j\le \mathrm{N_T}}{\arg\min} \ \frac{P_s|h_{sd}|^2}{P_e|h_{ed}^j|^2+\sigma_d^2} - \frac{P_s|h_{se}^i|^2}{P_e|h_{SI}^{ji}|^2+\sigma_e^2}. \end{aligned} \tag{31}$$

According to (31), the optimal AS scheme requires the full knowledge of all channel state information in order to decide on the selected antennas. The optimal AS scheme is difficult to realize in practice due to high computation and implementation complexity. However, it provides a good performance bound for practical antenna selection schemes.

2) Max-E AS Scheme: This scheme selects the best S-E link and then for given receive antenna at E, the weakest SI link is selected. In this way, the highest eavesdropping performance at the legitimate monitor can be achieved. Therefore, this antenna selection scheme is expressed as

$$\begin{aligned} i^* &= \underset{1\le i\le N_R}{\arg\max} \ |h_{se}^i|^2, \\ j^* &= \underset{1\le j\le N_T}{\arg\min} \ |h_{SI}^{ji^*}|^2. \end{aligned} \tag{32}$$

3) Min-D, Max-E AS Scheme: This scheme selects the best E-D and S-E links without considering the SI. According to this scheme, the received SINR at the suspicious receiver is minimized. This scheme can be mathematically represented by

$$\begin{aligned} j^* &= \underset{1\le j\le N_T}{\arg\max} \ |h_{ed}^j|^2, \\ i^* &= \underset{1\le i\le N_R}{\arg\max} \ \frac{P_s|h_{se}^i|^2}{P_e|h_{\mathsf{SI}}^{j^*i}|^2 + \sigma_e^2}. \end{aligned} \tag{33}$$

4) Two-stage AS Scheme: The aim of this AS scheme is to realize two purposes simultaneously. One is to ensure downlink user's SINR is realized, and the other is to maximize the non-outage eavesdropping probability of the system. Specifically, TAS scheme can be described in the following. The first stage is to build the following subset of the legitimate monitor's transmit antennas by focusing on the predefined level of the downlink user's SINR, i.e.,

$$\mathcal{A} = \left\{1 \le j \le \mathrm{N_T}: \quad \mathrm{SINR_U} = \frac{P_e|h_{eu}^j|^2}{P_s|h_{su}|^2 + \sigma_u^2} > \gamma_{\mathrm{th}}\right\}. \tag{34}$$

In the second stage, ”Max-E AS Scheme” or “Min-D, Max-E AS Scheme” can be implemented, with this difference that one transmit antenna is selected from $\mathcal{A}$. If ”Max-E AS Scheme” is used for the second stage, the selection is mathematically expressed as

$$i^* = \underset{1\le i\le N_R}{\arg\max} \ |h_{se}^i|^2, \tag{35}$$

$$j^* = \underset{j\in\mathcal{A}}{\arg\min} \ |h_{SI}^{ji^*}|^2. \tag{36}$$

5) Random AS Scheme: As a baseline for comparison, we consider the random AS scheme, which is commonly applied in the networks. With this scheme, one single receive antenna and one single transmit antenna are randomly selected at the legitimate monitor.

B. Performance Analysis

In this subsection, we study the eavesdropping non-outage probability of the proposed antenna selection schemes. By invoking (8), the eavesdropping non-outage probability of the system with antenna selection can be expressed as

$$\mathbb{E}\{X\} = \Pr\left(\frac{P_s|h_{se}^i|^2}{P_e|h_{SI}^{ji}|^2 + \sigma_u^2} \ge \frac{P_s|h_{sd}|^2}{P_e|h_{ed}^j|^2 + \sigma_d^2}\right). \tag{37}$$

Obtaining an analytical expression for the eavesdropping non-outage probability of the optimal AS scheme appears to be intractable due to the dependencies between the variables of $\mathrm{SINR_E}$ and $\mathrm{SINR_D}$. Therefore, in Section V, we will evaluate the eavesdropping non-outage performance of the optimal antenna selection scheme through the simulations. In what follows, we characterize the performance of the proposed suboptimal antenna selection schemes.

1) Max-E AS Scheme: The aim of this scheme is to select one transmit and one receive antenna at the legitimate monitor to maximize the $\mathrm{SINR_E}$, without considering $\mathrm{SINR_D}$. For max-E AS scheme, we now present a closed-form expression for the eavesdropping non-outage probability.

Proposition 3. *The exact eavesdropping non-outage probability for the max-E AS scheme can be derived as*

$$\begin{aligned} \mathbb{E}\{X\} =& \frac{\mathrm{N_T N_R}\lambda_{sd}\lambda_{ed}}{\varsigma^2\lambda_{se}\lambda_{\mathsf{SI}}}\Bigg(\mathcal{G}\left(\frac{\varsigma}{\lambda_{ed}\rho_e}, \frac{\varphi}{\varsigma}\right) \\ &- (\mathrm{N_R}-1)\sum_{p=0}^{\mathrm{N_R}-2}\frac{(-1)^p\binom{\mathrm{N_R}-2}{p}}{p+1}\,\mathcal{G}\left(\frac{\varsigma}{\lambda_{ed}\rho_e}, \frac{\varphi(p+2)}{\varsigma}\right)\Bigg) \\ &+ \mathrm{N_R}\left(\frac{1}{\lambda_{sd}}\mathrm{B}\left(1, \mathrm{N_R}\right) - \frac{1}{\lambda_{se}}\mathrm{B}\left(1 + \frac{\lambda_{se}}{\lambda_{sd}}\mu_1, \mathrm{N_R}\right)\right), \end{aligned} \tag{38}$$

where $\varsigma = \mu_1 + \frac{\mathrm{N_T}\lambda_{ed}}{\lambda_{\mathsf{SI}}}$, $\varphi = \mu_1 + \frac{\lambda_{sd}}{\lambda_{se}}$, *and*

$$\mathcal{Q}(x,y) = (1-y)^{-1}\left(I_2\left(x,y,1\right) - I_2\left(x,1,1\right)\right), \tag{39}$$

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

and

$$\mathcal{G}(x,y) = (1-y)^{-1} I_2(x,y,2) - (1-y)^{-2} \Big(I_2(x,y,1) - I_2(x,1,1) \Big), \tag{40}$$

with

$$I_2(\zeta_1,\zeta_2,m) = \begin{cases} e^{\zeta_1\zeta_2} E_1(\zeta_1\zeta_2) & m=1 \\ \sum_{p=0}^{m-1} \frac{(p-1)!}{(m-1)!} \frac{(-\zeta_1)^{m-p-1}}{\zeta_2^p} & \\ \quad + \frac{(-\zeta_1)^{m-1}}{(m-1)!} e^{\zeta_1\zeta_2} E_1(\zeta_1\zeta_2) & m \geq 2. \end{cases} \tag{41}$$

Proof: See Appendix B. ■

2) Min-D Max-E AS Scheme: With this scheme one transmit antenna at the legitimate monitor is first selected such that the $\mathrm{SINR_D}$ is minimized. Then, one receive antenna is selected to maximizes $\mathrm{SINR_E}$. In order to maximize $\mathrm{SINR_E}$, the best choice for receive antenna selection at the legitimate monitor is to select the antenna with and at the same time the antenna with strongest S-E link. However, since these two links are coupled to each other, the best receive antenna is selected such that $\frac{|h_{se}^i|^2}{|h_{\mathsf{SI}}^{j^*i}|^2}$ is maximized. To this end, in the following proposition, we present the key results for the eavesdropping non-outage probability of min-D max-E AS scheme.

