A Full-Duplex Active Eavesdropper in MIMO Wiretap Channels: Construction and Countermeasures

Amitav Mukherjee and A. Lee Swindlehurst
Electrical Engineering and Computer Science
University of California Irvine
{a.mukherjee;swindle}@uci.edu

Abstract—We examine the design of a full-duplex active eavesdropper in the 3-user MIMOME wiretap channel, where all nodes are equipped with multiple antennas. The adversary intends to optimize its transmit and receive sub-arrays and jamming signal parameters so as to minimize the MIMO secrecy rate of the main channel. The full-duplex operating mode of the adversary induces self-interference at its receive sub-array, which is factored into the adversary's optimization. We characterize the worst-case jamming covariance for arbitrary and Gaussian input signaling, and develop a numerical algorithm to compute the same. We then examine sub-optimal active eavesdropping schemes that comprise essentially an antenna subset selection problem for the adversary, followed by a brief discussion of a potential countermeasure where the transmitter allocates some of its spatial dimensions for jamming the eavesdropper. Numerical results are presented to verify the efficacy of the proposed adversarial optimization algorithms.

I. INTRODUCTION

The broadcast and superposition characteristics of the wireless propagation medium combine to present a formidable challenge in ensuring simultaneously secure and reliable communications in the presence of adversaries. The broadcast property makes it difficult to shield transmitted signals from unintended recipients, while superposition can lead to the overlapping of desired and unwanted signals at the receiver. As a result, adversarial users are commonly modeled either as (1) a passive *eavesdropper* that tries to listen in on an ongoing transmission without being detected [1], or (2) a malicious transmitter (*jammer*) that tries to degrade the reception of the information signal at the intended receiver.

A three-terminal network consisting of a legitimate transmitter-receiver pair and a passive eavesdropper is commonly referred to as the *wiretap* channel. The pivotal performance metric of the wiretap channel is the *secrecy capacity*, which quantifies the highest rate at which a transmitter can reliably send a secret message to the receiver, without the eavesdropper being able to decode it. The secrecy capacity of the multiple-input multiple-output (MIMO) wiretap channel has been studied in [2]-[4], for example.

This work was supported by the U.S. Army Research Office under the Multi-University Research Initiative (MURI) grant W911NF-07-1-0318.

The optimization of malicious jamming signals to maximally degrade a communication link is another problem of long-standing interest. A common approach is to model the transmitter and the jammer as players in a game-theoretic formulation with the mutual information as the payoff function, and to identify the optimal transmit strategies for both parties. Recent work has extended this technique to compute the optimal spatial power allocation for MIMO and relay channels with various levels of channel state information (CSI) available to the transmitters, as well as optimal jamming strategies without secrecy considerations [5]-[7].

In this paper, we consider a MIMO communication link in the presence of a more sophisticated adversary: a full-duplex active eavesdropper with the dual capability of simultaneously eavesdropping and jamming any ongoing transmission, with the objective of causing maximum disruption to the security of the main channel. This problem differs from scenarios where the jamming signal is allowed to be arbitrarily correlated with the information signal [5], since the prior emphasis was on minimizing the conventional MIMO rate. Initial work on MIMO active eavesdropping has considered the half-duplex attacker scenario in [8]. The design of full-duplex nodes has generally been restricted to single or multi-antenna *relay* nodes, for both non-secret and secure communication problems [9]-[17].

The remainder of this work is organized as follows. Section II introduces the mathematical model and the results on the optimal jamming covariance for arbitrary and Gaussian input signaling. Section III briefly describes the issues of self-interference cancelation and suboptimal jamming strategies along with a discussion of potential countermeasures, and we conclude in Section IV.

Notation: We will use $\mathcal{CN}(\mathbf{0}, \mathbf{Z})$ to denote a circularly symmetric complex Gaussian distribution with zero mean and covariance matrix $\mathbf{Z}$, $\mathcal{E}\{\cdot\}$ to denote expectation, $(\cdot)^T$ the transpose, $(\cdot)^H$ the Hermitian transpose, $(\cdot)^{-1}$ the matrix inverse, $\text{Tr}(\cdot)$ the trace operator, $|\cdot|$ the matrix determinant, and $\mathbf{I}$ an identity matrix of appropriate dimension.

