Robust Resource Allocation to Enhance Physical Layer Security in Systems With Full-Duplex Receivers: Active Adversary

Mohammad Reza Abedi, Nader Mokari, Hamid Saeedi, *Member, IEEE*, and Halim Yanikomeroglu, *Fellow, IEEE*

***Abstract*— We propose a robust resource allocation framework to improve the physical layer security in the presence of an active eavesdropper. In the considered system, we assume that both legitimate receiver and eavesdropper are full-duplex (FD) while most works in the literature concentrate on passive eavesdroppers and half-duplex (HD) legitimate receivers. In this paper, the adversary intends to optimize its transmit and jamming signal parameters so as to minimize the secrecy data rate of the legitimate transmission. In the literature, assuming that the receiver operates in HD mode, secrecy data rate maximization problems subject to the power transmission constraint have been considered in which cooperating nodes act as jammers to confound the eavesdropper. This paper investigates an alternative solution in which we take advantage of FD capability of the receiver to send jamming signals against the eavesdroppers. The proposed self-protection scheme eliminates the need for external helpers. Moreover, we consider the channel state information uncertainty on the links between the active eavesdropper and other legitimate nodes of the network. Optimal power allocation is then obtained based on the worst-case secrecy data rate maximization, under a legitimate transmitter power constraint in the presence of the active eavesdropper. Numerical results confirm the advantage of the proposed secrecy design and in certain conditions, demonstrate substantial performance gain over the conventional approaches.**

***Index Terms*— Physical layer security, robust resource allocation, full-duplex communications, active eavesdropping, jammer.**

I. Introduction

A. State of the Art

PHYSICAL layer security, as a possible alternative to the use of cryptographically secure schemes, has arisen as a prominent frontier in wireless networks to maintain secure data transmission between the transmitter and the legitimate receiver to deal with the challenges in wireless distribution and management of secret keys together with the fact that computational power is becoming easily available to users nowadays [1]–[3].

In traditional communication systems, it is assumed that terminals operate in half-duplex (HD) mode, i.e., they are not able to receive and transmit data simultaneously. Recent advances on electronics, antenna technology and signal processing allow the implementation of full-duplex (FD) terminals that can receive and transmit data at the same time and on the same frequency band as long as the self interference (SI) that leaks from the receiver output to the receiver input can be dealt with [4], [5]. Antenna isolation, time cancellation and spatial precoding have been proposed in the literature for the mitigation of SI [6]–[9].

An efficient way to increase the secrecy data rate in wireless systems is to degrade the decoding capability of the eavesdroppers by introducing controlled interference, or artificial noise [10]. When the transmitter has multiple antennas, the system can be designed such that a subset of antennas are used to generate artificial noise in a manner not affecting the legitimate receiver. When the transmitter is restricted to the use of one antenna, a group of external relays can be employed to collaboratively send jamming signals to degrade the eavesdropper channel. This approach is referred to as cooperative jamming (CJ). Note that a transmitter in a CJ based system can still have multiple antennas that are used to increase the diversity order or, in general, the degrees of freedom of the system. This is in fact the case in this paper.

In the physical layer secure communication, eavesdropping can be classified into two cases called passive and active eavesdropping. In the first case, the eavesdropper monitors communication and does not interfere with the communication channel [10]. In the second case, eavesdropper has the ability of observing the communication medium as well as modifying its contents [11].

In a system equipped with FD based legitimate terminals, a natural question is that whether one can take advantage of the FD capability to generate the required artificial noise, i.e, while receiving data whether it can simultaneously transmit friendly jamming signals to degrade the eavesdropper channel. This eliminates the need to deploy relays which is very welcome from practical point of view. Deployment of either HD or FD receivers together with the fact that we have to deal with

Manuscript received December 23, 2015; revised June 10, 2016 and October 7, 2016; accepted November 15, 2016. Date of publication November 29, 2016; date of current version February 9, 2017. This work was supported by the Iran National Science Foundation under Grant 92028129. This paper was presented in part at the Vehicular Technology Conference, Boston, MA, USA. The associate editor coordinating the review of this paper and approving it for publication was E. Koksal. *(Corresponding author: Hamid Saeedi.)*

M. R. Abedi, N. Mokari, and H. Saeedi are with the Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, 14115, Iran (e-mail: hsaeedi@modares.ac.ir).

H. Yanikomeroglu is with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, K1S 5B6, Canada.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2016.2633336

1536-1276 © 2016 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.

passive or active eavesdroppers (PE or AE), leaves us with four possible system categories: HD systems dealing with PE (abbreviated by HD-PE) or AE (HD-AE), and FD systems dealing with PE (abbreviated by FD-PE) or AE (FD-AE). While many works have been devoted to analyse the first category and to some extent the second category, only few works have analyzed the third category and basically no work has focused on the last category, i.e., FD-AE.

This paper aims to shed light on the potential benefits of using a FD terminal to provide physical layer security in the presence of an active eavesdropper (FD-AE category). We would like to see whether one can take advantage of the FD capability to generate the required artificial noise. In such a system, a secondary question follows: How the performance of such a system is compared with a traditional HD system that uses relays? To address this issue, we also consider HD systems in the presence of AE as well.

B. Related Works

Majority of works in the literature assume systems with HD terminals in the presence of passive eavesdroppers (HD-PE category). In this regard, we can point out [10], [12], [13] in which transmitters with multiple antennas are assumed to generate artificial noise. On the other hand, CJ strategy is deployed in [14]–[21] to generate artificial noise. Obtaining the optimal CJ relay weights for maximizing the secrecy data rate is investigated in [14] and [15]. An opportunistic selection of two relays, where one relay re-forwards the transmitted signal, while the other uses the CJ strategy is discussed in [16] in the context of a multi-relay network. In [17], authors study the secrecy outage probability using CJ for different levels of CSI. The optimal transmit beamforming together with artificial noise design for minimizing the secrecy outage probability is addressed in [18] and [19]. The work in [20] combines CJ with interference alignment. A destination-assisted jamming scheme is used in [21] to prevent the system from becoming interference-limited. In [14]–[21], it is assumed that the perfect CSI between the transmitter and the legitimate receiver as well as the eavesdropper is available at the transmitter which is not a practical assumption. Among few works in physical layer security that consider uncertainty on the CSI values, we can mention [22]–[24]. In these works, robust frameworks have been considered to take care of such uncertainty.

Few works have considered active eavesdropping in systems with HD terminals (HD-AE category). In [11], secure communications in the presence of malicious users which have the ability of either eavesdropping or jamming (but not both) has been considered. In this paper the optimal power allocation and the optimal strategy to alternate between jamming and eavesdropping modes is obtained. In [25], the authors formulate the secure communication in the presence of an active eavesdropper in the context of game theory. In [26], the authors consider the problem of power allocation of a user in the presence of an active eavesdropper in an orthogonal frequency division multiplexing scheme. In [27], the authors investigate the resilience of wireless multiuser networks to passive and active eavesdroppers under Rayleigh fading conditions. In [28], the authors investigate a FD eavesdropper with SI that optimizes its beamforming weights in order to minimize the secrecy data rate of the system.

As for the FD-PE category, only few works can be mentioned. A FD receiver that generates artificial noise is proposed in [29] to impair the eavesdropper's channel and the secrecy performance is evaluated based on the outage secrecy region from a geometric perspective. In [30], a FD receiver is assumed to generate artificial noise to improve physical layer security in a resource allocation framework. In this paper, perfect CSI is assumed between the eavesdropper and other nodes of the considered network. In contrast, in [31], a robust secure resource allocation scheme is proposed in which, assuming imperfect CSI values, the performance of a system with FD receiver is obtained and compared against a HD system that uses relays in a CJ scheme. In [32], the authors consider secure MIMO transmission in a wireless environment, in which one legitimate transmitter, one legitimate receiver and one eavesdropper are involved. In order to maximize the secrecy data rate, a joint optimization scheme is proposed to assign the transmit/receive antennas for legitimate receiver and to design the beamforming and power allocation for the legitimate transmitter's information and artificial noise. Finally, in a recent work [33], the authors provide a comprehensive review on the current state of physical layer security systems. However, no works on the FD-AE category other than [34], the conference version of this paper, can be found in the literature to the best of our knowledge.

C. Our Contributions

In this paper, we study the potential benefits of a FD receiver node simultaneously acting as a jammer and a receiver in the presence of an active FD based eavesdropper (the FD-AE category), with the goal of improving the secrecy data rate for the first time. We consider different scenarios in which we assume that the active eavesdropper is able to simultaneously overhear and jam. We maximize the secrecy data rate in the proposed system models in which we assume that the CSI of eavesdropper links are imperfect. We take care of this uncertainty through establishing a robust resource allocation framework. The performance is then compared against the traditional CJ strategy (the HD-AE category). Such a comparison is also missing from the literature even for passive eavesdropping (i.e. HD-PE versus FD-PE category).

We consider a legitimate transmitter (LT) which acts as the source, a legitimate receiver (LR) which acts as the destination, an active eavesdropper (AE), a jammer which are denoted by s, d, e, and j, respectively, when used as a subscript in our formulations. The LT wants to transmit data to LR while the AE overhears. Also, the AE tries to degrade the reception of the information signal at the intended receiver.

To address the questions proposed in Subsection I-A, four scenarios are studied, three with a HD receiver, which are compared against a fourth scenario with a FD receiver. The first scenario denoted by HD, represents a baseline scenario where the LT transmits data to LR. In the second scenario, denoted by HDJ, which in fact represents a simple typical

TABLE I
ABBREVIATIONS OF PROPOSED SCENARIOS

Proposed Scenarios	Description
HD	Half-duplex legitimate receiver
HDJ	Half-duplex legitimate receiver, friendly jammer(s)
HDR	Half-duplex legitimate receiver, half-duplex legitimate DF relay(s)
FD	Full-duplex legitimate receiver

CJ scenario; the LT transmits to LR and a relay is also used as a jammer. One may ask if the deployed relay can be used as a conventional cooperative node instead of a jammer. To address this question, we consider the third scenario accordingly, denoted by HDR, where we deploy a decode-and-forward (DF) relay. Finally, we consider a scenario where the LT transmits data to the FD receiver without the help of any relays. We also consider extensions of HDR and HDJ scenarios where we let more than one realy/jammer node and we use a simple relay selection strategy to obtain the best realy/jammer. In cases where FD scenario outperforms HDJ and HDR scenarios with a single realy/jammer, we figure out the number the extra relays/jammers necessary to outperform the FD scenario. A summary of the proposed scenarios has been given in Table I.

In all scenarios, we aim to maximize the achievable secrecy data rate by properly allocating the available resources. Moreover, we assume CSI uncertainty between the AE and the network nodes and consider robust secrecy data rate optimization problems based on the worst-case secrecy data rate approach. By incorporating the channel uncertainties and exploiting the S-Procedure [35], we show that these robust optimization problems can be formulated into convex ones so as to obtain a closed form solution.

Simulation results indicate that in many realistic system settings, the FD scenario can demonstrate a comparable performance to that of the HDJ/HDR scenarios. This is an important result from practical point of view as it eliminates the need to deploy relays to deal with eavesdroppers. Nevertheless, if more than one relay/jammer is allowed, the HDR/HDJ scenarios can always outperform the FD scenario.

The organization of this paper is as follows. In the next section, some notations and assumptions are reviewed. In Section III, system models are illustrated for the four considered scenarios. In Section IV, secrecy data rate maximization problems are presented for the four considered scenarios given in Table I. The performance of the proposed secrecy transmission approaches is studied using several simulation examples in Section VI, and conclusions are drawn in Section VII.

II. Notations and Assumptions

The following notations is used in the paper: $\mathbb{E}\cdot$ denotes expectation, $(\cdot)^H$ the Hermitian transpose, $\|\cdot\|$ the Euclidean norm, $(\cdot)^\dagger$ the pseudo-inverse, $\mathrm{Tr}(\cdot)$ is the trace operator, $\boldsymbol{I}$ is an identity matrix of appropriate dimension, $\mathbb{H}^N$ denotes the set of all N-by-N Hermitian matrices, $\mathbb{C}^{M\times N}$ represents an M-by-N complex matrix set, and $\mathcal{R}(.)$ is the range space of a matrix. Moreover, $\boldsymbol{A}\succeq 0(\boldsymbol{A}\succ 0)$ means $\boldsymbol{A}$ is a Hermitian positive semidefinite (definite) matrix.

We assume the LT, jammer and eavesdropper have N_s, N_j and N_e transmit antennas, respectively. All HD receivers are assumed to have a single antenna.[1] The legitimate FD receiver is assumed to have N_d transmit antennas. We let $\boldsymbol{g}_{sd}$ and $\boldsymbol{g}_{se}$ denote the $1\times N_s$ vectors of channel gains between LT and destination as well as LT and AE, respectively. In addition, $\boldsymbol{g}_{jd}$ and $\boldsymbol{g}_{je}$ denote the $1\times N_j$ vector of channel gains between jammer and LR as well as jammer and AE, respectively. Accordingly, $\boldsymbol{g}_{rd}$ and $\boldsymbol{g}_{re}$ denote the $1\times N_r$ vectors of channel gains between relay and LR, and relay and AE, respectively. Moreover, $\boldsymbol{g}_{ed}$ denotes the $1\times N_e$ vectors of channel gains between AE and LR. Finally for the scenario with FD legitimate receiver (FD-LR), we let $\boldsymbol{g}_{de}$ denote the $1\times N_d$ vector of channel gains between FD-LR and AE. The FD-LR and AE transmit a jamming signal while they simultaneously receive the LT transmitted signal. This creates a feedback loop channel between the input and output of the FD-LR as well as AE whose gains are denoted by vectors $\boldsymbol{h}_d$ and $\boldsymbol{h}_e$ of dimension $1\times N_d$ and $1\times N_e$, respectively. We assume that the naturally occurring noise at LR, relay and AE is zero-mean circular complex Gaussian with variance σ_d^2, σ_r^2 and σ_e^2, respectively. To simplify the notations, we will assume without loss of generality that $\sigma_d^2=\sigma_r^2=\sigma_e^2=\sigma^2$.

