Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers

Gan Zheng, *Senior Member, IEEE*, Ioannis Krikidis, *Senior Member, IEEE*, Jiangyuan Li, *Member, IEEE*, Athina P. Petropulu, *Fellow, IEEE*, and Björn Ottersten, *Fellow, IEEE*

Abstract—This paper studies secrecy rate optimization in a wireless network with a single-antenna source, a multi-antenna destination and a multi-antenna eavesdropper. This is an unfavorable scenario for secrecy performance as the system is interference-limited. In the literature, assuming that the receiver operates in half duplex (HD) mode, the aforementioned problem has been addressed via use of cooperating nodes who act as jammers to confound the eavesdropper. This paper investigates an alternative solution, which assumes the availability of a full duplex (FD) receiver. In particular, while receiving data, the receiver transmits jamming noise to degrade the eavesdropper channel. The proposed self-protection scheme eliminates the need for external helpers and provides system robustness. For the case in which global channel state information is available, we aim to design the optimal jamming covariance matrix that maximizes the secrecy rate and mitigates loop interference associated with the FD operation. We consider both fixed and optimal linear receiver design at the destination, and show that the optimal jamming covariance matrix is rank-1, and can be found via an efficient 1-D search. For the case in which only statistical information on the eavesdropper channel is available, the optimal power allocation is studied in terms of ergodic and outage secrecy rates. Simulation results verify the analysis and demonstrate substantial performance gain over conventional HD operation at the destination.

Keywords

Full-duplex, physical-layer security, jamming, beamforming, MIMO, convex optimization.

I. INTRODUCTION

Wireless communication technology has been integrated in almost all the aspects of social life. Cellular mobile networks, sensor/body networks, smart grid, smart home and smart cities are just some examples of wireless systems that people are using or will use in the near future. Under this uncontrolled growth of wireless personal information transfer, confidentiality and secret transmission is introduced as an emergent research topic. Traditionally, security is addressed at the upper layers of the protocol stack by using cryptographic tools, which basically rely on the computational limitations of the

Gan Zheng and Björn Ottersten are with the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, 4 rue Alphonse Weicker, L-2721 Luxembourg, E-mail: {gan.zheng, bjorn.ottersten}@uni.lu.

Ioannis Krikidis is with the Department of Electrical and Computer Engineering, University of Cyprus, Cyprus, E-mail: krikidis@ucy.ac.cy.

Jiangyuan Li and Athina P. Petropulu are with the Department of Electrical and Computer Engineering, Rutgers-The State University of New Jersey, New Brunswick, NJ 08854 USA, E-mail:{jiangyli,athinap}@rci.rutgers.edu.

eavesdroppers. Given that these approaches are sensitive to the wireless transmission and management of the secret keys, recently there has been growing interest to ensure secrecy and confidentiality at the physical (PHY) layer. PHY layer security is an information-theoretic approach and achieves secrecy by using channel codes and signal processing techniques. The seminal work of Wyner [1] introduced the degraded wiretap channel and the fundamental notion of secrecy capacity. Since then, several studies have been proposed in the literature from the viewpoints of both information theory [2]–[5] and signal processing [6]–[15].

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). When the transmitter has multiple antennas, this can be achieved by having the transmitter embed in its transmission artificial noise, [6][7][8], which can be designed to avoid the legitimate receiver and only affect the eavesdroppers [6][7]. Under imperfect eavesdroppers channel state information (CSI), an AN-aided outage secrecy-rate maximization problem was tackled in [8].

When the transmitter is restricted to the use of one antenna, a bank 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) [9]–[15]. The optimal CJ relay weights design for maximizing the secrecy rate is investigated in [9][10]. An opportunistic selection of two relays, where one relay re-forwards the transmitted signal, while the other uses the CJ strategy is discussed in [11] in the context of a multi-relay network. In [12], the authors study the secrecy outage probability using CJ for different levels of CSI. The optimal transmit beamforming together with AN design for minimizing the secrecy outage probability is addressed in [13][14]. The work in [15] combines CJ with interference alignment. The idea of using destination and source as jammers in the first phase of a two-phase relay network, is proposed in [16]. A destination-assisted jamming scheme is used in [17] to prevent the system becoming interference-limited.

Based on the existing literature, CJ approaches are mainly rely on external helpers, thus suffer from issues related to helper mobility, synchronization and trustworthiness. More recently, some approaches have been proposed that do not require external helpers for jamming, such as the *iJam* scheme of [18], in which the receiver acts as a jammer. In the *iJam* scheme, the source repeats the transmission, while the receiver randomly jams one of the transmitted copies in each sample

time; since the eavesdropper does not know which sample is "clean", it cannot decode the transmitted signal. However, this self-protection procedure requires a retransmission of the source signal which lowers throughput. In the majority of the literature, the terminals operate in half-duplex (HD) mode, thus are not able to receive and transmit data simultaneously. However, recent advances on electronics, antenna technology and signal processing allow the implementation of full duplex (FD) terminals that can receive and transmit data in the same time and on the same frequency band. When it comes to relaying, the FD operation can utilize the channel more effectively by achieving end-to-end transmission in one channel use, as long as the loop interference (LI) that leaks from the relay output to the relay input can be addressed [19], [20]. Antenna isolation, time cancelation and spatial precoding have been proposed in the literature for the mitigation of LI [21], [22], [23], [24]. Comparison of the HD and the FD systems with transmit power adaptation is given in [25].

In the context of PHY layer secrecy, the potential benefits of the FD relaying technology have not yet fully explored. In [26] the authors employ FD technology in a PHY layer secrecy context but from the adversary point of view; the paper investigates an FD eavesdropper with LI that optimizes its beamforming weights in order to minimize the secrecy rate of the system. An FD receiver generating AN is proposed in [27] to impair the eavesdropper's channel. The secrecy performance of that method is evaluated based on the outage secrecy region from a geometrical perspective. However, in [27] it is assumed that the LI can be perfectly canceled at the receiver, which might be too optimistic. To the best of our knowledge, the use of FD with spatial LI mitigation in order to enlarge the secrecy rate of the system has not been reported in the literature.

Inspired by the works in [17], [18], [26] and [27], in this paper we study the potential benefits of an FD destination node simultaneously acting as a jammer and a receiver, with the goal of improving the secrecy rate. We consider an unfavorable situation of a single-antenna source, thus source generated will not improve the secrecy rate a [6][27] as there are not enough degrees of freedom to design the jamming signal. The proposed approach provides a self-protection mechanism at the receiver side without requiring external assistance, out-of-band channel or data retransmission, and is mainly of interest in applications in which assisting nodes are not available and/or are not trusted. Remarkably, for the case in which the destination has multiple transmit or receive antennas, we show that the system is no longer interference-limited and the secrecy rate does not suffer from saturation at high signal-to-noise-ratio (SNR) as in the HD case. In order to tackle the problem of LI and maximize the secrecy rate, joint transmit and receive beamforming design is studied at the destination. Our contributions are summarized as follows:

- In contrast to previous works employing FD nodes [27], we do not assume complete self-interference cancellation, but we rather employ a LI model whose parameter describes the effect of the passive self-interference suppression.
- For the scenario of a destination with one transmit and one receive antenna, and a single antenna eavesdropper,

we derive the closed form solution for the power allocation at the receiver. It is shown that due to the LI, the destination usually does not use all the available power.
- When the destination has multiple transmit antennas, the system is no longer interference-limited. We show that in that case the optimal jamming covariance matrix is rank-1; and propose efficient algorithms to find the optimal covariance matrix. Both fixed and optimal linear receivers are considered.
- When only eavesdropper CDI is available, we optimize the power allocation with respect to ergodic secrecy rate and outage secrecy rate.

The organization of the paper is as follows. In Section II, we present the general system model and introduce the FD receiver and the self-jamming operation. Section III narrows down to a single-antenna case and derives the optimal power allocation for the destination and the source. Section IV deals with optimal jamming covariance design. In Section V, we address the jamming design and power allocation to maximize the ergodic secrecy rate and the outage secrecy rate. In Section VI, we study the optimal jamming covariance design when the eavesdropper knows the FD operation of the destination and also adopts the optimal linear receiver. Simulation results are presented in Section VII and Section VIII concludes this paper.

A. Notation

Throughout this paper, the following notation will be adopted. Vectors and matrices are represented by boldface lowercase and uppercase letters, respectively. $\| \cdot \|$ denotes the Frobenius norm. $(\cdot)^{\dagger}$ denotes the Hermitian operation of a vector or matrix. $\mathbb{E}[\cdot]$ denotes the expectation of a random variable. The notation $\mathbf{A} \in \mathbb{C}^{M \times N}$ indicates that $\mathbf{A}$ is complex matrix with dimensions $M \times N$. $\mathbf{A} \succeq \mathbf{0}$ means that $\mathbf{A}$ is positive semi-definite. $\mathbf{I}$ denotes an identity matrix of appropriate dimension. Finally, $\mathbf{x} \sim \mathcal{CN}(\mathbf{m}, \mathbf{\Theta})$ denotes a vector $\mathbf{x}$ of complex Gaussian elements with a mean vector of $\mathbf{m}$ and a covariance matrix of $\mathbf{\Theta}$.

II. SYSTEM MODEL

Consider a wireless communication system with one source S with a single antenna, one destination D and one passive eavesdropper E, with M and M_e antennas, respectively, as depicted in Fig. 1. D's total M antennas are divided to M_r receive antennas and M_t transmit antennas with $M = M_t + M_r$.

Let $\mathbf{h}_{sd} \in \mathbb{C}^{M_r \times 1}$, $\mathbf{h}_{se} \in \mathbb{C}^{M_e \times 1}$ and $\mathbf{H}_{ed} \in \mathbb{C}^{M_e \times M_t}$ denote the S$-$D, S$-$E and between D$-$E channels, respectively. $\mathbf{n}_D \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ and $\mathbf{n}_E \sim \mathcal{CN}(\mathbf{0}, \mathbf{I})$ represent noise at D and E, respectively. The transmit signal s is assumed to be a zero-mean complex Gaussian random variable with power constraint $\mathbb{E}[|s|^2] \leq P_s$.

In the considered network configuration, there is no external relay or helper to assist D against E. Instead, as shown in Fig. 1, D helps itself by operating in FD mode and transmitting jamming signals to degrade the quality of the eavesdropper's link to S. The receiver transmits a jamming signal while it simultaneously receives the source signal. This creates a

feedback loop channel from the relay output to the relay input through the effective channel $\mathbf{H}_{si} = \sqrt{\rho}\mathbf{H} \in \mathbb{C}^{M_r \times M_t}$, where $\mathbf{H}$ is a fading loop channel [19], [20], [21], [22]. In order to make our study more general, we parameterize the LI channel by introducing the variable ρ with $0 \leq \rho \leq 1$ [26]; this parameter models the effect of passive LI suppression such as antenna isolation [21]. Therefore, $\rho = 0$ refers to the ideal case of no LI (perfect antenna isolation) while $0 < \rho \leq 1$ corresponds to different LI levels.