II. ACTIVE EAVESDROPPER WIRETAP CHANNEL

We begin by considering a 3-terminal network with an N_a -antenna transmitter (Alice), an N_b -antenna receiver (Bob), and a malicious user (Eve) with N_m antennas. Eve uses N_e of the N_m elements in her antenna array to eavesdrop, and the remaining $N_j = N_m - N_e$ antennas for jamming Bob.

Fig. 1. System model.

In the strict sense of the term, full-duplex operation at Eve is interpreted as all her antennas being used simultaneously for eavesdropping and jamming: $N_j = N_e = N_m$. However, due to hardware limitations and to improve circuit isolation, it is more realistic to assume the array N_m is partitioned into eavesdropping and jamming sub-arrays N_e, N_j , respectively, ($N_j \cup N_e = N_m$) with a non-negligible cross-coupling (loop-back) matrix $\mathbf{H}_{si} \in \mathbb{C}^{N_e \times N_j}$, i.e., a “quasi” full-duplex mode.

The signals received by Bob and Eve at time t are

$$\mathbf{y}_b(t) = \mathbf{H}_{ba}\mathbf{x}_a(t) + \mathbf{H}_{be}\mathbf{x}_e(t) + \mathbf{n}_b(t) \quad (1)$$

$$\mathbf{y}_e(t) = \mathbf{H}_{ea}\mathbf{x}_a(t) + \sqrt{\rho}\mathbf{H}_{si}\mathbf{x}_e(t) + \mathbf{n}_e(t), \quad (2)$$

where $\mathbf{H}_{ba} \in \mathbb{C}^{N_b \times N_a}$, $\mathbf{H}_{ea} \in \mathbb{C}^{N_e \times N_a}$ are the channels from Alice, $\mathbf{H}_{be} \in \mathbb{C}^{N_b \times N_j}$ is the channel from Eve to Bob, $\mathbf{H}_{si}$ is the loop interference channel at Eve due to her full-duplex operation, and $\rho, 0 \leq \rho \leq 1$, represents the residual self-interference parameter of the eavesdropper after self-interference cancelation. In Sec. III, we briefly discuss methods of controlling ρ at the eavesdropper. Dropping the time index for brevity, the transmitted information signal is $\mathbf{x}_a \in \mathbb{C}^{N_a \times 1}$, $\mathbf{x}_e \in \mathbb{C}^{N_j \times 1}$ is the malicious signal, and $\mathbf{n}_b, \mathbf{n}_e$ are the independent background additive white complex Gaussian noise vectors: $\mathcal{E}\{\mathbf{n}_k\mathbf{n}_k^H\} = \sigma_k^2\mathbf{I}$, where $k = b, e$ indicates Bob or Eve, respectively.

We assume a block-fading scenario where the channels stay constant over a certain number of channel uses, and then transition independently to a new realization. Alice has perfect knowledge of $\mathbf{H}_{ba}$ and a potentially imperfect estimate of $\mathbf{H}_{ea}$; Eve possesses knowledge of $\mathbf{H}_{ba}, \mathbf{H}_{be}, \mathbf{H}_{ea}$ and a possibly imperfect estimate of $\mathbf{H}_{si}$. For example, Eve can capitalize on training signals emanating from Alice and Bob to learn $\mathbf{H}_{be}, \mathbf{H}_{ea}$ and eavesdrop on CSI feedback from Bob to acquire $\mathbf{H}_{ba}$, while the estimation of $\mathbf{H}_{si}$ is discussed in Sec. III.