For all channel gains between the AE and different network nodes, it is assumed that only an estimated version of the gain is available. In particular, LT only has the knowledge of an estimated version of $\boldsymbol{g}_{se}$, i.e., $\tilde{\boldsymbol{g}}_{se}$ and the channel error vector is defined as $\boldsymbol{e}_{\boldsymbol{g}_{se}}=\boldsymbol{g}_{se}-\tilde{\boldsymbol{g}}_{se}$. Moreover, the jammer only has the knowledge of an estimated version of $\boldsymbol{g}_{je}$, i.e., $\tilde{\boldsymbol{g}}_{je}$ and the channel error vector is defined as $\boldsymbol{e}_{\boldsymbol{g}_{je}}=\boldsymbol{g}_{je}-\tilde{\boldsymbol{g}}_{je}$. Similarly, the relay only has the knowledge of an estimated version of $\boldsymbol{g}_{re}$, i.e., $\tilde{\boldsymbol{g}}_{re}$ and the channel error vector is defined as $\boldsymbol{e}_{\boldsymbol{g}_{re}}=\boldsymbol{g}_{re}-\tilde{\boldsymbol{g}}_{re}$. Also, the AE only has the knowledge of an estimated version of $\boldsymbol{g}_{ed}$, i.e., $\tilde{\boldsymbol{g}}_{ed}$ and the channel error vectors are defined as $\boldsymbol{e}_{\boldsymbol{g}_{ed}}=\boldsymbol{g}_{ed}-\tilde{\boldsymbol{g}}_{ed}$, respectively. Finally, only an estimated version of $\boldsymbol{g}_{de}$, i.e., $\tilde{\boldsymbol{g}}_{de}$, is available to the FD-LR. We define the channel error vector as $\boldsymbol{e}_{\boldsymbol{g}_{de}}=\boldsymbol{g}_{de}-\tilde{\boldsymbol{g}}_{de}$. For all cases, we assume that the channel mismatches lie in bounded sets [22], i.e., $\mathcal{E}_{\boldsymbol{g}_{se}}=\{\boldsymbol{e}_{\boldsymbol{g}_{se}}:\|\boldsymbol{e}_{\boldsymbol{g}_{se}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{se}}\}$, $\mathcal{E}_{\boldsymbol{g}_{je}}=\{\boldsymbol{e}_{\boldsymbol{g}_{je}}:\|\boldsymbol{e}_{\boldsymbol{g}_{je}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{je}}\}$, $\mathcal{E}_{\boldsymbol{g}_{re}}=\{\boldsymbol{e}_{\boldsymbol{g}_{re}}:\|\boldsymbol{e}_{\boldsymbol{g}_{re}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{re}}\}$, $\mathcal{E}_{\boldsymbol{g}_{er}}=\{\boldsymbol{e}_{\boldsymbol{g}_{er}}:\|\boldsymbol{e}_{\boldsymbol{g}_{er}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{er}}\}$, $\mathcal{E}_{\boldsymbol{g}_{ed}}=\{\boldsymbol{e}_{\boldsymbol{g}_{ed}}:\|\boldsymbol{e}_{\boldsymbol{g}_{ed}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{ed}}\}$, $\mathcal{E}_{\boldsymbol{g}_{de}}=\{\boldsymbol{e}_{\boldsymbol{g}_{de}}:\|\boldsymbol{e}_{\boldsymbol{g}_{de}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{de}}\}$, where $\varepsilon^2_{\boldsymbol{g}_{se}}$, $\varepsilon^2_{\boldsymbol{g}_{je}}$, $\varepsilon^2_{\boldsymbol{g}_{ed}}$, $\varepsilon^2_{\boldsymbol{g}_{er}}$ and $\varepsilon^2_{\boldsymbol{g}_{de}}$ are known constants.

In several optimization problems throughout the paper, we indicate the variable that optimizes the utility function by adding a star to it as a superscript. For example for the problem $\max_a f(a)$, we set $a^*=\operatorname{argmax}_a f(a)$.

As far as self interference cancelation method is concerned, we remind that there are several methods in the literature such as: 1) antenna isolation, 2) time cancellation and 3) spatial precoding [6]–[9]. Time-domain cancellation and spatial null

[1]For simplicity, we assume that the eavesdropping is done by only one receiving antenna. Note that this framework can be easily extended to the case that adversary can exploit the multiple antennas for eavesdropping like jamming case.

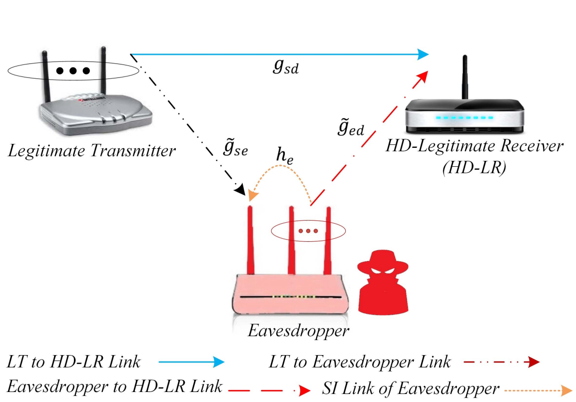


Fig. 1. Schematic of the HD scenario.

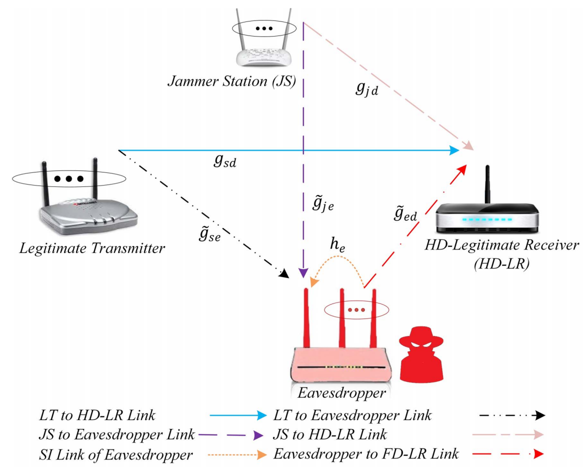


Fig. 2. Shcematic of the HDJ scenario.

space projection aim merely at minimizing the effect of loop interference. However, the degrees of freedom in the spatial domain allow for more sophisticated approach in which the useful signal power is also improved.

Self-interference suppression precoding includes the following 2 schemes: 1) The zero forcing (ZF) precoder. 2) The regularized channel inversion (RCI) precoder. The idea is to form the beams of the downlink signals to the legitimate receiver, while simultaneously form beams to the legitimate transmitter to send all-zero signals, which will avoid self-interference. The ZF precoder is designed to minimize the multiuser interference, while the RCI is designed to maximize the signal-to-interference-plus-noise ratio (SINR). In particular, [9] proposes to use a low-complexity ZF SI cancellation solution. A similar framework based on ZF has also been considered in [36] as well as in [37] and [38]. Although the ZF precoder can perfectly avoid multi-user interference, the RCI precoder has better performance by maximizing the SINR at each user at the expense of larger complexity. Meanwhile, simulation results in the [39] confirm that the sum-rate of the ZF precoder is very close to that of the RCI precoder which makes the ZF precoder more attractive. On the other hand in the context of physical layer security, [30] proposes to use a low-complexity ZF SI cancellation solution. In this paper we also follow the ZF approach as it makes it possible to obtain closed form solutions for achievable secrecy data rate.

III. System Models

A. The HD Scenario

In the first proposed scenario, we consider one LT transmitting data to LR while one AE is presented[2] as depicted in Fig. 1. In this model, LT sends private messages to LR in the presence of eavesdropper, who is able to eavesdrop on the link between LT and LR and able to degrade the reception of the information signal at the LR by transmitting jamming signal. The achievable secrecy data rate is expressed as, $R_e^{\mathrm{S}} = \max\{0, R_e^{\mathrm{D}} - R_e^{\mathrm{E}}\}$, where

$$R_e^{\mathrm{D}} = \log_2\left(1 + \frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_e, \boldsymbol{e}_{\boldsymbol{g}_{ed}})}\right), \tag{1}$$

and

$$R_e^{\mathrm{E}} = \log_2\left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}})}{\sigma^2 + \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H}\right), \tag{2}$$

where $\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}}) = (\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})^H$, $\Xi(\boldsymbol{Q}_e, \boldsymbol{e}_{\boldsymbol{g}_{ed}}) = (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})^H$, $[a]^+ = \max\{0, a\}$ and $\boldsymbol{Q}_s$ is the covariance matrix of the signal transmitted by LT, $\boldsymbol{x}_s$, which is given by $\boldsymbol{Q}_s = \mathbb{E}\{\boldsymbol{x}_s\boldsymbol{x}_s^H\}$, and the power constraint is imposed such that $\boldsymbol{Q}_s \in \mathcal{Q}_s = \{\boldsymbol{Q}_s : \boldsymbol{Q}_s \succeq 0, \mathrm{Tr}(\boldsymbol{Q}_s) \leq \acute{P}_s\}$ where $\acute{P}_s$ is the maximum allowable transmission power on LT in the HD Scenario, $\boldsymbol{Q}_e$ is the covariance matrix of the signal transmitted by AE, $\boldsymbol{x}_e$, and is given by $\boldsymbol{Q}_e = \mathbb{E}\{\boldsymbol{x}_e\boldsymbol{x}_e^H\}$, and the power constraint is imposed such that $\boldsymbol{Q}_e \in \mathcal{Q}_e = \{\boldsymbol{Q}_e : \boldsymbol{Q}_e \succeq 0, \mathrm{Tr}(\boldsymbol{Q}_e) \leq P_e\}$ where P_e is the maximum allowable transmit power on AE. We focus on optimizing the worst-case performance, where we maximize the secrecy data rate for the worst channel mismatch $\boldsymbol{e}_{\boldsymbol{g}_{se}}$ and $\boldsymbol{e}_{\boldsymbol{g}_{ed}}$ in the bounded set $\mathcal{E}_{\boldsymbol{g}_{se}}$ and $\mathcal{E}_{\boldsymbol{g}_{ed}}$, respectively.

B. The HDJ Scenario

In this subsection, we consider a cooperative jamming MISO communication system with an LT, a jammer, an LR, and an AE, as shown in Fig. 2. In this scenario, LT sends private messages to the LR in the presence of an AE, who is able to eavesdrop on the link between LT and LR. The jammer transmits artificial interference signals to confuse the AE. The data rate at the destination can be written as

$$R_{je}^{\mathrm{D}} = \log_2\left(1 + \frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{g}_{jd}\boldsymbol{Q}_j\boldsymbol{g}_{jd}^H + \Xi(\boldsymbol{Q}_e, \boldsymbol{e}_{\boldsymbol{g}_{ed}})}\right). \tag{3}$$

The data rate of eavesdropper can be expressed as

$$R_{je}^{\mathrm{E}} = \log_2\left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}})}{\sigma^2 + \Xi(\boldsymbol{Q}_j, \boldsymbol{e}_{\boldsymbol{g}_{je}}) + \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H}\right), \tag{4}$$

[2]Although we consider a single-carrier single user system, the extension to a multi-carrier multi-user system as in [40] and [41] is straightforward.

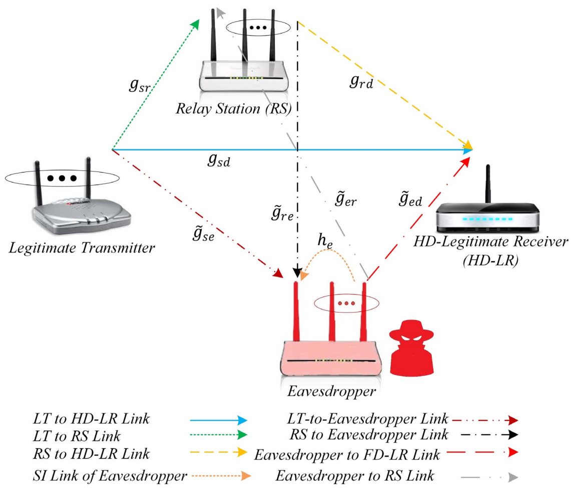


Fig. 3. Schematic of the HDR scenario.

where $\Xi(\boldsymbol{Q}_j, \boldsymbol{e}_{g_{je}}) = (\tilde{\boldsymbol{g}}_{je} + \boldsymbol{e}_{g_{je}})\boldsymbol{Q}_j(\tilde{\boldsymbol{g}}_{je} + \boldsymbol{e}_{g_{je}})^H$.

$\boldsymbol{Q}_j$ is the covariance matrix of the signal transmitted by jammer, $\boldsymbol{x}_j$, which is given by $\boldsymbol{Q}_j = \mathbb{E}\{\boldsymbol{x}_j \boldsymbol{x}_j^H\}$, and the power constraint is imposed such that $\boldsymbol{Q}_j \in \mathcal{Q}_j = \{\boldsymbol{Q}_j : \boldsymbol{Q}_j \succeq 0, \mathrm{Tr}(\boldsymbol{Q}_j) \leq P_j\}$ where P_j is the maximum predefined transmit power on jammer. Therefore, the secrecy data rate for the wiretap channel can be written as, $R_{je}^{\mathrm{S}} = \max\{0, R_{je}^{\mathrm{D}} - R_{je}^{\mathrm{E}}\}$.