We assume that D transmits the jamming signal $\mathbf{n} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q})$. The covariance matrix $\mathbf{Q}$ will be designed to a maximize the secrecy rate with power constraint $p_d = \text{trace}(\mathbf{Q}) \leq P_d$. We assume that E is not aware of the FD operation of D, and simply uses a maximum ratio combining (MRC) receiver, $\mathbf{h}_{se}^{\dagger}$ [1]. The received signal at E is $\mathbf{y}_E = \mathbf{h}_{se}s + \mathbf{H}_{ed}\mathbf{n} + n_e$. After applying MRC receiver, the data estimate at E is:

$$\hat{s}_e = \frac{\mathbf{h}_{se}^{\dagger}}{\|\mathbf{h}_{se}\|}(\mathbf{h}_{se}s + \mathbf{H}_{ed}\mathbf{n} + n_e). \tag{1}$$

D employs a linear receiver, $\mathbf{r}$, on its received signal, $\mathbf{y}_D = \mathbf{h}_{sd}s + \sqrt{\rho}\mathbf{H}\mathbf{n} + n_d$, to obtain the data estimate

$$\hat{s}_d = \mathbf{r}^{\dagger}(\mathbf{h}_{sd}s + \sqrt{\rho}\mathbf{H}\mathbf{n} + n_d), \text{ with } \|\mathbf{r}\| = 1. \tag{2}$$

The achievable secrecy rate is expressed as [12]

$$\begin{aligned} R_S &= \max\left\{0, \log_2\left(1 + \frac{P_s|\mathbf{r}^{\dagger}\mathbf{h}_{sd}|^2}{1 + \rho\mathbf{r}^{\dagger}\mathbf{H}\mathbf{Q}\mathbf{H}^{\dagger}\mathbf{r}}\right)\right. \\ &\left. - \log_2\left(1 + \frac{P_s\|\mathbf{h}_{se}\|^2}{1 + \frac{\mathbf{h}_{se}^{\dagger}\mathbf{H}_{ed}\mathbf{Q}\mathbf{H}_{ed}^{\dagger}\mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}}\right)\right\}. \end{aligned} \tag{3}$$

We should note that the above secrecy rate also corresponds to the case of an external jammer helper with M_t antennas, whose channels to D and E are $\rho\mathbf{H}$ and $\mathbf{H}_{ed}$, respectively. The difference in the considered case is that D needs to perform LI cancelation to achieve that rate. In this paper, we consider LI mitigation in the spatial domain, in order to keep the complexity low. For FD systems with multiple antennas, the suppression of LI in the spatial domain has been addressed in the literature i.e., [21], [24], where the low rank of the spatial LI channel is exploited to avoid the transmit signal noise, which is the main source of the residual LI. Alternatively, the LI can be mitigated in the time domain using analogue or/and digital LI cancelation. However, this approach requires expensive cancelation circuits and is sensitive to transmit noise due to non-idealities at the relay node [22]. It is worth noting that the time cancelation requires two rounds of pilots for the case of successive analogue/digital cancelation, which further increases the complexity of the suppression process [23].

Throughout this paper, we assume that positive secrecy rate is achievable. In the following, we will study the transmit beamforming optimization at D to maximize the secrecy rate R_S, with the power constraint P_d at D, or the joint $S - D$ power constraint P_T. We will begin with perfect CSI, and later consider the case in which the CSI of E is not known.

[1] Once E knows the FD mode of D, it may adapt its strategy as well, e.g., it can use the linear minimum mean square error (MMSE) receiver to mitigate the jamming from D. This will be analyzed in Section VI.

III. PERFECT CSI WITH SINGLE-ANTENNA TERMINALS

In this section, we assume that global CSI is available, E has a single receive antenna and D has one transmit and one receive antenna. In this case, the LI cannot be mitigated in the spatial domain but is controlled by the power control process. Although substantial isolation between the transmitter and receiver channels has been recently reported [28], the single-antenna case is mainly used as a baseline scheme for comparison reasons and as a guideline for the multiple-antenna case. The main focus of the work is the multiple-antenna case which allows LI mitigation in the spatial domain.

Following the conventional notation, we use lower-case letters to denote scalar channels. Because the jamming signal from D degrades the performance of both E and D via the LI channel, the destination needs to carefully choose the transmit power p_d to achieve a good balance. Using (3), the secrecy rate maximization via power control at D can be formulated as

$$\max_{0 \leq p_d \leq P_d} f_{\rho}(p_d) \triangleq \frac{1 + \frac{P_s|h_{sd}|^2}{1 + \rho p_d|h|^2}}{1 + \frac{P_s|h_{se}|^2}{1 + p_d|h_{ed}|^2}}. \tag{4}$$

One may observe that (4) looks as if there was an external helper who transmits jamming signals to improve the secrecy rate.

Before we derive its solution, we first study the conditions under which when positive secrecy rate is possible.

Lemma 1: The conditions under which the positive secrecy is achieved are

- $\rho < \min(\frac{|h_{ed}|^2}{|h|^2}, \frac{|h_{sd}|^2(1 + P_d|h_{ed}|^2)}{P_d|h|^2|h_{se}|^2} - \frac{1}{P_d|h|^2})$; or
- $\rho \geq \frac{|h_{ed}|^2}{|h|^2}$ and $|h_{sd}|^2 > |h_{se}|^2$.

Proof: The positive secrecy is achieved if and only if the optimal objective value of the following problem is strictly greater than 1:

$$\max_{0 \leq p_d \leq P_d} \frac{|h_{sd}|^2}{1 + \rho p_d|h|^2} \frac{1 + p_d|h_{ed}|^2}{|h_{se}|^2}. \tag{5}$$

It is not difficult to see that the optimal value is achieved at either $p_d^* = 0$ or $p_d^* = P_d$.

- When $\rho < \frac{|h_{ed}|^2}{|h|^2}$, $p_d^* = P_d$. Positive secrecy rate is achieved if and only if

$$\frac{|h_{sd}|^2}{1 + \rho P_d|h|^2} > \frac{|h_{se}|^2}{1 + P_d|h_{ed}|^2}, \quad \text{or} \tag{6}$$

$$\rho < \frac{|h_{sd}|^2(1 + P_d|h_{ed}|^2)}{P_d|h|^2|h_{se}|^2} - \frac{1}{P_d|h|^2}. \tag{7}$$

- When $\rho \geq \frac{|h_{ed}|^2}{|h|^2}$, $p_d^* = 0$. Positive secrecy rate is achieved if and only if

$$|h_{sd}|^2 > |h_{se}|^2. \tag{8}$$

This completes the proof. ∎

It is clearly seen that when the LI can be sufficiently suppressed, the positive secrecy region can be extended by the FD destination; when the LI is above a certain threshold, FD does not provide any performance gain therefore is not necessary.

Given that a positive secrecy rate is achievable, the optimal solution to (4) is given in the Proposition 1 and the proof is provided in Appendix A.

Proposition 1: Suppose the roots of $f'_\rho(p_d) = 0$ are $x_1(\rho), x_2(\rho)$. If they are both real, we assume $x_2(\rho) \geq x_1(\rho)$. If both are complex or non-positive, we define $x_2(\rho) = 0$. Let $\delta = \frac{|h_{sd}|^2|h_{ed}|^2}{|h_{se}|^2|h|^2}$. Then the optimal $p_d^*(\rho)$ to maximize $f_\rho(p_d)$ is given below:

i) If $\rho < \min(\delta, 1)$, $p_d^*(\rho) = \min(P_d, x_2(\rho))$;
ii) If $1 \geq \rho \geq \min(\delta, 1)$, $p_d^*(\rho) = 0$ or $p_d^*(\rho) = P_d$, whichever gives a higher objective value.

As a special case, when the $S-D$ and $S-E$ channels have the same strength or $S-E$ and $S-D$ have the same distances, we have the following result.

Corollary 1: $p_d(\rho)$ is a monotonically non-increasing function when $|h_{sd}|^2 = |h_{se}|^2$.

Proof: When $|h_{sd}|^2 = |h_{se}|^2$, the equation (51) reduces to $(b-d)x^2 - (1/d - 1/b)(1+a) = 0$ and we have the root $x_2(\rho) = \sqrt{\frac{1+a}{bd}} = \sqrt{\frac{1+P_s}{\rho|h|^2|h_{ed}|^2}}$, where a, b, c, d are defined in Appendix A.

i) When $\rho < \frac{|h_{ed}|^2}{|h|^2}$, $f'_\rho(p_d) > 0$ for $0 \leq p_d \leq x_2(\rho)$, so $p_d^*(x) = \min(P_d, x_2(\rho))$;
ii) When $\rho \geq \frac{|h_{ed}|^2}{|h|^2}$, $f'_\rho(p_d) \leq 0$ for $0 \leq p_d \leq x_2(\rho)$, so $p_d^*(x) = 0$. In this case, positive secrecy rate is not achievable.

Clearly $x_2(\rho)$ is a monotonically decreasing function and this completes the proof. ∎

Typical curves of p_d are shown in Fig. 2, where we plot the normalized $p_d(\rho)$ for two sets of randomly generated channel parameters. For each subfigure, we also plot the results by setting $|h_{sd}|^2 = |h_{se}|^2 = 1$, while keeping the other parameters fixed. We can see that in general the receiver may not always use full power and $p_d(\rho)$ is not necessarily monotonically changing with ρ.

This can be explained by the fact that when ρ is small, the self-interference is also small, so the receiver can use full or high power to confuse the eavesdropper; as ρ increases, the receiver needs to reduce its transmit power in order not to generate too much self-interference; when ρ is very close to 1, the receiver causes high interference to both itself and the eavesdropper, but if the eavesdropper suffers more, the receiver can still increase its transmit power, otherwise, it should decrease its power. The results in Fig. 2 verify our analysis given in Corollary 1.

Next we consider the case where S and D have a total power constraint P_T and we denote their power as p_s and p_d, respectively. We aim to maximize the secrecy rate below

$$f_\rho(p_s, p_d) \triangleq \frac{1 + \frac{p_s|h_{sd}|^2}{1+\rho p_d|h|^2}}{1 + \frac{p_s|h_{se}|^2}{1+p_d|h_{ed}|^2}}$$

by using optimal power allocation between S and D.

Proposition 2: If the source and the receiver has a total power constraint P_T and strictly positive secrecy rate is achievable, then full power should be used, i.e., $p_s + p_d = P_T$.