Alice's transmit power is assumed to be fixed at P_a :

$$\mathcal{E}\{\mathbf{x}_a\mathbf{x}_a^H\} = \mathbf{Q}_a \quad \text{Tr}(\mathbf{Q}_a) = P_a. \quad (3)$$

Eve has a maximum power constraint of P_e when in jamming mode:

$$\mathcal{E}\{\mathbf{x}_e\mathbf{x}_e^H\} = \mathbf{Q}_e \quad \text{Tr}(\mathbf{Q}_e) \leq P_e. \quad (4)$$

When the input $\mathbf{x}_a$ is drawn from an arbitrary distribution, the MIMO secrecy rate without prefix coding [2], [4] is given by

$$R_s = [I(\mathbf{x}_a; \mathbf{y}_b) - I(\mathbf{x}_a; \mathbf{y}_e)]^+ \quad (5)$$

where $[a]^+ = \max(0, a)$. For this scenario, the adversary seeks to solve

$$\min_{N_j} \min_{\mathbf{Q}_e \in \Omega} R_s \quad (6)$$

where $\Omega = \{\mathbf{Q}_e | \mathbf{Q}_e \in \mathbb{C}^{N_j \times N_j}, \mathbf{Q}_e \succeq 0, \text{Tr}(\mathbf{Q}_e) \leq P_e\}$ is the non-empty, convex set of feasible jamming covariances.

Note that due to our particular definition of full-duplex adversarial operation, the optimal attack strategy consists of an outer optimization over the subset of antennas allocated for jamming versus eavesdropping (i.e., an antenna selection problem), and an inner optimization over $\mathbf{Q}_e$ for a given choice of N_j . In the remainder of this section we focus on the inner optimization of $\mathbf{Q}_e$ for a fixed set N_j , bearing in mind that an exhaustive search over N_j has complexity that grows exponentially with N_m . In ensuing sections, we switch gears and examine the antenna selection issue assuming a fixed structure for $\mathbf{Q}_e$.

Proposition 1: For a fixed jamming subarray N_j , the optimal jamming covariance for the MIMO wiretap channel with arbitrary input distribution satisfies the fixed-point equation

$$\lambda \mathbf{Q}_e = -(\nabla_{\mathbf{Q}_e} (R_s)) \mathbf{Q}_e \quad (7)$$

where

$$\begin{aligned} \nabla_{\mathbf{Q}_e} (R_s) = & -\mathbf{H}_{be}^H \mathbf{K}_b^{-1} \mathbf{H}_{ba} \mathbf{E}_b \mathbf{H}_{ba}^H \mathbf{K}_b^{-1} \mathbf{H}_{be} \\ & + \rho \mathbf{H}_{si}^H \mathbf{K}_e^{-1} \mathbf{H}_{ea} \mathbf{E}_e \mathbf{H}_{ea}^H \mathbf{K}_e^{-1} \mathbf{H}_{si}, \end{aligned} \quad (8)$$

$\mathbf{E}_i = E[(\mathbf{x}_a - E[\mathbf{x}_a|\mathbf{y}_i])(\mathbf{x}_a - E[\mathbf{x}_a|\mathbf{y}_i])^H]$, $i = b, e$, are the associated minimum mean-square error matrices, and λ is a non-negative scale factor.

Proof: Form the Lagrangian of the inner optimization in (6) as

$$L(\mathbf{Q}_e, \mu, \mathbf{\Gamma}) = R_s - \mu(\text{Tr}(\mathbf{Q}_e) - P_e) + \text{Tr}(\mathbf{\Gamma}\mathbf{Q}_e) \quad (9)$$

where $\mu, \mathbf{\Gamma}\mathbf{Q}_e$ are the KKT multipliers associated with the trace and semi-definite constraints on $\mathbf{Q}_e$. Since the objective function is non-convex in $\mathbf{Q}_e$, the KKT conditions are necessary but not sufficient for optimality. The KKT conditions lead us to

$$\nabla_{\mathbf{Q}_e} (R_s) - \mu\mathbf{I} + \mathbf{\Gamma} = \mathbf{0} \quad (10)$$

