Secure Robust Resource Allocation in the Presence of Active Eavesdroppers using Full-Duplex Receivers

Mohmmad R. Abedi[1], Nader Mokari[1], Hamid Saeedi[1], and Halim Yanikomeroglu[2]
[1]Department of Electrical and Computer Engineering, Tarbiat Modares University, Tehran, Iran.
[2]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada.

***Abstract*—We propose a robust resource allocation framework to provide physical layer security for a multiple input single output (MISO) communication system. In the considered system, we assume that the both legitimate receiver and eavesdropper are in full-duplex (FD) mode and compare the corresponding performance to conventional cooperative jamming frameworks where a half-duplex (HD) receiver is at hand. In the present paper, the adversary intends to optimize its transmit and jamming signal parameters so as to minimize the MISO secrecy rate between the legitimate transmitter and receivers. The proposed self-protection scheme eliminates the need for external helpers and provides system robustness. Moreover, we investigate robustness against channel state information uncertainty. Optimal power allocation is obtained based on worst-case secrecy rate maximization, under legitimate transmitter power constraint in the presence of an active eavesdropper. Numerical results are then provided to confirm the advantages of using FD receivers.**

***Index Terms*—Full Duplex Receiver, Cooperative Jamming, Imperfect Channel State Information, Physical Layer Security, Semi Definite Programming, Active Eavesdropper.**

I. Introduction

Physical layer (PHY) security has arisen as a prominent frontier in wireless networks to maintain secure data transmission between the transmitter and the legitimate receiver [1]. In Wyner seminal paper on the three-node wiretap channel, he showed that perfect secrecy of transmitted data from the source node can be achieved when the physical channel to the eavesdropper is noisier than the channel to the intended destination, that is, when the channel is a degraded broadcast channel [2]. Accordingly, a given secrecy rate is achievable if messages can be reliably transmitted on that rate to the receiver while being kept perfectly secret from the eavesdropper.

An efficient way to increase the secrecy rate in wireless systems is to degrade the decoding capability of the eavesdroppers by introducing controlled interference, or artificial noise (AN) [3]. 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).

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]. In particular, [10] proposes to use a low-complexity zero forcing (ZF) SI cancellation solution. A similar framework based on ZF has also been considered in [11] and [12]. In this paper we also follow ZF approach as it makes it possible to obtain closed form solutions for achievable secrecy rate.

In the PHY 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. Majority of works in the literature on passive eavesdropping assume systems with HD terminals in a CJ framework [13]–[19]. Few works [10], [20] have considered to deploy FD receivers. In the second case, which is the focus of this paper, eavesdropper can observe the communication medium as well as modify its contents. Only few works have addressed this case: [21]–[24].

In [21], the authors consider the problem of secure communications in the presence of an active eavesdropper. The malicious user has the ability of either eavesdropping or jamming but not both at the same time. They obtain the optimal power allocation and optimal strategy to alternate between jamming and eavesdropping mode. In [22], the authors formulate the secure communication in presence of an active eavesdropper in the context of game theory. In their formulation, the legitimate user is one player of the game whose aim is to maximize the secrecy rate and the malicious user is another player whose aim is to minimize the secrecy rate of legitimate user. The authors analyze the game and obtain the Nash equilibrium of the game. In [23], the authors consider the problem of power allocation of an orthogonal frequency-division multiplexing (OFDM) user in the presence of an active attacker. The malicious user has the ability of either eavesdropping of ongoing connection or jamming it. However, it can not function as both the eavesdropper and jammer at the same time. The attackers policy is to choose between eavesdropping and jamming such that the ultimate secrecy rate is minimized.

In a system equipped with a FD based receiver, one may take advantage of the FD capability to generate the required AN, i.e, while receiving data, the receiver simultaneously transmits friendly jamming signals to degrade the eaves-

This work was in part supported by Iran National Elites Foundation.

978-1-4799-8091-8/15/$31.00 ©2015 IEEE

dropper channel. This eliminates the need to deploy relays which is very welcome from practical point of view. If so, a question follows: how the performance of such a system is compared with a traditional HD system that uses relays? We have addressed this question for the case of passive eavesdroppers in our recent paper [25]. This paper aims to shed light on the potential benefits of using FD terminal to provide physical layer security in the presence of an active FD based eavesdropper. To the best of our knowledge, there is no work in the literature that has analyzed systems with FD receivers in the presence of active eavesdroppers.