Proposition 4. *The exact eavesdropping non-outage probability of the min-D max-E AS scheme can be derived as*

$$\mathbb{E}\{X\} = 1 - \frac{\mathrm{N_T}}{\lambda_{sd}\lambda_{ed}} \int_0^\infty e^{-\frac{\sigma_d^2}{\lambda_{sd}}w} \left(1 - \frac{e^{-\frac{\sigma_u^2}{\lambda_{se}}w}}{1+\frac{\lambda_{\mathsf{SI}}P_e}{\lambda_{se}}w} \right)^{\mathrm{N_R}} \\ \times \left(\frac{P_e}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{1}{\lambda_{ed}}\right)^2} + \frac{\sigma_d^2}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{1}{\lambda_{ed}}\right)} - (\mathrm{N_T}-1) \right. \\ \left. \times \sum_{p=0}^{\mathrm{N_T}-2} \frac{(-1)^p \binom{\mathrm{N_T}-2}{p}}{p+1} \left(\frac{P_e}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{p+2}{\lambda_{ed}}\right)^2} + \frac{\sigma_d^2}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{p+2}{\lambda_{ed}}\right)} \right) \right) dw. \tag{42}$$

Proof: See Appendix C. ■

The integral in (42) does not admit a closed-form solution. Fortunately, it can be efficiently evaluated numerically using standard mathematical software tools.

3) Two-stage AS Scheme: With TAS scheme one transmit and one receive antenna at the legitimate monitor are selected to maximize the $\mathrm{SINR_E}$, where the selected transmit antenna is forced to meet the SINR requirement of the downlink user.

Proposition 5. *The exact eavesdropping non-outage probability for the TAS Scheme with max-E AS scheme at the second stage can be written as*

$$\mathbb{E}\{X\} = \sum_{\ell=1}^{\mathrm{N_T}} \mathbb{E}\{X_{\mathrm{ME}}\}_{|\mathrm{N_T}=\ell} \binom{\mathrm{N_T}}{\ell} \mathcal{Q}^\ell (1-\mathcal{Q})^{\mathrm{N_T}-\ell} \tag{43}$$

where $\mathbb{E}\{X_{\mathrm{ME}}\}$ *denotes the eavesdropping non-outage probability of the Max-E AS scheme and*

$$\mathcal{Q} = \frac{e^{-\frac{\gamma_{\mathrm{th}}}{\lambda_{eu}}\frac{\sigma_u^2}{P_e}}}{1+\gamma_{\mathrm{th}}\frac{\lambda_{su}}{\lambda_{eu}}\frac{P_s}{P_e}}. \tag{44}$$

Proof: By considering the description of the second stage of the AS, the eavesdropping non-outage probability can be expressed as

$$\mathbb{E}\{X\} = \sum_{\ell=1}^{\mathrm{N_T}} \underbrace{\Pr\left(\frac{P_s|h_{se}^i|^2}{P_e|h_{SI}^{ji}|^2+\sigma_u^2} \geq \frac{P_s|h_{sd}|^2}{P_e|h_{ed}^j|^2+\sigma_d^2} \middle| |\mathcal{A}|=\ell \right)}_{\mathcal{P}_{\mathcal{A}\ell}} \\ \times \Pr\left(|\mathcal{A}|=\ell\right). \tag{45}$$

where $\mathcal{P}_{\mathcal{A}\ell}$ denotes the non-outage eavesdropping probability under the condition that there are ℓ transmit antenna at the legitimate monitor that guarantee the target SINR at the downlink user. It can be readily checked that $\mathcal{P}_{\mathcal{A}\ell}$ coincides the eavesdropping non-outage probability of the Max-E AS Scheme, in which $\mathrm{N_T} = \ell$. Moreover, $\Pr(|\mathcal{A}|=\ell)$ can be obtained as

$$\Pr\left(|\mathcal{A}|=\ell\right) = \binom{\mathrm{N_T}}{\ell} \prod_{n=1}^{\mathrm{N_T}-\ell} \left[1-\Pr\left(\mathrm{SINR_U} \geq \gamma_{\mathrm{th}}\right)\right] \\ \times \prod_{n=\mathrm{N_T}-\ell+1}^{\mathrm{N_T}} \Pr\left(\mathrm{SINR_U} \geq \gamma_{\mathrm{th}}\right) \\ = \binom{\mathrm{N_T}}{\ell} \mathcal{Q}^\ell (1-\mathcal{Q})^{\mathrm{N_T}-\ell}. \tag{46}$$

To this end, substituting (44) into (45), the desired result in (43) is obtained. ■

4) Random AS Scheme: The following proposition provides the key result for the random AS scheme.

Proposition 6. *The exact eavesdropping non-outage probability of the random As scheme is given by*

$$\mathbb{E}\{X\} = \frac{\sigma_d^2}{P_e\lambda_{ed}} \mathcal{Q}\left(\frac{\varphi\lambda_{se}}{\lambda_{sd}\lambda_{\mathsf{SI}}\rho_e}, \frac{\lambda_{sd}\lambda_{\mathsf{SI}}}{\lambda_{se}\lambda_{ed}} \right) \\ + \frac{\lambda_{sd}\lambda_{\mathsf{SI}}}{\lambda_{se}\lambda_{ed}} \mathcal{G}\left(\frac{\varphi\lambda_{se}}{\lambda_{sd}\lambda_{\mathsf{SI}}\rho_e}, \frac{\lambda_{sd}\lambda_{\mathsf{SI}}}{\lambda_{se}\lambda_{ed}} \right). \tag{47}$$

Proof: The proof follows by using the same arguments in Proposition 4 and hence is omitted. ■

V. Numerical Results and Discussions

In this section, we present the numerical results to validate the analysis accuracy and evaluate the performance of the proposed beamforming designs and antenna selection schemes. Unless otherwise stated, in all the simulations, we have set $\lambda_{se} = \lambda_{su} = \lambda_{eu} = 0.1$, $\lambda_{sd} = \lambda_{ed} = 1$, and $\sigma_d^2 = \sigma_e^2 = 1$.

In our simulations, we further include the performance of the maximum ratio combining (MRC)/MRT beamforming design as a baseline for comparison where $\mathbf{w}_r$ and $\mathbf{w}_t$ are matched to S-E and E-D links, respectively. We would like to point out that neither ZF/MRT beamforming designs nor MRC/MRT design can certainly ensure SINR requirement γ_{th} at the downlink user. Therefore, for fair comparison between the optimum and suboptimum beamforming designs, we use 10^5 independent fading channel realizations at each value of ρ_e. Then, in the case of ZF/MRT and MRC/MRT beamforming designs, the average is only taken over the results obtained from those channel realizations that ensure the received SINR at downlink user is grater than γ_{th}.

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

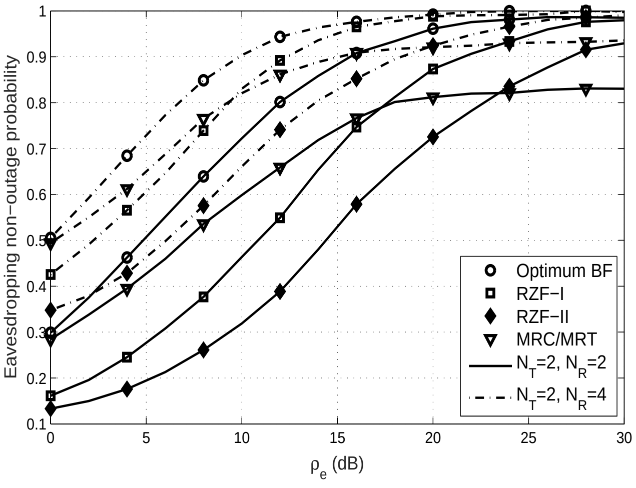


Fig. 2: $\mathbb{E}\{X\}$ versus ρ_e for the proposed optimum and suboptimum beamforming designs ($\mathrm{N_R} = 3$, $\mathrm{N_T} = 3$, and $\rho_s = 10$ dB).

