Optimal Strategies for Countering Dual-Threat Jamming/Eavesdropping-Capable Adversaries in MIMO Channels

Amitav Mukherjee and A. Lee Swindlehurst
Electrical Engineering and Computer Science
University of California
Irvine, CA 92697-2625
a.mukherjee@uci.edu; swindle@uci.edu

***Abstract*—This paper investigates transmission strategies in a MIMO wiretap channel with a transmitter, receiver and wiretapper, each equipped with multiple antennas. In a departure from existing work, the wiretapper is able to act either as a passive eavesdropper or as an active jammer per channel use, under a half-duplex constraint. The transmitter therefore faces a choice between dynamically allocating all of its power for data; or broadcasting artificial noise along with the information signal in order to selectively degrade the eavesdropper's channel. We model the network as a zero-sum game in strategic form with the MIMO secrecy rate as the payoff function. We first carry out a detailed analysis of the various rate outcomes that result from the possible actions of the agents. We then discuss the conditions for equilibrium outcomes in the strategic form of the game. Finally, numerical simulations are presented to corroborate the analytical results.**

I. INTRODUCTION

The two fundamental characteristics of the wireless medium, namely *broadcast* and *superposition*, present different challenges in ensuring secure communications in the presence of adversaries. The broadcast nature of wireless communications makes it difficult to shield transmitted signals from unintended recipients, while superposition can lead to the overlapping of multiple 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, or (2) a malicious transmitter (*jammer*) that tries to degrade the signal at the intended receiver. Two distinct lines of research have developed to analyze networks compromised by either type of adversary, as summarized below.

A network consisting of a transmitter-receiver pair and a passive eavesdropper is commonly referred to as the *wiretap* channel. The information-theoretic aspects of this scenario have been explored in some detail [1], [2]. In particular, this work led to the development of the notion of *secrecy capacity*, which quantifies the rate at which a transmitter can reliably send a secret message to the receiver, without the eavesdropper being able to decode it. Ultimately, it was shown that a non-zero secrecy capacity can only be obtained if the eavesdropper's channel is of lower quality than that of the intended recipient. The work cited above assumes single antenna nodes; secrecy capacity for the multiple-input multiple-output (MIMO) wiretap channel, where all nodes may possess multiple antennas, has been studied in [3]-[5], for example.

The impact of malicious jammers on the quality of a communication link is another problem of long-standing interest, especially in mission-critical and military networks. 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 strategies for both parties [6], [7]. Recent work has extended this technique to MIMO and relay channels with various levels of channel state information (CSI) available to the transmitters [8]-[12].

In this paper, we consider a MIMO communication link in the presence of a more sophisticated adversary: a wiretapper with the dual capability of either eavesdropping passively or jamming any ongoing transmission, also referred to as an active eavesdropper. A strategic game formulation of the system where one of the nodes moves first is investigated. However, in a departure from the previous work referenced above, the game payoff function is now chosen to be the *MIMO secrecy rate* between the legitimate transmitter-receiver pair. [13] independently considered the active eavesdropper scenario with single-antenna nodes and proposed robust secrecy-preserving encoding schemes.

The paper is organized as follows. In the next section, the assumed mathematical and active eavesdropper model is presented. The secrecy rate outcomes are analyzed in Section III, followed by a description of the strategic game framework in Section IV. The resulting system performance is studied via simulation in Section V, and we conclude in Section VI.

Notation: $\mathcal{E}\{\cdot\}$ denotes expectation, $(\cdot)^T$ the transpose, $(\cdot)^H$ the Hermitian transpose, $(\cdot)^{-1}$ the matrix inverse, $\mathrm{Tr}(\cdot)$ is the trace operator, $[\mathbf{A}]_{p,q}$ denotes the (p,q) entry of matrix $\mathbf{A}$, $|\cdot|$ is the matrix determinant, and $\mathbf{I}$ is an identity matrix of appropriate dimension.