In this paper, we consider a legitimate transmitter (LT) which acts as the source, a legitimate receiver (LR) which acts as the destination, an active eavesdropper (AE), and a relay used as 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 is overhearing it. The AE transmitter tries to degrade the reception of the information signal at the intended receiver. Then we assume three scenarios. The first one, denoted by HD, includes nodes s, d, and e. This is in fact a baseline scenario where neither a relay nor a FD receiver is present to send jamming signals. The second scenario, denoted by HDJ, includes nodes s, d, e, and j (a CJ scenario) where the receiver d is in HD mode. The third scenario, denoted by FD, includes nodes s, d, and e where the receiver d is in FD mode.

In all scenarios, in the presence of a FD eavesdropper, we aim to maximize the achievable secrecy rate by properly allocating the available resources. Moreover, we assume channel state information (CSI) uncertainty between the AE and the network nodes and consider robust secrecy rate optimization problems solved based on the worst-case secrecy rate approach. This is also not considered in [21]–[24]. By incorporating the channel uncertainties and exploiting the S-Procedure [26], we show that these robust optimization problems can be formulated into convex ones so as to obtain a closed form solution.

The organization of this paper is as follows. In the next section, some notations and assumptions are reviewed. In Sections III, IV, and V, secrecy rate maximization problems are presented for the considered system models. The performance of the proposed secrecy transmission approaches is studied using several simulation examples in Section VI, and conclusions are drawn in Section VII. Due to space limitation, the solutions to the proposed problems are removed and have been included in the extended version of this paper [27].

II. Notations and assumptions

The following notation is used in the paper: $\mathbb{E}$ denotes expectation, $(\cdot)^H$ the Hermitian transpose, $\|\cdot\|$ the Euclidean norm, $(\cdot)^\dagger$ the pseudo-inverse, $tr(\cdot)$ is the trace operator, and I is an identity matrix of appropriate dimension, $\boldsymbol{A}\succeq 0(\boldsymbol{A}\succ 0)$ 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 single antenna. The legitimate FD receiver is assumed to have N_d transmit antennas.

We assume $\boldsymbol{g}_{sd}$ and $\boldsymbol{g}_{se}$ denote the $1\times N_s$ channel vectors gain between LT and destination and LT and AE, respectively. Moreover, $\boldsymbol{g}_{jd}$ and $\boldsymbol{g}_{je}$ denote the $1\times N_j$ channel vectors gain between jammer and LR and jammer and AE, respectively. $\boldsymbol{g}_{ed}$ denotes the $1\times N_e$ channel vectors gain between AE and LR, respectively. Finally for the system with FD legitimate receiver (FD-LR), we let $\boldsymbol{g}_{de}$ denote the $1\times N_d$ channel gain vector between FD-LR and AE, where N_d is the number of LR's transmitter antenna. The FD-LR and FD-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 and FD-AE whose vector gains are denoted by $\boldsymbol{h}_d$ and $\boldsymbol{h}_e$ with dimensions $1\times N_d$ and $1\times N_e$, respectively.

We assume that the naturally occurring noise at LR and AE is zero-mean circular complex Gaussian with variance σ_d^2 and σ_e^2, respectively. To simplify the notations, we will assume without loss of generality that $\sigma_d^2=\sigma_e^2=\sigma^2$.