Proof: Strictly positive secrecy rate implies that there exists a solution (p_s, p_d) such that

$$\frac{p_s|h_{sd}|^2}{1+\rho p_d|h|^2} > \frac{p_s|h_{se}|^2}{1+p_d|h_{ed}|^2},$$

and this means $f(p_s, p_d)$ is increasing in p_s. So if there is any unused power Δp, we can always add it to p_s to obtain $f(p_s + \Delta p, p_d) > f(p_s, p_d)$. ∎

Consequently, the power allocation problem can be formulated as

$$\max_{0 \leq \alpha \leq 1} \frac{1 + \frac{\alpha P_T|h_{sd}|^2}{1+\rho(1-\alpha)P_T|h|^2}}{1 + \frac{\alpha P_T|h_{se}|^2}{1+(1-\alpha)P_T|h_{ed}|^2}},$$

where we have assumed that $p_s = \alpha P_T$ and $P_d = (1-\alpha)P_T$ with $0 \leq \alpha \leq 1$.

For simplicity, we assume that $|h_{sd}|^2 = |h_{se}|^2 = 1$, i.e., the channels to D and E have the same normalized strength, then we have the following solution:

$$\alpha^* = \begin{cases} 0, & \text{if } \rho \geq \frac{|h_{ed}|^2}{|h|^2}; \\ \frac{1}{1+\sqrt{\frac{P_T+1}{(P_T|h_{ed}|^2+1)(P_T|h|^2\rho+1)}}}, & \text{if } 0 \leq \rho < \frac{|h_{ed}|^2}{|h|^2}. \end{cases} \tag{9}$$

It can be seen that when $0 \leq \rho < \frac{|h_{ed}|^2}{|h|^2}$, i.e., positive secrecy rate is possible, the source power p_s is monotonically increasing in ρ. This is because the larger ρ is, the less the receiver power p_d is, and the conclusion follows due to constant sum power of S and D.

We have shown that for the single-antenna case, D may not use full transmit power P_d. To conclude this section, we study the performance at high signal-to-noise (SNR). Suppose $\frac{p_s}{p_d} = \beta$ remains constant, then

$$\lim_{p_d \to \infty} R_S = \max\left(0, \log\left(1 + \frac{\beta|h_{sd}|^2}{\rho|h|^2}\right) - \log\left(1 + \frac{\beta|h_{se}|^2}{|h_{ed}|^2}\right)\right), \tag{10}$$

which indicates the secrecy rate will saturate when $p_d \to \infty$. This is because the self-interference cannot be fully canceled [22] and becomes a limiting factor at high SNR.

IV. MULTIPLE-ANTENNA RECEIVER

In this section, we study the transmitter design when both the destination and the eavesdropper has multiple antennas. Based on (3), we first formulate the secrecy rate maximization problem with power constraint at D, i.w.,

$$\max_{\mathbf{Q}, \|\mathbf{r}\|=1} \frac{1 + \frac{P_s|\mathbf{r}^\dagger \mathbf{h}_{sd}|^2}{1+\rho\mathbf{r}^\dagger \mathbf{HQH}^\dagger\mathbf{r}}}{1 + \frac{P_s\|\mathbf{h}_{se}\|^2}{1+\frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{QH}_{ed}^\dagger\mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}}} \tag{11}$$

$$\text{s.t.} \quad \mathbf{Q} \succeq \mathbf{0}, \ \text{trace}(\mathbf{Q}) \leq P_d.$$

Different from the single-antenna case, the secrecy rate can keep increasing with transmit power, as stated in Lemma 2 below.

Lemma 2: Given $M_t > 1$ or $M_r > 1$, the system is not interference-limited.

Proof: It suffices to show that there exists a scheme whose achievable secrecy rate does not saturate. It is easily seen that as long as D has either multiple transmit or receive antennas, $\mathbf{r}$ and $\mathbf{Q}$ can be chosen according to the zero-forcing (ZF)

criterion such that $\mathbf{r}^\dagger \mathbf{H}\mathbf{Q}\mathbf{H}^\dagger \mathbf{r} = 0$ but $\mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{Q}\mathbf{H}_{ed}^\dagger \mathbf{h}_{se} > 0$. As a result, the secrecy rate becomes

$$
\begin{aligned}
R_{S,ZF} = & \max\left(0, \log\left(1 + P_s \|\mathbf{h}_{sd}\|^2\right)\right. \\
& \left. - \log\left(1 + \frac{P_s \|\mathbf{h}_{se}\|^2}{1 + \frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{Q}\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}}\right)\right). \quad (12)
\end{aligned}
$$

It is noted that the jamming signal sent by D does not affect itself but degrades the received signal-to-noise plus interference (SINR) at E. Therefore, $R_{S,ZF}$ is a strictly monotonically increasing function of trace($\mathbf{Q}$). The system is no longer interference-limited, and the secrecy rate $R_{S,ZF}$ can increase with P_d without saturation. This completes the proof. ∎

In the following, we assume that $M_t > 1$ and derive the optimal solutions to problem (11). When $M_t = 1$, the jamming covariance matrix design reduces to jamming power optimization, and has been addressed in the previous section. Before we address the optimal jamming covariance design, we will present two useful lemmas about the properties of the optimal $\mathbf{Q}^*$.

Lemma 3: The optimal $\mathbf{Q}^*$ to solve (11) should be rank-1.

Proof: Let $\mathbf{Q}^*, \mathbf{r}^*$ be any solution to the problem (11). If $\mathbf{Q}^*$ is rank one, the desired result is obtained. If $\mathbf{Q}^*$ is not rank-1, let $\mathbf{r}^\dagger \mathbf{H}\mathbf{Q}^*\mathbf{H}^\dagger \mathbf{r} = x$, $\mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{Q}^*\mathbf{H}_{ed}^\dagger \mathbf{h}_{se} = y$ and consider the following problem

$$
\min_{\mathbf{Q}} \mathbf{r}^\dagger \mathbf{H}\mathbf{Q}\mathbf{H}^\dagger \mathbf{r}, \quad \text{s.t.} \quad \text{Tr}(\mathbf{Q}\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}\mathbf{h}_{se}^\dagger \mathbf{H}_{ed}) = y, \ \text{Tr}(\mathbf{Q}) \le P_d. \quad (13)
$$

Obviously, $\mathbf{Q}^*$ is feasible for the above problem. We want to prove that $\mathbf{Q}^*$ is also the optimal solution to (13). Let $\mathbf{Q}'$ be any solution to the above problem (13). Then it holds that $\mathbf{r}^\dagger \mathbf{H}\mathbf{Q}'\mathbf{H}^\dagger \mathbf{r} = x$. This is because if $\mathbf{r}^\dagger \mathbf{H}\mathbf{Q}'\mathbf{H}^\dagger \mathbf{r} < x$, then $\mathbf{Q}'$ is feasible for the problem of (11) but achieves a strictly larger objective value than $\mathbf{Q}^*$ in (11). But this contradicts the fact that $\mathbf{Q}^*$ is the optimal solution to (11), so $\mathbf{Q}^*$ is also the optimal solution to (13).

Problem (13) is a homogeneous quadratically constrained quadratic program (QCQP) with two constraints. According to the results in [29], it has a rank-1 solution. Thus it follows that the problem of (11) has a rank-1 solution $\mathbf{Q}^*$. ∎
The next lemma is about the power consumption of jamming signals.

Lemma 4: Given that $\mathbf{H}^\dagger \mathbf{r}$ does not align with $\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}$, i.e., there exists no scalar g such that $\mathbf{H}^\dagger \mathbf{r} = g\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}$, the optimal $\mathbf{Q}^*$ satisfies trace($\mathbf{Q}^*$) = P_d.

Proof: We prove it by contradiction. Suppose the optimal solution is $\mathbf{Q}_1$ and trace($\mathbf{Q}_1$) $< P_d$. We then choose $\mathbf{x}$ such that $\mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{x} = 0$, $\mathbf{r}^\dagger \mathbf{H}\mathbf{x} \ne 0$ and trace($\mathbf{Q}_1$) + $\|\mathbf{x}\|^2 = P_d$. This is possible due to the assumption that $\mathbf{H}^\dagger \mathbf{r}$ does not align with $\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}$. Construct a new solution $\mathbf{Q}_2 = \mathbf{Q}_1 + \mathbf{x}\mathbf{x}^\dagger$. It is easy to verify that $\mathbf{Q}_2$ is a strictly better solution than $\mathbf{Q}_1$ with trace($\mathbf{Q}_2$) = P_d, which contradicts the optimality of $\mathbf{Q}_1$. This completes the proof. ∎

In the special case in which the condition $\mathbf{H}^\dagger \mathbf{r} = g\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}$ holds, the equivalent channels for the two links $\text{D}-\text{D}$ and $\text{D}-\text{E}$ align with each other. This is not desired and can normally be avoided by D via proper design of $\mathbf{r}$. Because this condition is easy to detect, in the sequel we assume it does not hold.

By introducing $\mathbf{Q} = P_d\mathbf{q}\mathbf{q}^\dagger$ and $\|\mathbf{q}\| = 1$, problem (11) becomes

$$
\max_{\|\mathbf{q}\|=1, \|\mathbf{r}\|=1} \frac{1 + \frac{P_s |\mathbf{r}^\dagger \mathbf{h}_{sd}|^2}{1+\rho P_d \mathbf{r}^\dagger \mathbf{H}\mathbf{q}\mathbf{q}^\dagger \mathbf{H}^\dagger \mathbf{r}}}{1 + \frac{P_s \|\mathbf{h}_{se}\|^2}{1 + \frac{P_d \mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{q}\mathbf{q}^\dagger \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}}}. \quad (14)
$$

Next we will study problem (14). We begin with a fixed receiver and then move to the optimal linear receiver; the analysis is also extended for the case of joint power allocation at $\mathbf{S}$ and $\mathbf{D}$.

A. Optimal Solution with a Fixed Receiver

Let us assume that the receiver $\mathbf{r}$ is fixed and independent of $\mathbf{Q}$. Possible choices include the MRC and the minimum mean square error (MMSE) receivers.