C. The HDR Scenario

Here we consider a scenario consisting of an LT node, a DF relay node, a LR node, and an AE (see Fig. 3). The transmission happens in two stages. In the first stage, the LT broadcasts its encoded symbols to the relay. In the second stage, relay that is assumed to have successfully decoded the message, re-encodes the message and cooperatively transmits the re-encoded symbols to the LR. For a two-hop DF-based relay channel, the data rate through the relay link can be written as [42]

$$R_{re}^{\mathrm{D}} = \frac{1}{2}\Bigg[\min\Bigg\{\log_2\left(1 + \frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}})}\right), \log_2\left(1 + \frac{\boldsymbol{g}_{rd}\boldsymbol{Q}_r\boldsymbol{g}_{rd}^H + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_{e1}, \boldsymbol{e}_{g_{ed}})}\right)\Bigg\}\Bigg], \tag{5}$$

where $\Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}}) = (\tilde{\boldsymbol{g}}_{er} + \boldsymbol{e}_{g_{er}})\boldsymbol{Q}_{e2}(\tilde{\boldsymbol{g}}_{er} + \boldsymbol{e}_{g_{er}})^H$ and $\Xi(\boldsymbol{Q}_{e1}, \boldsymbol{e}_{g_{ed}}) = (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}})\boldsymbol{Q}_{e1}(\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}})^H$. Note that we have two covariance matrices for the signal transmitted by the eavesdropper: 1) Covariance matrix of the signal transmitted by the eavesdropper to destination, Q_{e1}, and 2) Covariance matrix of the signal transmitted by the eavesdropper to relay station, Q_{e2}. Factor $\frac{1}{2}$ appears because the relay transmission is divided into two stages. Eavesdropper receives data during both hops, and the corresponding data rate can be expressed as

$$R_{re}^{\mathrm{E}} = \frac{1}{2}\log_2\left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{g_{se}}) + \Xi(\boldsymbol{Q}_r, \boldsymbol{e}_{g_{re}})}{\sigma^2 + \boldsymbol{h}_e\boldsymbol{Q}_{e1}\boldsymbol{h}_e^H + \boldsymbol{h}_e\boldsymbol{Q}_{e2}\boldsymbol{h}_e^H}\right), \tag{6}$$

where $\Xi(\boldsymbol{Q}_r, \boldsymbol{e}_{g_{re}}) = (\tilde{\boldsymbol{g}}_{re} + \boldsymbol{e}_{g_{re}})\boldsymbol{Q}_r(\tilde{\boldsymbol{g}}_{re} + \boldsymbol{e}_{g_{re}})^H$. Therefore, the secrecy data rate for the DF relaying wiretap channel can be written as

$$\begin{aligned} R_{re}^{\mathrm{S}} &= \max\{0, R_{re}^{\mathrm{D}} - R_{re}^{\mathrm{E}}\} \\ &= \frac{1}{2}\Bigg[\min\Bigg\{\log_2\left(1 + \frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}})}\right), \\ &\qquad \log_2\left(1 + \frac{\boldsymbol{g}_{rd}\boldsymbol{Q}_r\boldsymbol{g}_{rd}^H + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_{e1}, \boldsymbol{e}_{g_{ed}})}\right)\Bigg\} \\ &\qquad - \log_2\left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{g_{se}}) + \Xi(\boldsymbol{Q}_r, \boldsymbol{e}_{g_{re}})}{\sigma^2 + \boldsymbol{h}_e\boldsymbol{Q}_{e1}\boldsymbol{h}_e^H + \boldsymbol{h}_e\boldsymbol{Q}_{e2}\boldsymbol{h}_e^H}\right)\Bigg]^+. \end{aligned} \tag{7}$$

Since the data rate of the relay link is limited by the SINR of the inferior hop, for a single data stream the transmit power for source and the relay should be adjusted such that $\frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}})} \leq \frac{\boldsymbol{g}_{rd}\boldsymbol{Q}_r\boldsymbol{g}_{rd}^H + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e1}, \boldsymbol{e}_{g_{ed}})}$.[3] The data rate through the relay link is equivalent to

$$R_{re}^{\mathrm{D}} = \frac{1}{2}\log_2\left(1 + \frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}})}\right), \tag{8}$$

Therefore, we can rewrite the secrecy data rate for a DF relaying wiretap channel as

$$\begin{aligned} R_{re}^{\mathrm{S}} &= \frac{1}{2}\Bigg[\log_2\left(1 + \frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2 + \Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}})}\right) \\ &\qquad - \log_2\left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{g_{se}}) + \Xi(\boldsymbol{Q}_r, \boldsymbol{e}_{g_{re}})}{\sigma^2 + \boldsymbol{h}_e\boldsymbol{Q}_{e1}\boldsymbol{h}_e^H + \boldsymbol{h}_e\boldsymbol{Q}_{e2}\boldsymbol{h}_e^H}\right)\Bigg]^+. \end{aligned} \tag{9}$$

D. The FD Scenario

Here, we consider one LT transmitting data to FD-LR while one AE eavesdrops the FD-LR as depicted in Fig. 4. In other words, in this scenario, source sends private messages to destination in the presence of an eavesdropper, who is able to eavesdrop and jam the link between source and distinction. The achievable secrecy data rate is expressed as follows:

$$\begin{aligned} R_{e}^{\mathrm{S}} &= \Bigg[\log_2\left(1 + \frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{h}_d\boldsymbol{Q}_d\boldsymbol{h}_d^H + \Xi(\boldsymbol{Q}_e, \boldsymbol{e}_{g_{ed}})}\right) \\ &\qquad - \log_2\left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{g_{se}})}{\sigma^2 + \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H + \Xi(\boldsymbol{Q}_d, \boldsymbol{e}_{g_{de}})}\right)\Bigg]^+, \end{aligned} \tag{10}$$

where $\Xi(\boldsymbol{Q}_d, \boldsymbol{e}_{g_{de}}) = (\tilde{\boldsymbol{g}}_{de} + \boldsymbol{e}_{g_{de}})\boldsymbol{Q}_d(\tilde{\boldsymbol{g}}_{de} + \boldsymbol{e}_{g_{de}})^H$.

IV. Problem Formulations and Solutions

A. The HD Scenario

For the HD scenario, the optimization problem can be written as follows:

[3]Note that to solve O^{HDR}, we can also assume $\frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e2}, \boldsymbol{e}_{g_{er}})} \geq \frac{\boldsymbol{g}_{rd}\boldsymbol{Q}_r\boldsymbol{g}_{rd}^H + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e1}, \boldsymbol{e}_{g_{ed}})}$. This does not change the solution method.

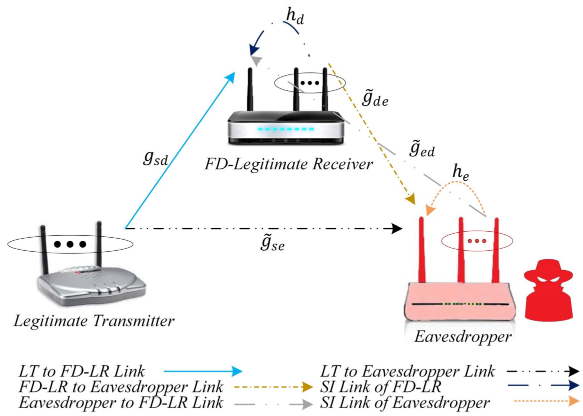


Fig. 4. Schematic of the FD scenario.

Problem O^{HD}:

$$\max_{\boldsymbol{Q}_s \in \mathcal{Q}_s} \min_{\substack{\boldsymbol{Q}_e \in \mathcal{Q}_e; \boldsymbol{e}_{g_{se}} \in \mathcal{E}_{g_{se}};\\ \boldsymbol{e}_{g_{ed}} \in \mathcal{E}_{g_{ed}}}} R_e^{\mathrm{D}}, \tag{11a}$$

$$\text{s.t. } \mathrm{Tr}(\boldsymbol{Q}_s) \leq \acute{P}_s, \tag{11b}$$

$$\mathrm{Tr}(\boldsymbol{Q}_e) \leq P_e, \tag{11c}$$

$$\| \boldsymbol{e}_{g_{se}} \|^2 \leq \varepsilon_{g_{se}}^2, \tag{11d}$$

$$\| \boldsymbol{e}_{g_{ed}} \|^2 \leq \varepsilon_{g_{ed}}^2, \tag{11e}$$

$$\boldsymbol{Q}_s \succeq 0, \tag{11f}$$

$$\boldsymbol{Q}_e \succeq 0, \tag{11g}$$

where (11b) and (11c) are the LT and AE power constraints. At first, the covariance matrix of the signal transmitted by eavesdropper is obtained by solving the following optimization:

Problem $\tilde{O}_1^{HD}$:

$$\max_{\boldsymbol{Q}_e \in \mathcal{Q}_e} \min_{\boldsymbol{e}_{g_{ed}} \in \mathcal{E}_{g_{ed}}} (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}}) \boldsymbol{Q}_e (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}})^H, \tag{12a}$$

$$\text{s.t. } \boldsymbol{h}_e \boldsymbol{Q}_e \boldsymbol{h}_e^H = 0, \quad (11c), (11e), (11g). \tag{12b}$$

Note that Q_e itself is an optimization variable and we find it for the worst case of LT and the best case of eavesdropper. We consider constraint (12b) to cancel self-interference in full duplex nodes. In this regard, we use a ZF constraint on the eavesdropping signal, which is equivalent to $\boldsymbol{h}_e \boldsymbol{Q}_e \boldsymbol{h}_e^H = 0$. The maximin problem $\tilde{O}_1^{HD}$ can be transformed to

Problem $\tilde{O}_2^{HD}$:

$$\max_{\boldsymbol{Q}_e \in \mathcal{Q}_e, \nu} \nu, \tag{13a}$$

$$\text{s.t. } (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}}) \boldsymbol{Q}_e (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}})^H \geq \nu, \quad (11c), (11e), (11g), (12b), \tag{13b}$$

where the constraints (13b) and (11e) can also be expressed as

$$\boldsymbol{e}_{g_{ed}} \boldsymbol{Q}_e \boldsymbol{e}_{g_{ed}}^H + 2Re\left(\tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e \boldsymbol{e}_{g_{ed}}^H\right) + \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e \tilde{\boldsymbol{g}}_{ed}^H - \nu \geq 0, \tag{14a}$$

$$-\boldsymbol{e}_{g_{ed}} \boldsymbol{e}_{g_{ed}}^H + \varepsilon_{g_{ed}}^2 \geq 0. \tag{14b}$$

To make the problem more tractable to solve and analyze, the next step is to turn (14a) and (14b) into linear matrix inequalities (LMIs), using the S-procedure [35]. Using the S-procedure, we know that there exists an $\boldsymbol{e}_{g_{ed}} \in \mathbb{C}^{N_e}$ satisfying both the above inequalities if and only if there exists a $\mu \geq 0$ such that

$$\begin{bmatrix} \mu \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e & \boldsymbol{Q}_e \tilde{\boldsymbol{g}}_{ed}^H \\ \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e & \tilde{\boldsymbol{g}}_{ed}^H \boldsymbol{Q}_e \tilde{\boldsymbol{g}}_{ed} - \mu \varepsilon_{g_{ed}}^2 - \nu \end{bmatrix} \succeq 0. \tag{15}$$

Letting $\psi = \tilde{\boldsymbol{g}}_{ed}^H \boldsymbol{Q}_e \tilde{\boldsymbol{g}}_{ed} - \mu \varepsilon_{g_{ed}}^2 - \nu$, where $\psi \geq 0$, $\tilde{O}_2^{HD}$ can then be expressed as

Problem $\tilde{O}_3^{HD}$:

$$\max_{\substack{\boldsymbol{Q}_e \in \mathcal{Q}_e;\\ \mu \geq 0; \psi \geq 0}} -\psi + \mathrm{Tr}(\boldsymbol{Q}_e \boldsymbol{g}_{ed}^H \tilde{\boldsymbol{g}}_{ed}) - \mu \varepsilon_{g_{ed}}^2, \tag{16a}$$

$$\text{s.t. } \begin{bmatrix} \mu \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e & \boldsymbol{Q}_e \tilde{\boldsymbol{g}}_{ed}^H \\ \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e & \psi \end{bmatrix} \succeq 0, \quad (11c), (11g), (12b). \tag{16b}$$

Problem $\tilde{O}_3^{HD}$ is a semidefinite program (SDP) that consists of a linear objective function, together with a set of LMI constraints. Therefore, we can solve this problem efficiently and obtain the optimal solution $\boldsymbol{Q}_e^*$. Note that although $\boldsymbol{e}_{g_{ed}}$ does not explicitly appear in $\tilde{O}_3^{HD}$, the optimal robust covariance $\boldsymbol{Q}_e^*$ is already based on the hidden worst-case $\boldsymbol{e}_{g_{ed}}^*$ that can be expressed explicitly through the following problem:

Problem $\tilde{O}_4^{HD}$:

$$\min_{\boldsymbol{e}_{g_{ed}}} (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}}) \boldsymbol{Q}_e^* (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{g_{ed}})^H, \tag{17a}$$

$$\text{s.t. } \| \boldsymbol{e}_{g_{ed}} \|^2 \leq \varepsilon_{g_{ed}}^2. \tag{17b}$$

The above problem is a convex problem and thus strong duality holds for (17a) and its dual.