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 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 is defined as $\boldsymbol{e}_{\boldsymbol{g}_{je}}=\boldsymbol{g}_{je}-\tilde{\boldsymbol{g}}_{je}$. 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 is defined as $\boldsymbol{e}_{\boldsymbol{g}_{ed}}=\boldsymbol{g}_{ed}-\tilde{\boldsymbol{g}}_{ed}$. 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 vectors as $\boldsymbol{e}_{\boldsymbol{g}_{de}}=\boldsymbol{g}_{de}-\tilde{\boldsymbol{g}}_{de}$. For all cases, we assume that the channel mismatches lie in the bounded set [28], i.e., $\mathcal{E}_{\boldsymbol{g}_{se}}=\{\boldsymbol{e}_{\boldsymbol{g}_{se}}:\|\boldsymbol{e}_{\boldsymbol{g}_{se}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{se}}\}$, $\mathcal{E}_{\boldsymbol{g}_{je}}=\{\boldsymbol{e}_{\boldsymbol{g}_{je}}:\|\boldsymbol{e}_{\boldsymbol{g}_{je}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{je}}\}$, $\mathcal{E}_{\boldsymbol{g}_{ed}}=\{\boldsymbol{e}_{\boldsymbol{g}_{ed}}:\|\boldsymbol{e}_{\boldsymbol{g}_{ed}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{ed}}\}$, $\mathcal{E}_{\boldsymbol{g}_{de}}=\{\boldsymbol{e}_{\boldsymbol{g}_{de}}:\|\boldsymbol{e}_{\boldsymbol{g}_{de}}\|^2\leq\varepsilon^2_{\boldsymbol{g}_{de}}\}$, where $\varepsilon^2_{\boldsymbol{g}_{se}}$, $\varepsilon^2_{\boldsymbol{g}_{je}}$, $\varepsilon^2_{\boldsymbol{g}_{ed}}$ and $\varepsilon^2_{\boldsymbol{g}_{de}}$ are known constants.

III. The HD Scenario

In the first proposed system, we consider one LT transmitting data to LR while one AE eavesdrops the LR. In this model, LR 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 rate is expressed as follows

$$R_s=\left[\log_2\left(1+\frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2+(\tilde{\boldsymbol{g}}_{ed}+\boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed}+\boldsymbol{e}_{\boldsymbol{g}_{ed}})^H}\right)-\log_2\left(1+\frac{(\tilde{\boldsymbol{g}}_{se}+\boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s(\tilde{\boldsymbol{g}}_{se}+\boldsymbol{e}_{\boldsymbol{g}_{se}})^H}{\sigma^2+\boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H}\right)\right]^+, \quad (1)$$

where $[a]^+=\max\{0,a\}$ and $\boldsymbol{Q}_s$ is the covariance matrix of the signal transmitted by LT, $\boldsymbol{x}_s$, and is given by $\boldsymbol{Q}_s=\mathbb{E}\{\boldsymbol{x}_s\boldsymbol{x}_s^H\}$, and the power constraint is imposed such that $\boldsymbol{Q}_s\in\boldsymbol{\mathcal{Q}}_s=\{\boldsymbol{Q}_s:\boldsymbol{Q}_s\succeq 0, tr(\boldsymbol{Q}_s)\leq P_s\}$ where P_s is the maximum allowable transmission power on LT, $\boldsymbol{Q}_e$ 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 $\boldsymbol{Q}_e \in \boldsymbol{\mathcal{Q}}_e = \{\boldsymbol{Q}_e : \boldsymbol{Q}_e \succeq 0, tr(\boldsymbol{Q}_e) \leq P_e\}$ where P_e is the maximum allowable transmit power on AE. We focus on optimizing the worst-case performance, where we maximize the secrecy 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. Therefore, the optimization problem can be written as follows

Problem $\mathcal{O}^{HD}$:

$$\max_{\boldsymbol{Q}_s\in\boldsymbol{\mathcal{Q}}_s}\ \min_{\substack{\boldsymbol{Q}_e\in\boldsymbol{\mathcal{Q}}_e;\boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}};\\ \boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}}}} R_s, \tag{2a}$$

$$\text{s.t.} \quad tr(\boldsymbol{Q}_s) \leq P_s, \tag{2b}$$

$$tr(\boldsymbol{Q}_e) \leq P_e, \tag{2c}$$

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

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

$$\boldsymbol{Q}_s \succeq 0, \tag{2f}$$

$$\boldsymbol{Q}_e \succeq 0, \tag{2g}$$

where (2b) and (2c) are the LT and AE power constraints.

IV. The HDJ Scenario

In this section, we consider a cooperative jamming multiple input single output (MISO) communication system with an LT, a jammer, an LR, and an AE. In this model, LT sends the private messages to the LR in the presence of an AE, who is able to eavesdrop on the link between LT and LR as well as to degrade the reception of the information signal at the LR by transmitting jamming signal. The jammer transmits artificial interference signals to confuse the AE.