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

II. MATHEMATICAL MODEL

We study the MIMO wiretap problem in which three multiple-antenna nodes are present: a transmitter (Alice), a receiver (Bob), and a malicious user (Eve). Alice does not have knowledge of the instantaneous CSI of the eavesdropper, but she knows its distribution. Therefore, Alice has the option of utilizing all her power for transmitting data to Bob, regardless of channel conditions or potential eavesdroppers. Alternatively, she can split her power and simultaneously transmit the information vector and an 'artificial interference' signal that jams any unintended receivers other than Bob. While suboptimal in general, the artificial interference scheme does not require knowledge of Eve's instantaneous CSI and is therefore suitable for deployment against passive eavesdroppers [5], [14]–[17]. Eve seeks to disrupt the information rate between Alice and Bob by choosing to either eavesdrop or jam Bob in every transmission interval.

A. MIMO Wiretap Channel

Assuming Eve jams Bob, the signals received by Bob and Eve can be represented as follows:

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

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

where $\mathbf{x}_a$ is the signal vector transmitted by Alice, $\mathbf{x}_e$ is the Gaussian, spatially white jamming signal from Eve, $\mathbf{n}_b, \mathbf{n}_e$ are the naturally occurring additive noise at Bob and Eve, respectively, and $\mathbf{H}_{ba}, \mathbf{H}_{be}, \mathbf{H}_{ea}$ are the corresponding $N_b \times N_a, N_b \times N_e, N_e \times N_a$ complex Gaussian channel matrices with standard normal elements. Alice is assumed to have perfect knowledge of the realization of $\mathbf{H}_{ba}$ and the statistics of $\mathbf{H}_{be}, \mathbf{H}_{ea}$. On the other hand, Eve knows the instantaneous value of $\mathbf{H}_{ea}$ and the statistics of $\mathbf{H}_{be}, \mathbf{H}_{ba}$. An operational coding scheme for Alice is to employ Gaussian signaling with appropriate spatial power allocation over her transmit antennas [5].

The background noise at all receivers is assumed to be spatially white and zero-mean complex Gaussian:

$$\mathcal{E}\{\mathbf{n}_k\mathbf{n}_k^H\} = \sigma_k^2\mathbf{I}; \quad k = b, e.$$

Alice's transmit power is assumed to be bounded,

$$\mathcal{E}\{\mathbf{x}_a\mathbf{x}_a^H\} = \mathbf{Q}_a \qquad \mathrm{Tr}(\mathbf{Q}_a) \le P_a.$$

Similarly, Eve has a power constraint of P_e when in jamming mode.

In the most general scenario where Alice jams Eve, we have

$$\mathbf{x}_a = \mathbf{T}\mathbf{z} + \mathbf{T}\mathbf{z}', \quad (3)$$

where $\mathbf{T}, \mathbf{T}'$ are the $N_a \times d$, $N_a \times (N_a - d)$ beamforming matrices for the $d \times 1$ information vector $\mathbf{z}$ and uncorrelated $(N_a - d) \times 1$ jamming signal $\mathbf{z}'$, respectively. To ensure the orthogonality of the information and artificial noise signals when received by Bob, $\mathbf{T}$ and $\mathbf{T}'$ can be formed from the columns of the right singular vectors of $\mathbf{H}_{ba}$, for example. Thus, $\mathbf{Q}_a$ may be expressed as

$$\mathbf{Q}_a = \mathbf{T}\mathbf{Q}_z\mathbf{T}^H + \mathbf{T}'\mathbf{Q}_z'\mathbf{T}'^H, \quad (4)$$

where $\mathbf{Q}_z, \mathbf{Q}_z'$ are covariance matrices associated with $\mathbf{z}$ and $\mathbf{z}'$, respectively, $\mathrm{Tr}(\mathbf{T}\mathbf{Q}_z\mathbf{T}^H) \le \rho P_a$, and $\mathrm{Tr}(\mathbf{T}'\mathbf{Q}_z'\mathbf{T}'^H) \le (1-\rho)P_a$.