The problem of (14) is complicated and difficult to solve it directly. Instead, we solve the following problem by introducing an auxiliary variable t:

$$
\begin{aligned}
\max_{\mathbf{q}} \quad & \mathbf{h}_{se}^\dagger \mathbf{H}_{ed}\mathbf{q}\mathbf{q}^\dagger \mathbf{H}_{ed}^\dagger \mathbf{h}_{se} \quad (15) \\
\text{s.t.} \quad & \mathbf{r}^\dagger \mathbf{H}\mathbf{q}\mathbf{q}^\dagger \mathbf{H}^\dagger \mathbf{r} = t, \|\mathbf{q}\| = 1.
\end{aligned}
$$

By denoting its optimal objective value as $g(t)$, the original problem of (14) becomes

$$
\max_{t \ge 0} f(t) \triangleq \frac{1 + \frac{P_s |\mathbf{r}^\dagger \mathbf{h}_{sd}|^2}{1+\rho t}}{1 + \frac{P_s \|\mathbf{h}_{se}\|^2}{1 + \frac{P_d g(t)}{\|\mathbf{h}_{se}\|^2}}}. \quad (16)
$$

We develop the following intermediate results to efficiently solve the problem of (15).

Lemma 5: Let $\mathbf{c}_2 = \frac{\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\mathbf{H}_{ed}^\dagger \mathbf{h}_{se}\|}$, $\mathbf{c}_1 = \frac{\mathbf{H}^\dagger \mathbf{r}}{\|\mathbf{H}^\dagger \mathbf{r}\|}$ and $r = |\mathbf{c}_1^\dagger \mathbf{c}_2|$. Then $g(t) = 1 - (r\sqrt{1-t} - \sqrt{(1-r^2)t})^2$ and is a concave function in t.

Proof: With the defined notation, (15) becomes

$$
\begin{aligned}
\max_{\mathbf{q}} \quad & \mathbf{q}^\dagger \mathbf{c}_2\mathbf{c}_2^\dagger \mathbf{q}, \\
\text{s.t.} \quad & \mathbf{q}^\dagger \mathbf{c}_1\mathbf{c}_1^\dagger \mathbf{q} = t, \quad \|\mathbf{q}\| = 1. \quad (17)
\end{aligned}
$$

The closed-form solution $g(t)$ then follows from Lemma 2 in [30]. The concavity can be proven by confirming that the second order derivative of $g(t)$ is negative. ∎
Note that a similar problem as (17) has been studied in [10, (14)] where individual constraints on each element of $\mathbf{q}$ are assumed, hence, a closed-form solution is not possible. The closed-form solution in Lemma 5 speeds up the algorithm to solve (16).

Given Lemma 5, we have the following theorem that can be used to develop efficient algorithms to solve (16).

Theorem 1: $f(t)$ is quasi-concave in t and its maximum can be found via bisection search.

Proof: Given that $g(t)$ is a concave function, the result follows from Theorem 3 in [10]. ∎

B. Optimal Solution with The Optimal Linear Receiver

In this section, we aim to jointly optimize $\mathbf{q}$ as well as the receiver design at D. From (3), the optimal linear receiver to maximize the received SINR at D is given by

$$\mathbf{r} = \frac{\left(\rho\mathbf{H}\mathbf{Q}\mathbf{H}^\dagger + \mathbf{I}\right)^{-1}\mathbf{h}_{sd}}{\|\left(\rho\mathbf{H}\mathbf{Q}\mathbf{H}^\dagger + \mathbf{I}\right)^{-1}\mathbf{h}_{sd}\|}. \qquad (18)$$

Then the achievable secrecy rate is expressed as

$$
\begin{aligned}
R_S &= \max\left(0, \log_2\left(1 + P_s\mathbf{h}_{sd}^\dagger\left(\rho\mathbf{H}\mathbf{Q}\mathbf{H}^\dagger + \mathbf{I}\right)^{-1}\mathbf{h}_{sd}\right)\right.\\
&\quad \left.- \log_2\left(1 + \frac{P_s\|\mathbf{h}_{se}\|^2}{1 + \frac{\mathbf{h}_{se}^\dagger\mathbf{H}_{ed}\mathbf{Q}\mathbf{H}_{ed}^\dagger\mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}}\right)\right)\\
&= \max\left(0, \log_2\left(1 + P_s\|\mathbf{h}_{sd}\|^2 - \frac{\rho P_s P_d|\mathbf{h}_{sd}^\dagger\mathbf{H}\mathbf{q}|^2}{1 + \rho P_d\mathbf{q}^\dagger\mathbf{H}^\dagger\mathbf{H}\mathbf{q}}\right)\right.\\
&\quad \left.- \log_2\left(1 + \frac{P_s\|\mathbf{h}_{se}\|^2}{1 + \frac{P_d|\mathbf{h}_{se}^\dagger\mathbf{H}_{ed}\mathbf{q}|^2}{\|\mathbf{h}_{se}\|^2}}\right)\right), \qquad (19)
\end{aligned}
$$

where we have used the rank-1 property of $\mathbf{Q}$ and the notation $\mathbf{Q} = P_d\mathbf{q}\mathbf{q}^\dagger$ and $\|\mathbf{q}\| = 1$, together with matrix inversion lemma.

The secrecy rate expression R_S in (19) is still complicated. To tackle it, we study the following problem with the parameter t:

$$\max_{\mathbf{q}} \quad |\mathbf{h}_{se}^\dagger\mathbf{H}_{ed}\mathbf{q}|^2 \qquad (20)$$

$$\text{s.t.} \quad \frac{|\mathbf{h}_{sd}^\dagger\mathbf{H}\mathbf{q}|^2}{1 + \rho P_d\mathbf{q}^\dagger\mathbf{H}^\dagger\mathbf{H}\mathbf{q}} = t, \ \|\mathbf{q}\|^2 = 1,$$

which is a nonconvex quadratic optimization problem and difficult to solve, instead, we first study a modified problem below by introducing $\tilde{\mathbf{Q}} = \mathbf{q}\mathbf{q}^\dagger$:

$$\max_{\tilde{\mathbf{Q}}} \quad \text{trace}(\mathbf{h}_{se}^\dagger\mathbf{H}_{ed}\tilde{\mathbf{Q}}\mathbf{H}_{ed}^\dagger\mathbf{h}_{se}) \qquad (21)$$

$$\text{s.t.} \quad \text{trace}(\tilde{\mathbf{Q}}(\mathbf{H}^\dagger\mathbf{h}_{sd}\mathbf{h}_{sd}^\dagger\mathbf{H} - t\rho P_d\mathbf{H}^\dagger\mathbf{H})) = t,$$

$$\tilde{\mathbf{Q}} \succeq \mathbf{0}, \ \text{trace}(\tilde{\mathbf{Q}}) = 1.$$

(21) is a semidefinite programming problem and the method to solve (21) is provided in Appendix B. Note that in Appendix B, we have shown that the optimal $\tilde{\mathbf{Q}}$ should be rank-1, so (20) and (21) are equivalent in the sense that given the optimal solution $\tilde{\mathbf{Q}}^*$ to (21), the optimal $\mathbf{q}^*$ to solve (20) can be extracted via $\tilde{\mathbf{Q}}^* = \mathbf{q}^*\mathbf{q}^{*\dagger}$. Denote its optimal objective value as $h(t)$, the secrecy rate maximization problem can be formulated as

$$\max_{t \geq 0} \quad R(t) \triangleq \log\left(\frac{1 + P_s\|\mathbf{h}_{sd}\|^2 - \rho P_s P_d t}{1 + \frac{P_s\|\mathbf{h}_{se}\|^2}{1 + \frac{P_d h(t)}{\|\mathbf{h}_{se}\|^2}}}\right). \qquad (22)$$

Thus the maximum of $R(t)$ can be found via a one-dimensional search.

C. Joint S-D Power Allocation

1) Optimal Solution: If D and S can share a total power P_T, then the problem is revised to

$$\max_{\mathbf{Q}\succeq\mathbf{0}, p_s \geq 0, \ p_s + \text{trace}(\mathbf{Q}) \leq P_T} \quad R_S, \qquad (23)$$

where we have used p_s to denote the source power as a variable. Since we have derived the solution when there is only power constraint P_d on D with a parameter t, we can perform a 2-D search over p_s and t to find the optimal $\mathbf{Q}$ and power allocation p_s. This is because all power should be used up at the optimum, i.e., $p_s + \text{trace}(\mathbf{Q}) = P_T$.

For the fixed linear receiver, we can reduce 2-D search to a 1-D search. To achieve that, we first define a new objective function based on (16):

$$f(p_s, t) \triangleq \frac{1 + \frac{p_s|\mathbf{r}^\dagger\mathbf{h}_{sd}|^2}{1 + \rho t}}{1 + \frac{p_s\|\mathbf{h}_{se}\|^2}{1 + \frac{(P_T - p_s)g(t)}{\|\mathbf{h}_{se}\|^2}}}. \qquad (24)$$

For fixed t, setting its derivative regarding p_s to be zero leads to the following quadratic equation

$$Ap_s^2 + Bp_s + C = 0, \qquad (25)$$

where $A \triangleq -\frac{g(t)}{\|\mathbf{h}_{se}\|^2}(\|\mathbf{h}_{se}\|^2 - \frac{g(t)}{\|\mathbf{h}_{se}\|^2}), B \triangleq -\frac{g(t)}{\|\mathbf{h}_{se}\|^2}(1 + P_T\frac{g(t)}{\|\mathbf{h}_{se}\|^2}), C \triangleq (1 + P_T\frac{g(t)}{\|\mathbf{h}_{se}\|^2})((1 + P_T\frac{g(t)}{\|\mathbf{h}_{se}\|^2}) - \frac{(1+\rho t)\|\mathbf{h}_{se}\|^2}{|\mathbf{r}^\dagger\mathbf{h}_{sd}|^2})$. The optimal p_s^* should either be P_T or one root of the equation (25) and denote it as $P_S(t)$. Then the total power constrained secrecy optimization problem (23) for a fixed receiver becomes

$$\max_{t \geq 0} \quad \frac{1 + \frac{P_S(t)|\mathbf{r}^\dagger\mathbf{h}_{sd}|^2}{1 + \rho t}}{1 + \frac{P_S(t)\|\mathbf{h}_{se}\|^2}{1 + \frac{(P_T - P_S(t))g(t)}{\|\mathbf{h}_{se}\|^2}}}. \qquad (26)$$

Its optimal solution can be obtained via 1-D optimization over t only.

For the optimal linear receiver, it is not possible to apply this procedure because $h(t)$, obtained from (21), is also a complex function of p_d. Due to this non-separability, we have to use 2-D search to find the optimal power allocation.

2) ZF Solution: In this section, we study a simple closed-form solution based on the ZF criterion. For conciseness, we only consider the case of the optimal receiver. This corresponds to $t = 0$ in the problem of (22).