The data rate at the destination can be written as

$$R_d = \log_2\left(1 + \frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{g}_{jd}\boldsymbol{Q}_j\boldsymbol{g}_{jd}^H + (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})^H}\right).$$

The data rate of eavesdropper can be expressed as

$$R_e = \log_2\left(1 + \frac{(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})^H}{\sigma^2 + (\tilde{\boldsymbol{g}}_{je} + \boldsymbol{e}_{\boldsymbol{g}_{je}})\boldsymbol{Q}_j(\tilde{\boldsymbol{g}}_{je} + \boldsymbol{e}_{\boldsymbol{g}_{je}})^H + \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H}\right).$$

Therefore, the secrecy data rate for the wiretap channel can be written as

$$R_s = \max\{0, R_d - R_e\} =$$

$$\left[\log_2\left(1+\frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{g}_{jd}\boldsymbol{Q}_j\boldsymbol{g}_{jd}^H + (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})^H}\right)\right.$$

$$\left. - \log_2\left(1+\frac{(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})^H}{\sigma^2 + (\tilde{\boldsymbol{g}}_{je} + \boldsymbol{e}_{\boldsymbol{g}_{je}})\boldsymbol{Q}_j(\tilde{\boldsymbol{g}}_{je} + \boldsymbol{e}_{\boldsymbol{g}_{je}})^H + \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H}\right)\right]^+,$$

where $\boldsymbol{Q}_j$ is the covariance matrix of the signal transmitted by jammer, $\boldsymbol{x}_j$, and is given by $\boldsymbol{Q}_j = \mathbb{E}\{\boldsymbol{x}_j\boldsymbol{x}_j^H\}$, and the power constraint is imposed such that $\boldsymbol{Q}_j \in \boldsymbol{\mathcal{Q}}_j = \{\boldsymbol{Q}_j : \boldsymbol{Q}_j \succeq 0, tr(\boldsymbol{Q}_j) \leq P_j\}$ where P_j is the maximum predefined transmit power on jammer. Therefore, the optimization problem can be written as follows

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

$$\max_{\substack{\boldsymbol{Q}_s\in\boldsymbol{\mathcal{Q}}_s;\\ \boldsymbol{Q}_j\in\boldsymbol{\mathcal{Q}}_j}}\ \min_{\substack{\boldsymbol{Q}_e\in\boldsymbol{\mathcal{Q}}_e;\boldsymbol{e}_{\boldsymbol{g}_{se}}\in\mathcal{E}_{\boldsymbol{g}_{se}};\\ \boldsymbol{e}_{\boldsymbol{g}_{je}}\in\mathcal{E}_{\boldsymbol{g}_{je}};\\ \boldsymbol{e}_{\boldsymbol{g}_{ed}}\in\mathcal{E}_{\boldsymbol{g}_{ed}}}} R_s, \tag{3a}$$

$$\text{s.t.} \quad tr(\boldsymbol{Q}_j) \leq P_j, \tag{3b}$$

$$\| \boldsymbol{e}_{\boldsymbol{g}_{je}} \|^2 \leq \varepsilon^2_{\boldsymbol{g}_{je}}, \tag{3c}$$

$$\boldsymbol{Q}_j \succeq 0, \tag{3d}$$

$$(2b), (2c), (2e), (2f), (2g), (2d).$$

V. The FD Scenario

In this Section, we consider one LT transmitting data to FD-LR while one FD-AE eavesdrops the FD-LR as depicted in Fig. 1. In other words, in this model, source sends private messages to destination in the presence of eavesdropper, who is able to eavesdrop on the link between source and distinction. The eavesdropper has only imperfect CSI for its channels to destination.

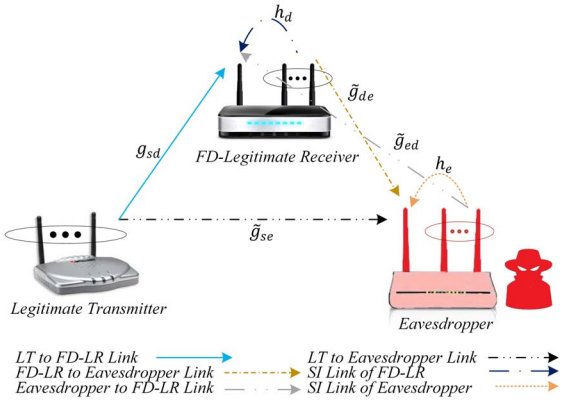


Fig. 1. A schematic of system model for FD-LR.