$$\text{Tr}(\mathbf{Q}_e) \leq P_e \quad (11)$$

$$\text{Tr}(\mathbf{\Gamma}\mathbf{Q}_e) = 0 \quad (12)$$

$$\mathbf{Q}_e \succeq \mathbf{0} \quad (13)$$

$$\mathbf{\Gamma} \succeq \mathbf{0}, \mu \geq 0. \quad (14)$$

Since the input distribution is arbitrary, a closed-form expression for the secrecy rate is unavailable. However, we can

$$\begin{aligned} \frac{d}{d\mathbf{Q}_e} R_s(\mathbf{Q}_e) &= \frac{1}{\ln 2} \left\{ \mathbf{H}_{be}^H (\mathbf{Z}_b + \mathbf{H}_{be} \mathbf{Q}_e \mathbf{H}_{be}^H)^{-1} \mathbf{H}_{be} \right\}^T - \frac{1}{\ln 2} \left\{ \mathbf{H}_{be}^H (\sigma_b^2 \mathbf{I} + \mathbf{H}_{be} \mathbf{Q}_e \mathbf{H}_{be}^H)^{-1} \mathbf{H}_{be} \right\}^T \\ &\quad - \frac{\rho}{\ln 2} \left\{ \mathbf{H}_{si}^H (\mathbf{Z}_e + \rho \mathbf{H}_{si} \mathbf{Q}_e \mathbf{H}_{si}^H)^{-1} \mathbf{H}_{si} \right\}^T + \frac{\rho}{\ln 2} \left\{ \mathbf{H}_{si}^H (\sigma_e^2 \mathbf{I} + \rho \mathbf{H}_{si} \mathbf{Q}_e \mathbf{H}_{si}^H)^{-1} \mathbf{H}_{si} \right\}^T \end{aligned} \quad (19)$$

exploit the relation between mutual information and MMSE [18] in vector Gaussian channels to obtain the gradient of R_s with respect to the jamming covariance matrix as in (8). Next, (12)-(14) reveal that the positive-definite matrices $\mathbf{Q}_e$ and $\mathbf{\Gamma}$ have the same eigenvectors and $\mathbf{\Gamma} \mathbf{Q}_e = \mathbf{0}$. Multiplying $\mathbf{Q}_e$ on both sides of (10), we obtain (7). ■

Proposition 1 characterizes a robust jamming strategy by the adversary for an arbitrary input distribution chosen by the legitimate transmitter. For the MIMO wiretap channel with a passive eavesdropper, a Gaussian input signal is known to be optimal [2]. Similarly, Gaussian signaling is the capacity-achieving input distribution against worst-case Gaussian jamming in the MIMO channel without secrecy considerations [5]. Therefore, it is of interest to specialize to Gaussian input signals of the form $\mathbf{x}_a \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}_a)$. In the Gaussian MIMOME wiretap channel with a passive eavesdropper, the asymptotically optimal linear transmission strategy for Alice (assuming knowledge of $\mathbf{H}_{ea}$ and noise pre-whitening of $\mathbf{y}_b$ at Bob) is known to be the generalized singular value decomposition (GSVD) precoder [2], which provides us with a potential choice of $\mathbf{Q}_a$. We are interested in the optimization at the eavesdropper, who seeks to solve the following

$$\min_{\mathbf{Q}_e \in \Omega} R_s. \quad (15)$$

For the proposed system with specialization to Gaussian signaling, define the MIMO secrecy rate as

$$\begin{aligned} R_s(\mathbf{Q}_e) &= \log |\mathbf{I} + \mathbf{H}_{ba} \mathbf{Q}_a \mathbf{H}_{ba}^H \mathbf{K}_b^{-1}| \\ &\quad - \log |\mathbf{I} + \mathbf{H}_{ea} \mathbf{Q}_a \mathbf{H}_{ea}^H \mathbf{K}_e^{-1}| \end{aligned} \quad (16)$$

where $\mathbf{K}_b, \mathbf{K}_e$ are the receive interference-plus-noise covariance matrices at Bob and Eve, respectively:

$$\begin{aligned} \mathbf{K}_b &= \mathbf{H}_{be} \mathbf{Q}_e \mathbf{H}_{be}^H + \sigma_b^2 \mathbf{I} \\ \mathbf{K}_e &= \rho \mathbf{H}_{si} \mathbf{Q}_e \mathbf{H}_{si}^H + \sigma_e^2 \mathbf{I}. \end{aligned} \quad (17)$$

If the eavesdropper does not adopt any self-interference cancellation techniques as a worst-case assumption, then $\rho = 1$. This would be the case if the jamming and eavesdropping arrays are actually co-located devices with limited coordination capabilities, for example.