In (19), we can see that $\mathbf{h}_{sd}^\dagger\mathbf{H}\mathbf{q}$ is a self-interference term that may limit the system performance, so we impose an additional constraint that self-interference is zero, i.e., $\mathbf{h}_{sd}^\dagger\mathbf{H}\mathbf{q} = \mathbf{0}$. Using this condition together with the matrix inversion lemma, we can derive that the optimal linear receiver in (18) reduces to $\mathbf{r} = \frac{\mathbf{h}_{sd}}{\|\mathbf{h}_{sd}\|}$, which is essentially the MRC receiver. Therefore (19) is simplified to

$$
\begin{aligned}
R_S &= \max\left(0, \log\left(1 + p_s\|\mathbf{h}_{sd}\|^2\right) - \right.\\
&\quad \left.\log\left(1 + \frac{p_s\|\mathbf{h}_{se}\|^2}{1 + \frac{p_d|\mathbf{h}_{se}^\dagger\mathbf{H}_{ed}\mathbf{q}|^2}{\|\mathbf{h}_{se}\|^2}}\right)\right), \|\mathbf{q}\| = 1. (27)
\end{aligned}
$$

To maximize (27), we first study a simple problem below:

$$\max_{\mathbf{q}} \quad \|\mathbf{h}_{se}^\dagger \mathbf{H}_{ed} \mathbf{q}\|^2 \tag{28}$$

$$\text{s.t.} \quad \mathbf{h}_{sd}^\dagger \mathbf{H} \mathbf{q} = \mathbf{0}, \|\mathbf{q}\|^2 = 1.$$

The optimal solution and the optimal objective value of (28) are given by, respectively,

$$\mathbf{q}_{ZF} = \frac{\Pi_{\mathbf{H}^\dagger \mathbf{h}_{sd}}^\perp \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\Pi_{\mathbf{H}^\dagger \mathbf{h}_{sd}}^\perp \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}\|} \text{ and } \|\Pi_{\mathbf{H}^\dagger \mathbf{h}_{sd}}^\perp \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}\|^2, \tag{29}$$

where $\Pi_{\mathbf{X}}^\perp \triangleq \mathbf{I} - \mathbf{X}(\mathbf{X}^\dagger \mathbf{X})^{-1} \mathbf{X}^\dagger$ denotes orthogonal projection onto the orthogonal complement of the column space of $\mathbf{X}$ and has the property $\Pi_{\mathbf{X}}^\perp \Pi_{\mathbf{X}}^\perp = \Pi_{\mathbf{X}}^\perp$. The resulting secrecy rate is then written as

$$\begin{aligned} R_S = \quad & \max \left(0, \log\left(1 + p_s \|\mathbf{h}_{sd}\|^2\right)\right. \\ & \left. - \log\left(1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{p_d \|\Pi_{\mathbf{H}^\dagger \mathbf{h}_{sd}}^\perp \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}\|^2}{\|\mathbf{h}_{se}\|^2}}\right)\right). \end{aligned} \tag{30}$$

The optimal power allocation with a total power constraint $p_s + p_d = P_T$ can then be optimized similar to (24).

V. TRANSMISSION DESIGN WITH CDI

In the previous sections, we assumed that the eavesdropper CSI is perfectly known. This information can be available when E is also an active user in the network (unauthorized user) but in general it is difficult to obtain. In this section, we study the case in which both S and D have perfect CSI, $\mathbf{h}_{sd}$, but only CDI on E. For simplicity, we assume that the elements of $\mathbf{h}_{se}$ and $\mathbf{H}_{ed}$ are zero-mean independent and identically distributed (i.i.d.) Gaussian random variables with variances σ_s^2 and σ_d^2, respectively.

A. Expected Secrecy Rate

With CDI only, we first aim to maximize the ergodic secrecy rate [31], i.e.,

$$\begin{aligned} \max_{\mathbf{Q}, p_s, \|\mathbf{r}\|=1} \quad & \mathbb{E}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\log_2 \left(1 + \frac{p_s |\mathbf{r}^\dagger \mathbf{h}_{sd}|^2}{1 + \rho \mathbf{r}^\dagger \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger \mathbf{r}}\right) \right. \\ & \left. - \log_2 \left(1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}}\right) \right) \end{aligned} \tag{31}$$

$$\text{s.t.} \quad \mathbf{Q} \succeq \mathbf{0}, p_s \geq 0, \ p_s + \text{trace}(\mathbf{Q}) \leq P_T.$$

Due to the lack of instantaneous knowledge about the channels to E, we consider a suboptimal MRC receiver based only on local information: $\mathbf{r} = \frac{\mathbf{h}_{sd}}{\|\mathbf{h}_{sd}\|}$ and $\mathbf{Q}$ is chosen as $\mathbf{Q} = \frac{p_d \mathbf{W} \mathbf{W}^\dagger}{M_t - 1}$, where $\mathbf{W}$ is an orthogonal basis of the null space of $\mathbf{H}^\dagger \mathbf{r}$, i.e., $\mathbf{r}^\dagger \mathbf{H} \mathbf{W} = \mathbf{0}, \mathbf{W} \in \mathbb{C}^{M_t \times (M_t - 1)}, \mathbf{W}^\dagger \mathbf{W} = \mathbf{I}_{(M_t - 1)}$. Then (31) becomes

$$\begin{aligned} \max_{p_d, p_s} \quad & \mathbb{E}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\log_2 \left(1 + p_s \|\mathbf{h}_{sd}\|^2\right) \right. \\ & \left. - \log_2 \left(1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + p_d \frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed} \mathbf{W} \mathbf{W}^\dagger \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{(M_t - 1) \|\mathbf{h}_{se}\|^2}}\right) \right) \end{aligned} \tag{32}$$

$$\text{s.t.} \quad p_s \geq 0, \ p_s + p_d \leq P_T.$$

The expectation is still difficult to evaluate, so we optimize its approximation below by taking expectation operations on each individual random terms:

$$\max_{p_d, p_s} \quad \log_2 \left(1 + p_s \|\mathbf{h}_{sd}\|^2\right) \tag{33}$$

$$- \log_2 \left(1 + \frac{p_s \mathbb{E}_{\mathbf{h}_{se}}(\|\mathbf{h}_{se}\|^2)}{1 + p_d \mathbb{E}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left[\frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed} \mathbf{W} \mathbf{W}^\dagger \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{(M_t - 1) \|\mathbf{h}_{se}\|^2}\right]}\right)$$

$$\text{s.t.} \quad p_s \geq 0, \ p_s + p_d \leq P_T.$$

Notice that this approximation provides neither an upper nor a lower bound of the original problem (32). Its effect will be evaluated in Fig. 6.

We find the following lemma is useful to solve (33).

Lemma 6: $X = \frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed} \mathbf{W} \mathbf{W}^\dagger \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2}$ is a central chi-square random variable with $2(M_t - 1)$ degrees of freedom.

Proof:

Suppose a matrix decomposition $\frac{\mathbf{h}_{se}}{\|\mathbf{h}_{se}\|} = \mathbf{U}\mathbf{d}$, where $\mathbf{U}$ is a unitary matrix and $\mathbf{d}$ is a zero vector except its first element being 1. Define eigenvalue decomposition of $\mathbf{W} = \mathbf{U}_w \mathbf{D}_w \mathbf{U}_w^\dagger$, where $\mathbf{U}_w$ is a unitary matrix and $\mathbf{D}_w$ is a diagonal matrix with all diagonal entries being 1 except one element being 0.

Then $X = \frac{\mathbf{h}_{se}^\dagger \mathbf{H}_{ed} \mathbf{W} \mathbf{W}^\dagger \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}}{\|\mathbf{h}_{se}\|^2} = \mathbf{d}^\dagger \mathbf{U}^\dagger \mathbf{H}_{ed} \mathbf{U}_w \mathbf{D}_w \mathbf{U}_w^\dagger \mathbf{H}_{ed}^\dagger \mathbf{U}\mathbf{d}$. Statistically X is identical to

$$\mathbf{d}^\dagger \mathbf{H}_{ed} \mathbf{D}_w \mathbf{H}_{ed} \mathbf{d} = \sum_{n=1}^{M_t - 1} \|\mathbf{H}_{ed}(1, n)\|^2, \tag{34}$$

where $\mathbf{H}_{ed}(1, n)$ denotes $\mathbf{H}_{ed}$'s $(1, n)$-th element. This completes the proof.

∎

Using Lemma 6, $\frac{E[X]}{(M_t - 1)} = 1$, so we have the following formulation:

$$\max_{p_d, p_s} \quad \log_2 \left(1 + p_s \|\mathbf{h}_{sd}\|^2\right) - \log_2 \left(1 + \frac{p_s M_e \sigma_s^2}{1 + p_d \sigma_d^2}\right) \tag{35}$$

$$\text{s.t.} \quad p_s \geq 0, \ p_s + p_d \leq P_T.$$

Its solution can be found using similar procedures to solve (24).

B. Outage Secrecy Rate

Now we take a different design criterion regarding the available CDI for a slow fading channel, and we aim to maximize the ϵ-outage secrecy rate r defined by

$$\begin{aligned} \text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\log_2 \left(1 + p_s |\mathbf{r}^\dagger \mathbf{h}_{sd}|^2\right) \right. \\ \left. - \log_2 \left(1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{p_d x}{M_t - 1}}\right) \leq r \right) = \epsilon, \end{aligned} \tag{36}$$

where we have used the assumption $\mathbf{Q} = \frac{p_d \mathbf{W} \mathbf{W}^\dagger}{M_t - 1}$ and x is a random variable defined in Lemma 6. The outage secrecy rate

maximization problem can be formulated as

$$\max_{p_s, p_d} \quad r \tag{37}$$

$$\text{s.t.} \quad \text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\frac{1 + p_s \|\mathbf{h}_{sd}\|^2}{1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{p_d x}{M_t - 1}}} \leq 2^r \right) \leq \epsilon,$$

$$p_s \geq 0, \ p_s + p_d \leq P_T.$$

We can use bisection method to find the optimal r. The remaining problem is how to calculate the outage probability, which is rewritten below:

$$\text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\frac{1 + p_s \|\mathbf{h}_{sd}\|^2}{1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{p_d x}{M_t - 1}}} \leq 2^r \right) \tag{38}$$

$$= \text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\frac{1 + p_s \|\mathbf{h}_{sd}\|^2}{2^r} \leq 1 + \frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{p_d x}{M_t - 1}} \right)$$

$$= \text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\frac{p_s \|\mathbf{h}_{se}\|^2}{1 + \frac{p_d x}{M_t - 1}} \geq \frac{1 + p_s \|\mathbf{h}_{sd}\|^2}{2^r} - 1 \triangleq \alpha \right)$$

$$= \text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\frac{p_s}{\alpha} \|\mathbf{h}_{se}\|^2 - \frac{p_d x}{M_t - 1} \geq 1 \right)$$

$$= \text{Prob}_{\mathbf{h}_{se}, \mathbf{H}_{ed}} \left(\gamma \triangleq \mathbf{z}^\dagger \mathbf{D} \mathbf{z} \geq 1 \right), \ \text{and} \ \mathbf{z} \sim \mathcal{CN}(0, \mathbf{I}),$$

where $\mathbf{D} \triangleq \text{diag} \left(\left[\underbrace{\frac{p_s}{\alpha}, \cdots, \frac{p_s}{\alpha}}_{M_e}, \underbrace{-p_d, \cdots, -p_d}_{M_t - 1} \right] \right)$. It can be

seen that γ is an indefinite quadratic form in complex normal variables and the outage probability can be derived as [32]

$$\text{Prob}(\gamma \geq 1) = \frac{e^{-\frac{1}{\bar{a}}}}{\bar{a}^m \bar{b}^n (m-1)!(n-1)!} \tag{39}$$

$$\times \sum_{i=0}^{m-1} \sum_{k=0}^{m-i-1} \frac{(m-1)!(n+i-1)!}{i!(m-i-1)!k!} \left(\frac{\bar{a} + \bar{b}}{\bar{a}\bar{b}} \right)^{-(i+n)} \bar{a}^{m-i-k},$$

where $\bar{a} \triangleq \frac{p_s}{\alpha}, \bar{b} \triangleq p_d, m \triangleq M_e, n \triangleq M_t - 1$.