Define $\mathbf{H} \triangleq \{\mathbf{H}_{ba}, \mathbf{H}_{be}, \mathbf{H}_{ea}\}$ for brevity.The resultant performance metric adopted in this work is the MIMO secrecy rate achieved by Gaussian signaling and uniform spatial power allocation by Alice and Eve:

$$R_s = \mathcal{E}_{\mathbf{H}}\left\{\log_2\left|\sigma_b^2\mathbf{I} + \mathbf{H}_{ba}\mathbf{T}\mathbf{Q}_z\mathbf{T}^H\mathbf{H}_{ba}^H\mathbf{Q}_b^{-1}\right| - \log_2\left|\sigma_e^2\mathbf{I} + \mathbf{H}_{ea}\mathbf{T}\mathbf{Q}_z\mathbf{T}^H\mathbf{H}_{ea}^H\mathbf{Q}_e^{-1}\right|\right\}; \quad (5)$$

where $\mathbf{Q}_b, \mathbf{Q}_e$ are the received interference-plus-noise covariance matrices at Bob and Eve. Note that Alice must decide how many spatial dimensions are to be used for artificial noise, and what is the optimal fraction ρP_a of transmit power distributed over them. An exhaustive search for the above was used in [14], while the authors proposed a low-complexity suboptimal approach in [16]. For the MISO wiretap channel, it was shown in [17] that an equal power allocation ($\rho = 0.5$) is close to optimal. The game-theoretic results obtained in this paper hold for either an optimal or a pre-determined power and data stream allocation.

III. RATE THRESHOLDS

It is vital to compare the various rate outcomes resulting from Alice and Eve's actions as a precursor to the game-theoretic development of Section IV. To accomplish this, we first review some general results from random matrix theory that assist our analysis of the MIMO rate outcomes.

A. Asymptotic MIMO Rates

Let $\mathbf{X}$ represent the MIMO channel from a desired source with signal-to-noise ratio (SNR) α, and $\mathbf{Y}$ the channel from an interferer with interference-to-noise ratio (INR) η. Assuming uniform power allocation at both transmitters, the ergodic MIMO information rate with interference and Gaussian background noise is given by

$$R_I = \mathcal{E}_{\mathbf{X},\mathbf{Y}}\left\{\log\left|\mathbf{I} + \alpha\mathbf{X}\mathbf{X}^H\left(\mathbf{I} + \eta\mathbf{Y}\mathbf{Y}^H\right)^{-1}\right|\right\}. \quad (6)$$

When interference is absent and thermal noise is the only impairment at the receiver, the MIMO information rate in (6) reduces to $R = E\left\{\log\left|\mathbf{I} + \alpha\mathbf{X}\mathbf{X}^H\right|\right\}$. Let λ represent an arbitrary eigenvalue of the Wishart matrix $\mathbf{X}\mathbf{X}^H$. Then, since the determinant function is equal to the product of the eigenvalues of the argument, we can write

$$R = \min(N_a, N_b)\mathcal{E}_\lambda\left\{\log\left(1 + \alpha\lambda\right)\right\}. \quad (7)$$

The closed-form expression for this expectation in terms of generalized Laguerre polynomials is well known in the literature [18].

However, a more tractable expression for the ergodic MIMO capacity is available based on asymptotic results in the limit of a large number of antennas, as described next. Define $\beta \triangleq \frac{N_b}{N_a}$ as the ratio of transmit to receive antennas. For Wishart matrices, the asymptotic marginal probability density function of an arbitrary (unordered) eigenvalue is known to be [18]

$$p(\lambda) = \begin{cases} \frac{1}{\pi}\sqrt{\frac{\beta}{\lambda} - \frac{1}{4}\left(1+\frac{\beta-1}{\lambda}\right)^2}, & \left(\sqrt{\beta}-1\right)^2 \leqslant \lambda \leqslant \left(\sqrt{\beta}+1\right)^2 \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