Let $\mathbf{H}_{ba} = \mathbf{U} \text{diag}(d_{ii}) \mathbf{V}^H$ be the singular value decomposition of the Alice-Bob channel. It is then straightforward to evaluate the following special cases.

Proposition 2(a): For the scenario when $\rho = 0$, the optimal jamming covariance given uniform power allocation at Alice is

$$\mathbf{H}_{be} \mathbf{Q}_e \mathbf{H}_{be}^H = \mathbf{U} \text{diag}(\sigma_i^*) \mathbf{U}^H$$

where

$$\sigma_i^* = -\frac{d_{ii}^2 P_a}{2\sigma_b^2} + \frac{d_{ii}^2 P_a}{2\sigma_b^2} \sqrt{1 + \frac{4\sigma_b^2}{\alpha d_{ii}^2 P_a}} - 1, \alpha \leq \frac{d_{ii}^2 P_a}{\sigma_b^2 + d_{ii}^2 P_a}$$

and α is chosen to satisfy the jammer power constraint.

Proposition 2(b): For the MISOSE channel ($N_a \geq 1, N_b = N_m = 1$) where the transmitter employs a beamformer $\mathbf{w}$, $\mathbf{W} \triangleq \mathbf{w} \mathbf{w}^H$, the adversary dedicates its antenna to jamming if and only if

$$\frac{1 + \frac{P_a \mathbf{H}_{ba} \mathbf{W}^H \mathbf{H}_{ba}^H}{\sigma_b^2}}{\left(1 + \frac{P_a \mathbf{H}_{ba} \mathbf{W}^H \mathbf{H}_{ba}^H}{\sigma_b^2 + |\mathbf{H}_{be}|^2 P_e}\right)} < \left(1 + \frac{P_a \mathbf{H}_{ea} \mathbf{W}^H \mathbf{H}_{ea}^H}{\sigma_e^2}\right),$$

otherwise Eve eavesdrops.

Proof: (a) When there is no self-interference at the adversary, the second term in (16) is independent of $\mathbf{Q}_e$. Therefore, the jamming covariance must minimize the mutual information between Alice and Bob, which reduces to the conventional MIMO jamming problem which has a known waterfilling-type solution (e.g., see [6]); (b) follows directly from comparing (16) when Eve chooses to jam versus eavesdropping. ■

Proposition 3: For a fixed jamming subarray $\mathcal{N}_j$, the optimal jamming covariance for the MIMO wiretap channel with Gaussian input signaling satisfies the fixed-point equation

$$\mu \mathbf{Q}_e = - \left(\frac{d}{d\mathbf{Q}_e} R_s(\mathbf{Q}_e) \right) \mathbf{Q}_e \quad (18)$$

where the derivative $\frac{d}{d\mathbf{Q}_e} R_s(\mathbf{Q}_e)$ is defined in (19) at the top of the page.

