Secure Robust Resource Allocation 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*—This paper studies a robust resource allocation framework to enhance physical layer security where it is assumed that the system is equipped with a full-duplex (FD) receiver in contrast to conventional frameworks where a half-duplex (HD) receiver is at hand. Conventionally, relays are used as jammer to reduce the signal quality received by the eavesdroppers so as to increase the secrecy transmission rate between the legitimate transmitter and receiver. This is referred to as cooperative jamming (CJ). In a system equipped with a FD receiver, we propose to use the FD receiver as the jammer, i.e., the FD receiver simultaneously transmits jamming signals toward the eavesdropper while receiving data from the transmitter. The proposed scheme eliminates the need for external helpers, i.e., jamming relays which is welcome from practical point of view. We consider different scenarios to compare the proposed scheme against the CJ scheme in which, under a legitimate transmitter power constraint, optimal power allocation is obtained for each scenario to maximize the secrecy rate. To take into account the impact of imperfect state information of the channels between the eavesdropper and other nodes on the network, worst-case optimization approaches are considered. Simulation results demonstrate that for certain positions of the jamming relay and eavesdropper, the proposed system can outperform the conventional CJ schemes.**

I. Introduction

Secure transmission in wireless networks is an important concern in most applications. Traditionally, security is considered as an issue addressed above the physical (PHY) layer, i.e., cryptography methods [1]. The challenges in wireless distribution and management of secret keys together with the fact that computational power is becoming easily available to users nowadays have led to a growing interest to ensure secrecy and confidentiality at the PHY layer.

The theoretical basis of this area was initiated by Wyner, who introduced and studied the wiretap channel where the eavesdropper's received signal is a degraded version of the legitimate receiver's signal [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.

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 at the same time and in the same frequency band. It is expected that advances in electronics, antenna technology and signal processing will allow the implementation of full-duplex (FD) terminals as long as the self interference (SI) that leaks from the receiver output to the receiver input can be dealt with [3]– [4]. In particular, [5] and [6] propose to use a low-complexity zero-forcing (ZF) SI cancellation solution which is also used in this paper.

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) [7]. One way to generate AN is to employ a group of external relays to collaboratively send jamming signals to degrade the eavesdropper channel. This approach is referred to as cooperative jamming (CJ).

The the CJ strategy has been utilized in many works such as [8]–[15]. The computation of the optimal CJ relay weights for maximizing the secrecy rate is investigated in [8], [9]. An opportunistic selection of two relays, where one relay re-forwards the transmitted signal, while the other uses the CJ strategy, is discussed in [10] in the context of a multi-relay network. In [11], authors study the secrecy outage probability using CJ for different levels of the channel state information (CSI). The optimal transmit beamforming together with AN design for minimizing the secrecy outage probability is addressed in [12], [13]. The work in [14] combines CJ with interference alignment. Destination-assisted jamming scheme is used in [15] to prevent the system from becoming interference-limited. In [8]–[14], 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 might not be a practical assumption. Among few works in physical layer security that consider uncertainty on the CSI values, we can mention [15]–[18].

In a system equipped with FD terminals, a natural question is whether one can take advantage of the FD capability to generate the required AN, i.e, while receiving data, whether the terminal can simultaneously transmit jamming signals to degrade the eavesdropper channel. This eliminates the need to deploy relays which is very welcome from practical point of view. If so, a secondary question follows: how is the performance of such a system compared with a traditional HD system that uses CJ relays?

In this paper, we study the potential benefits of a FD receiver node simultaneously acting as a jammer and a receiver, with the goal of improving the secrecy rate. We consider a legitimate transmitter (LT) which acts as the source, a legitimate receiver (LR) which acts as the destination, a passive eavesdropper (PE), 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 PE is overhearing it. 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 three scenarios, we aim to maximize the achievable secrecy rate by properly allocating the available resources. Moreover, we assume CSI uncertainty between the PE and the network nodes and consider robust secrecy rate optimization problems based on the worst-case secrecy rate approach. By incorporating the channel uncertainties and exploiting the S-Procedure [19], we show that these robust optimization problems can be formulated as convex ones which result in closed-form solutions.