Based on (8), a closed-form expression can be found for the asymptotic ergodic MIMO capacity with uniform power allocation as [21]

$$N_a \mathcal{E}_\lambda \left\{\log\left(1+\alpha\lambda\right)\right\} = N_a \cdot F(\beta,\alpha), \tag{9}$$

where

$$\begin{aligned} F(\beta,\alpha) &= \log\left(1+\alpha\left(\sqrt{\beta}+1\right)^2\right) \\ &+ \left(\sqrt{\beta}+1\right)\log\left(\frac{1+\sqrt{1-a}}{2}\right) \\ &- \log(e)\sqrt{\beta}\frac{1-\sqrt{1-a}}{1+\sqrt{1-a}} \\ &+ (\beta-1)\log\left(\frac{1+\gamma}{\gamma+\sqrt{1-a}}\right) \end{aligned} \tag{10}$$

and

$$a = \frac{4\alpha\sqrt{\beta}}{1+\alpha\left(\sqrt{\beta}+1\right)^2}; \quad \gamma = \frac{\sqrt{\beta}-1}{\sqrt{\beta}+1}. \tag{11}$$

Though originally derived under an asymptotic assumption, (9) has been shown to be very accurate even for small and medium-sized antenna array dimensions.

Next, we revisit the general MIMO information rate with interference in (6). Under an interference-limited assumption, $R_I \approx \mathcal{E}_{\mathbf{X},\mathbf{Y}}\left\{\log\left|\mathbf{I}+\alpha\mathbf{X}\mathbf{X}^H\left(\eta\mathbf{Y}\mathbf{Y}^H\right)^{-1}\right|\right\}$. Subsequently, we can reformulate the expectation in terms of the eigenvalues of the F-distributed random matrix $\mathbf{X}\mathbf{X}^H\left(\mathbf{Y}\mathbf{Y}^H\right)^{-1}$, and for which a cumbersome closed-form expression is computed in terms of the Gaussian hypergeometric function in [eq. (23)][20].

The asymptotic random matrix analysis technique has been extended to the MIMO capacity with interference in [22], [23], for example. In [22], a set of four simple closed-form expressions for the MIMO rate in the high-SNR regime is derived for different ratios of N_a/N_b (transmitter to receiver antennas), under the assumption $N_a = N_e$. In [23], the replica approach is used to obtain a more involved expression for the first-order approximation of the mean value of the MIMO mutual information at any SNR. However, we propose to extend the result of (9) in a straightforward manner to obtain a unified and more usable expression for the ergodic MIMO rate under interference.

Lemma 1: In a MIMO channel where the legitimate transmitter, receiver, and interferer have N_a, N_b, N_e antennas respectively, the asymptotic MIMO information rate with receive SNR α and INR η can be bounded as

$$R_I \leqslant (N_a+N_e)\,F\left(\frac{N_b}{N_a+N_e},(\alpha+\eta)\right) - N_e F\left(\frac{N_b}{N_e},\eta\right), \tag{12}$$

where $F(\beta,\alpha)$ is defined in (10).

Proof: Rewrite (6) as

$$\begin{aligned} R_I &= E_{\mathbf{X},\mathbf{Y}}\left\{\log\left|\mathbf{I}+\alpha\mathbf{X}\mathbf{X}^H+\eta\mathbf{Y}\mathbf{Y}^H\right|\right\} \\ &\quad - E_{\mathbf{Y}}\left\{\log\left|\mathbf{I}+\eta\mathbf{Y}\mathbf{Y}^H\right|\right\}. \end{aligned} \tag{13}$$

The first term is equivalent to the sum rate of a two-user MIMO multiple access channel (MIMO MAC) with uniform power allocation at each transmitter. The second term represents the MIMO rate between the interferer and the destination when treating the jamming signal as information. Since the transmitters cannot cooperate in the MIMO MAC, the sum rate of the MIMO MAC is upper-bounded by the rate of the equivalent point-to-point MIMO channel with composite channel $\mathbf{H} = \begin{bmatrix}\mathbf{X} & \mathbf{Y}\end{bmatrix}$, (N_a+N_e) transmit antennas, and effective SNR $(\alpha+\eta)$. This leads to an upper bound on the MIMO interference rate as

$$R_I \leqslant E_{\mathbf{H}}\left\{\log\left|\mathbf{I}+(\alpha+\eta)\,\mathbf{H}\mathbf{H}^H\right|\right\} - E_{\mathbf{Y}}\left\{\log\left|\mathbf{I}+\eta\mathbf{Y}\mathbf{Y}^H\right|\right\}. \tag{14}$$

Applying the expression for the asymptotic MIMO rate without interference in (9) to each of the two terms on the right hand side of (14) leads to (12).