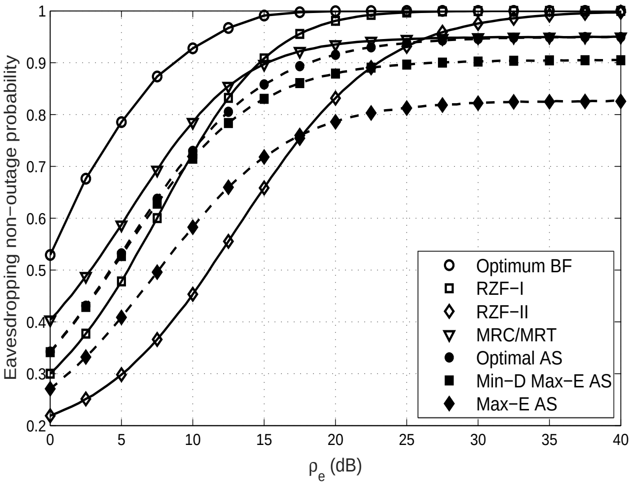


Fig. 3: $\mathbb{E}\{X\}$ versus ρ_e for the proposed antenna selection schemes and beamforming designs ($\mathrm{N_R} = 3$, $\mathrm{N_T} = 3$, and $\rho_s = 10$ dB).

Fig. 2 shows the eavesdropping non-outage probability versus ρ_e for the proposed optimum and suboptimum beamforming designs with different antenna configurations. We observe that MRC/MRT beamforming design outperforms the RZF-I and RZF-II beamforming designs in the low-SNR regime, and becomes inferior to the purposed ZF/MRT beamforming designs in the medium-to-high SNR regime. This behavior is intuitive since at low SNRs, overall interference can be treated as noise and therefore MRC filtering helps to maximize the SNR. Moreover, when the number of receive antennas $\mathrm{N_R}$ is increased, the ZF/MRT beamforming designs outperform the MRC/MRT scheme at lower values of ρ_e. For example, the RZF-I scheme starts to beat the MRC/MRT design at $\rho_e = 10$ dB with $\mathrm{N_R} = 4$, while it beats at $\rho_e = 16$ dB with $\mathrm{N_R} = 2$. This is due to the fact that increasing $\mathrm{N_R}$ results in strong SI, which is detrimental for the MRC/MRT design. We further observe that, among the proposed suboptimum designs, RZF-II (2, 4) achieves the best performance in the medium-to-high SNR operating regimes. Interestingly, RZF-II and optimum design have the same performance for high SNR regime. Moreover, MRC/MRT design performs remarkably inferior to RZF-I and RZF-II beamforming designs in the high SNR regime. This observation clearly shows the critical importance of suppressing the SI at the legitimate monitor. However, for low values of ρ_e, where the SI strength is low, the RZF designs perform worse than the MRC/MRT design since they sacrifice one d.o.f for SI suppression. It can be also observed that an increase in $\mathrm{N_R}$ tends to improve the eavesdropping non-outage probability of all beamforming designs, while the relative difference between the curves gets smaller. Moreover, proposed ZF/MRT beamforming designs outperform the MRC/MRT beamforming design at lower values of ρ_e. This is rather intuitive since using more receive antennas at the legitimate monitor provides multiple copies of the overheard signal, thus improving $\mathrm{SINR_E}$ and accordingly the eavesdropping non-outage probability.

Fig. 3 plots the eavesdropping non-outage probability of the system versus ρ_e for the proposed antenna selection and beamforming schemes. As can be observed, when ρ_e increases eavesdropping non-outage probability improves for all schemes. Moreover, optimum beamforming design outperforms the optimal AS scheme over the entire ρ_e region. However, the performance gap between optimum beamforming design and optimal AS scheme decreases with increasing ρ_e. In addition, with much lower computational complexity, the min-D max-E AS scheme can achieve the same performance as that of the optimal AS scheme in the range of low SNRs, while becomes inferior at the medium-to-high SNR regime. However, it can provide 10%” gain over the max-E AS scheme at high SNR regime. Furthermore, we see that in the low SNR regime, RZF-II shows the worst performance among all beamforming designs and antenna selection schemes. This is because the transmit beamformer of the RZF-II is designed to improve the SINR at the downlink user. Therefore, only one d.o.f (i.e., $\mathbf{w}_r$) is remained for improving the eavesdropping non-outage probability. This observation validates the effectiveness of the proposed optimum beamforming design in improving the surveillance performance of the system and providing the QoS requirement of downlink user at the same time. Finally, we observe that each one of the suboptimum beamforming designs and antenna selection schemes can surpass other beamforming and antenna selection schemes depending on the value of ρ_e. This observation shows the existence of different design choices when performance-complexity tradeoff is considered.

Fig. 4 depicts the eavesdropping non-outage probability versus the SI strength, λ_{SI}, for the proposed beamforming and antenna selection schemes, where the analytical curves are based on Propositions 1, 3, and 4. A close match between the analytical (solid line) and simulation (dashed line) curves can be observed. We note that results for the MRC/MRT beamforming design and optimal AS were obtained via simulation. It can be seen that the analytical results match the simulation results for proposed beamforming designs and proposed antenna selection schemes, which validates the derived

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

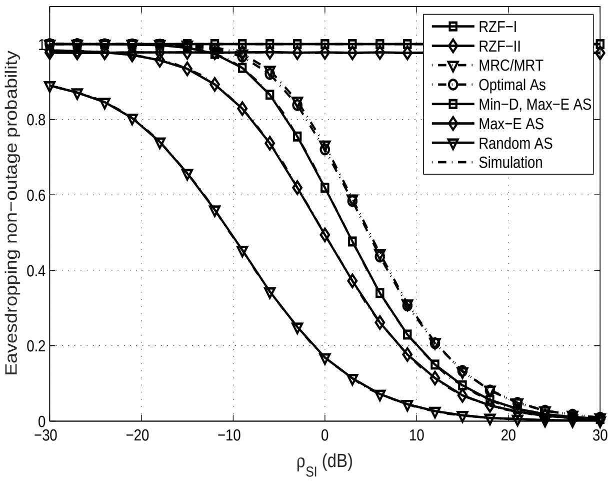
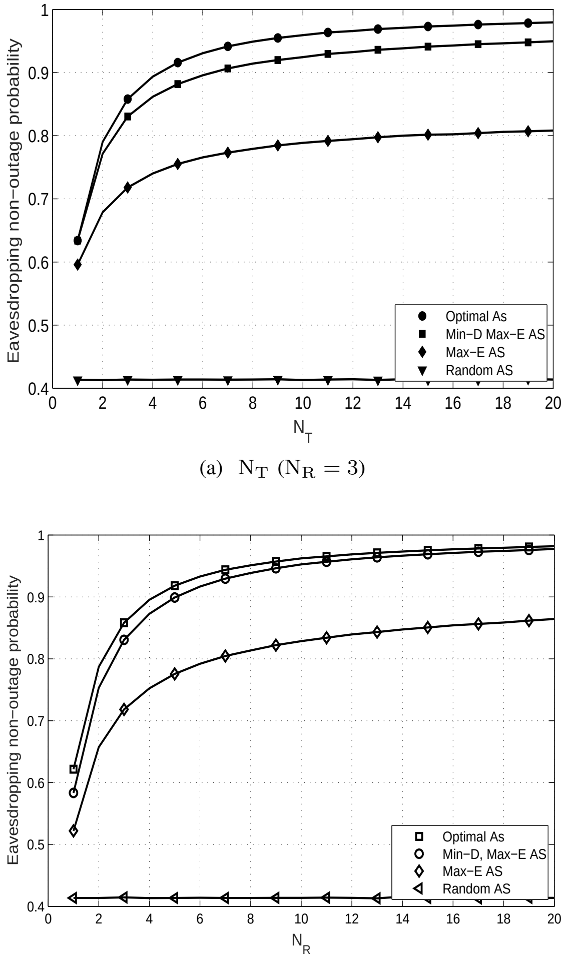