Among the works in literature that use FD receivers in the context of PHY layer security, we can mention [20] and [21]. A FD receiver that generates AN is proposed in [20] to impair the eavesdroppers channel. However, in contrast to our work, no resource allocation framework is considered. Instead, the secrecy performance is evaluated based on the outage secrecy region from a geometric perspective. In [21] a FD receiver is assumed to generate AN to improve physical layer security in a resource allocation framework. However, as opposed to this paper, prefect CSI is assumed between the eavesdropper and other nodes of the considered network. Moreover, in [21], parts of the proposed solution to the optimization problem rely on one- and two-dimensional searches to find certain intermediate parameters which are necessary to obtain the optimal solution. This is quite different from our approach in which through some transformations, the problem is modified to a semi-definite program (SDP) problem and can be solved efficiently.

The organization of this paper is as follows. In the next section, the notation and assumptions are reviewed. In Sections III, IV, and V, secrecy rate maximization problems are presented for the considered scenarios. 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 notation is used in the paper: $\mathbb{E}$ denotes expectation, $(\cdot)^H$ the Hermitian transpose, $\|\cdot\|$ the Euclidean norm, $(\cdot)^\dagger$ the pseudo-inverse, $\mathrm{tr}(\cdot)$ is the trace operator, and I is an identity matrix of appropriate dimension.

We assume the LT and the jammer have N_s and N_j transmit antennas, respectively. All HD receivers as well as the PE are assumed to have signal antenna.

The $1\times N_s$ vectors $\boldsymbol{g}_{sd}$ and $\boldsymbol{g}_{se}$ denote the gain of the channels between LT and destination and LT and PE, respectively. Moreover, the $1\times N_j$ vectors, $\boldsymbol{g}_{jr}$ and $\boldsymbol{g}_{je}$, denote the channel gains between jammer and LR and jammer and PE, 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 PE, where N_d is the number of LR's transmitter antenna. The FD-LR transmits a jamming signal while it simultaneously receives the LT transmitted signal. This creates a feedback loop channel between the input and output of the FD-LR whose gain is denoted by $\boldsymbol{h}_d$.

We assume that the naturally occurring noise at LR and PE 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 PE 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 $\boldsymbol{e}_{\boldsymbol{g}_{je}}=\boldsymbol{g}_{je}-\tilde{\boldsymbol{g}}_{je}$. 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 [16], i.e.,

$\mathcal{E}_{\boldsymbol{g}_{se}}=\{\boldsymbol{e}_{\boldsymbol{g}_{se}}:\|\boldsymbol{e}_{\boldsymbol{g}_{se}}\|^2\le\varepsilon^2_{\boldsymbol{g}_{se}}\}$,
$\mathcal{E}_{\boldsymbol{g}_{je}}=\{\boldsymbol{e}_{\boldsymbol{g}_{je}}:\|\boldsymbol{e}_{\boldsymbol{g}_{je}}\|^2\le\varepsilon^2_{\boldsymbol{g}_{je}}\}$,
$\mathcal{E}_{\boldsymbol{g}_{de}}=\{\boldsymbol{e}_{\boldsymbol{g}_{de}}:\|\boldsymbol{e}_{\boldsymbol{g}_{de}}\|^2\le\varepsilon^2_{\boldsymbol{g}_{de}}\}$,
where $\varepsilon^2_{\boldsymbol{g}_{se}}$, $\varepsilon^2_{\boldsymbol{g}_{je}}$, and $\varepsilon^2_{\boldsymbol{g}_{de}}$, are known constants.

III. The HD Scenario

In the first proposed system, there is one LT transmitting data to an LR while one PE is overhearing it as depicted in Fig. 1. In this model the LT sends private messages to LR in the presence of PE, who is able to eavesdrop on the link between the LT and RT.

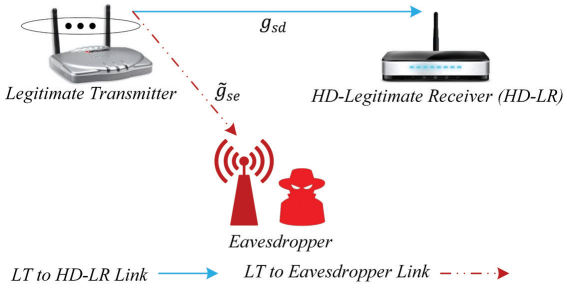

Fig. 1. A schematic of the HD scenario.