B. MIMO Secrecy Rate Analysis

We now return our attention to the rate outcomes of the MIMO wiretap game. We focus on the achievable MIMO secrecy rate instead of maximizing the mutual information to compute the secrecy capacity. The lack of instantaneous knowledge of $\mathbf{H}_{be}$ and the half-duplex constraint prevents Eve from detecting the transmitted signal $\mathbf{z}$ and then applying correlated jamming [8]. Therefore, Eve is assumed to employ a Gaussian jamming signal with uniform per-antenna power allocation.

Define the effective channels conveying information $\mathbf{z}$ from Alice to Bob and Eve as $\tilde{\mathbf{H}}_{ba} \triangleq \mathbf{H}_{ba}\mathbf{T}$ and $\tilde{\mathbf{H}}_{ea} \triangleq \mathbf{H}_{ea}\mathbf{T}$, respectively. Since $\mathbf{T}$ is a submatrix of an isotropically-random unitary matrix, $\tilde{\mathbf{H}}_{ba}$ and $\tilde{\mathbf{H}}_{ea}$ are also zero-mean complex Gaussian matrices with i.i.d elements. Furthermore, $\mathcal{E}\left\{\left(\mathbf{H}_{ea}\mathbf{T}'\right)^H\mathbf{H}_{ea}\mathbf{T}\right\} = 0$ due to the orthonormality of $\mathbf{T},\mathbf{T}'$. However, the elements of $\tilde{\mathbf{H}}_{ba}$ have a variance greater than unity due to the truncation of (N_a-d) eigenvalues. In order to apply the random matrix results stated thus far, it is necessary to normalize the effective channel $\tilde{\mathbf{H}}_{ba}$ to obtain unit variance elements. The exact normalization constant is difficult to obtain analytically, therefore we scale $\tilde{\mathbf{H}}_{ba}$ by an approximate factor $\sqrt{d/N_a}$ [14]. In the sequel, this normalization factor is absorbed into the transmit power constraint.

From the general expression in (5), the secrecy rate between Alice and Bob when Eve is in eavesdropping mode is

$$R_{i,E} = \mathcal{E}_{\mathbf{H}}\{\log\left|\mathbf{I}+\mathbf{H}_{ba}\mathbf{T}\mathbf{Q}_z\mathbf{T}^H\mathbf{H}_{ba}^H/\sigma_b^2\right| - \log\left|\mathbf{I}+g_1\mathbf{H}_{ea}\mathbf{T}\mathbf{Q}_z\mathbf{T}^H\mathbf{H}_{ea}^H\mathbf{Q}_e^{-1}/\sigma_e^2\right|\}; \quad (15)$$

whereas the transmission rate of the main channel while being jammed by Eve is

$$R_{i,J} = \mathcal{E}_{\mathbf{H}}\left\{\log\left|\mathbf{I}+\mathbf{H}_{ba}\mathbf{T}\mathbf{Q}_z\mathbf{T}^H\mathbf{H}_{ba}^H\mathbf{Q}_b^{-1}/\sigma_b^2\right|\right\}, \quad (16)$$

where $i = F, A$ denotes the transmission strategies available to Alice, and the interference-plus-noise covariance matrices for Bob and Eve are

$$\mathbf{Q}_b = g_2\frac{P_e}{N_e}\mathbf{H}_{be}\mathbf{H}_{be}^H + \sigma_b^2\mathbf{I} \quad (17)$$

$$\mathbf{Q}_e = g_1\mathbf{H}_{ea}\mathbf{T}'\mathbf{Q}_z'\mathbf{T}'^H\mathbf{H}_{ea}^H + \sigma_e^2\mathbf{I}. \quad (18)$$