VI. DESIGN OF $\mathbf{Q}$ WITH THE OPTIMAL LINEAR MMSE RECEIVER AT BOTH D AND E

In previous sections, we have assumed that E is not aware of the FD operation of D and simply uses an MRC receiver $\mathbf{h}_{se}^\dagger$. However, once E learns that there is additional interference, it can adopt more advanced linear MMSE receiver:

$$\mathbf{r}_e = \frac{(\mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger + \mathbf{I})^{-1} \mathbf{h}_{se}}{\|(\mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger + \mathbf{I})^{-1} \mathbf{h}_{se}\|}, \tag{40}$$

which, assuming that D also uses the optimal linear MMSE receiver, leads to the secrecy rate

$$R_S' = \max \left(0, \log \left(1 + P_s \mathbf{h}_{sd}^\dagger (\rho \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger + \mathbf{I})^{-1} \mathbf{h}_{sd} \right) \right.$$

$$\left. - \log \left(1 + P_s \mathbf{h}_{se}^\dagger (\rho \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger + \mathbf{I})^{-1} \mathbf{h}_{se} \right) \right) \tag{41}$$

This results in the following secrecy rate maximization problem:

$$\max_{\mathbf{Q}} \quad F(\mathbf{Q}) \triangleq \log \left(1 + P_s \mathbf{h}_{sd}^\dagger (\rho \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger + \mathbf{I})^{-1} \mathbf{h}_{sd} \right) \tag{42}$$

$$- \log \left(1 + P_s \mathbf{h}_{se}^\dagger (\rho \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger + \mathbf{I})^{-1} \mathbf{h}_{se} \right)$$

$$\text{s.t.} \quad \mathbf{Q} \succeq \mathbf{0}, \ \text{trace}(\mathbf{Q}) \leq P_d.$$

For simplicity, we assume that perfect CSI is available. The problem of (42) is in general not convex and the optimal design of $\mathbf{Q}$ to maximize R_S' is a cumbersome optimization problem, so we propose to use the DC (difference of convex functions) programming [33] to find a stationary point. First, we express $F(\mathbf{Q})$ as a difference of two concave functions $f(\mathbf{Q})$ and $g(\mathbf{Q})$:

$$F(\mathbf{Q}) = \log \det(\mathbf{I} + P_s \mathbf{h}_{sd} \mathbf{h}_{sd}^\dagger + \rho \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger)$$

$$- \log \det(\mathbf{I} + P_s \mathbf{h}_{se} \mathbf{h}_{se}^\dagger + \rho \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger)$$

$$- \log \det(\mathbf{I} + \rho \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger) + \log \det(\mathbf{I} + \rho \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger)$$

$$\triangleq f(\mathbf{Q}) - g(\mathbf{Q}) \tag{43}$$

where

$$f(\mathbf{Q}) \triangleq \log \det(\mathbf{I} + P_s \mathbf{h}_{sd} \mathbf{h}_{sd}^\dagger + \rho \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger)$$

$$+ \log \det(\mathbf{I} + \rho \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger), \tag{44}$$

$$g(\mathbf{Q}) \triangleq \log \det(\mathbf{I} + \rho \mathbf{H} \mathbf{Q} \mathbf{H}^\dagger)$$

$$+ \log \det(\mathbf{I} + P_s \mathbf{h}_{se} \mathbf{h}_{se}^\dagger + \rho \mathbf{H}_{ed} \mathbf{Q} \mathbf{H}_{ed}^\dagger). \tag{45}$$

The linearization of g around the point $\mathbf{Q}_k$ is

$$g_L(\mathbf{Q}; \mathbf{Q}_k) = \log \det(\mathbf{I} + \rho \mathbf{H} \mathbf{Q}_k \mathbf{H}^\dagger) \tag{46}$$

$$+ \log \det(\mathbf{I} + P_s \mathbf{h}_{se} \mathbf{h}_{se}^\dagger + \rho \mathbf{H}_{ed} \mathbf{Q}_k \mathbf{H}_{ed}^\dagger)$$

$$+ \text{Tr} \left(\rho \mathbf{H}^\dagger (\mathbf{I} + \rho \mathbf{H} \mathbf{Q}_k \mathbf{H}^\dagger)^{-1} \mathbf{H} (\mathbf{Q} - \mathbf{Q}_k) \right)$$

$$+ \text{Tr} \left(\rho \mathbf{H}_{ed}^\dagger (\mathbf{I} + P_s \mathbf{h}_{se} \mathbf{h}_{se}^\dagger + \rho \mathbf{H}_{ed} \mathbf{Q}_k \mathbf{H}_{ed}^\dagger)^{-1} \mathbf{H}_{ed} (\mathbf{Q} - \mathbf{Q}_k) \right).$$

DC programming is used to sequentially solve the following convex problem, $k = 0, 1, \cdots$,

$$\mathbf{Q}_{k+1} = \arg \max_{\mathbf{Q}} \ f(\mathbf{Q}) - g_L(\mathbf{Q}; \mathbf{Q}_k) \tag{47}$$

$$\text{s.t.} \quad \mathbf{Q} \succeq \mathbf{0}, \ \text{Tr}(\mathbf{Q}) \leq 1.$$

To conclude this section, problem (42) can be solved by i) choosing an initial point $\mathbf{Q}_0$; and ii) for $k = 0, 1, \cdots$, solving (47) until the termination condition is met.

VII. NUMERICAL RESULTS

Computer simulations are conducted to evaluate the performance of the proposed FD scheme. All channel entries are i.i.d. drawn from the Gaussian distribution $\mathcal{CN}(0, 1)$. Unless otherwise specified, it is assumed that E is equipped with the same number of receive antennas as D, i.e., $M_e = M_r$, $M_t = M_r = 2$ and $\rho = 0.5$. The total transmit SNR, P_T in dB, is used as power metric.

We will compare the secrecy rate performance of the proposed FD scheme with the baseline HD system, in which the achievable secrecy capacity is expressed as:

$$C_{S,HD} = \max \left(0, \log_2(1 + P_s \|\mathbf{h}_{sd,HD}\|^2) - \log_2(1 + P_s \|\mathbf{h}_{se}\|^2) \right), \tag{48}$$

where $\mathbf{h}_{sd,HD}$ denotes the channel between S and all antennas at D in the HD mode. We maintain the same total power for the HD and the FD systems.

For the optimization with fixed receiver, we consider the following (non-optimized) MMSE receiver

$$\mathbf{r} = \frac{\left(\rho\mathbf{HH}^\dagger + \mathbf{I}\right)^{-1}\mathbf{h}_{sd}}{\|\left(\rho\mathbf{HH}^\dagger + \mathbf{I}\right)^{-1}\mathbf{h}_{sd}\|} \tag{49}$$

which takes into account the self-interference channel as well as noise power.

In Fig. 3, we evaluate the achievable secrecy rate against total transmit SNR for the single-antenna case. We simulate both cases with fixed equal power allocation between S and D, and optimal power allocation. It is seen that both FD schemes outperform the HD operation for transmit SNR greater than 10 dB, and substantial secrecy rate gain is achieved in the high SNR region. The performance of the HD scheme saturates when the transmit SNR is higher than 25 dB while ceiling effects for both FD schemes start to appear when the transmit SNR is 50 dB.

In Fig. 4, we show the same results as those in Fig. 3 for the default multi-antenna setting. Firstly, it is observed that for the HD mode, the secrecy rate saturates from very low SNR, because E has the same number of antennas as D, while S has a single antenna and there is no external helper. On the other hand, for all FD schemes, the secrecy rate can keep increasing as the transmit SNR increases without hitting a ceiling; this is due to the fact that multiple transmit antennas at D help suppress self-interference and generate jamming signal to E. It can be also seen that the joint S−D power allocation only gives marginal performance gain in this case. The optimal linear receiver at D can improve the secrecy rate by approximately 10% compared to a fixed MMSE receiver. When an MMSE receiver is used at E, the achievable secrecy rate starts to outperform the FD case only when the SNR is greater than 10 dB, and the performance gain is reduced compared to the case where E uses simple MRC receiver.

In Fig. 5, we examine the impact of residual self-interference, ρ, when the total transmit SNR is 15 dB. The HD mode does not suffer from self-interference, therefore the secrecy rate remains constant. As expected, the secrecy rates of all FD schemes decrease as ρ increases. All FD schemes outperform the HD scheme, even when ρ is as high as 0.9. It can also be seen that the performance gap between the optimal linear receiver and the MMSE receiver becomes larger for higher ρ. This is because the optimal linear receiver is much more effective in compensating the higher self-interference. When an MMSE receiver is used at E, much lower secrecy rate is achieved as compared to the case in which E uses simple MRC receiver, but the FD approach still outperforms the HD one.

In Fig. 6, we provide the results of ergodic secrecy rate against the total transmit SNR. The approximation of the ergodic secrecy rate, which is used for power allocation, is also shown for comparison. Similar to the perfect CSI case, the ergodic secrecy rate of the HD scheme saturates from very low SNR, while using the FD scheme, the ergodic secrecy rate can increase without ceiling effect.

In Fig. 7, we plot the results of outage secrecy rate, where the target outage probability is 10%. It is seen that for the HD case, the achievable secrecy rate is very close to zero for all SNR regions. Using the FD operation at D, the secrecy rate can be increased with SNR, even with fixed power allocation at S and D.