The achievable secrecy rate is expressed as follows: [16]

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

where $\Xi(\boldsymbol{Q}_s,\boldsymbol{e}_{\boldsymbol{g}_{se}})=(\tilde{\boldsymbol{g}}_{se}+\boldsymbol{e}_{\boldsymbol{g}_{se}})\boldsymbol{Q}_s(\tilde{\boldsymbol{g}}_{se}+\boldsymbol{e}_{\boldsymbol{g}_{se}})^H$, $[a]^+=\max\{0,a\}$ and $\boldsymbol{Q}_s$ is the covariance matrix of the signal transmitted by LT, $\boldsymbol{x}_s$, which is given by $\boldsymbol{Q}_s=\mathbb{E}\{\boldsymbol{x}_s\boldsymbol{x}_s^H\}$. In (1) the power constraint is imposed such that $\boldsymbol{Q}_s\in\boldsymbol{\mathcal{Q}}_s=\{\boldsymbol{Q}_s:\boldsymbol{Q}_s\succeq\boldsymbol{0},(\boldsymbol{Q}_s)\le P_s\}$ where P_s is the maximum allowable transmission power for LT.

We focus on optimizing the worst-case performance, where we maximize the secrecy rate for the worst channel mismatch

$\boldsymbol{e}_{\boldsymbol{g}_{se}}$ in the bounded set $\mathcal{E}_{\boldsymbol{g}_{se}}$. Therefore, the optimization problem can be written as follows:

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

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

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

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

$$\boldsymbol{Q}_s \succeq 0. \tag{2d}$$

The solution to the above optimization problem has already been proposed in [16].

IV. The HDJ Scenario

In this section, we consider a cooperative jamming MISO communication system with an LT, a jammer, an LR, and a PE, as shown in Fig. 2. In this model, LT sends the private messages to the LR in the presence of a PE, who is able to eavesdrop on the link between LT and LR. The jammer transmits artificial interference signals to confuse the PE.

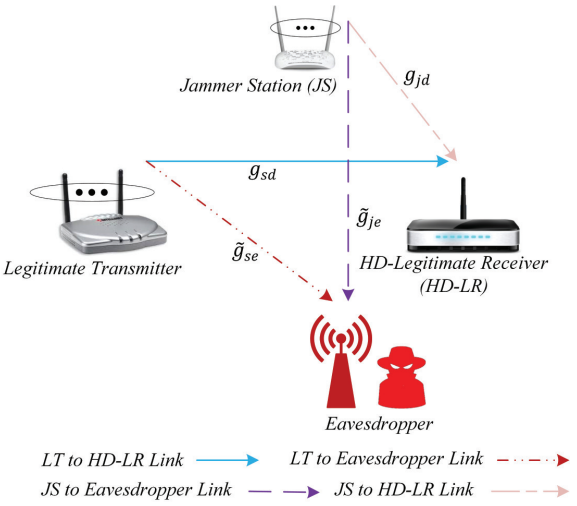

Fig. 2. A schematic of the HDJ scenario.

The data rate at the LR can be written as

$$R_d = \log_2 \left(1 + \frac{\boldsymbol{g}_{sd} \boldsymbol{Q}_s \boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{g}_{jd} \boldsymbol{Q}_j \boldsymbol{g}_{jd}^H} \right). \tag{3}$$

The data rate of PE can be expressed as

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

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

$$R_s = \max\{0, R_d - R_e\} = \left[\log_2 \left(1 + \frac{\boldsymbol{g}_{sd} \boldsymbol{Q}_s \boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{g}_{jd} \boldsymbol{Q}_j \boldsymbol{g}_{jd}^H} \right) - \log_2 \left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}})}{\sigma^2 + \Xi(\boldsymbol{Q}_j, \boldsymbol{e}_{\boldsymbol{g}_{je}})} \right) \right]^+, \tag{5}$$

where $\boldsymbol{Q}_j$ 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 $\boldsymbol{Q}_j \in \boldsymbol{\mathcal{Q}}_j = \{\boldsymbol{Q}_j : \boldsymbol{Q}_j \succeq 0, \text{tr}(\boldsymbol{Q}_j) \leq P_j\}$ where P_j is the maximum predefined transmit power on jammer. Therefore, the optimization problem can be written as follows:

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

$$\max_{\boldsymbol{Q}_s \in \boldsymbol{\mathcal{Q}}_s, \boldsymbol{Q}_j \in \boldsymbol{\mathcal{Q}}_j} \min_{\boldsymbol{e}_{\boldsymbol{g}_{se}} \in \mathcal{E}_{\boldsymbol{g}_{se}}, \boldsymbol{e}_{\boldsymbol{g}_{je}} \in \mathcal{E}_{\boldsymbol{g}_{je}}} \quad R_s, \tag{6a}$$

$$\text{s.t.} \quad \text{tr}(\boldsymbol{Q}_j) \leq P_j, \tag{6b}$$

$$||\boldsymbol{e}_{\boldsymbol{g}_{je}}||^2 \leq \varepsilon^2_{\boldsymbol{g}_{je}}, \tag{6c}$$

$$\boldsymbol{Q}_j \succeq 0, \tag{6d}$$

$$(2b), (2c), (2d).$$

The solution to this optimization problem has been proposed in [16].