Proof: As a step towards characterizing the optimal $\mathbf{Q}_e$, we can obtain the necessary KKT conditions from the Lagrangian function

$$L(\mathbf{Q}_e, \mu, \mathbf{\Gamma}) = R_s(\mathbf{Q}_e) - \mu (\text{Tr}(\mathbf{Q}_e) - P_e) + \text{Tr}(\mathbf{\Gamma} \mathbf{Q}_e) \quad (20)$$

where $\mu, \mathbf{\Gamma} \mathbf{Q}_e$ are the KKT multipliers associated with the trace and semi-definite constraints on $\mathbf{Q}_e$. The KKT conditions lead us to

$$\frac{d}{d\mathbf{Q}_e} R_s(\mathbf{Q}_e) - \mu \mathbf{I} + \mathbf{\Gamma} = \mathbf{0} \quad (21)$$

$$\text{Tr}(\mathbf{\Gamma} \mathbf{Q}_e) = 0 \quad (22)$$

$$\text{Tr}(\mathbf{Q}_e) \leq P_e \quad (23)$$

$$\mathbf{Q}_e \succeq \mathbf{0} \quad (24)$$

$$\mathbf{\Gamma} \succeq \mathbf{0}, \mu \geq 0 \quad (25)$$

The remainder of the proof is similar to Proposition 1. ■

While there exist more complex non-convex optimization techniques such as reformulation-linearization that theoretically guarantee finding a globally optimal solution, we consider adopting a relatively simple two-stage numerical search

algorithm for $\mathbf{Q}_e$. In the first step, a gradient projection (GP) method is applied to generate a candidate covariance [19]. The output of the GP algorithm is then used as an initialization to a set of fixed-point iterations that exploit the property of Proposition 3, as summarized in algorithmic form in the table on the next page.

Algorithm 1 Gradient Projection+Fixed-Point Iteration (GP-FP) search for optimal $\mathbf{Q}_e$

Require: $P_e > 0$

Initialize $\mathbf{Q}_e^{(0)}$, $k = 0$

do

  Compute gradient $\nabla R_s(\mathbf{Q}_e^{(k)})$

$\tilde{\mathbf{Q}}_e^{(k)} = \mathbf{Q}_e^{(k)} + \alpha^{(k)} \nabla R_s(\mathbf{Q}_e^{(k)})$

$\mathbf{Q}'_e^{(k)} = \text{projection of } \tilde{\mathbf{Q}}_e^{(k)} \text{ onto } \Omega$

$\mathbf{Q}_e^{(k+1)} = \mathbf{Q}_e^{(k)} + \beta^{(k)} (\mathbf{Q}'_e^{(k)} - \mathbf{Q}_e^{(k)})$

if $\|\mathbf{Q}_e^{(k+1)}\|_F - \|\mathbf{Q}_e^{(k)}\|_F > \epsilon$ **then**

$k = k + 1$

end if

  Initialize $y = 0$, $\mathbf{Q}_{e,FP}^{(y)} = \mathbf{Q}_e^{(k+1)}$

  Update $\mathbf{Q}_{e,FP}^{(y+1)}$ from (18) until convergence.

Since $R_s(\mathbf{Q}_e^{(k)})$ is a real-valued function, the gradient is simply $\nabla R_s(\mathbf{Q}_e^{(k)}) = 2 \left(\frac{d}{d\mathbf{Q}_e^{(k)}} R_s(\mathbf{Q}_e^{(k)}) \right)^*$. The step sizes $\alpha^{(k)}, \beta^{(k)}$, can be chosen based on Armijo's rule along the feasible direction [19]. The projection step onto set Ω involves scaling the eigenvalues of the Hermitian matrix $\tilde{\mathbf{Q}}_e^{(k)}$ so as to satisfy the trace constraint of P_e .

In Fig. 2, we present a numerical example for i.i.d. Rayleigh fading channels comparing the secrecy rate with GSVD precoding at Alice (best-case scenario where she knows $\mathbf{H}_{ea}$) and three choices of jamming covariances: uniform power allocation, waterfilling on $\mathbf{H}_{be}$, and the iterative GP-FP solution. The optimal jamming subarray set $\mathcal{N}_j$ is chosen via exhaustive search, and we observe that the optimal $\mathbf{Q}_e$ allows the adversary to best suppress the channel secrecy rate.