Proposition 1: The worst-case channel mismatch for (17a) is given by

$$\boldsymbol{e}_{g_{ed}}^* = -\tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* (\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*)^{-1}, \tag{18}$$

where λ is the solution of the following SDP problem:

$$\max_{\lambda \geq 0, \gamma} \gamma, \tag{19a}$$

$$\text{s.t. } \begin{bmatrix} \lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^* & \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H \\ \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* & \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H - \lambda \varepsilon_{g_{ed}}^2 - \gamma \end{bmatrix} \succeq 0, \tag{19b}$$

where γ is a non-negative auxiliary optimization variable.

Proof: See Appendix. ■

With optimal values $\boldsymbol{Q}_e^*$ and $\boldsymbol{e}_{g_{ed}}^*$, we can formulate the optimization problem over $\boldsymbol{Q}_s$ as

Problem $\hat{O}_1^{HD}$:

$$\max_{\boldsymbol{Q}_s \in \mathcal{Q}_s} \min_{\boldsymbol{e}_{g_{se}} \in \mathcal{E}_{g_{se}}} \frac{\sigma^4 + \sigma^2 \boldsymbol{g}_{sd} \boldsymbol{Q}_s \boldsymbol{g}_{sd}^H + \sigma^2 \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{g_{ed}}^*)}{\left[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{g_{ed}}^*)\right]\left[\sigma^2 + \Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{g_{se}})\right]},$$

$$\text{s.t. } (11b), (11d), (11f). \tag{20a}$$

The optimization problem $\hat{O}_1^{HD}$ can be transformed to

Problem $\tilde{O}_2^{HD}$:

$$\max_{\boldsymbol{Q}_s \in \mathcal{Q}_s, \nu} \frac{\sigma^4 + \sigma^2 \boldsymbol{g}_{sd} \boldsymbol{Q}_s \boldsymbol{g}_{sd}^H + \sigma^2 \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)}{\nu}, \tag{21a}$$

$$\text{s.t.} \left[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\right]\left[\sigma^2 + \Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}})\right] \leq \nu, \quad (11b), (11d), (11f). \tag{21b}$$

The constraints (21b) and (11d) can also be expressed as

$$-\boldsymbol{e}_{\boldsymbol{g}_{se}} \boldsymbol{Q}_s \boldsymbol{e}_{\boldsymbol{g}_{se}}^H - 2Re\left(\tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s \boldsymbol{e}_{\boldsymbol{g}_{se}}^H\right) - \tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s \tilde{\boldsymbol{g}}_{se}^H - \sigma^2 + \frac{\nu}{\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)} \geq 0, \tag{22a}$$

$$-\boldsymbol{e}_{\boldsymbol{g}_{se}} \boldsymbol{e}_{\boldsymbol{g}_{se}}^H + \varepsilon_{\boldsymbol{g}_{se}}^2 \geq 0. \tag{22b}$$

Using the S-procedure [35], we know that there exists an $\boldsymbol{e}_{\boldsymbol{g}_{se}}$ satisfying both the above inequalities if and only if there exists a $\mu \geq 0$ such that

$$\begin{bmatrix} \mu \boldsymbol{I}_{N_s} - \boldsymbol{Q}_s & -\boldsymbol{Q}_s \tilde{\boldsymbol{g}}_{se}^H \\ -\tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s & \psi \end{bmatrix} \succeq 0, \tag{23}$$

where $\boldsymbol{I}_{N_s}$ is the identity matrix of dimension N_s and $\psi = -\tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s \tilde{\boldsymbol{g}}_{se}^H - \mu \varepsilon_{\boldsymbol{g}_{se}}^2 - \sigma^2 + \frac{\nu}{\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)}$, then $\hat{O}_2^{HD}$ can be converted into

Problem $\tilde{O}_3^{HD}$:

$$\min_{\substack{\boldsymbol{Q}_s \in \mathcal{Q}_s; \\ \psi \geq 0; \mu \geq 0}} \frac{\left[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\right]\left[\psi + \mu \varepsilon_{\boldsymbol{g}_{se}}^2 + \sigma^2 + \text{Tr}(\boldsymbol{Q}_s \tilde{\boldsymbol{g}}_{se}^H \tilde{\boldsymbol{g}}_{se})\right]}{\sigma^4 + \sigma^2 \boldsymbol{g}_{sd} \boldsymbol{Q}_s \boldsymbol{g}_{sd}^H + \sigma^2 \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)}, \tag{24a}$$

$$\text{s.t.} \begin{bmatrix} \mu \boldsymbol{I}_{N_s} - \boldsymbol{Q}_s & -\boldsymbol{Q}_s \tilde{\boldsymbol{g}}_{se}^H \\ -\tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s & \psi \end{bmatrix} \succeq 0, \quad (11b), (11f), \tag{24b}$$

Problem $\tilde{O}_3^{HD}$ consists of a linear fractional objective function with a positive denominator, and thus is quasi-convex. We rewrite this problem by defining the non-negative variable t, using the Charnes-Cooper transformation [43], [44] and letting $\mu = \acute{\mu}/\gamma$, $\psi = \acute{\psi}/\gamma$ and $\boldsymbol{Q}_s = \acute{\boldsymbol{Q}}_s/\gamma$ for some $\gamma > 0$ as

Problem $\tilde{O}_4^{HD}$:

$$\min_{\substack{t; \acute{\boldsymbol{Q}}_s \succeq 0; \acute{\mu} \geq 0; \\ \acute{\psi} \geq 0, \gamma}} \quad t,$$

$$\text{s.t.} \left[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\right] \tag{25a}$$

$$\left[\acute{\psi} + \acute{\mu} \varepsilon_{\boldsymbol{g}_{se}}^2 + \gamma \sigma^2 + \text{Tr}(\acute{\boldsymbol{Q}}_s \tilde{\boldsymbol{g}}_{se}^H \tilde{\boldsymbol{g}}_{se})\right] \leq t, \tag{25b}$$

$$\gamma \sigma^4 + \sigma^2 \,\text{Tr}(\acute{\boldsymbol{Q}}_s \boldsymbol{g}_{sd}^H \boldsymbol{g}_{sd}) + \gamma \sigma^2 \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*) = 1, \tag{25c}$$

$$\begin{bmatrix} \acute{\mu} \boldsymbol{I}_{N_s} - \acute{\boldsymbol{Q}}_s & -\acute{\boldsymbol{Q}}_s \tilde{\boldsymbol{g}}_{se}^H \\ -\tilde{\boldsymbol{g}}_{se} \acute{\boldsymbol{Q}}_s & \acute{\psi} \end{bmatrix} \succeq 0, \tag{25d}$$

$$\text{Tr}(\acute{\boldsymbol{Q}}_s) \leq \gamma P_s. \tag{25e}$$

Note that the solution for the optimal covariance, $\boldsymbol{Q}_s^*$, obtained from $\tilde{O}_4^{HD}$ is already based on a hidden worst-case channel mismatch $\boldsymbol{e}_{\boldsymbol{g}_{se}}^*$. Next, we will explicitly express $\boldsymbol{e}_{\boldsymbol{g}_{se}}^*$ under the norm-bounded constraint. The problem is formulated as

Problem $\tilde{O}_5^{HD}$:

$$\min_{\boldsymbol{e}_{\boldsymbol{g}_{se}} \in \mathcal{E}_{\boldsymbol{g}_{se}}} \quad (\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}}) \boldsymbol{Q}_s^* (\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})^H, \tag{26a}$$

$$s.t. \quad \| \boldsymbol{e}_{\boldsymbol{g}_{se}} \|^2 \leq \varepsilon_{\boldsymbol{g}_{se}}^2. \tag{26b}$$

The above problem is a non-convex problem since we want to maximize a convex function. However, similar to Proposition 1, we can still obtain the global optimum by solving its dual problem, given by

$$\boldsymbol{e}_{\boldsymbol{g}_{se}}^* = \tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s^* (\lambda \boldsymbol{I}_{N_s} - \boldsymbol{Q}_s^*)^{\dagger}, \tag{27}$$

where λ is the solution of the following problem:

$$\max_{\lambda \geq 0, \gamma} \quad \gamma, \tag{28a}$$

$$\text{s.t.} \begin{bmatrix} \lambda \boldsymbol{I}_{N_s} - \boldsymbol{Q}_s^* & \boldsymbol{Q}_s^* \tilde{\boldsymbol{g}}_{se}^H \\ \tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s^* & -\tilde{\boldsymbol{g}}_{se} \boldsymbol{Q}_s^* \tilde{\boldsymbol{g}}_{se}^H - \lambda \varepsilon_{\boldsymbol{g}_{se}}^2 - \gamma \end{bmatrix} \succeq 0. \tag{28b}$$

The above optimization problem is a SDP and hence can be solved efficiently using, for example, the interior-point method [35].

It is important to note that using conventional convex optimization methods, the multi-variable optimization problems can be decoupled into multiple sub-problems to simplify the solution and reduce the computational complexity [22], [35], [45]. Thus, we use the the primal decomposition method (for more details, refer to [46]–[48]) by decomposing the original problem into several subproblems controlled by a master problem, and use an iterative method to find the solution. In this case, from the previous section, we know that the subproblems involving Q_s and Q_e in (16) and (25) are both convex for a given p_1 and p_2. Hence, our first step will be to estimate Q_s and Q_e for some initial p_1 and p_2, and then we will find optimal values p_1 and p_2 for the resulting Q_s and Q_e. We then continue iteratively to find the channel mismatches and power allocation. The steps for the joint optimization that considers both the channel mismatches and the power allocation between LT and eavesdropper are outlined in a pseudo-code of Fig. 5.

Step 1: Set iteration number, $\varrho = 0$, and $p_1^{(0)} = p_1^{(0)} = P/2$.
Step 2: For iteration ϱ.
Step 2.1: Let $P_s = p_1^{(\varrho-1)}$, Let $P_e = p_2^{(\varrho-1)}$ and solve problem (16), (17), (25) and (26) to obtain $\boldsymbol{Q}_e$, $\boldsymbol{e}_{g_{ed}}$, $\boldsymbol{Q}_s$ and $\boldsymbol{e}_{\boldsymbol{g}_{se}}$ respectively.
Step 2.2: Let $\bar{\boldsymbol{Q}}_s^{(\varrho)} = \boldsymbol{Q}_s^{(\varrho)} / \text{Tr}(\boldsymbol{Q}_s^{(\varrho)})$, $\bar{\boldsymbol{Q}}_e^{(\varrho)} = \boldsymbol{Q}_e^{(\varrho)} / \text{Tr}(\boldsymbol{Q}_e^{(\varrho)})$ and $p_1^{(\varrho)} = \boldsymbol{Q}_s^{(\varrho)} / \bar{\boldsymbol{Q}}_s^{(\varrho)}$ and $p_1^{(\varrho)} = \boldsymbol{Q}_e^{(\varrho)} / \bar{\boldsymbol{Q}}_e^{(\varrho)}$.
Step 2.3: Apply the resulting $p_1^{(\varrho)}$ and $p_2^{(\varrho)}$ to Step 2.
Step 3: $\varrho = \varrho + 1$.
Step 4: If stopping criterion is fulfilled, $\| \boldsymbol{Q}_s^{(\varrho+1)} \|_F - \| \boldsymbol{Q}_s^{(\varrho)} \|_F \leq \epsilon$, go to Step 5, otherwise go to Step 2.
Step 5: End.

Fig. 5. The pseudo code of Iterative algorithm for finding the LT's transmitted power and eavesdropper's transmitted power and channel mismatches.

B. The HDJ Scenario

For HDJ scenario, the optimization problem can be written as follows:

Problem $\tilde{O}^{HDJ}$:

$$\max_{\substack{\boldsymbol{Q}_s\in\mathcal{Q}_s;\\ \boldsymbol{Q}_j\in\mathcal{Q}_j}} \min_{\substack{\boldsymbol{Q}_e\in\mathcal{Q}_e;\boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}};\\ \boldsymbol{e}_{\boldsymbol{g}_{je}}\in\mathcal{E}_{\boldsymbol{g}_{je}};\boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}}}} R_{je}^{\mathrm{S}}, \tag{29a}$$

$$\text{s.t. } \mathrm{Tr}(\boldsymbol{Q}_s)\le P_s, \tag{29b}$$

$$\mathrm{Tr}(\boldsymbol{Q}_j)\le P_j, \tag{29c}$$

$$\|\boldsymbol{e}_{\boldsymbol{g}_{je}}\|^2\le \varepsilon_{\boldsymbol{g}_{je}}^2, \tag{29d}$$

$$\boldsymbol{Q}_j\succeq 0,$$
$$(11c),(11d),(11e),(11f),(11g), \tag{29e}$$

where P_s is the maximum allowable transmission power on LT in the HDJ, HDR and FD scenarios. As the first step, the covariance matrix of the signal transmitted by eavesdropper, $\boldsymbol{Q}_e$, is obtained. Hence, the corresponding optimization problem is formulated as follows:

Problem $\tilde{O}_1^{HDJ}$:

$$\max_{\boldsymbol{Q}_e\in\mathcal{Q}_e} \min_{\boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}}} (\tilde{\boldsymbol{g}}_{ed}+\boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed}+\boldsymbol{e}_{\boldsymbol{g}_{ed}})^H, \tag{30a}$$

$$\text{s.t. } \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H=0,$$
$$(11c),(11e),(11g). \tag{30b}$$

Problem $\tilde{O}_1^{HDJ}$ can be solved in a similar way as that of $\tilde{O}_1^{HD}$. Then the covariance matrix of the signal transmitted by jamming is obtained, and the optimization problem becomes