The achievable secrecy rate is expressed as follows

$$R_s = \left[\log_2\left(1 + \frac{\boldsymbol{g}_{sd}\boldsymbol{Q}_s\boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{h}_d\boldsymbol{Q}_d\boldsymbol{h}_d^H + (\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})\boldsymbol{Q}_e(\tilde{\boldsymbol{g}}_{ed} + \boldsymbol{e}_{\boldsymbol{g}_{ed}})^H}\right)\right.$$

$$\left. - \log_2\left(1 + \frac{(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s(\tilde{\boldsymbol{g}}_{se} + \boldsymbol{e}_{\boldsymbol{g}_{se}})^H}{\sigma^2 + \boldsymbol{h}_e\boldsymbol{Q}_e\boldsymbol{h}_e^H + (\tilde{\boldsymbol{g}}_{de} + \boldsymbol{e}_{\boldsymbol{g}_{de}})\boldsymbol{Q}_d(\tilde{\boldsymbol{g}}_{de} + \boldsymbol{e}_{\boldsymbol{g}_{de}})^H}\right)\right]^+.$$

where $\boldsymbol{Q}_d$ is the covariance matrix of the signal transmitted by the FD-LR, $\boldsymbol{x}_d$, and is given by $\boldsymbol{Q}_d = \mathbb{E}\{\boldsymbol{x}_d\boldsymbol{x}_d^H\}$, and the power constraint is imposed such that $\boldsymbol{Q}_d \in \boldsymbol{\mathcal{Q}}_d = \{\boldsymbol{Q}_d : \boldsymbol{Q}_d \succeq 0, tr(\boldsymbol{Q}_d) \leq P_d\}$ where P_d is the maximum predefined transmit power on LR. We also let $\boldsymbol{h}_d$ denote $1\times N_d$ SI channel power gain vector for LR.

The secrecy rate maximization problem in case of active eavesdropper is given as follows

Problem $\mathcal{O}^{FD}$:

$$\max_{\substack{\boldsymbol{Q}_s\in\mathcal{Q}_s;\\ \boldsymbol{Q}_d\in\mathcal{Q}_d}} \quad \min_{\substack{\boldsymbol{Q}_e\in\mathcal{Q}_e;\boldsymbol{e}_{g_{se}}\in\mathcal{E}_{g_{se}};\\ \boldsymbol{e}_{g_{de}}\in\mathcal{E}_{g_{de}};\\ \boldsymbol{e}_{g_{ed}}\in\mathcal{E}_{g_{ed}}}} R_s, \tag{4a}$$

$$\text{s.t.} \quad tr(\boldsymbol{Q}_d) \leq P_d, \tag{4b}$$

$$\| \boldsymbol{e}_{g_{de}} \|^2 \leq \varepsilon^2_{\boldsymbol{g}_{de}}, \tag{4c}$$