III. PRACTICAL CONSIDERATIONS

Theoretically, the jamming signal $\mathbf{x}_e(t)$ can either be an arbitrary function of the information signal $\mathbf{x}_a(t - \tau)$ where τ is the processing delay of the adversary's decoder, i.e., a correlated jamming signal [5], or independent, spatially-white Gaussian noise, or some linear combination of the two. As shown in the previous section, finding a closed-form solution for the optimal interference covariance is elusive. As a simplifying assumption, let us assume the jamming signal $\mathbf{x}_e$ is spatially-white complex Gaussian noise uncorrelated with the source signal $\mathbf{x}_a$. In this suboptimal setting, we can frame the attacker's optimization problem as an antenna subset selection issue.

We observe there is a tradeoff between allocating resources for eavesdropping versus jamming. Allotting a large number for N_e allows Eve to overhear more of the information signal,

Fig. 2. $P_e = 10\text{dB}$, $N_a = N_b = 4$, $N_m = 3$.

but leaves less antennas for jamming Bob; if Bob has a sufficiently large antenna array he can suppress the low-rank jamming signal. Similarly, jamming Bob with full power and a large N_j can significantly degrade the received signal at both Bob and Eve. A sub-optimal but low-complexity approach when $P_e \ll P_a$ or $N_m \gg N_a$ is for Eve to initialize her eavesdropping sub-array with the 'strongest' receive antenna (largest column norm of $\mathbf{H}_{ea}$), and progressively enlarge $\mathcal{N}_e$ in a greedy manner, thereby exploiting her natural advantage for eavesdropping. If $P_e \gg P_a$ or $N_m \gg N_b$, then priority is given to jamming Bob and the greedy antenna subset selection is initialized with Eve's strongest transmit antenna to Bob.

In the absence of a dedicated training phase, Eve is assumed to possess the following estimate of the self-interference channel

$$\hat{\mathbf{H}}_{si} = \mathbf{H}_{si} + \Delta\mathbf{H}_{si} \quad (26)$$

where $\Delta\mathbf{H}_{si}$ is a (deterministic) error term whose size is assumed to be bounded by Eve's chosen jamming power:

$$\|\Delta\mathbf{H}_{si}\|_F^2 \leq P_e. \quad (27)$$

The additional difficulty in estimating $\mathbf{H}_{si}$ as compared to the other channels in the network is due to the limited dynamic range of the RF front end: the difference in self-interference and desired incoming signal powers can be as large as 100dB [14].

Since Eve knows her jamming signal perfectly in principle, it can presumably be canceled out from her received signal to provide

$$\tilde{\mathbf{y}}_e = \mathbf{H}_{ea}\mathbf{x}_a - \Delta\mathbf{H}_{si}\mathbf{x}_e + \mathbf{n}_e. \quad (28)$$

However, the limitations of dynamic range also come to the fore in the self-canceling operation, since the transmitted jamming signal at the output of Eve's jamming sub-array cannot be known perfectly due to unavoidable DAC and amplifier non-linearities. The cross-coupling factor ρ therefore quantifies the impact of imperfect self-interference channel

estimation and an arbitrary cancelation process, and is assumed to be directly proportional to the variance of the residual interference-plus-noise at Eve [9], [14].

Eve can also use her spatial dimensions to mitigate the self-interference. Let the jamming signal be pre-processed by the $N_j \times N$ precoding matrix $\mathbf{P}$ as $\mathbf{x}_e = \mathbf{P}\mathbf{z}$, where $\mathbf{z}$ is an N -dimensional spatially white Gaussian noise signal. If Eve applies a linear receive filter $\mathbf{D} \in \mathbb{C}^{N_e \times N'}$ to detect $\mathbf{x}_a$ from (2), then we can attempt to impose the condition $\mathbf{D}^H \hat{\mathbf{H}}_{si} \mathbf{P} = \mathbf{0}$. While more sophisticated spatial interference mitigation techniques can also be constructed [9], we refrain from a more detailed analysis in the current work.