Fig. 4: $\mathbb{E}\{X\}$ for the proposed beamforming and antenna selection schemes versus SI strength ($\mathrm{N_R} = 5$, $\mathrm{N_T} = 3$, $\rho_e = 25$ dB, and $\rho_s = 10$ dB).

analytical expressions in Section IV. Furthermore, the RZF-I and RZF-II beamforming designs do not suffer from SI, hence the eavesdropping non-outage probability remains constant. On the contrary, the eavesdropping non-outage probability of the MRC/MRT and all AS schemes decreases as λ_{SI} increases. Moreover, the performances of the optimal, min-D max-E, and max-E AS schemes are much better than that of the random AS, since these schemes utilize the benefit brought by the multiple antennas settings at the legitimate monitor.

The eavesdropping non-outage probability is plotted versus $\mathrm{N_T}$ in Fig. 5 (a) and versus $\mathrm{N_R}$ in Fig. 5 (b). We observe that the eavesdropping non-outage probability of the random AS keeps constant when $\mathrm{N_T}$ and $\mathrm{N_R}$ are increased. The reason is that random AS does not properly exploit the multiple antenna setting but chooses one antenna at FD monitor randomly. Moreover, when $\mathrm{N_T}/\mathrm{N_R}$ increases, the eavesdropping non-outage probability of all antenna selection schemes improves. Nevertheless, the performance improvement of the min-D max-E AS scheme is more pronounced for high number of receive antennas. Interestingly, min-D max-E AS has a similar performance as the optimal AS scheme for high number of $\mathrm{N_R}$. Therefore, for high $\mathrm{N_R}$ the suboptimal min-D max-E AS scheme presents a better performance/implementation complexity trade-off compared to optimal AS, whose complexity would become unaffordable when the numbers of antennas at the monitor become large.

Fig. 6 shows the eavesdropping non-outage probability of the proposed TAS scheme and optimum beamforming design versus γ_{th} and for two different power allocation pairs at E and S. The analytical results are based on Proposition 5. It can be seen that analytical results match well with simulation results. As expected, optimum beamforming design provides the best performance and TAS with min-D max-E criterion outperforms TAS with min-D criterion. Moreover, in all schemes, when $\rho_e > \rho_s$, the range of γ_{th} which can be satisfied for the unsuspicious user is increased. This observation can be explained as follows. In this case, the interference caused by the suspicious transmitter is decreased, and thus according to (34) the number of candidate antennas in $\mathcal{A}$ is increased. Therefore, d.o.f at the transmit side of the monitor is increased, and accordingly the eavesdropping non-outage probability is improved.



(a) $\mathrm{N_T}$ ($\mathrm{N_R} = 3$)

(b) $\mathrm{N_R}$ ($\mathrm{N_T} = 3$)

Fig. 5: Eavesdropping non-outage probability for the proposed antenna selection schemes for different antenna configurations ($\rho_e = 25$ dB and $\rho_s = 10$ dB).

VI. Conclusion

In this paper, we designed and analyzed a proactive eavesdropping scheme. It is based on an FD monitor, which eavesdrops on communications between a pair of suspicious users. This multi-antenna monitor has spatial degrees of freedom, which can be exploited for the security tasks. Thus, we seek that it has an optimal joint receive/transmit beamforming design. The resulting non-convex optimization problem was relaxed and a two-layer problem was formulated. The inner-layer problem was recast as an SDP and a rank-one optimum solution was always guaranteed. Accordingly, the optimal solution to the outer-layer problem was obtained, by using one-dimensional line search. We also presented sub-optimum beamforming designs and derived exact closed-form expressions for the resulting eavesdropping non-outage

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

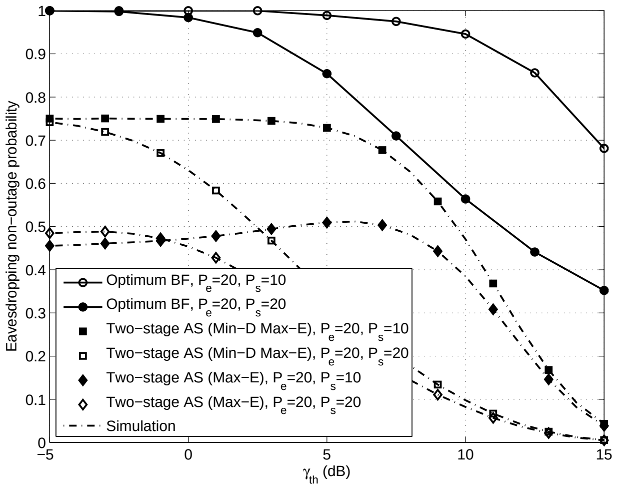


Fig. 6: $\mathbb{E}\{X\}$ for the proposed beamforming and TAS schemes versus $\gamma_{\rm th}$ ($\rm N_R = 4$, $\rm N_T = 6$).

probability. As an alternative that reduces system complexity, we studied antenna selection and presented several antenna selection schemes and derived their eavesdropping non-outage probability. Our results revealed that each one of the suboptimum beamforming designs and antenna selection schemes can surpass other beamforming and antenna selection schemes depending on the system parameters. This observation offers much-needed design choice flexibility for consideration of performance complexity trade offs. An interesting future line of research would be consideration of multiple suspicious pairs in a multi-cell scenario with massive antenna arrays.

Appendix A
Proof of Proposition 1

In case of RZF-I beamforming design, we have $W = \frac{U_1}{V_1}$ where $U_1 \triangleq |h_{sd}|^2$ and $V_1 \triangleq \rho_e \|\mathbf{h}_{ed}\|^2 + \mu_1$. The pdf of W can be expressed as

$$f_W(w) = \int_{\mu_1}^{\infty} y f_{U_1}(wy) f_{V_1}(y) dy. \tag{48}$$

Noticing that $\|\mathbf{h}_{ed}\|^2 \sim \chi^2_{2\rm N_T}$ and U_1 is exponentially distributed RV, $f_W(w)$ can be obtained as