Problem $\check{O}_1^{HDJ}$:

$$\max_{\boldsymbol{Q}_j\in\mathcal{Q}_j} \min_{\boldsymbol{e}_{\boldsymbol{g}_{je}}\in\mathcal{E}_{\boldsymbol{g}_{je}}} (\tilde{\boldsymbol{g}}_{je}+\boldsymbol{e}_{\boldsymbol{g}_{je}})\boldsymbol{Q}_j(\tilde{\boldsymbol{g}}_{je}+\boldsymbol{e}_{\boldsymbol{g}_{je}})^H, \tag{31a}$$

$$\text{s.t. } \boldsymbol{g}_{jd}\boldsymbol{Q}_j\boldsymbol{g}_{jd}^H=0,$$
$$(29c),(29d),(29e). \tag{31b}$$

We can use a similar processing flow as $\tilde{O}_1^{HD}$ to solve $\check{O}_1^{HDJ}$ and to obtain $\boldsymbol{Q}_j^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{je}}^*$. With optimal values for $\boldsymbol{Q}_j^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{je}}^*$, we can formulate the optimization problem over $\boldsymbol{Q}_s$ as

Problem $\hat{O}_1^{HDJ}$**:**

$$\max_{\boldsymbol{Q}_s\in\mathcal{Q}_s} \min_{\boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}}} \frac{A}{B},$$
$$\text{s.t. } (29b),(11d),(11f), \tag{32}$$

where $A=\left[\sigma^2+\Xi(\boldsymbol{Q}_j^*,\boldsymbol{e}_{\boldsymbol{g}_{je}}^*)\right]\left[\sigma^2+\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H+\Xi(\boldsymbol{Q}_e^*,\boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\right]$, $B=\left[\sigma^2+\Xi(\boldsymbol{Q}_e^*,\boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\right]\left[\sigma^2+\Xi(\boldsymbol{Q}_s,\boldsymbol{e}_{\boldsymbol{g}_{se}})+\Xi(\boldsymbol{Q}_j^*,\boldsymbol{e}_{\boldsymbol{g}_{je}}^*)\right]$ and $\Xi(\boldsymbol{Q}_j^*,\boldsymbol{e}_{\boldsymbol{g}_{je}}^*)=(\tilde{\boldsymbol{g}}_{je}+\boldsymbol{e}_{\boldsymbol{g}_{je}}^*)\boldsymbol{Q}_j^*(\tilde{\boldsymbol{g}}_{je}+\boldsymbol{e}_{\boldsymbol{g}_{je}}^*)^H$. Solutions of $\hat{O}^{HDJ}$ can be easily obtained by following the same line of arguments we made for $\hat{O}^{HD}$. Thus, we can obtain $\boldsymbol{Q}_s^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{se}}^*$.

C. The HDR Scenario

For the HDR scenario, the optimization problem can be written as follows:

Problem O^{HDR}:

$$\max_{\substack{\boldsymbol{Q}_s\in\mathcal{Q}_s;\\ \boldsymbol{Q}_r\in\mathcal{Q}_r}} \min_{\substack{\boldsymbol{Q}_{e1}\in\mathcal{Q}_e;\boldsymbol{Q}_{e2}\in\mathcal{Q}_e;\\ \boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}};\boldsymbol{e}_{\boldsymbol{g}_{re}}\in\mathcal{E}_{\boldsymbol{g}_{re}};\\ \boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}};\boldsymbol{e}_{\boldsymbol{g}_{er}}\in\mathcal{E}_{\boldsymbol{g}_{er}}}} R_{re}^{\mathrm{S}}, \tag{33a}$$

$$\text{s.t. } \mathrm{Tr}(\boldsymbol{Q}_r)\le P_r, \tag{33b}$$

$$\mathrm{Tr}(\boldsymbol{Q}_{e1})\le P_e, \tag{33c}$$

$$\mathrm{Tr}(\boldsymbol{Q}_{e2})\le P_e, \tag{33d}$$

$$\|\boldsymbol{e}_{\boldsymbol{g}_{re}}\|^2\le \varepsilon_{\boldsymbol{g}_{re}}^2, \tag{33e}$$

$$\|\boldsymbol{e}_{\boldsymbol{g}_{er}}\|^2\le \varepsilon_{\boldsymbol{g}_{er}}^2, \tag{33f}$$

$$\boldsymbol{Q}_{e1}\succeq 0, \tag{33g}$$

$$\boldsymbol{Q}_{e2}\succeq 0, \tag{33h}$$

$$\boldsymbol{Q}_r\succeq 0,$$
$$(11d),(11e),(11f),(29b). \tag{33i}$$

Similar to HD and HDJ scenarios, we initially obtain the covariance matrix of the signal transmitted by the eavesdropper, $\boldsymbol{Q}_{e1}$ and $\boldsymbol{Q}_{e2}$. Now, by dropping the logarithm in (9), the optimization problem $\tilde{O}^{HDR}$ is modified as follows:

Problem $\tilde{O}^{HDR}$:

$$\max_{\substack{\boldsymbol{Q}_s\in\mathcal{Q}_s;\\ \boldsymbol{Q}_r\in\mathcal{Q}_r}} \min_{\substack{\boldsymbol{Q}_{e1}\in\mathcal{Q}_e;\boldsymbol{Q}_{e2}\in\mathcal{Q}_e;\\ \boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}};\boldsymbol{e}_{\boldsymbol{g}_{re}}\in\mathcal{E}_{\boldsymbol{g}_{re}};\\ \boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}};\boldsymbol{e}_{\boldsymbol{g}_{er}}\in\mathcal{E}_{\boldsymbol{g}_{er}}}} \frac{1+\frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e2},\boldsymbol{e}_{\boldsymbol{g}_{er}})}}{1+\frac{\Xi(\boldsymbol{Q}_s,\boldsymbol{e}_{\boldsymbol{g}_{se}})+\Xi(\boldsymbol{Q}_r,\boldsymbol{e}_{\boldsymbol{g}_{re}})}{\sigma^2+\boldsymbol{h}_e\boldsymbol{Q}_{e1}\boldsymbol{h}_e^H+\boldsymbol{h}_e\boldsymbol{Q}_{e2}\boldsymbol{h}_e^H}}, \tag{34a}$$

$$\text{s.t. } \frac{\boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e2},\boldsymbol{e}_{\boldsymbol{g}_{er}})}\le\frac{\boldsymbol{g}_{rd}\boldsymbol{Q}_r\boldsymbol{g}_{rd}^H+\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2+\Xi(\boldsymbol{Q}_{e1},\boldsymbol{e}_{\boldsymbol{g}_{ed}})} \tag{34b}$$
$$(11d),(11e),(11f),(29b),(33c),(33d),(33h),$$
$$(33i),(33b),(33e),(33f),(33g).$$

$\boldsymbol{Q}_{e1}$ and $\boldsymbol{Q}_{e2}$ are obtained by solving the following optimization problems:

Problem $\tilde{O}_1^{HDR}$:

$$\max_{\boldsymbol{Q}_{e1}\in\mathcal{Q}_e} \min_{\boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}}} (\tilde{\boldsymbol{g}}_{ed}+\boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_{e1}(\tilde{\boldsymbol{g}}_{ed}+\boldsymbol{e}_{\boldsymbol{g}_{ed}})^H, \tag{35a}$$

$$\text{s.t. } \boldsymbol{h}_e\boldsymbol{Q}_{e1}\boldsymbol{h}_e^H=0,$$
$$(11e),(33c),(33h), \tag{35b}$$

and *Problem* $\tilde{O}_1^{HDR}$:

$$\max_{\boldsymbol{Q}_{e2}\in\mathcal{Q}_e} \min_{\boldsymbol{e}_{\boldsymbol{g}_{er}}\in\mathcal{E}_{\boldsymbol{g}_{er}}} (\tilde{\boldsymbol{g}}_{er}+\boldsymbol{e}_{\boldsymbol{g}_{er}})\boldsymbol{Q}_{e2}(\tilde{\boldsymbol{g}}_{er}+\boldsymbol{e}_{\boldsymbol{g}_{er}})^H, \tag{36a}$$

$$\text{s.t. } \boldsymbol{h}_e\boldsymbol{Q}_{e2}\boldsymbol{h}_e^H=0,$$
$$(33f),(33d),(33i). \tag{36b}$$

Problems $\tilde{O}_1^{HDR}$ and $\hat{O}_1^{HDR}$ are solved using a method similar to $\tilde{O}_1^{HD}$. As a result, $\boldsymbol{e}_{\boldsymbol{g}_{ed}}^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{er}}^*$ are also obtained. We can formulate the optimization problem over $\boldsymbol{Q}_r$ as

Problem $\tilde{O}_1^{HDR}$

$$\min_{\boldsymbol{Q}_r\in\mathcal{Q}_r} \min_{\boldsymbol{e}_{\boldsymbol{g}_{re}}\in\mathcal{E}_{\boldsymbol{g}_{re}}} (\tilde{\boldsymbol{g}}_{re}+\boldsymbol{e}_{\boldsymbol{g}_{re}})\boldsymbol{Q}_r(\tilde{\boldsymbol{g}}_{re}+\boldsymbol{e}_{\boldsymbol{g}_{re}})^H,$$
$$\text{s.t. } (33b),(33e),(33g). \tag{37}$$

We can solve this problem efficiently in a similar way as that of $\tilde{O}_1^{HD}$ and obtain the optimal solution $\boldsymbol{Q}_r^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{re}}^*$. With optimal values $\boldsymbol{Q}_r^*$, $\boldsymbol{e}_{\boldsymbol{g}_{re}}^*$, $\boldsymbol{Q}_{e1}^*$, $\boldsymbol{Q}_{e2}^*$, $\boldsymbol{e}_{\boldsymbol{g}_{er}}^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{ed}}^*$, we can formulate the optimization problem over $\boldsymbol{Q}_s$ as *Problem* $\breve{O}_1^{HDR}$*:*

$$\max_{\boldsymbol{Q}_s \in \mathcal{Q}_s} \min_{\boldsymbol{e}_{\boldsymbol{g}_{se}} \in \mathcal{E}_{\boldsymbol{g}_{se}}} \frac{C}{D}, \quad \text{s.t. } (29b), (11d), (11f), (34b). \tag{38}$$

where $C = \sigma^2\big[\sigma^2 + \Xi(\boldsymbol{Q}_{e2}^*, \boldsymbol{e}_{\boldsymbol{g}_{er}}^*) + \boldsymbol{g}_{sr}\boldsymbol{Q}_s\boldsymbol{g}_{sr}^H\big]$ and $D = \big[\sigma^2 + \Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}}) + \Xi(\boldsymbol{Q}_r^*, \boldsymbol{e}_{\boldsymbol{g}_{re}}^*)\big]\big[\sigma^2 + \Xi(\boldsymbol{Q}_{e2}^*, \boldsymbol{e}_{\boldsymbol{g}_{er}}^*)\big]$. Solution of $\breve{O}_5^{HDR}$ can be easily obtained by following the same line of argument we made for $\hat{O}_5^{HD}$.

D. The FD Scenario

In the FD scenario, the secrecy data rate maximization problem is given as

Problem O^{FD}*:*

$$\max_{\substack{\boldsymbol{Q}_s \in \mathcal{Q}_s;\\ \boldsymbol{Q}_d \in \mathcal{Q}_d}} \min_{\substack{\boldsymbol{Q}_e \in \mathcal{Q}_e; \boldsymbol{e}_{\boldsymbol{g}_{se}} \in \mathcal{E}_{\boldsymbol{g}_{se}};\\ \boldsymbol{e}_{\boldsymbol{g}_{de}} \in \mathcal{E}_{\boldsymbol{g}_{de}}; \boldsymbol{e}_{\boldsymbol{g}_{ed}} \in \mathcal{E}_{\boldsymbol{g}_{ed}}}} R_e^{\mathrm{S}}, \tag{39a}$$

$$\text{s.t. } \operatorname{Tr}(\boldsymbol{Q}_d) \le P_d, \tag{39b}$$

$$\| \boldsymbol{e}_{\boldsymbol{g}_{de}} \|^2 \le \varepsilon_{\boldsymbol{g}_{de}}^2, \tag{39c}$$

$$\boldsymbol{Q}_d \succeq \boldsymbol{0}, \quad (29b), (11c), (11d), (11e), (11f), (11g). \tag{39d}$$

Similar to previous scenarios, the covariance matrix of the signal transmitted by eavesdropper is obtained first. Accordingly, the corresponding optimization problem is written as follows:

Problem $\tilde{O}_1^{FD}$*:*

$$\max_{\boldsymbol{Q}_e \in \mathcal{Q}_e} \min_{\boldsymbol{e}_{\boldsymbol{g}_{ed}} \in \mathcal{E}_{\boldsymbol{g}_{ed}}} (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})^H, \tag{40a}$$

$$\text{s.t. } \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H = 0, \quad (11c), (11e), (11g). \tag{40b}$$

We can solve this problem efficiently and obtain the optimal solution $\boldsymbol{Q}_e^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{ed}}^*$. Then, the covariance matrix of the signal transmitted by jammer is obtained. Accordingly, the corresponding optimization problem is written as follows:

Problem $\hat{O}_1^{FD}$*:*

$$\max_{\boldsymbol{Q}_d \in \mathcal{Q}_d} \min_{\boldsymbol{e}_{\boldsymbol{g}_{de}} \in \mathcal{E}_{\boldsymbol{g}_{de}}} (\tilde{\boldsymbol{g}}_{de} + \boldsymbol{e}_{\boldsymbol{g}_{de}})\boldsymbol{Q}_d(\tilde{\boldsymbol{g}}_{de} + \boldsymbol{e}_{\boldsymbol{g}_{de}})^H, \tag{41a}$$

$$\text{s.t. } \boldsymbol{h}_d\boldsymbol{Q}_d\boldsymbol{h}_d^H = 0, \quad (39b), (39c), (39d). \tag{41b}$$