Finally in Fig. 8, we investigate the impact of different combinations of transmit and receive antennas at D assuming there are $M_r + M_t = 4$ antennas in total. E has $M_e = 4$ receive antennas. We can see that $(M_r = 2, M_t = 2)$ provides the best performance, and this is because the joint transmit and receive beamforming design can handle the self-interference efficiently. Another interesting observation is that the case of $(M_r = 3, M_t = 1)$ greatly outperforms the case of $(M_r = 1, M_t = 3)$. This is due the fact that at D, the receiver design takes care of both useful signal and self-interference, while the transmitter design mainly aims to suppress self-interference and effectively jam E. In this sense, receiver design is more important than the transmitter design, therefore more receive antennas can provide additional performance gain.

VIII. CONCLUSIONS

In this paper, we have proposed a new self-protection scheme against passive eavesdropping achieved by the FD operation at the destination. This is of particular interest when the secrecy performance of the system is interference-limited and trusted external helpers are not available. To deal with LI and maximize the achievable secrecy rate, we have studied the optimal jamming covariance matrix at the destination and possible power allocation between the source and the destination with both perfect CSI and CDI. We have shown that the optimal jamming covariance matrix is rank-1 and can be found via an efficient 1-D search. In addition, a low-complexity ZF solution and the associated achievable secrecy rate have been derived in closed-form. Using the proposed FD scheme, the system is shown to be no longer interference-limited, in contrast to the HD case. Substantial performance gains are observed compared with the conventional HD operation at the destination.

An interesting future direction is to study more sophisticated scenarios, where the eavesdropper knows the FD strategy employed at the destination, and performs a similar FD operation; this is likely to be studied within the framework of non-cooperative game theory.

APPENDICES

A. PROOF OF PROPOSITION 1

Proof: For simplicity, we define $a \triangleq P_s|h_{sd}|^2, b \triangleq \rho|h|^2, c \triangleq P_s|h_{se}|^2$, and $d \triangleq |h_{ed}|^2$. Then $f_\rho(x)$ can be re-expressed as

$$f_\rho(x) = \frac{1 + \frac{a}{1+bx}}{1 + \frac{c}{1+dx}}. \tag{50}$$

Setting its first-order derivative of $f_\rho(x)$ to be zero leads to

$$(cb - ad)x^2 + 2(c-a)x - \frac{a}{d}(1+c) + \frac{c}{b}(1+a) = 0. \tag{51}$$

We first consider a trivial case that $cb - ad = 0$. In this case, positive secrecy rate is possible only when $a > c$. Consequently, the first-order derivative is negative, which indicates that $p_d^*(\rho) = 0$ is the optimal solution. In the following, we assume that $cb - ad \neq 0$.

We show that $x_1(\rho)$ and $x_2(\rho)$ cannot be both positive, which requires

$$x_1(\rho) + x_2(\rho) = \frac{a - c}{cb - ad} > 0, \qquad (52)$$

$$x_1(\rho)x_2(\rho) = \frac{cd(1 + a) - ab(1 + c)}{bd(cb - ad)} > 0. \qquad (53)$$

We assume the first equality is true, i.e., $x_1(\rho) + x_2(\rho) = \frac{a - c}{cb - ad} > 0$, in the following, we show that the second one cannot be satisfied.

1) $a \geq c$:
   In this case, $cb - ad > 0$ and $b > d$. We have

   $$cd(1+a) - ab(1+c) \leq cb(1+a) - ab(1+c) = (c-a)b \leq 0.$$

   Thus, $x_1(\rho)x_2(\rho) = \frac{cd(1+a)-ab(1+c)}{bd(cb-ad)} \leq 0$.

2) $a < c$:
   In this case, $cb - ad < 0$ and $b < d$. We have

   $$cd(1+a) - ab(1+c) > cb(1+a) - ab(1+c) = (c-a)b > 0.$$

   Thus, $x_1(\rho)x_2(\rho) = \frac{cd(1+a)-ab(1+c)}{bd(cb-ad)} < 0$.

As a result, we know that $x_2(\rho)$ is the only possible positive root of $f_\rho'(x) = 0$ if there exists one.

When $\frac{ad}{cb} = \frac{\delta}{\rho} > 1$ or $\rho \leq \delta$, $f_\rho'(p_d) > 0$ for $0 \leq p_d \leq x_2(\rho)$, so $p_d^*(\rho) = \min(P_d, x_2(\rho))$; when $\rho > \delta$, it can be verified that $f_\rho'(p_d) < 0$ for $0 \leq p_d \leq x_2(\rho)$ and $f_\rho'(p_d) > 0$ for $p_d > x_2(\rho)$. So if $x_2(\rho) \geq P_d$, $p_d^*(\rho) = 0$; otherwise $p_d^*(\rho) = 0$ or $p_d^*(\rho) = P_d$. The proof is completed. ∎

APPENDIX B

In this appendix, we derive the solution to the problem below:

$$\max_{\mathbf{Q} \succeq \mathbf{0}} \quad \mathbf{a}^\dagger \mathbf{Q} \mathbf{a} \qquad (54)$$
$$\text{s.t.} \quad \text{trace}(\mathbf{Q}\mathbf{R}) = t, \text{trace}(\mathbf{Q}) = 1,$$

where $\mathbf{Q}$ is an $M_t \times M_t$ matrix variable, $\mathbf{R} = \mathbf{H}^\dagger \mathbf{h}_{sd} \mathbf{h}_{sd}^\dagger \mathbf{H} - t\rho P_d \mathbf{H}^\dagger \mathbf{H}$ is a Hermitian matrix which is not positive semidefinite and $\mathbf{a} = \mathbf{H}_{ed}^\dagger \mathbf{h}_{se}$ is an $M_t \times 1$ vector. t is a positive scalar.

The dual problem is

$$\min_{\lambda_1, \lambda_2} \quad \lambda_1 t + \lambda_2 \qquad (55)$$
$$\text{s.t.} \quad \lambda_2 \mathbf{I} + \lambda_1 \mathbf{R} - \mathbf{a}\mathbf{a}^\dagger \succeq \mathbf{0}.$$

It can be checked that $\lambda_2 > 0$, otherwise, the secondary matrix inequality cannot be satisfied. It is also known that there is at least one rank-1 optimal solution $\mathbf{q}$ that satisfies $\mathbf{Q} = \mathbf{q}\mathbf{q}^\dagger$.

Due to the complementary slackness, we know that

$$(\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R} - \mathbf{a}\mathbf{a}^\dagger)\mathbf{q} = \mathbf{0}. \qquad (56)$$

We first consider a special case that $\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R}$ is positive semi-definite and its smallest eigenvalue is 0. Then we have the following inequality:

$$\begin{aligned}
0 &= \lambda_{\min}(\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R} - \mathbf{a}\mathbf{a}^\dagger) & (57) \\
&= \min_{\|\mathbf{x}\|=1} \mathbf{x}^\dagger (\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R} - \mathbf{a}\mathbf{a}^\dagger)\mathbf{x} & (58) \\
&= \min_{\|\mathbf{x}\|=1} (\mathbf{x}^\dagger (\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R})\mathbf{x} - \mathbf{x}^\dagger \mathbf{a}\mathbf{a}^\dagger \mathbf{x}) & (59) \\
&\leq \min_{\|\mathbf{x}\|=1} (\mathbf{x}^\dagger (\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R})\mathbf{x} + \lambda_{\max}(-\mathbf{a}\mathbf{a}^\dagger)) & (60) \\
&= \min_{\|\mathbf{x}\|=1} \mathbf{x}^\dagger (\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R})\mathbf{x} & (61) \\
&= 0. & (62)
\end{aligned}$$

Suppose one eigenvector that achieves $\min_{\|\mathbf{x}\|=1} \mathbf{x}^\dagger(\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R})\mathbf{x}$ is $\mathbf{q}_1$, i.e., $\mathbf{q}_1^\dagger(\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R})\mathbf{q}_1 = 0$, then the equality sign is attained iff $\mathbf{q}_1^\dagger \mathbf{a} = 0$, which is a trivial case.

In the following, we assume $\lambda_2 \mathbf{I} + \lambda_1 \mathbf{R} \succ \mathbf{0}$. It is easy to verify that at the optimum, $\mathbf{a}^\dagger(\lambda_1 \mathbf{R} + \lambda_2 \mathbf{I})^{-1}\mathbf{a} = 1$. Suppose the eigenvalue decomposition of $\mathbf{R}$ is $\mathbf{R} = \mathbf{U}\mathbf{D}\mathbf{U}^\dagger, \mathbf{U}\mathbf{U}^\dagger = \mathbf{I}, \mathbf{D} = \text{diag}(d_1, \cdots, d_{M_t})$, then $\mathbf{q}$ can be expressed as

$$\mathbf{q} = \mathbf{U}(\bar{\lambda}_1 \mathbf{D} + \bar{\lambda}_2 \mathbf{I})^{-1}\mathbf{b}, \mathbf{b} \triangleq \mathbf{U}^\dagger \mathbf{a} = [b_1, \cdots, b_{M_t}]^T, \quad (63)$$

where $\bar{\lambda}_1 = s\lambda_1, \bar{\lambda}_2 = s\lambda_2, s = \frac{1}{\mathbf{b}^\dagger(\lambda_1 \mathbf{D} + \lambda_2 \mathbf{I})^{-1}\mathbf{b}}$. The remaining task is to identify the optimal $\bar{\lambda}_1$ and $\bar{\lambda}_2$.

Substitute (63) into the two equality constraints in (54), then we get the following two equations:

$$\begin{cases} \sum_{i=1}^{M_r} |b_i|^2 \frac{d_i}{(\lambda_1 d_i + \lambda_2)^2} = t \\ \sum_{i=1}^{M_t} |b_i|^2 \frac{1}{(\lambda_1 d_i + \lambda_2)^2} = 1, \end{cases} \qquad (64)$$

from which we can solve all solutions $(\bar{\lambda}_1, \bar{\lambda}_2)$ and choose the one which satisfies $\bar{\lambda}_2 > 0$ and returns the maximum objective value $\bar{\lambda}_1 t + \bar{\lambda}_2$.

REFERENCES

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

[2] A.O. Hero, "Secure space-time communication" *IEEE Trans. Inform. Theory*, vol. 49, no. 12, pp. 3235-3249, Dec. 2003.

[3] Y. Liang, H. V. Poor and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[4] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, pp. 2083–2114, April 2011.

[5] C. Ling, L. Luzzi, and J. -C. Belfiore, "Lattice codes achieving strong secrecy over mod-Λ Gaussian channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, USA, July 2012, pp. 2306–2310.

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

[7] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Taiwan, Apr. 2009, pp. 2437-2440.

[8] 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. Sign. Systems Comp.*, Pacific Grove, CA, Nov. 2011, pp. 207 - 211.