$$\begin{aligned}
f_W(w) &= \left(\frac{\rm N_T}{\lambda_{ed}\rho_e}\right)^{\rm N_T} \frac{1}{\lambda_{sd}\Gamma(\rm N_T)} \\
&\quad \times \int_{\mu_1}^{\infty} y(y-\mu_1)^{\rm N_T-1} e^{-\frac{wy}{\lambda_{sd}}} e^{-\frac{\rm N_T}{\lambda_{ed}\rho_e}(y-\mu_1)} dy \\
&\overset{(a)}{=} \left(\frac{\rm N_T}{\lambda_{ed}\rho_e}\right)^{\rm N_T} \frac{e^{-\frac{w\mu_1}{\lambda_{sd}}}}{\lambda_{sd}\Gamma(\rm N_T)} \sum_{k=0}^{\rm N_T-1} \binom{\rm N_T}{k} \mu_1^{\rm N_T-k-1} \\
&\quad \times \int_{0}^{\infty} y^{k+1} e^{-\left(\frac{w}{\lambda_{sd}}+\frac{\rm N_T}{\lambda_{ed}\rho_e}\right)y} dy \\
&\overset{(b)}{=} \left(\frac{\rm N_T}{\lambda_{ed}\rho_e}\right)^{\rm N_T} \frac{e^{-\frac{w\mu_1}{\lambda_{sd}}}}{\lambda_{sd}\Gamma(\rm N_T)} \sum_{k=0}^{\rm N_T-1} \frac{\binom{\rm N_T}{k}\mu_1^{\rm N_T-k-1}\Gamma(k+1)}{\left(\frac{w}{\lambda_{sd}}+\frac{\rm N_T}{\lambda_{ed}\rho_e}\right)^{k+2}},
\end{aligned} \tag{49}$$

where (a) follows by applying the binomial theorem $(ax+1)^m = \sum_{\ell=0}^{m}\binom{m}{\ell}(ax)^{\ell}$ and (b) follows by invoking the integral identity [29, Eq. (3.351.3)]. Next, according to (25) and using the cdf of RV $Y \sim \chi^2_{2(\rm N_R-1)}$, we have

$$\begin{aligned}
\mathbb{E}\{X^I\} &= \frac{1}{\Gamma(\rm N_T)} \left(\frac{\rm N_T\mu_1}{\lambda_{ed}\rho_e}\right)^{\rm N_T} \sum_{j=0}^{\rm N_R-2}\sum_{k=0}^{\rm N_T-1} \binom{\rm N_T}{k} \left(\frac{\lambda_{sd}}{\mu_1}\right)^{k+1} \\
&\quad \times \frac{\Gamma(k+1)}{\Gamma(j+1)\lambda_{se}^j} \underbrace{\int_0^{\infty} \frac{w^j e^{-\left(\frac{\mu_1}{\lambda_{sd}}+\frac{1}{\lambda_{se}}\right)w}}{\left(w+\frac{\lambda_{sd}\rm N_T}{\lambda_{ed}\rho_e}\right)^{k+2}} dw}_{\mathcal{I}_1}.
\end{aligned} \tag{50}$$

where the integral $\mathcal{I}_1$, can be expressed [40, Eq. (8.4.3.1)] in terms of the Meijer G-function as

$$\mathcal{I}_1 = \int_0^{\infty} \frac{w^j}{\left(w+\frac{\lambda_{sd}\rm N_T}{\lambda_{ed}\rho_e}\right)^{k+2}} G_{01}^{10}\left(\left(\frac{\mu_1}{\lambda_{sd}}+\frac{1}{\lambda_{se}}\right)w \,\Big|\, {}_{0}\right) dw. \tag{51}$$

By invoking the integral identity [40, Eq. (2.24.2.4)], after some algebraic manipulations, the desired result in (26a) is obtained.

We now derive the eavesdropping non-outage probability of the RZF-II beamforming design. With RZF-II beamforming design, $W = \frac{U_2}{V_2}$ where $U_2 \triangleq |h_{sd}|^2$ and $V_2 \triangleq \rho_e X_1 + \mu_1$ with $X_1 = \frac{|\mathbf{h}_{ed}^{\dagger}\mathbf{h}_{eu}|^2}{\|\mathbf{h}_{eu}\|^2}$. Noticing that X_1 follows the exponential distribution with mean λ_{ed} [41], by using (48) the pdf of W can be expressed as

$$\begin{aligned}
f_W(w) &= \frac{e^{\frac{\mu_1}{\rho_e\lambda_{ed}}}}{\rho_e\lambda_{ed}\lambda_{sd}} \int_{\mu_1}^{\infty} y e^{-\left(\frac{w}{\lambda_{sd}}+\frac{\lambda_{sd}}{\rho_e\lambda_{ed}}\right)y} dy \\
&= \frac{e^{\frac{\mu_1}{\rho_e\lambda_{ed}}}}{\rho_e\lambda_{ed}} \left(\left(w+\frac{\lambda_{sd}}{\rho_e\lambda_{ed}}\right)^{-2} + \mu_1\left(w+\frac{\lambda_{sd}}{\rho_e\lambda_{ed}}\right)^{-1}\right),
\end{aligned} \tag{52}$$

where the integral identity [29, Eq. (3.351.3)] has been used to derive the final solution. According to (25) and using the cdf of RV $Y \sim \chi^2_{2(\rm N_R-1)}$, we have

$$\begin{aligned}
\mathbb{E}\{X^{II}\} &= \frac{e^{\frac{\mu_1}{\rho_e\lambda_{ed}}}}{\rho_e\lambda_{ed}} \sum_{j=0}^{\rm N_R-2} \frac{1}{\lambda_{se}^j\Gamma(j+1)} \\
&\quad \times \int_0^{\infty} \left(\frac{w^j e^{-\frac{w}{\lambda_{se}}}}{\left(w+\frac{\lambda_{sd}}{\rho_e\lambda_{ed}}\right)^2} + \mu_1 \frac{w^j e^{-\frac{w}{\lambda_{se}}}}{\left(w+\frac{\lambda_{sd}}{\rho_e\lambda_{ed}}\right)}\right) dw.
\end{aligned} \tag{53}$$

The above integral can be solved with the help of [29, Eq. (8.4.3.1)] and [29, Eq. (2.24.2.4)] to yield the desired result in (26b).

Appendix B
Proof of Proposition 3

For the notation convenience, let $Z = \frac{|h_{sd}|^2}{|h_{se}^i|^2}$ and $Q = \frac{|h_{ed}^j|^2}{|h_{SI}^{ji}|^2}$. following similar approach as in [17], $\mathbb{E}\{X\}$ can be

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

expressed as

$$\begin{aligned}\mathbb{E}\{X\} &= \underbrace{\Pr(Q<\mu_1)\times\Pr(Z<\mu_1\mid Q<\mu_1)}_{\mathcal{O}_1}\\ &+\underbrace{\Pr(Z<\mu_1<Q)\times 1}_{\mathcal{O}_2}\\ &+\underbrace{\Pr\left(\mu_1<Z<Q\right)\times\Pr\left(\frac{Z-\mu_1}{|h_{SI}^{ji}|^2}\leq\rho_e(Q-Z)\middle|\mu_1<Z<Q\right)}_{\mathcal{O}_3}\\ &+\underbrace{\Pr(\mu_1<Q<Z)\times 0}_{\mathcal{O}_4}. \end{aligned} \qquad (54)$$