We can solve this problem efficiently in a similar way and obtain the optimal solution $\boldsymbol{Q}_d^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{de}}^*$. With optimal values $\boldsymbol{Q}_e^*$, $\boldsymbol{e}_{\boldsymbol{g}_{ed}}^*$, $\boldsymbol{Q}_d^*$ and $\boldsymbol{e}_{\boldsymbol{g}_{de}}^*$, we can formulate the optimization problem over $\boldsymbol{Q}_s$ and $\boldsymbol{e}_{\boldsymbol{g}_{se}}$ as

Problem $\breve{O}_1^{FD}$*:*

$$\max_{\boldsymbol{Q}_s \in \mathcal{Q}_s} \min_{\boldsymbol{e}_{\boldsymbol{g}_{se}} \in \mathcal{E}_{\boldsymbol{g}_{se}}} \frac{E}{F}, \quad \text{s.t. } (29b), (11d), (11f). \tag{42a}$$

where $E = \Big[\sigma^2 + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\Big]\Big[\Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*) + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H + \sigma^2\Big]$ and $F = \Big[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\Big]\Big[\sigma^2 + \Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}}) + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\Big]$. The optimization problem $\breve{O}_1^{FD}$ can be transformed to

Problem $\breve{O}_2^{FD}$*:*

$$\max_{\boldsymbol{Q}_s \in \mathcal{Q}_s, \nu} \frac{\Big[\sigma^2 + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\Big]\Big[\Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*) + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H + \sigma^2\Big]}{\nu}, \tag{43a}$$

$$\text{s.t. } \Big[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\Big]\Big[\sigma^2 + \Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}}) + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\Big] \le \nu, \tag{43b}$$

$$\| \boldsymbol{e}_{\boldsymbol{g}_{se}} \|^2 \le \varepsilon_{\boldsymbol{g}_{se}}^2, \quad (29b), (11f). \tag{43c}$$

The constraints (43b) and (43c) can also be expressed as

$$-\boldsymbol{e}_{\boldsymbol{g}_{se}}\boldsymbol{Q}_s\boldsymbol{e}_{\boldsymbol{g}_{se}}^H - 2Re\Big(\tilde{\boldsymbol{g}}_{se}\boldsymbol{Q}_s\boldsymbol{e}_{\boldsymbol{g}_{se}}^H\Big) - \tilde{\boldsymbol{g}}_{se}\boldsymbol{Q}_s\tilde{\boldsymbol{g}}_{se}^H - \sigma^2 - \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*) + \frac{\nu}{\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)} \ge 0, \tag{44a}$$

$$-\boldsymbol{e}_{\boldsymbol{g}_{se}}\boldsymbol{e}_{\boldsymbol{g}_{se}}^H + \varepsilon_{\boldsymbol{g}_{se}}^2 \ge 0. \tag{44b}$$

Using the S-procedure [35], we know that there exists an $\boldsymbol{e}_{\boldsymbol{g}_{se}}$ satisfying both the above inequalities if and only if there exists a $\mu \ge 0$ such that

$$\begin{bmatrix} \mu\boldsymbol{I}_{N_s} - \boldsymbol{Q}_s & -\boldsymbol{Q}_s\tilde{\boldsymbol{g}}_{se}^H \\ -\tilde{\boldsymbol{g}}_{se}\boldsymbol{Q}_s & \psi \end{bmatrix} \succeq 0. \tag{45}$$

where $\psi = -\tilde{\boldsymbol{g}}_{se}\boldsymbol{Q}_s\tilde{\boldsymbol{g}}_{se}^H - \mu\varepsilon_{\boldsymbol{g}_{se}}^2 - \sigma^2 - \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*) + \frac{\nu}{\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)}$, then $\breve{O}_2^{FD}$ can be converted into

Problem $\breve{O}_3^{FD}$*:*

$$\min_{\substack{\boldsymbol{Q}_s \in \mathcal{Q}_s;\\ \psi \ge 0; \mu \ge 0}} \frac{G}{H}, \tag{46a}$$

$$\text{s.t. } \begin{bmatrix} \mu\boldsymbol{I}_{N_s} - \boldsymbol{Q}_s & -\boldsymbol{Q}_s\tilde{\boldsymbol{g}}_{se}^H \\ -\tilde{\boldsymbol{g}}_{se}\boldsymbol{Q}_s & \psi \end{bmatrix} \succeq 0, \quad (29b), (11f). \tag{46b}$$

where $G = \Big[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\Big]\Big[\psi + \mu\varepsilon_{\boldsymbol{g}_{se}}^2 + \sigma^2 + \operatorname{Tr}(\boldsymbol{Q}_s\tilde{\boldsymbol{g}}_{se}^H\tilde{\boldsymbol{g}}_{se}) + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\Big]$ and $H = \Big[\sigma^2 + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\Big]\Big[\Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*) + \boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H + \sigma^2\Big]$. Problem $\breve{O}_3^{FD}$ consists of a linear fractional objective function with a positive denominator, and thus is quasi-convex. We use the Charnes-Cooper transformation, by letting $\mu = \acute{\mu}/\gamma$, $\psi = \acute{\psi}/\gamma$ and $\boldsymbol{Q}_s = \acute{\boldsymbol{Q}}_s/\gamma$ for some $\gamma > 0$, and rewriting $\breve{O}_3^{FD}$ as

Problem $\check{O}_4^{FD}$:

$$\min_{\substack{t;\acute{\boldsymbol{Q}}_s\succeq 0;\\ \acute{\mu}\geq 0,\acute{\psi}\geq 0,\gamma}} \quad t, \tag{47a}$$

$$\text{s.t.} \left[\sigma^2 + \Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*)\right] \left[\acute{\psi} + \acute{\mu}\varepsilon_{\boldsymbol{g}_{se}}^2 + \gamma\sigma^2 + \mathrm{Tr}(\acute{\boldsymbol{Q}}_s\tilde{\boldsymbol{g}}_{se}^H\tilde{\boldsymbol{g}}_{se}) + \gamma\,\Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\right] \leq t, \tag{47b}$$

$$\left[\sigma^2 + \Xi(\boldsymbol{Q}_d^*, \boldsymbol{e}_{\boldsymbol{g}_{de}}^*)\right] \left[\gamma\,\Xi(\boldsymbol{Q}_e^*, \boldsymbol{e}_{\boldsymbol{g}_{ed}}^*) + \mathrm{Tr}(\acute{\boldsymbol{Q}}_s\boldsymbol{g}_{sd}^H\boldsymbol{g}_{sd}) + \gamma\sigma^2\right] = 1, \tag{47c}$$

$$\begin{bmatrix} \acute{\mu}\boldsymbol{I}_{N_s} - \acute{\boldsymbol{Q}}_s & -\acute{\boldsymbol{Q}}_s\tilde{\boldsymbol{g}}_{se}^H \\ -\tilde{\boldsymbol{g}}_{se}\acute{\boldsymbol{Q}}_s & \acute{\psi} \end{bmatrix} \succeq 0, \tag{47d}$$

$$\mathrm{Tr}(\acute{\boldsymbol{Q}}_s) \leq \gamma P_s. \tag{47e}$$

Note that the solution for the optimal covariance $\boldsymbol{Q}_s^*$ obtained from $\check{O}_4^{FD}$ is already based on a hidden worst-case channel mismatch $\boldsymbol{e}_{\boldsymbol{g}_{se}}^*$. Next, we will explicitly express $\boldsymbol{e}_{\boldsymbol{g}_{se}}^*$ under the norm-bounded constraint. The problem is formulated as

Problem $\check{O}_5^{FD}$:

$$\min_{\boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}}} \quad (\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s^*(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})^H, \tag{48a}$$

$$s.t.\ \parallel \boldsymbol{e}_{\boldsymbol{g}_{se}} \parallel^2 \leq \varepsilon_{\boldsymbol{g}_{se}}^2. \tag{48b}$$

$\check{O}_5^{FD}$ can be easily solved by following the same line of argument we made for $\hat{O}_5^{HD}$.

V. Multi Node Scenarios

A. Multi Relay

We assume there are R relays in the HDJ scenario instead of one. The set of relays is denoted by $\mathcal{R} = \{1, 2, \ldots, R\}$. Based on the optimal power allocation scheme proposed in the HDR scenario for each relay, the LT can calculate the secrecy rate for any relay by solving optimization problem for each relay. Therefore, the LT can select the relay corresponding to the maximum secrecy rate. This can be done, via a simple exhaustive search as, $r^* = \arg\max_r R_{re}^{\mathrm{S}}$.

B. Multi Jammer

We assume there are J jammers in the HDJ scenario instead of one. The set of jammers is denoted by $\mathcal{J} = \{1, 2, \ldots, J\}$. Based on the optimal power allocation scheme proposed in the HDJ scenario for each jammer, the source can calculate the secrecy rate for any jammer. Therefore, the source can select the jammer corresponding to the maximum secrecy rate. This can be done, via a simple exhaustive search as, $j^* = \arg\max_j R_{je}^{\mathrm{S}}$.

VI. Simulation Results

This section presents the numerical results of the proposed scenarios. The proposed schemes have been evaluated in terms of secrecy data rate. We assume the LT, jammer, relay, AE and FD-LR have four transmit antennas,

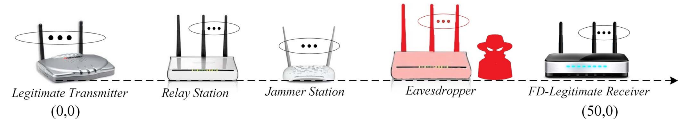


Fig. 6. Typical positioning model of the network nodes.

i.e., $N_s = N_d = N_r = N_j = N_e = 4$, while each HD receiver has one. The channel matrices are assumed to be composed of independent, zero-mean Gaussian random variables with unit variance. We perform Monte Carlo experiments consisting of 1000 independent trials to obtain the average results. Similar to [22], the normalized background noise power is assumed to be the same at LR and AE where $\sigma_d^2 = \sigma_r^2 = \sigma_e^2 = 0$ dB and for the transmit power of different nodes we assume $\acute{P}_s = 2P$, $P_s = P_d = P_j = P_r = P = 5$dB, $P_e = 4$dB, where $\acute{P}_s$ is the transmit power of the source for the HD scenario and P_s, P_d, P_j, and P_r are the transmit power for the source, destination, jammer, and relay, respectively for all other scenarios. P_e represents the transmit power of the AE. Unless otherwise stated, we let $\varepsilon_{\boldsymbol{g}_{se}}^2 = \varepsilon_{\boldsymbol{g}_{de}}^2 = \varepsilon_{\boldsymbol{g}_{je}}^2 = \varepsilon_{\boldsymbol{g}_{re}}^2 = \varepsilon_{\boldsymbol{g}_{er}}^2 = \varepsilon_{\boldsymbol{g}_{ed}}^2 = 0.5$.

For simplicity, we consider a simple one-dimensional system model, as illustrated in Fig. 6, in which the LT, jammer, relay, LR, and AE are placed along a line. The LT-relay/jammer distance is always assumed to be smaller than the LT-RT or the LT-AE distance. Channels between any two nodes are simply modelled through distance-dependent attenuation. For example, $g_{sd} = d_{sd}^{-c/2}$ where d_{sd} is the distance between the LT and LR where c is the path-loss exponent. We set $c = 3.5$ which is a typical value in the literature, nevertheless, other values for c also lead to similar results. The LT and LR distance is considered to be constant, in particular, we assume LT is located at the origin, i.e., coordinates (0,0) and the LR stays at coordinates (50,0) (all the distance units are in meters.).

A. Effect of Source-Eavesdropper Distance

Fig. VI-A shows secrecy data rate versus different positions of the eavesdropper. The total transmit power is fixed at $P = 5$ dB [22]. We fix the jammer/relay location at coordinates (25,0) (i.e., in an equal distance from LT and LR) and move the position of the AE from coordinates (30,0) to (90,0). As expected, the secrecy data rate for the HD scenario becomes zero when the LR is at a farther position (to the LT) than the AE. As observed, when the AE moves away from the LT, the secrecy data rate increases for the HDR scenario, since the received signal power at the AE decreases. For the HDJ scenario, it is interesting to see that the secrecy data rate at first decreases, then increases, and eventually becomes equal to the secrecy data rate of the HD scenario. The reduction in secrecy data rate is because more jamming power is needed for creating larger interference and less power is available for the LT to transmit the message signal, when the AE moves away from the jammer. However, when the AE gets very far away from the jammer and also the LT, we should spend most of the power on transmitting the message signal. In this situation,

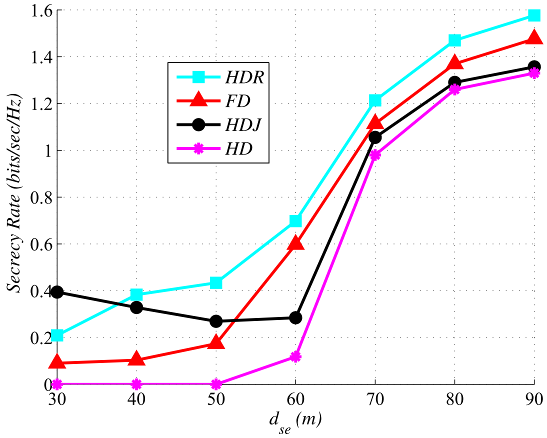


Fig. 7. Secrecy data rate, R, *vs*. LT and eavesdropper distance, d_{se} for HD, HDJ, and FD scenarios. The position of eavesdroppers varies from (30,0) to (90,0). The jammer/rely location is fixed at (25,0).

it is not worth spending a large amount of power on transmitting the jamming signal, since the received power of the message signal at the AE is always small (regardless of jamming) due to the large path loss. This explains why the secrecy data rate could increase. In the FD scenario, when the AE moves away from the LT and gets close to LR, the secrecy data rate increases, since the received jammer signal power at the AE increases.