V. The FD Scenario

In this section, we consider a system with one FD-LR (Full duplex-legitimate receiver), one LT and one PE as depicted in Fig. 3. As mentioned before, since in FD transmission, bidirectional communications happens on the same time and same frequency band, the resulting large SI should be taken care of. In this paper, we use the ZF method for SI cancellation [5].

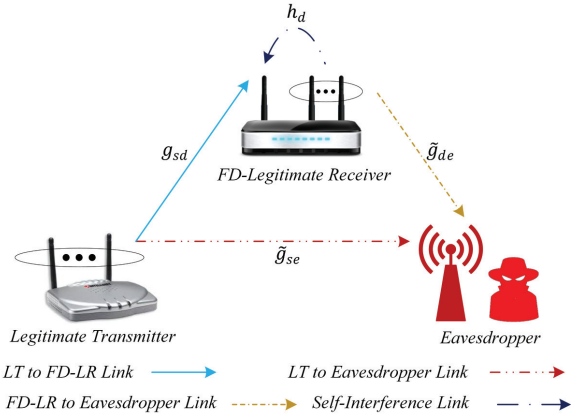

Fig. 3. A schematic of the FD scenario.

The achievable secrecy rate is expressed as follows:

$$R_s = \left[\log_2 \left(1 + \frac{\boldsymbol{g}_{sd} \boldsymbol{Q}_s \boldsymbol{g}_{sd}^H}{\sigma^2 + \boldsymbol{h}_d \boldsymbol{Q}_d \boldsymbol{h}_d^H} \right) - \log_2 \left(1 + \frac{\Xi(\boldsymbol{Q}_s, \boldsymbol{e}_{\boldsymbol{g}_{se}})}{\sigma^2 + \Xi(\boldsymbol{Q}_d, \boldsymbol{e}_{\boldsymbol{g}_{de}})} \right) \right]^+, \tag{7}$$

where $\Xi(\boldsymbol{Q}_d, \boldsymbol{e}_{\boldsymbol{g}_{de}}) = (\tilde{\boldsymbol{g}}_{de} + e_{\boldsymbol{g}_{de}})\boldsymbol{Q}_d(\tilde{\boldsymbol{g}}_{de} + e_{\boldsymbol{g}_{de}})$ and $\boldsymbol{Q}_d$ is the covariance matrix of the signal transmitted by 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 $\boldsymbol{Q}_d \in \boldsymbol{\mathcal{Q}}_d = \{\boldsymbol{Q}_d : \boldsymbol{Q}_d \succeq 0, \mathrm{tr}(\boldsymbol{Q}_d) \leq P_d\}$ 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 is then as follows:

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

$$\max_{\boldsymbol{Q}_s \in \boldsymbol{\mathcal{Q}}_s, \boldsymbol{Q}_d \in \boldsymbol{\mathcal{Q}}_d} \quad \min_{\boldsymbol{e}_{\boldsymbol{g}_{se}} \in \mathcal{E}_{\boldsymbol{g}_{se}}, \boldsymbol{e}_{\boldsymbol{g}_{de}} \in \mathcal{E}_{\boldsymbol{g}_{de}}} \quad R_s, \tag{8a}$$

$$\text{s.t.} \quad \mathrm{tr}(\boldsymbol{Q}_d) \leq P_d, \tag{8b}$$

$$\boldsymbol{Q}_d \succeq 0, \tag{8c}$$

$$(2b), (2d).$$

In general, maximization of $\mathcal{O}^{FD}$ over both $\boldsymbol{Q}_s$ and $\boldsymbol{Q}_d$ is a nonconvex problem. When the channel state information of PE is perfectly known, an iterative approach can be shown to converge to the optimal solution. However, our problem involves imperfect channel state information of PE and dose not lend itself to such an approach. To simplify the problem, we use a ZF constraint on the SI signal. This assumption allows us to convert the problem into a convex one. In particular, with the ZF constraint, the maximization of R with respect to $\boldsymbol{Q}_d$ dose not depend on $\boldsymbol{Q}_s$, although the optimal $\boldsymbol{Q}_s$ still depends on $\boldsymbol{Q}_d$. We can then decouple the optimization process into two convex problems, in which $\boldsymbol{Q}_d$ is dealt with first followed by $\boldsymbol{Q}_s$. The detailed solution can be found in the extended version of this paper [22].