According to [17], $\mathcal{O}_1$ and $\mathcal{O}_2$ can be calculated as

$$\begin{aligned}\mathcal{O}_1+\mathcal{O}_2 &= F_Z(\mu_1)F_Q(\mu_1)+F_Z(\mu_1)\left(1-F_Q(\mu_1)\right)\\ &= F_Z(\mu_1),\end{aligned} \qquad (55)$$

which indicates that, to derive $\mathbb{E}\{X\}$, the cdf of RV Z must be derive. When max-E AS scheme is deployed at the legitimated monitor, $|h_{sd}|^2$ and $|h_{ed}^j|^2$ are exponential RVs with parameters λ_{sd} and λ_{ed}, respectively. Moreover, $|h_{se}^i|^2$ and $|h_{\mathsf{SI}}^{ji^*}|^2$ are the maximum and minimum of N_R and N_T exponential RVs with mean λ_{se} and λ_{SI}, respectively. Accordingly, $F_Z(x)$ can be derived as

$$\begin{aligned}F_Z(x) &= \frac{\mathrm{N}_\mathrm{R}}{\lambda_{sd}\lambda_{se}}\int_0^\infty\int_0^{xz} e^{-\frac{y}{\lambda_{sd}}-\frac{z}{\lambda_{se}}}\left(1-e^{-\frac{z}{\lambda_{se}}}\right)^{\mathrm{N}_\mathrm{R}-1}dydz\\ &= \mathrm{N}_\mathrm{R}\left(\frac{1}{\lambda_{sd}}\mathrm{B}\left(1,\mathrm{N}_\mathrm{R}\right)-\frac{1}{\lambda_{se}}\mathrm{B}\left(1+\frac{\lambda_{se}}{\lambda_{sd}}x,\mathrm{N}_\mathrm{R}\right)\right),\end{aligned} \qquad (56)$$

where the integral identity [29, Eq. (3.312.1)] has been used to obtain the final result. Therefore, $F_Z(\mu_1)$ in (55) can be obtained as

$$\begin{aligned}F_Z(\mu_1) &= \mathcal{O}_1+\mathcal{O}_2\\ &= \mathrm{N}_\mathrm{R}\left(\frac{1}{\lambda_{sd}}\mathrm{B}\left(1,\mathrm{N}_\mathrm{R}\right)-\frac{1}{\lambda_{se}}\mathrm{B}\left(1+\frac{\lambda_{se}}{\lambda_{sd}}\mu_1,\mathrm{N}_\mathrm{R}\right)\right),\end{aligned} \qquad (57)$$

Now we derive $\mathcal{O}_3$, which can be written as

$$\begin{aligned}\mathcal{O}_3 &= \Pr\left(\frac{Z\sigma_e^2-\sigma_d^2}{|h_{ed}|^2-Z|h_{SI}^{ji}|^2}\leq P_e,\mu_1<Z<Q\right)\\ &= \int_{\mu_1}^\infty e^{-\frac{x\sigma_e^2-\sigma_d^2}{\lambda_{ed}P_e}}(1-F_Q(x))f_Z(x)dx.\end{aligned} \qquad (58)$$

Therefore, $f_Z(x)$ and $F_Q(x)$ are required. Let us denote $Z=\frac{Z_1}{Z_2}$, where $Z_1=|h_{sd}|^2$ and $Z_2=|h_{se}^i|^2$. Therefore, using (48), $f_Z(x)$ can be written as

$$f_Z(x)=\frac{\mathrm{N}_\mathrm{R}}{\lambda_{sd}\lambda_{se}}\int_0^\infty ze^{-z\left(\frac{x}{\lambda_{sd}}+\frac{1}{\lambda_{se}}\right)}\left(1-e^{-\frac{z}{\lambda_{se}}}\right)^{\mathrm{N}_\mathrm{R}-1}dz. \qquad (59)$$

To this end, by using [29, Eq. (3.351.3)] and applying the binomial expansion

$$\left(1-e^{-\frac{z}{\lambda_{se}}}\right)^{\mathrm{N}_\mathrm{R}-1}=1-\left(\mathrm{N}_\mathrm{R}-1\right)\sum_{p=0}^{\mathrm{N}_\mathrm{R}-2}\frac{(-1)^p\binom{\mathrm{N}_\mathrm{R}-2}{p}}{p+1}e^{-\frac{p+1}{\lambda_{se}}z}. \qquad (60)$$

we get

$$\begin{aligned}f_Z(x) &= \frac{\mathrm{N}_\mathrm{R}}{\lambda_{sd}\lambda_{se}}\int_0^\infty ze^{-z\left(\frac{x}{\lambda_{sd}}+\frac{1}{\lambda_{se}}\right)}\left(1-e^{-\frac{z}{\lambda_{se}}}\right)^{\mathrm{N}_\mathrm{R}-1}dz\\ &= \frac{\mathrm{N}_\mathrm{R}\lambda_{sd}\lambda_{se}}{\left(x\lambda_{se}+\lambda_{sd}\right)^2}-\lambda_{sd}\lambda_{se}\mathrm{N}_\mathrm{R}(\mathrm{N}_\mathrm{R}-1)\\ &\quad\times\sum_{p=0}^{\mathrm{N}_\mathrm{R}-2}\frac{(-1)^p\binom{\mathrm{N}_\mathrm{R}-2}{p}}{(p+1)\left(x\lambda_{se}+\lambda_{sd}(p+2)\right)^2},\end{aligned} \qquad (61)$$

Moreover, using the corresponding cdf and pdf of $|h_{ed}^j|^2$ and $|h_{SI}^{ji}|^2$, after some algebraic manipulation, $F_Q(x)$ is obtained as

$$F_Q(x)=1-\frac{1}{1+\frac{\lambda_{\mathsf{SI}}}{\lambda_{ed}\mathrm{N}_\mathrm{T}}x}. \qquad (62)$$

By substituting (61) and (62) into (58), we get

$$\begin{aligned}\mathcal{O}_3 = \mathrm{N}_\mathrm{R}\mathrm{N}_\mathrm{T}\frac{\lambda_{sd}\lambda_{ed}}{\lambda_{se}\lambda_{\mathsf{SI}}}e^{\frac{\sigma_d^2}{\lambda_{ed}P_e}}&\left(\int_{\mu_1}^\infty\frac{e^{-wx}dx}{\left(x+\frac{\lambda_{ed}\mathrm{N}_\mathrm{T}}{\lambda_{\mathsf{SI}}}\right)\left(x+\frac{\lambda_{sd}}{\lambda_{se}}\right)^2}\right.\\ &-(\mathrm{N}_\mathrm{R}-1)\sum_{p=0}^{\mathrm{N}_\mathrm{R}-2}\frac{(-1)^p\binom{\mathrm{N}_\mathrm{R}-2}{p}}{p+1}\\ &\left.\times\int_{\mu_1}^\infty\frac{e^{-wx}}{\left(x+\frac{\lambda_{ed}\mathrm{N}_\mathrm{T}}{\lambda_{\mathsf{SI}}}\right)\left(x+\frac{\lambda_{sd}}{\lambda_{se}}(p+2)\right)^2}\,dx\right).\end{aligned} \qquad (63)$$

By making a variable change $t=\frac{1}{\varsigma}(x-\mu_1)$ we transform (63) into

$$\begin{aligned}\mathcal{O}_3 = \frac{\mathrm{N}_\mathrm{T}\mathrm{N}_\mathrm{R}\lambda_{sd}\lambda_{ed}}{\varsigma^2\lambda_{se}\lambda_{\mathsf{SI}}}&\left(\int_0^\infty\frac{e^{-\varsigma\omega t}}{(t+1)\left(t+\frac{\varphi}{\varsigma}\right)^2}dt-(\mathrm{N}_\mathrm{R}-1)\right.\\ &\left.\times\sum_{p=0}^{\mathrm{N}_\mathrm{R}-2}\frac{(-1)^p\binom{\mathrm{N}_\mathrm{R}-2}{p}}{p+1}\int_0^\infty\frac{e^{-\varsigma\omega t}}{(t+1)\left(t+\frac{\varphi(p+2)}{\varsigma}\right)^2}\,dt\right),\end{aligned} \qquad (64)$$

where $\omega=\frac{1}{\lambda_{ed}\rho_e}$. Moreover, ς and φ, were defined in (38). By using [42, Lemma 3], $\mathcal{O}_3$ can be obtained as

$$\begin{aligned}\mathcal{O}_3 = \frac{\mathrm{N}_\mathrm{T}\mathrm{N}_\mathrm{R}\lambda_{sd}\lambda_{ed}}{l^2\lambda_{se}\lambda_{\mathsf{SI}}}&\left(\mathcal{G}\left(\frac{\varsigma}{\lambda_{ed}\rho_e},\frac{\varphi}{\varsigma}\right)-(\mathrm{N}_\mathrm{R}-1)\right.\\ &\left.\times\sum_{p=0}^{\mathrm{N}_\mathrm{R}-2}\frac{(-1)^p\binom{\mathrm{N}_\mathrm{R}-2}{p}}{p+1}\mathcal{G}\left(\frac{\varsigma}{\lambda_{ed}\rho_e},\frac{\varphi(p+2)}{\varsigma}\right)\right).\end{aligned} \qquad (65)$$

Finally, by substituting (57) and (65) into (54), we arrive at the desired result in (38).