$$\boldsymbol{Q}_d \succeq \boldsymbol{0}, \tag{4d}$$

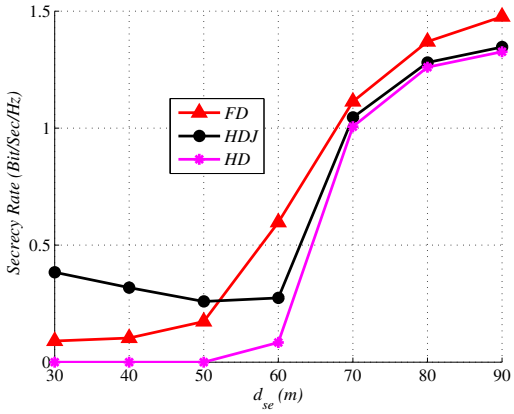
$$(2b), (2c), (2e), (2f), (2g), (2d).$$

VI. Simulation Results

This section presents the numerical results of the proposed system schemes. The proposed schemes have been evaluated in terms of secrecy data rate. We assume LT, jammer, AE and FD-LR have four transmit antennas, i.e., $N_s = N_d = N_j = N_e = 4$, 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. The normalized background noise power is assumed to be the same at LR, AE, and relay, $\sigma_d^2 = \sigma_e^2 = 0$ dB as in [28]. For simplicity, we consider a simple one-dimensional system model, in which the LT, jammer, LR, and AE are placed along a line. Channels between any two nodes are simply modeled through distance-dependent attenuation. For example, $g_{sd} = d_{sd}^{-c/2}$ where d_{sd} is the distance between the LT and LR. 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., at coordinates (0,0), and LR at coordinates (50,0) (all the distances are in meters.). We also assume that the values of channel mismatch are all equal to 0.5, i.e., $\varepsilon^2_{\boldsymbol{g}_{se}} = \varepsilon^2_{\boldsymbol{g}_{de}} = \varepsilon^2_{\boldsymbol{g}_{je}} = \varepsilon^2_{\boldsymbol{g}_{ed}} = 0.5$.

A. Effect of Source-Eavesdropper Distance

Fig. 4 shows secrecy rate versus different positions of the eavesdropper from (30,0) to (90,0). The total transmit power constraint is fixed at $P = 5$ dB [28]. We fix the relay and jammer locations at coordinates (25,0) (i.e., in equal distance from LT and LR) and move the position of the AE from coordinates (30,0) to (90,0). As expected, the secrecy rate for 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 rate increases for HDR scenario, since the received signal power at the AE decreases. For HDJ scenario, it is interesting to see that the secrecy rate at first decreases, then increases, and eventually becomes equal to the secrecy rate of HD scenario. The decrease of secrecy 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 relay. However, when the AE gets very far away from the relay and also the LT, we should spend most of the power on transmitting the message signal. In this situation, it is not worthy 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 rate could increase. In FD scenario, when the AE moves away from the LT and gets close to LR, the secrecy rate increases, since the received jammer signal power at the AE increases.



(a)

Fig. 2. Secrecy 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 location are fixed at (25,0). System parameters: $P_s = P_d = P_j = 5$ dB, $P_e = 4$ dB, $\varepsilon^2_{\boldsymbol{g}_{se}} = \varepsilon^2_{\boldsymbol{g}_{de}} = \varepsilon^2_{\boldsymbol{g}_{je}} = \varepsilon^2_{\boldsymbol{g}_{ed}}$, $N_s = N_d = N_j = N_e = 4$.

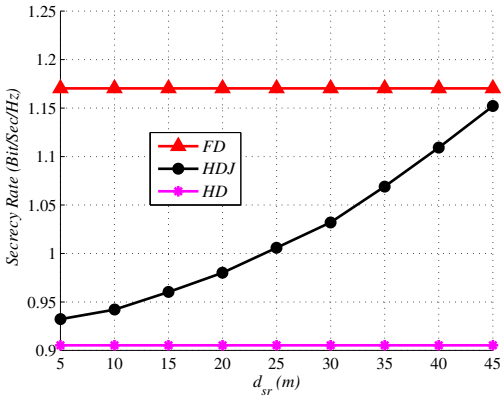
B. Effect of Source-Jammer Distance

In Fig. 3(a), we fix the AE location at coordinates (70,0), and change the position of the jammer from (5,0) to (45,0). All other parameters are the same as those used in Fig. 4. As expected, the secrecy rate of HD and FD scenarios are independent of the jammer locations. The secrecy rate of HDJ scenario monotonically increases as the jammer gets closer close to the AE since the received jamming power at AE is larger for a smaller jammer-AE distance.

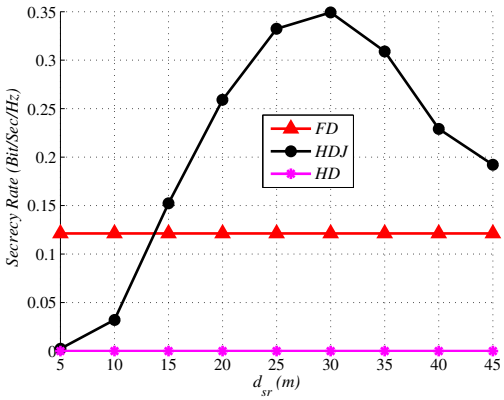
In Fig. 3(b), we fix the AE location at (30,0), and move the position of the jammer from (5,0) to (45,0). All other parameters are the same as those used in Fig. 4. As expected, the secrecy rate of HD and FD scenarios are independent of the jammer locations. When jammer move away from the LT, the secrecy rate for HDJ scenario first increases and then decreases, and there is an optimal jammer locations somewhere between LT and LR. In this case, HDJ scenario produces a better performance than FD scenario.