VI. Simulation Results

In this section, we present the numerical results on the secrecy rate of the systems studied in the paper. We assume LT, jammer, and FD-LR have four transmit antennas, i.e., $N_s = N_d = N_j = N_r = 4$, 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 considered to be the same at LR, PE, and jammer and we assume $\sigma_d^2 = \sigma_e^2 = 0$ dB as in [16]. We also assume $P_s = P_d = P_j = 5$ dB as in [16]. For simplicity, we consider a simple one-dimensional system model, as illustrated in Fig. 4, in which the LT, jammer, LR, and PE are placed along a straight line. The LT-jammer distance is always assumed to be smaller than the LT-RT or the LT-PE distance. 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 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., 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., $\varepsilon_{\boldsymbol{g}_{se}}^2 = \varepsilon_{\boldsymbol{g}_{de}}^2 = \varepsilon_{\boldsymbol{g}_{je}}^2 = 0.5$.

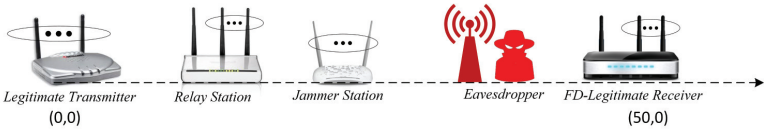

Fig. 4. A typical positioning model of the network nodes.

A. Effect of Source-Eavesdropper Distance

We fix the jammer location at coordinates (25,0) (i.e., in equal distance from LT and LR) and move the position of the PE from coordinates (30,0) to (90,0). The achievable secrecy rate is shown in Fig. 5 in which the total transmit power constraint is fixed at $P = 5$ dB [16]. For HDJ scenario, it is interesting to see that the secrecy rate at first decreases, then increases. The decrease of secrecy rate is due to the fact that more jamming power is needed for creating larger interference and less power is available for the LT to transmit the message signal, when the PE moves away from the jammer. However, when the PE 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, 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 PE is always small (regardless of jamming) due to a large amount of path loss. This explains why the secrecy rate could increase. In FD scenario, when the PE moves away from the LT and gets close to LR, the secrecy rate increases, since the received jammer signal power at the PE increases.

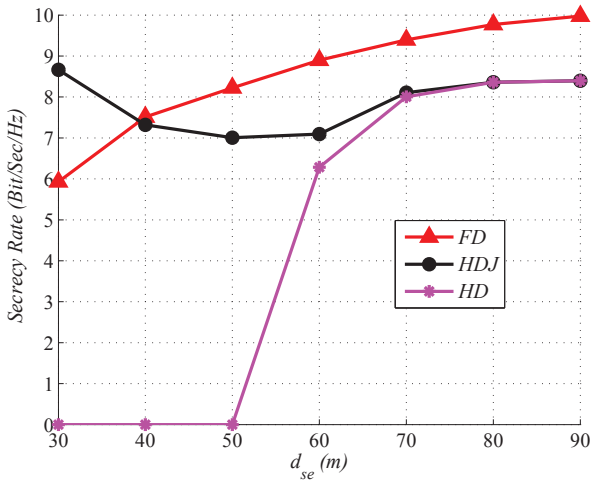

Fig. 5. Secrecy rate, R, *vs.* LT and eavesdropper distance, d_{se} for HD, HDJ and FD scenarios. The position of eavesdroppers varies from (30,0) to (90,0). The jammer location is fixed at (25,0).

B. Effect of Source-Jammer Distance

In Fig. 6(a), we fix the PE 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. 5. As expected, the secrecy rate of FD scenario is independent of the jammer location. When the jammer moves away from the LT,

the secrecy rate of HDJ scenario monotonically increases as the jammer gets closer to the PE since the received jamming power at PE is larger for a smaller jammer-PE distance.

In Fig. 6(b), we fix the PE 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. 5. As expected, the secrecy rate of the HD scenario is zero in this case and the secrecy rate of FD scenario is independent of the jammer location. When the jammer moves away from the LT, the secrecy rate for the HDJ scenario first increases and then decreases, and there is an optimal jammer location somewhere between LT and LR. In this case, HDJ scenario produces a better performance than the FD scenario.