We now describe a countermeasure that allows the legitimate transmitter to mitigate the impact of the active eavesdropper. Specifically, Alice can split her transmit spatial dimensions and allocate d streams for data, and the remaining $(N_a - d)$ dimensions for transmitting artificial interference designed to jam Eve [2]. Setting $d = N_a$ would potentially be beneficial when Eve uses all her antennas for jamming. On the other hand, Alice can use some or all of her antennas to selectively jam Eve assuming she is eavesdropping, which can potentially improve the secrecy rate. Therefore, a tradeoff clearly exists at Alice regarding her optimal spatial stream and power allocation; however she can optimize the achieved secrecy rate only if some knowledge of Eve's CSI is available. The preceding discussion points to a game-theoretic formulation with the MIMO secrecy rate as the payoff function [1] as a method to solve for the optimal transmit and attack strategies. In particular, a strategic zero-sum game where both players move simultaneously [20] and must therefore play their maximin (minimax) responses is ideal for capturing the essence of the transmitter-eavesdropper interactions.

IV. CONCLUSION

We have examined optimal jamming strategies for a full-duplex active eavesdropper that seeks to minimize the channel secrecy rate of the 3-user MIMOME wiretap channel. We characterize the worst-case jamming covariance for arbitrary and Gaussian input signaling, and develop a numerical algorithm to compute the same. We then examine sub-optimal active eavesdropping schemes that comprise essentially an antenna selection problem for the adversary, followed by a brief discussion of a potential countermeasure where the transmitter allocates some of its spatial dimensions for jamming the eavesdropper.

REFERENCES

- [1] A. Mukherjee, A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical-layer security in multiuser wireless networks: A survey," 2010. [Online]. Available: <http://arxiv.org/abs/1011.3754>
- [2] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515-5532, Nov. 2010.
- [3] J. Li and A. Petropulu, "Transmitter optimization for achieving secrecy capacity in Gaussian MIMO wiretap channels," [Online]. Available at: <http://arxiv.org/abs/0909.2622v1>
- [4] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journ. Wireless Commun. Networking*, Nov. 2009.
- [5] A. Kasyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119-2123, Sep. 2004.
- [6] M. R. D. Rodrigues and G. Ramos, "On multiple-input multiple-output Gaussian channels subject to jamming," in *Proc. IEEE ISIT*, Jun. 2009.
- [7] A. Bayesteh, M. Ansari, and A. K. Khandani, "Effect of jamming on the capacity of MIMO channels," *Proc. 42nd Allerton Conf.*, 2004.
- [8] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," [Online]. Available at: <http://arxiv.org/abs/1011.5274>
- [9] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex MIMO relays," *IEEE Trans. Signal Process.*, vol. 59, no. 12, pp. 5983-5993, Dec. 2011.
- [10] D. W. Bliss, P. A. Parker, and A. R. Margetts, "Simultaneous transmission and reception for improved wireless network performance," in *Proc. IEEE 14th Workshop Statistical Signal Process.*, Aug. 2007.
- [11] P. Larsson and M. Prytz, "MIMO on-frequency repeater with self-interference cancellation and mitigation," in *Proc. IEEE VTC*, 2009.
- [12] H. Ju, E. Oh, and D. Hong, "Improving efficiency of resource usage in two-hop full duplex relay systems based on resource sharing and interference cancellation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3933-3938, Aug. 2009.
- [13] Y. Y. Kang and J. H. Cho, "Capacity of MIMO wireless channel with full-duplex amplify-and-forward relay," in *Proc. IEEE PIMRC*, Sep. 2009.
- [14] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex MIMO relaying: Achievable rates under limited dynamic range," [Online]. Available: <http://arxiv.org/abs/1111.2618v1>
- [15] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, 2008.
- [16] M. Yuksel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st CISS*, pp. 1318, Mar. 2007.
- [17] Y. Oohama, "Capacity theorems for relay channels with confidential messages," in *Proc. IEEE ISIT*, Jun. 2007.
- [18] D. P. Palomar and Sergio Verdú, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 141-154, Jan. 2006.
- [19] D. P. Bertsekas, *Nonlinear Programming*. Belmont, MA: Athena Scientific, 1995.
- [20] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.