VII. Conclusion

In this paper, we consider a framework to provide physical layer security in the presence of an active eavesdropper. We considered 3 scenarios, namely, HD, HDJ and FD, to assess the performance of a FD receiver and to determine whether it can replace the more conventional CJ scheme. Taking the uncertainty of CSI into account, we proposed robust power allocation problems for each scenario and solved them based no the worst-case optimization methods. Simulation results reveal that the preference of deploying the FD scenario over CJ, or viceversa, highly depends on where the jammer and



(a)



(b)

Fig. 3. Secrecy rate, R, *vs*. LT and relay distance, d_{sj} for HD, HDJ, and FD scenarios. The position of jammer varies from (5,0) to (45,0). The eavesdropper location is fixed at a) (70,0) and b) (30,0) . System parameters: $P_s = P_d = P_j = 5$ dB, $\varepsilon^2_{\boldsymbol{g}_{se}} = \varepsilon^2_{\boldsymbol{g}_{de}} = \varepsilon^2_{\boldsymbol{g}_{je}} = \varepsilon^2_{\boldsymbol{g}_{ed}} = 0.5$, $N_s = N_d = N_j = N_e = 4$.

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 which is very favorable from practical point of view as we can remove the need for an extra network node.

REFERENCES

[1] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, January 1975.

[3] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 1058–1072, January 2014.

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

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

[6] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 12, pp. 5983–5993, December 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 Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1541–1553, September 2012.

[8] M. Duarte, A. Sabharwal, V. Aggarwal, R. Jana, K. K. Ramakrishnan, C. Rice, and N. K. Shankaranarayanan, "Design and characterization of a full-duplex multi-antenna system for WiFi networks," *IEEE Transactions on Vehicular Technology*, vol. 36, no. 3, pp. 1160–1177, October 2012.

[9] P. Lioliou, M. Viberg, M. Coldrey, and F. Athley, "Self-interference suppression in full-duplex MIMO relays," *Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA*, vol. 63, no. 3, pp. 658–662, November 2007.

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

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

[12] R. Louie, Y. Li, and B. Vucetic, "Zero forcing in general two-hop relay networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 1, pp. 191–202, January 2010.

[13] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, March 2011.

[14] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, October 2009.

[15] J.Vilela, M. Bloch, J. Barros, and S.W.McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Theory, Forensics Security*, vol. 6, no. 2, pp. 256–266, Junuray 2011.

[16] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Transactions on Information Theory, Forensics Security*, vol. 7, no. 2, pp. 704–716, April 2012.

[17] S. Luo, J. Li, and A. Petropulu, "Outage constrained secrecy rate maximization using cooperative jamming," *Statistical Signal Processing Workshop (SSP), Ann Arbor, MI, USA*, August 2012.

[18] Z. Ding, M. Peng, and H.-H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Transactions on Communications*, vol. 60, no. 11, pp. 3461–3471, November 2012.

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

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

[21] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fastfading channels: A block-markov wyner secrecy encoding scheme," *IEEE Transactions On Information Theory*, vol. 58, no. 7, pp. 4660–4677, July 2012.

[22] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Transactions On Signal Processing*, vol. 61, no. 1, pp. 82–91, January 2013.

[23] M. R. Javan and N. Mokari, "Resource allocation for maximizing secrecy rate in presence of active eavesdropper," in *The 22nd Iranian Conference on Electrical Engineering (ICEE 2014)*. Iran, Shahid Beheshti University, May 2014, pp. 20–22.

[24] A. Chortiy, S. M. Perlazay, Z. Hanz, and H. V. Poory, "On the resilience of wireless multiuser networks to passive and active eavesdroppers," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1850–1863, September 2013.

[25] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Secure robust resource allocation using full-duplex receivers," *International Conference on Communications (ICC), Workshop on Wireless Physical Layer Security (WPLS), London, UK*, June 2015.

[26] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[27] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *to be Submitted to IEEE Transactions on Signal Processing*, 2015.

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