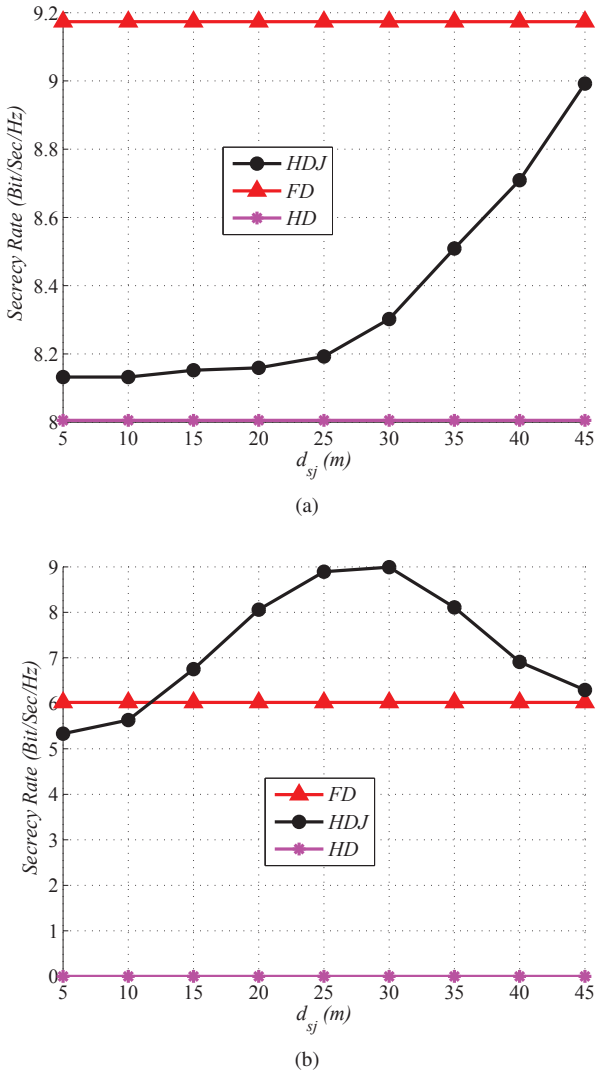

Fig. 6. (a) Secrecy rate, R, *vs*. LT and jammer distance, d_{sj} for HD, HDJ and FD scenarios. The position of jammer varies from (5,0) to (45,0). The eavesdropper location is fixed at (70,0). (b) Secrecy rate, R, *vs*. LT and jammer distance, d_{sj}, for HD, HDJ and FD scenarios. The position of jammer varies from (5,0) to (45,0). The eavesdropper location is fixed at (30,0).

C. Summary

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

· In general, the performance of HDJ and FD scenarios highly depend on where the jammer and PE are located.

· When the jammer is equally distant from the LT and RT (Fig. 5), the FD scenario outperforms the HDJ 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 jammer is considered to be portable and an estimate of the location of the eavesdropper is at hand, CJ scheme may be preferred over the FD scenario if the jammer can be placed close enough to the eavesdropper (Fig. 6(b)). Otherwise, the FD scenario still outperforms the HDJ scenario or in fact the conventional CJ scheme (Fig. 6(a)).

VII. Conclusion

In this paper, we studied robust transmit designs for MISO wiretap channels with imperfect CSI for different 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. Robust transmit covariance matrices were obtained for the proposed scenarios, based on the worst-case secrecy rate maximization. We then transformed the resulting non-convex optimization problems into quasi-convex problems. Simulation results reveal that the preference of deploying the FD scenario over CJ, or viceversa, highly depends on where the jammer 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 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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Junuary 2008.

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

[9] 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.

[10] 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.

[11] 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, Januray 2011.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] L. Zhang, Y.-C. Liang, Y. Pei, and R. Zhang, "Robust beamforming design: From cognitive radio MISO channels to secrecy MISO channels," in *Proc. Global Telecommunications Conference, (GLOBECOM)*, November 2009, pp. 1–5.

[18] B. Yang, W. Wang, B. Yao, and Q. Yin, "Destination assisted secret ¿¿ wireless communication with cooperative helpers," *IEEE Signal Processing Letters*, vol. 20, no. 11, pp. 1030–1033, November 2013.

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

[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. 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.

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