B. Effect of Source-Jammer/Relay Distance

In Fig. 8(a), we fix the AE location at coordinates (70,0), and change the position of the jammer/relay from (5,0) to (45,0). All other parameters are the same as those used in Fig. VI-A. As expected, the secrecy data rate of the HD and FD scenarios are independent of the jammer/relay locations. When the jammer/relay moves away from the LT, the secrecy data rate for the HDR scenario first increases and then decreases, and there is an optimal relay location somewhere between the LT and LR. The secrecy data rate of the HDJ scenario, on the other hand, monotonically increases as the jammer gets closer to the AE since the received jamming power at AE is larger for a smaller jammer-AE distance.

In Fig. 8(b), we fix the AE location at (30,0), and move the position of the jammer/relay from (5,0) to (45,0). All other parameters are the same as those used in Fig. VI-A. As expected, the secrecy data rate of HD and FD scenarios are independent of the jammer/relay locations. When the jammer/relay moves away from the LT, the secrecy data rate for the HDJ scenario first increases and then decreases, and there is an optimal location for jammer somewhere between LT and LR. In this case, the HDJ scenario produces a better performance than the HDR scenario.

Note that for both figures, the HDR scenario outperforms others despite the fact that the whole time slot is divided into two equal slots; which would result in the reduction of secrecy rate intuitively. However, the effect of boosting the received SNR in HDR scheme is so pronounced that it compensates for this rate reduction.

Finally, in Figures 9(a) and 9(b), for different locations of the AE between (5,0) to (70,0), we investigate the conditions

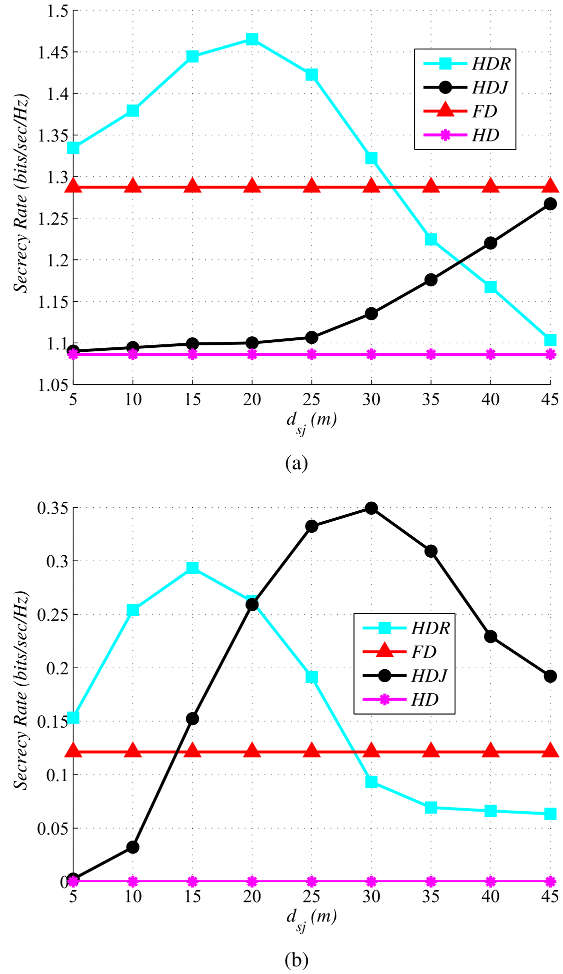
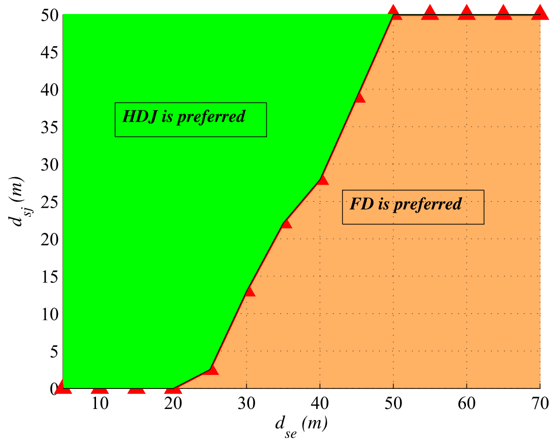


Fig. 8. (a) Secrecy data rate R *vs*. LT and jammer/relay distance d_{sj} for HD, HDJ, and FD scenarios. The position of jammer/relay varies from (5,0) to (45,0). The eavesdropper location is fixed at (70,0). (b) Secrecy data rate R *vs*. LT and jammer/relay distance d_{sj} for HD, HDJ, and FD scenarios. The position of jammer/relay varies from (5,0) to (45,0). The eavesdropper location is fixed at (30,0).

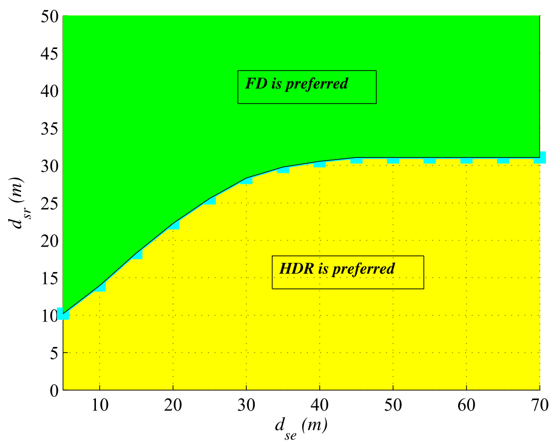
on the realy/jammer location between (0,0) to (50,0) under which the FD scenario is preferred over the HDJ and HDR scenarios. As can be seen, when AE is close to the source, for the majority of the considered range, HDJ scenario outperforms FD. For example, if AE is located on (5,0), HDJ scenario is preferred over FD on the whole considered range. However, when the AE is placed closer to the destination, FD scenario takes over in a broader range such that when AE is located on (50,0), FD is preferred for the whole range. For the HDR scenario the observation is different. When the AE is located closer to the source, FD scenario outperforms HDR in a broader range. For example, if AE is located on (5,0), HDR outperforms FD only when the relay is located on (10,0) or closer to the source. Interestingly, as AE moves towards the destination, FD takes over in a more limited range.

C. Effect of Multi Jammer/Relay

For this part, we fix the AE location at coordinate (70,0) and initially look for the conditions under which FD scenario outperforms HDR and HDJ with one relay/jammer. For example as can be seen in Fig. 8(a), FD scenario performs considerably

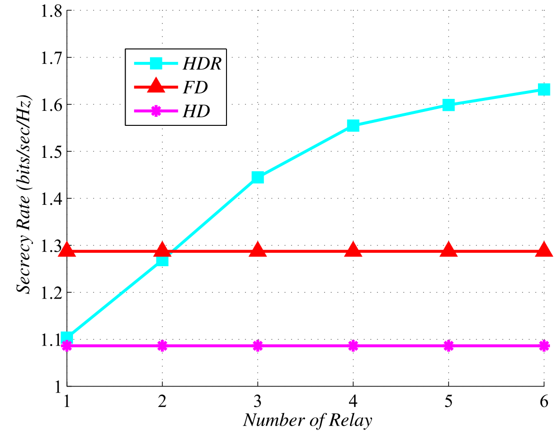


(a)

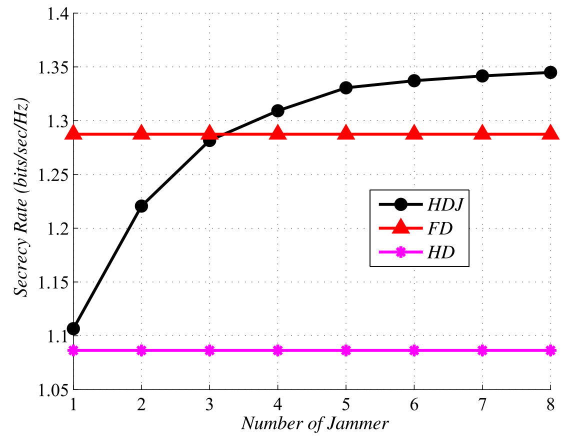


(b)

Fig. 9. (a) Jammer location d_{sj} for which the FD and HDJ scenarios produce the same secrecy rate *vs* LT and eavesdropper distance d_{se} for HDJ and FD scenarios. (b) Relay location d_{sr} for which the FD and HDR scenarios produce the same secrecy rate *vs* LT and eavesdropper distance d_{se} for HDR and FD scenarios.



(a)



(b)

Fig. 10. (a) Secrecy data rate R *vs*. number of relays for HD, HDJ, HDR, and FD scenarios. (b) Secrecy data rate R *vs*. number of jammers, for HD, HDJ, HDR, and FD scenarios. The locations of jammer/relay and eavesdropper are fixed at (45,0) and (70,0), respectively.

better than HDR and HDJ scenarios when the relay and jammer are located at coordinates (45, 0) and (70,0), respectively. We now uniformly add some relays between coordinates (40,0) and (50,0) and apply the best relay selection strategy. Fig. 10(a) shows the secrecy rate for different numbers of relays in this case. As can be seen, for $R \geq 2$, the secrecy rate of HDR scenario takes over that of the FD scenario. We repeat the same experiment with jammers. This time, the jammer are uniformly place between coordinates (20,0) to (30,0). Fig. 10(b) shows the secrecy rate for different numbers of jammers. As can be seen, for $J \geq 3$, the secrecy rate of the HDJ scenario takes over that of the FD scenario.

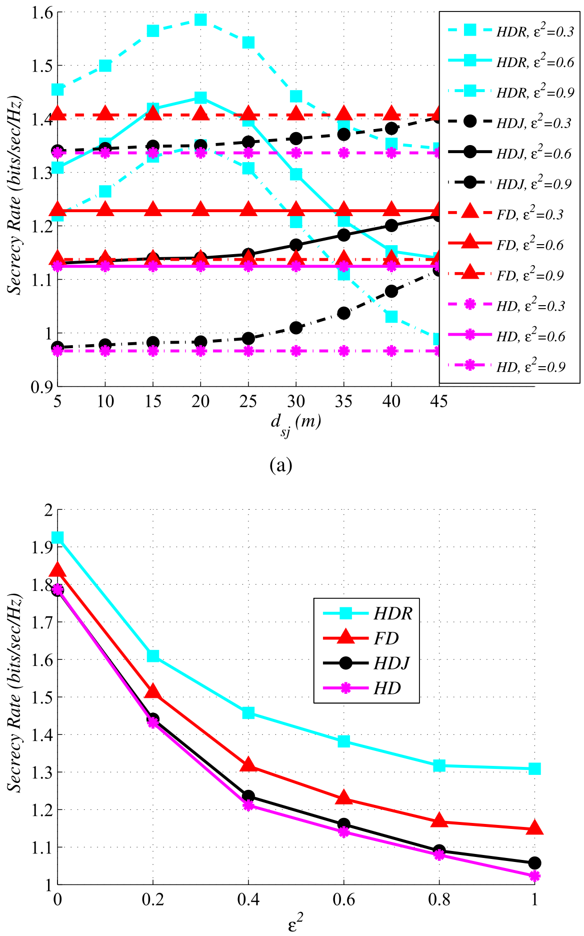
D. Effect of CSI Uncertainty

Fig. 11(a) considers the same scheme as that of 8(a) but for different values of ε^2. As expected, smaller values of ε^2 produce higher secrecy rates. Moreover, no specific difference can be seen in the behaviour of the considered scenarios with respect to each other. Fig. 11(b) plots the secrecy data rate for different values of $\varepsilon^2_{g_{se}} = \varepsilon^2_{g_{de}} = \varepsilon^2_{g_{je}} = \varepsilon^2_{g_{re}} = \varepsilon^2_{g_{er}} = \varepsilon^2_{g_{ed}} = \varepsilon^2$ from 0 to 1. We assume the same locations as the last figure for the network nodes. It can be seen from Fig. 11(b) that the secrecy data rate decreases as ε^2 increases. This is due to the fact that when ε^2 increases, a larger fraction of the transmit power must be devoted to each transmitter in order to reach a higher secrecy data rate.

E. Summary

For the considered simulation setup, the following conclusions can be drawn:

- In all cases the HD scenario has the weakest performance.
- In general, the performance of the HDJ and FD scenarios highly depend on where the jammer/relay and AE are located.
- When the jammer/relay is equally distant from the LT and RT (Fig. VI-A) and if the AE is not too close to the jammer/relay, the FD scenario outperforms the HDJ scenario and performs only slightly inferior to the HDR scenario. This is a very attractive situation from practical point of view as we can remove the need for an extra network node.
- In case the relay/jammer is considered to be portable and an estimate of the location of the eavesdropper is



(a)

(b)

Fig. 11. (a) Secrecy data rate *vs.* $d_s j$ for different values of ε^2. (b) Secrecy data rate R *vs.* channel mismatch between the eavesdropper and network nodes $\varepsilon^2_{g_{se}} = \varepsilon^2_{g_{de}} = \varepsilon^2_{g_{je}} = \varepsilon^2_{g_{re}} = \varepsilon^2_{g_{er}} = \varepsilon^2_{g_{ed}} = \varepsilon^2$ for HD, HDJ, HDR, and FD scenarios. The positions of eavesdropper and jammer/relay are at fixed at (70,0) and (25,0), respectively.

at hand, the HDJ scenario may be preferred over the FD scenario if the jammer can be placed close enough to the eavesdropper (Fig. 8(b)). A similar statement can be made for the HDR scenario. Otherwise, the FD scenario still outperforms the HDR as well as the HDJ scenario or in fact the conventional CJ scheme (Fig. 8(a)).