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

[10] G. Zheng, Li-Chia Choo, and K. K. Wong, "Optimal Cooperative Jamming To Enhance Physical Layer Security Using Relays," *IEEE Trans. on Sig. Proc.*, vol. 59, no. 3, pp. 1317 - 1322, Mar. 2011.

[11] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 5003–5011, Oct. 2009.

[12] J. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forens. Sec.*, vol. 6, pp. 256–266, June 2011.

[13] S. Gerbracht, C. Scheunert and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," *IEEE Trans. Inf. Forens. Sec.*, vol. 7, no. 2, pp. 704-716, Apr. 2012.

[14] S. Luo, J. Li and A. Petropulu, "Outage Constrained Secrecy Rate Maximization Using Cooperative Jamming," in *Proc. 2012 IEEE Statistical Signal Processing Workshop (SSP2012)*, Ann Arbor, MI, Aug. 2012.

[15] Z. Ding, M. Peng, and H. -H. Chen, "A general relaying transmission protocol for MIMO secrecy communications," *IEEE Trans. Commun.*, vol. 60, pp. 3461–3471, Nov. 2012.

[16] Jing Huang and A. Lee Swindlehurst, "Cooperative Jamming for Secure Communications in MIMO Relay Networks," *IEEE Trans. Sig. Proc.*, vol. 59, no. 10, Oct. 2011.

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

[18] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE Int. Conf. Comp. Commun.*, Shanghai, China, April 2011, pp. 1125–1133.

[19] T. Riihonen, S. Werner, and R. Wichman, "Optimized gain control for single-frequency relaying with loop interference," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 2801–2806, June 2009.

[20] 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.

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

[22] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex MIMO relaying: achievable rates under limited dynamic range," *IEEE J. Selec. Areas Commun.*, vol. 30, pp. 1541–1553, Sept. 2012.

[23] 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 Trans. Vehic. Tech.*, submitted for publication, Oct. 2012. [Available Online: http://arxiv.org/pdf/1210.1639v2.pdf].

[24] P. Lioliou, M. Viberg, M. Coldrey, and F. Athley, "Self-Interference Suppression in Full-Duplex MIMO Relays," in *Proc. Asilomar Conf. Sign. Systems Comp.*, Pacific Grove, CA, Nov. 2007, pp. 658-662.

[25] T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 3074-3085, Sept. 2011.

[26] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. Asilomar Conf. Sign. Systems Comp.*, Pacific Grove, CA, Nov. 2011, pp. 265-269.

[27] 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.

[28] M.E. Knox, "Single antenna full duplex communications using a common carrier," in *the 13th annual IEEE Wireless and Microwave Technology Conference (WAMICON 2012)*, Orlando, Florida, Apr 7-9, 2013, pp. 1-6.

[29] Y. Huang and S. Zhang, "Complex Matrix Decomposition and Quadratic Programming," *Mathematics of Operations Research*, vol. 32, no. 3, pp. 758-768, 2007.

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

[31] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. on Inf. Theory (ISIT)*, Nice, France, June 2007, pp. 2466-2470.

[32] D. Raphaeli, "Distribution of noncentral indefinite quadratic forms in complex normal variables," *IEEE Trans. Inform. Theory*, vol. 42, no. 3, pp. 1002-1007, May 1996.

[33] Le Thi Hoai An and Pham Dinh Tao, "The DC (difference of convex functions) programming and DCA revisited with DC models of real world nonconvex optimization problems," *Annals of Operations Research*, vol. 133, pp. 23-46, 2005.
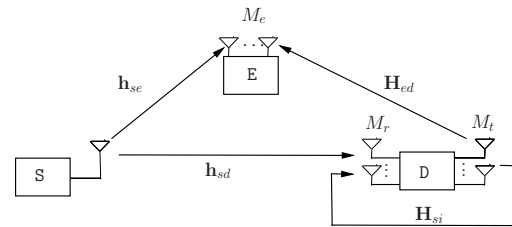
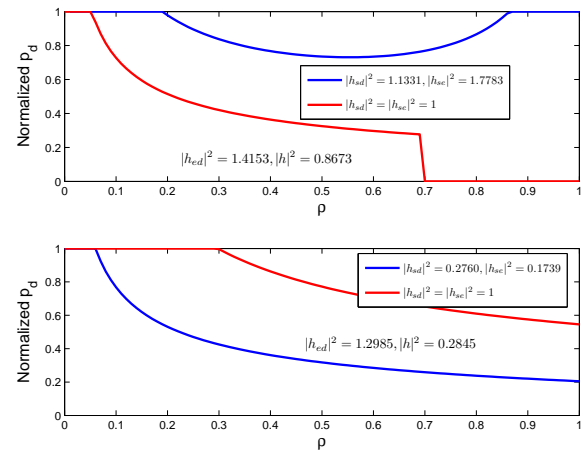Fig. 1. System model with FD receiver.

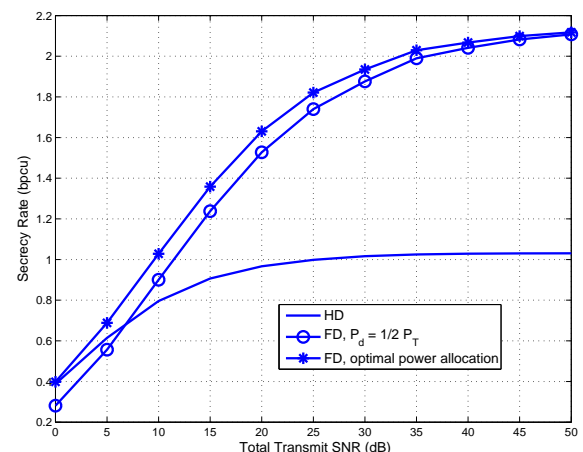Fig. 2. The impacts of ρ on the optimal power allocation at D.

Fig. 3. Secrecy rate vs. total transmit power for the single-antenna case.
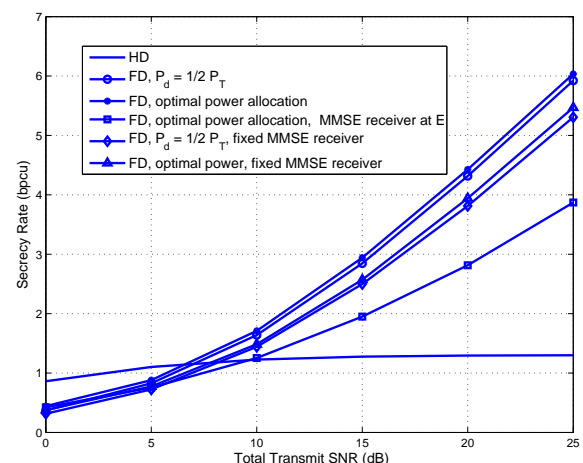

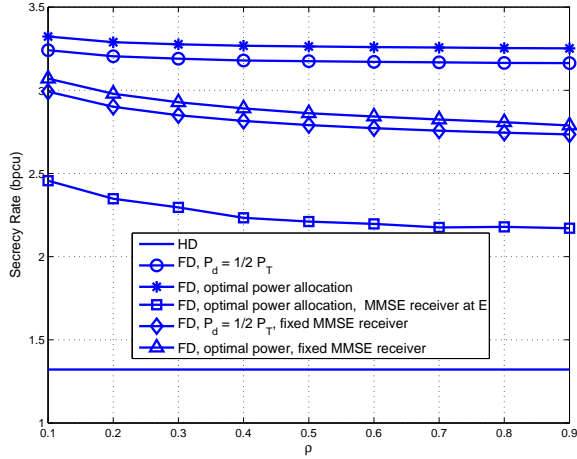Fig. 4. Secrecy rate vs. total transmit power for the multi-antenna case.

Fig. 5.   The effects of the LI channel strength ρ on the achievable secrecy rate.
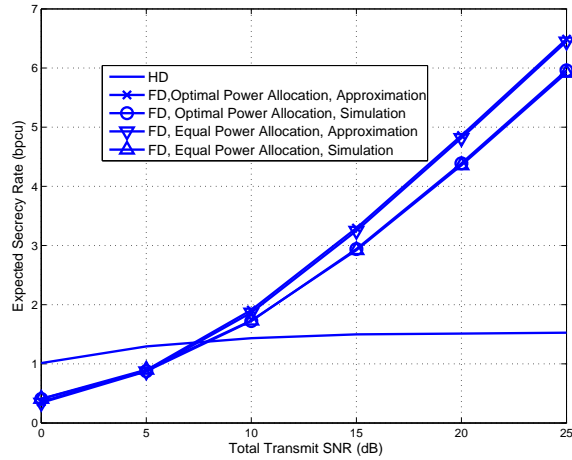

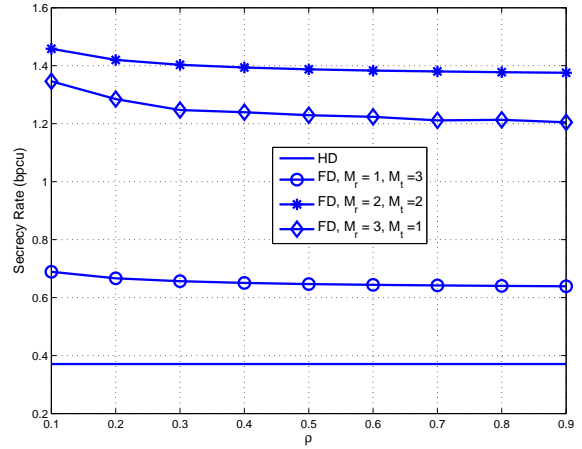Fig. 6.   Ergodic secrecy rate performance for the fast fading channel when only the CDI about E is available.

Fig. 8.   The impacts of ρ and antenna configurations at D on the achievable secrecy rate.
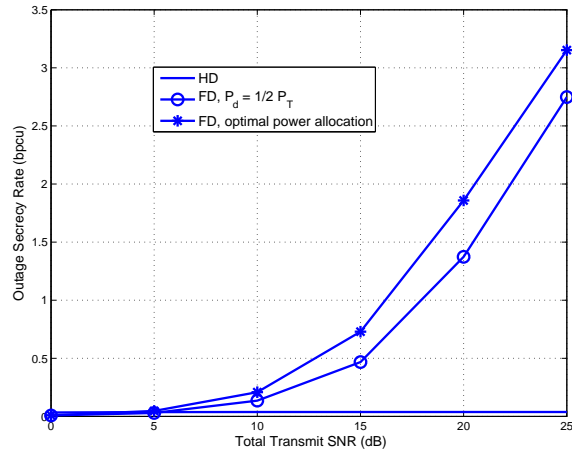

Fig. 7.   Outage secrecy rate for the slow fading channel when only the CDI about E is available.