Appendix C
Proof of Proposition 4

Let define $R=\frac{X_3}{P_eX_4+\sigma_d^2}$, where in case of min-D max-E AS scheme, $X_3=|h_{sd}|^2$ and $X_4=\max_{1\leq j\leq\mathrm{N}_\mathrm{T}}|h_{ed}^j|^2$. By using (37), $\mathbb{E}\{X\}$ of the min-D max-E AS scheme can be expressed as

$$\mathbb{E}\{X\}=1-\int_0^\infty F_T(w)f_R(w)dw, \qquad (66)$$

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

$$\begin{aligned}
f_R(w) &= \int_0^\infty (P_e y + \sigma_d^2) f_{X_3}(w(P_e y + \sigma_d^2)) f_{X_4}(y) dy \\
&= \frac{\mathrm{N_T} e^{-\frac{\sigma_d^2}{\lambda_{sd}} w}}{\lambda_{sd}\lambda_{ed}} \left(\int_0^\infty \left(1 - (\mathrm{N_T}-1) \sum_{p=0}^{\mathrm{N_T}-2} \frac{(-1)^p \binom{\mathrm{N_T}-2}{p}}{p+1} e^{-\frac{p+1}{\lambda_{ed}} y} \right) (P_e y + \sigma_d^2) e^{-\left(\frac{P_e w}{\lambda_{sd}} + \frac{1}{\lambda_{ed}}\right) y} dy \right) \\
&= \frac{\mathrm{N_T} e^{-\frac{\sigma_d^2}{\lambda_{sd}} w}}{\lambda_{sd}\lambda_{ed}} \left(\frac{P_e}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{1}{\lambda_{ed}}\right)^2} + \frac{\sigma_d^2}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{1}{\lambda_{ed}}\right)} - (\mathrm{N_T}-1) \sum_{p=0}^{\mathrm{N_T}-2} \frac{(-1)^p \binom{\mathrm{N_T}-2}{p}}{p+1} \left(\frac{P_e}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{p+2}{\lambda_{ed}}\right)^2} + \frac{\sigma_d^2}{\left(\frac{P_e w}{\lambda_{sd}} + \frac{p+2}{\lambda_{ed}}\right)} \right) \right),
\end{aligned} \tag{68}$$

where $T = \max_{1\le i\le \mathrm{N_R}} T_i$ with $T_i = \frac{|h_{se}^i|^2}{P_e|h_{SI}^{ji}|^2+\sigma_u^2}$. Noticing that when min-D AS scheme is deployed at the legitimate monitor, $|h_{se}^i|^2$ and $|h_{SI}^{ji}|^2$ follow exponential distribution, the cdf of T can be readily obtained as

$$F_T(w) = \left(1 - \frac{e^{-\frac{\sigma_u^2}{\lambda_{se}} w}}{1 + \frac{\lambda_{\mathsf{SI}} P_e}{\lambda_{se}} w} \right)^{\mathrm{N_R}}. \tag{67}$$

We note that X_3 is simply an exponential RV with parameter λ_{sd} and X_4 is the largest of $\mathrm{N_T}$ exponential RVs with parameter λ_{ed}. Therefore, by substituting the pdf of X_3 and X_4 into (48), $f_R(w)$ as (68) at the top of the page,

where the second equality in (68) follows by using the binomial expansion of $\left(1 - e^{-\frac{y}{\lambda_{ed}}}\right)^{\mathrm{N_T}-1}$ and the last equality is obtained by using [29, Eq. (3.351.3)]. Finally, by plugging (67) and (68) into (66), the desired result in (42) is obtained.

References

[1] F. Feizi, M. Mohammadi, and Z. Mobini, "Proactive eavesdropping via jamming in full-duplex cellular networks with antenna selection," in *Proc. 9th Int. Symp. on Telecommun. (IST' 2018)*, Tehran, Iran, Dec. 2018, pp. 641–646.

[2] 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.

[3] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Y. Le Goff, "Secrecy rate optimizations for a MIMO secrecy channel with a cooperative jammer," *IEEE Trans. Veh. Technol.*, vol. 64, pp. 1833–1847, May 2015.

[4] Z. Mobini, M. Mohammadi, and C. Tellambura, "Wireless-powered full-duplex relay and friendly jamming for secure cooperative communications," *IEEE Trans. Inf. Forensics and Security*, vol. 14, no. 3, pp. 621–634, Mar. 2019.

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

[6] 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.

[7] J. Xu, L. Duan, and R. Zhang, "Surveillance and intervention of infrastructure-free mobile communications: A new wireless security paradigm," *IEEE Wireless Commun. Mag.*, vol. 24, no. 4, pp. 152–159, Aug. 2017.

[8] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1449–1461, Dec. 2016.

[9] J. Moon, H. Lee, C. Song, S. Kang, and I. Lee, "Relay-assisted proactive eavesdropping with cooperative jamming and spoofing," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6958–6971, Oct. 2018.

[10] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 2790–2806, May 2017.

[11] ——, "Proactive eavesdropping via jamming for rate maximization over rayleigh fading channels," *IEEE Wireless Commun. Letts.*, vol. 5, no. 1, pp. 80–83, Feb 2016.

[12] D. Korpi, J. Tamminen, M. Turunen, T. Huusari, Y. Choi, L. Anttila, S. Talwar, and M. Valkama, "Full-duplex mobile device: pushing the limits," *IEEE Commun. Mag.*, vol. 54, pp. 80–87, Sep. 2016.

[13] D. Bharadia and S. Katti, "Full-duplex MIMO radios," in *Proc. 11th USENIX Symp. Networked Syst. Design and Implementation (NSDI '14)*, Seattle, WA, Apr. 2014, pp. 359–372.

[14] D. Hu, Q. Zhang, P. Yang, and J. Qin, "Proactive monitoring via jamming in amplify-and-forward relay networks," *IEEE Signal Process. Lett.*, vol. PP, pp. 1–1, 2017.

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

[16] H. Cai, Q. Zhang, Q. Li, and J. Qin, "Proactive monitoring via jamming for rate maximization over MIMO Rayleigh fading channels," *IEEE Commun. Lett.*, vol. 21, pp. 2021–2024, Sep. 2017.

[17] C. Zhong, X. Jiang, F. Qu, and Z. Zhang, "Multi-antenna wireless legitimate surveillance systems: Design and performance analysis," *IEEE Trans. Wireless Commun.*, vol. 16, no. 7, pp. 4585–4599, July 2017.

[18] Y. Cai, C. Zhao, Q. Shi, G. Y. Li, and B. Champagne, "Joint beamforming and jamming design for mmwave information surveillance systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1410–1425, July 2018.