- If mutiple realys/jammers are permitted, the HDR/HDJ scenarios can take over FD most of the times.

VII. Conclusion

In this paper, we proposed a robust resource allocation framework to improve physical layer security in the presence of an active eavesdropper. Four different scenarios, namely, HD, HDJ, HDR, and FD were analysed to assess the performance of a system with FD receiver as compared with conventional CJ schemes. To solve the proposed optimization problem, we obtained robust transmit covariance matrices for the proposed scenarios based on worst-case secrecy data rate maximization. We then transformed the resulting non-convex optimization problems into quasi-convex problems.

Simulation results show that the preference of deploying the FD scenario over CJ or vice versa highly depends on where the jammer/relay and eavesdropper are located. In general one can conclude that if the jammer can be placed close enough to the eavesdropper, a better performance is achieved compared to the FD system. Otherwise, the FD scenario can generally take over and if this is the case, it would be very favorable from practical point of view as we can remove the need for an extra network node.

Appendix
Proof of Proposition 1

Problem $\tilde{O}_4^{HD}$ can be rewritten as

$$\min_{\boldsymbol{e}_{g_{ed}}} \ \boldsymbol{e}_{g_{ed}} \boldsymbol{Q}_e^* \boldsymbol{e}_{g_{ed}}^H + 2\Re(\tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \boldsymbol{e}_{g_{ed}}^H) + \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H, \quad \text{(A.1a)}$$

$$\text{s.t.} \ \ \| \boldsymbol{e}_{g_{ed}} \|^2 \leq \varepsilon^2_{g_{ed}}, \quad \text{(A.1b)}$$

with the Lagrangian

$$\begin{aligned} \mathcal{L}(\boldsymbol{e}_{g_{ed}}, \lambda) &= \boldsymbol{e}_{g_{ed}} (\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*) \boldsymbol{e}_{g_{ed}}^H + 2\Re(\tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \boldsymbol{e}_{g_{ed}}^H) \\ &\quad + \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H - \lambda \varepsilon^2_{g_{ed}}, \end{aligned} \quad \text{(A.2)}$$

where $\lambda \geq 0$ and the dual function is given by

$$g(\lambda) = \inf_{\boldsymbol{e}_{g_{ed}}} \mathcal{L}(\boldsymbol{e}_{g_{ed}}, \lambda) = \begin{cases} O \succeq 0, & \boldsymbol{Q}_e^* \boldsymbol{e}_{g_{ed}}^H \in \mathcal{R}(\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*); \\ -\infty, & \text{otherwise.} \end{cases} \quad \text{(A.3)}$$

where $O = \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \boldsymbol{e}_{g_{ed}}^H - \lambda \varepsilon^2_{g_{ed}} - \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* (\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*)^\dagger \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H + \lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*$. The unconstrained minimization of $\mathcal{L}(\boldsymbol{e}_{g_{ed}}, \lambda)$ with respect to $\boldsymbol{e}_{g_{ed}}$ is achieved when $\boldsymbol{e}_{g_{ed}} = -\tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* (\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*)^\dagger$, and the dual problem is thus obtained as

$$\max_{\lambda} \ \tilde{\boldsymbol{e}}_{g_{ed}} \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H - \lambda \varepsilon^2_{g_{ed}} - \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* (\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*)^\dagger \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H, \quad \text{(A.4a)}$$

$$\text{s.t.} \ \lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^* \succeq 0, \quad \text{(A.4b)}$$

$$\boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H \in \mathcal{R}(\lambda \boldsymbol{I}_{N_e} + \boldsymbol{Q}_e^*). \quad \text{(A.4c)}$$

Using the Schur complement, the dual problem can be converted to the following SDP:

$$\max_{\lambda \geq 0, \gamma} \ \gamma, \quad \text{(A.5a)}$$

$$\text{s.t.} \ \begin{bmatrix} \lambda \boldsymbol{I} + \boldsymbol{Q}_e^* & \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H \\ \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* & \tilde{\boldsymbol{g}}_{ed} \boldsymbol{Q}_e^* \tilde{\boldsymbol{g}}_{ed}^H - \lambda \varepsilon^2_{g_{ed}} - \gamma \end{bmatrix} \succeq 0, \quad \text{(A.5b)}$$

which completes the proof.

References

[1] M. Debbah, "Mobile flexible networks: The challenges ahead," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Hanoi, Vietnam, Oct. 2008, pp. 3–7.

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

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

[4] T. Riihonen, S. Werner, and R. Wichman, "Optimized gain control for single-frequency relaying with loop interference," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 2801–2806, Jun. 2009.

[5] I. Krikidis, H. Suraweera, S. Yang, and K. Berberidis, "Full-duplex relaying over block fading channels: A diversity perspective," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, pp. 4524–4535, Dec. 2012.

[6] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983–5993, Dec. 2011.

[7] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex MIMO relaying: Achievable rates under limited dynamic range," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1541–1553, Sep. 2012.

[8] M. Duarte *et al.*, "Design and characterization of a full-duplex multi-antenna system for WiFi networks," *IEEE Trans. Veh. Technol.*, vol. 36, no. 3, pp. 1160–1177, Oct. 2012.

[9] P. Lioliou, M. Viberg, M. Coldrey, and F. Athley, "Self-interference suppression in full-duplex MIMO relays," in *Proc. Rec. Asilomar Conf. Signals, Syst. Comput. (ASILOMAR)*, Pacific Grove, CA, USA, Nov. 2010, pp. 658–662.

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

[11] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: A block-Markov Wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, Jul. 2012.

[12] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[13] Q. Li, W. Ma, and A. So, "Safe convex approximation to outage-based MISO secrecy rate optimization under imperfect CSI and with artificial noise," in *Proc. Asilomar Conf. Signals, Syst., Comput.*, Pacific Grove, CA, USA, Nov. 2011, pp. 207–211.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[15] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1317–1322, Mar. 2011.

[16] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.

[17] J. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256–266, Jun. 2011.

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

[19] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," in *Proc. Statist. Signal Process. Workshop (SSP)*, Ann Arbor, MI, USA, Aug. 2012, pp. 389–392.

[20] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3461–3471, Nov. 2012.

[21] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[22] J. Huang and A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.

[23] L. Zhang, Y. C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Honolulu, HI, USA, Nov. 2009, pp. 1–5.

[24] J. Wang and D. P. Palomar, "Worst-case robust MIMO transmission with imperfect channel knowledge," *IEEE Trans. Signal Process.*, vol. 57, no. 8, pp. 3086–3100, Aug. 2009.

[25] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[26] M. R. Javan and N. Mokari, "Resource allocation for maximizing secrecy rate in presence of active eavesdropper," in *Proc. 22nd Iranian Conf. Electr. Eng. (ICEE)*, Tehran, Iran, May 2014, pp. 20–22.

[27] A. Chortiy, S. M. Perlazay, Z. Hanz, and H. V. Poory, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2013.

[28] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Conf. Rec. 45th Asilomar Signals Syst. Comput. (ASILOMAR)*, Nov. 2011, pp. 265–269.

[29] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[30] 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.

[31] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Secure robust resource allocation using full-duplex receivers," in *Proc. Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 497–502.

[32] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure MIMO communication: Achievable secrecy rate based optimization," *IEEE Signal Process. Lett.*, vol. 21, no. 7, pp. 804–808, Jul. 2014.

[33] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[34] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Secure robust resource allocation in the presence of active eavesdroppers using full-duplex receivers," in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC Fall)*, Sep. 2015, pp. 1–5.

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

[36] J. Bai and A. Sabharwal, "Decode-and-cancel for interference cancellation in a three-node full-duplex network," in *Proc. Conf. Rec. 46th Signals Syst. Comput. (ASILOMAR)*, Nov. 2012, pp. 1285–1289.

[37] G. Amarasuriya, C. Tellambura, and M. Ardakani, "Performance analysis of zero-forcing for two-way MIMO AF relay networks," *IEEE Wireless Commun. Lett.*, vol. 1, no. 2, pp. 53–56, Apr. 2012.

[38] R. H. Y. Louie, Y. Li, and B. Vucetic, "Zero forcing in general two-hop relay networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 191–202, Jan. 2010.

[39] B. Yin, M. Wu, C. Studer, J. R. Cavallaro, and J. Lilleberg, "Full-duplex in large-scale wireless systems," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Nov. 2013, pp. 1623–1627.

[40] N. Mokari, P. Azmi, and H. Saeedi, "Quantized ergodic radio resource allocation in OFDMA-based cognitive DF relay-assisted networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 10, pp. 5110–5123, Oct. 2013.

[41] M. R. Abedi, N. Mokari, M. R. Javan, and H. Yanikomeroglu, "Limited rate feedback scheme for resource allocation in secure relay-assisted OFDMA networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 2604–2618, Apr. 2016.

[42] J. N. Laneman, D. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[43] Q. Li and W. K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE J. Signal Process.*, vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[44] J. Li, A. P. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

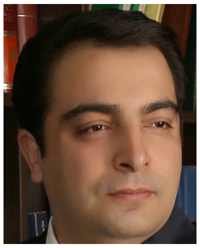
[45] A. N. D. Bertsekas and A. Ozdaglar, *Convex Analysis and Optimization*. Belmont, MA, USA: Athena Scientific, 2003.

[46] D. P. Bertsekas, *Nonlinear Programming*, 2nd ed. Belmont, MA, USA: Athena Scientific, 1999.

[47] D. P. Palomar, "Convex primal decomposition for multicarrier linear MIMO transceivers," *IEEE Trans. Signal Process.*, vol. 53, no. 12, pp. 4661–4674, Dec. 2005.

[48] R. Mo and Y. H. Chew, "MMSE-based joint source and relay precoding design for amplify-and-forward MIMO relay networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 9, pp. 4668–4676, Sep. 2009.

Mohammad Reza Abedi received the B.Sc. and M.Sc. degrees in electrical engineering from the Amirkabir University of Technology, Tehran, Iran. He is currently a Research Associate with Tarbiat Modares University, Tehran. His research interests include different aspects of wireless communications with concentration on radio resource allocation techniques.



Nader Mokari received the Ph.D. degree in electrical engineering from Tarbiat Modares University, Tehran, Iran, in 2014. He joined the Department of Electrical and Computer Engineering, Tarbiat Modares University, as an Assistant Professor, in 2015. He has been involved in a number of large scale network design and consulting projects in the telecom industry. His research interests include design, analysis, and optimization of communication networks.

Hamid Saeedi (S'01–M'08) received the B.Sc. and M.Sc. degrees from the Sharif University of Technology, Tehran, Iran, in 1999 and 2001, respectively, and the Ph.D. degree from Carleton University, Ottawa, ON, Canada, in 2007, all in electrical engineering. From 2008 to 2009, he was a Postdoctoral Fellow with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA, USA. In 2010, he joined the Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran. His current research interests include coding and information theory, wireless communications, and resource allocation in conventional, heterogeneous, and cognitive radio networks.

Dr. Saeedi has been a technical program committee member of some international conferences, including the Vehicular Technology Conference 2012, the Wireless Communication and Networking Conference 2014, 2015, and 2016, and the International Conference on Communications 2015. He was a recipient of some awards, including the Carleton University Senate Medal for Outstanding Academic Achievement, the Natural Sciences and Engineering Council of Canada Industrial Research and Development Fellowship, and the Ontario Graduate Scholarship. He is currently an Editor of the IEEE COMMUNICATIONS LETTERS.

Halim Yanikomeroglu (S'96–M'98–SM'12–F'17) was born in Giresun, Turkey, in 1968. He received the B.Sc. degree in electrical and electronics engineering from the Middle East Technical University, Ankara, Turkey, in 1990, and the M.A.Sc. degree in electrical engineering and the Ph.D. degree in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1992 and 1998, respectively. From 1993 to 1994, he was with the Research and Development Group of Marconi Kominikasyon A. S., Ankara, Turkey. Since 1998, he has been with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, where he is currently a Full Professor. He was a Visiting Professor with the TOBB University of Economics and Technology, Ankara, Turkey, from 2011 to 2012. His research interests include wireless technologies with a special emphasis on wireless networks. In recent years, his research has been funded by Huawei, Telus, Allen Vanguard, Blackberry, Samsung, Communications Research Centre of Canada, and DragonWave. This collaborative research resulted in over 25 patents (granted and applied). He was a recipient of the IEEE Ottawa Section Outstanding Educator Award in 2014, Carleton University Faculty Graduate Mentoring Award in 2010, the Carleton University Graduate Students Association Excellence Award in Graduate Teaching in 2010, and the Carleton University Research Achievement Award in 2009. He is a Registered Professional Engineer in Ontario, Canada. He has been involved in the organization of the IEEE Wireless Communications and Networking Conference (WCNC) from its inception, including serving as a Steering Committee Member and the Technical Program Chair or Co-Chair of the WCNC 2004, Atlanta, GA, USA, the WCNC 2008, Las Vegas, NV, USA, and the WCNC 2014, Istanbul, Turkey. He was the General Co-Chair of the IEEE Vehicular Technology Conference (VTC) 2010-Fall held in Ottawa, and he is serving as the General Chair of the IEEE VTC 2017-Fall which will be held in Toronto. He has served on the Editorial Boards of the IEEE TRANSACTIONS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, and the *IEEE Communications Surveys and Tutorials*. He was the Chair of the IEEE Wireless Technical Committee. He is a Distinguished Lecturer of the IEEE Communications Society and a Distinguished Speaker of the IEEE Vehicular Technology Society.