[19] S. Huang, Q. Zhang, Q. Li, and J. Qin, "Robust proactive monitoring via jamming with deterministically bounded channel errors," *IEEE Signal Process. Lett.*, vol. 25, no. 5, pp. 690–694, May 2018.

[20] H. Zhang, L. Duan, and R. Zhang, "Jamming-assisted proactive eavesdropping over two suspicious communication links," *IEEE Trans. Wireless Commun.*, pp. 1–1, 2020.

[21] Z. Mobini, B. K. Chalise, M. Mohammadi, H. A. Suraweera, and Z. Ding, "Proactive eavesdropping using UAV systems with full-duplex ground terminals," in *Proc. IEEE Intl. Conf. on Commun. Workshops (ICCW'18)*, Kansas City, MO, USA, May 2018, pp. 1–6.

[22] H. Lu, H. Zhang, H. Dai, W. Wu, and B. Wang, "Proactive eavesdropping in UAV-aided suspicious communication systems," *IEEE Trans. Veh. Technol.*, vol. 68, pp. 1993–1997, Feb. 2019.

[23] D. Xu, H. Zhu, and Q. Li, "Jammer-assisted legitimate eavesdropping in wireless powered suspicious communication networks," *IEEE Access*, vol. 7, pp. 20 363–20 380, 2019.

[24] J. Yao, T. Wu, Q. Zhang, and J. Qin, "Proactive monitoring via passive reflection using intelligent reflecting surface," *IEEE Commun. Lett.*, pp. 1–1, 2020.

[25] D. Xu, "Legitimate surveillance of suspicious communications with QoS guarantees for unsuspicious users," *IEEE Commun. Lett.*, pp. 1–1, 2020.

[26] A. F. Molisch and M. Z. Win, "MIMO systems with antenna selection," *IEEE Microw. Mag.*, vol. 5, pp. 46–56, Mar. 2004.

[27] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun 2012.

[28] J. Zhu, Y. Zou, G. Wang, Y. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214–225, Jan. 2016.

[29] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed. San Diego, CA: Academic Press, 2007.

[30] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, pp. 5983–5993, Dec. 2011.

[31] R. A. Horn and C. A. Johnson, *Matrix Analysis*. 2nd ed. Cambridge, U.K.: Cambridge Univ. Press,, 2013.

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCOMM.2020.3022349, IEEE Transactions on Communications

[32] Z. Zhu, Z. Chu, N. Wang, S. Huang, Z. Wang, and I. Lee, "Beamforming and power splitting designs for AN-aided secure multi-user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[33] A. De Maio, Y. Huang, D. P. Palomar, S. Zhang, and A. Farina, "Fractional QCQP with applications in ML steering direction estimation for radar detection," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 172–185, Jan. 2011.

[34] G. Pataki, "On the rank of extreme matrices in semidefinite programs and the multiplicity of optimal eigenvalues," *Math. Oper. Res.*, vol. 23, no. 2, pp. 339–358, 1998.

[35] Y. Huang and D. P. Palomar, "Rank-constrained separable semidefinite programming with applications to optimal beamforming," *IEEE Trans. Signal Process.*, vol. 58, no. 2, pp. 664–678, Feb. 2010.

[36] Z. Luo, W. Ma, A. M. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Process. Mag.*, vol. 27, pp. 20–34, May 2010.

[37] M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng, and I. Krikidis, "Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems," *IEEE Trans. Commun.*, vol. 64, pp. 1769–1785, Apr. 2016.

[38] H. A. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. J. Smith, "Low-complexity end-to-end performance optimization in MIMO full-duplex relay systems," *IEEE Trans. Wireless Commun.*, vol. 13, pp. 913–927, Jan. 2014.

[39] M. Mohammadi, Z. Mobini, H. A. Suraweera, and Z. Ding, "Antenna selection in full-duplex cooperative noma systems," in *Proc. IEEE Intl. Conf. on Commun. (ICC'18)*, Kansas City, USA, May 2018, pp. 1–6.

[40] A. P. Prudnikov, Y. A. Brychkov, and O. I. Marichev, *Integral and Series. Vol. 3: More Special Functions*. Amsterdam: Gordon and Breach Science Publishers, 1986.

[41] M. Mohammadi, H. A. Suraweera, and C. Tellambura, "Uplink/downlink rate analysis and impact of power allocation for full-duplex cloud-RANs," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 5774–5788, Sep. 2018.

[42] J. Zhang, R. W. H. Jr., M. Kountouris, and J. G. Andrews, "Mode switching for the multi-antenna broadcast channel based on delay and channel quantization," *EURASIP J. Adv. Signal Process.*, Feb. 2009.

Farnaz Feizi received the B.S. and the M.S. degrees in Electrical Engineering from the Shahrekord University, Shahrekord, Iran, in 2016 and 2018, respectively. She is currently pursuing Ph.D. degree in Electrical Engineering at Isfahan University of Technology, Isfahan, Iran. Her research interests include wireless communication systems, full-duplex communications and statistical/array signal processing.

Mohammadali Mohammadi (S'09, M'15) received the B.S. degree in electrical engineering from Isfahan University of Technology, Isfahan, Iran, in 2005, and the M.S. and Ph.D. degrees in electrical engineering from K. N. Toosi University of Technology, Tehran, Iran in 2007 and 2012, respectively. From November 2010 to November 2011, he was a visiting researcher in the Research School of Engineering, the Australian National University, Australia, working on cooperative networks. He is currently an assistant professor in the Faculty of Engineering, Shahrekord University, Iran. His main research interests include cooperative communications, energy harvesting and Green communications, full-duplex communications and stochastic geometry.

Zahra Mobini (S'09, M'15) received the B.S. degree in electrical engineering from Isfahan University of Technology, Isfahan, Iran, in 2006, and the M.S and Ph.D. degrees, both in electrical engineering, from the M. A. University of Technology and K. N. Toosi University of Technology, Tehran, Iran, respectively. From November 2010 to November 2011, she was a Visiting Researcher at the Research School of Engineering, Australian National University, Canberra, ACT, Australia. She is currently an Assistant Professor with the Faculty of Engineering, Shahrekord University, Shahrekord, Iran. Her research interests include wireless communication systems, cooperative networks, and network coding.

Chintha Tellambura (F'11) received the B.Sc. degree (with first-class honor) from the University of Moratuwa, Sri Lanka, the MSc degree in Electronics from King's College, University of London, United Kingdom, and the PhD degree in Electrical Engineering from the University of Victoria, Canada. He was with Monash University, Australia, from 1997 to 2002. Presently, he is a Professor with the Department of Electrical and Computer Engineering, University of Alberta. His current research interests include the design, modelling and analysis of cognitive radio, heterogeneous cellular networks, 5G wireless networks and machine learning algorithms.

Prof. Tellambura served as an editor for both IEEE Transactions on Communications (1999-2011) and IEEE Transactions on Wireless Communications (2001-2007) and for the latter he was the Area Editor for Wireless Communications Systems and Theory during 2007-2012. He has received best paper awards in the Communication Theory Symposium in 2012 IEEE International Conference on Communications (ICC) in Canada and 2017 ICC in France. He is the winner of the prestigious McCalla Professorship and the Killam Annual Professorship from the University of Alberta. In 2011, he was elected as an IEEE Fellow for his contributions to physical layer wireless communication theory. In 2017, he was elected as a Fellow of Canadian Academy of Engineering. He has authored or coauthored over 500 journal and conference papers with an h-index of 66 (Google Scholar).

0090-6778 (c) 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
Authorized licensed use limited to: UNIVERSITY OF ALBERTA. Downloaded on September 12,2020 at 15:24:27 UTC from IEEE Xplore. Restrictions apply.