In view of (9) and (12), the asymptotic rate outcomes are

$$R_{A,E} \approx d\cdot F\left(\frac{N_b}{d}, \rho P_a\frac{N_a}{d}\right) - [N_a F\left(\frac{N_e}{N_a}, g_1 P_a\right) - (N_a - d)F\left(\frac{N_e}{N_a-d}, g_1(1-\rho)P_a\right)] \quad (19)$$

$$R_{A,J} \approx (N_e+d)F\left(\frac{N_b}{N_e+d}, \rho P_a\frac{N_a}{d} + g_2P_e\right) - N_eF\left(\frac{N_b}{N_e}, g_2P_e\right) \quad (20)$$

$$R_{F,E} \approx N_aF\left(\frac{N_b}{N_a}, P_a\right) - N_aF\left(\frac{N_e}{N_a}, g_1P_a\right) \quad (21)$$

$$R_{F,J} \approx (N_e+N_a)F\left(\frac{N_b}{N_a+N_e}, P_a+g_2P_e\right) - N_eF\left(\frac{N_b}{N_e}, g_2P_e\right). \quad (22)$$

The asymptotic rates are compared with the exact rate expressions obtained through Monte Carlo trials in Fig. 1, which demonstrates reasonable accuracy at low to intermediate SNRs even for small antenna arrays.

In [5], the instantaneous MIMO secrecy rate with artificial interference at high SNR is characterized in terms of the generalized singular values of $(\mathbf{H}_{ba}, \mathbf{H}_{ea})$. A closed-form lower bound for the ergodic MISO ($N_b = 1$) secrecy rate with artificial interference is derived using the Gauss hypergeometric function in [17]. In contrast, the expressions derived in (19)-(22) explicitly display the various system parameters, and are also amenable to analysis.

It is apparent that any comparison of the relative magnitudes of a pair of rates taken from those defined in (15)-(16) would involve a large number of parameters. It is therefore convenient to vary a subset of the parameters while holding the others constant when comparing the different rate outcomes as:

1) The relative transmit power budgets P_a and P_e.
2) The relative antenna array dimensions N_a and N_e.
3) The relative channel qualities $\sqrt{g_1}$ and $\sqrt{g_2}$.

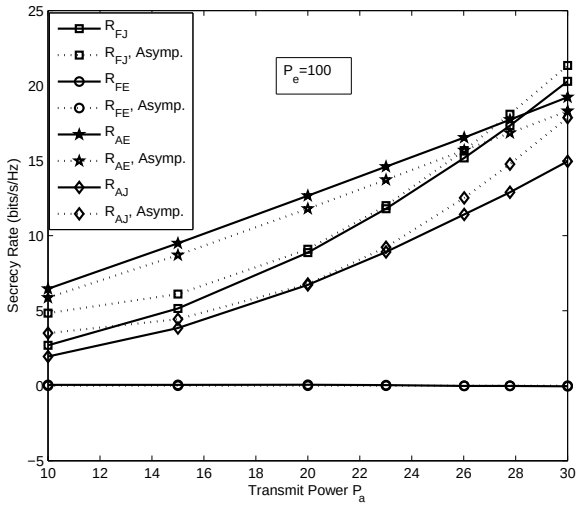

Fig. 1. Comparison of exact and asymptotic MIMO rate outcomes, $N_a = 7, N_b = N_e = 5$ and $g_1 = 0.8, g_2 = 1.2$.

This exercise is demonstrated for several cases in the numerical results in Sec. V.

It is instructive to examine the behavior of the rate outcomes for several limiting cases. As an example, consider the scenario where N_b and N_e both grow asymptotically large with respect to N_a, i.e., $\frac{N_b}{N_a} \to \infty$, $\frac{N_e}{N_a} \to \infty$, and $\frac{N_b}{N_e} \to 1$, while transmit powers and channel gains remain finite. It can be shown that $F(\beta, \alpha) \approx \log(\beta)$ as $\beta \to \infty$, whereas $F(1, \alpha) \approx \log(1+4\alpha) - 2 - \log(e)$ if $\beta \to 1$. Consequently, for the large-antenna regime we obtain

$$R_{A,E} \approx d\log\left(\frac{N_b}{d}\right) - N_a\log\left(\frac{N_e}{N_a}\right) + (N_a-d)\log\left(\frac{N_e}{N_a-d}\right) \quad (23)$$

$$R_{A,J} \approx (N_e+d)\log\left(1+4\left(\rho P_a\frac{N_a}{d} + g_2P_e\right)\right) - N_e\log(1+4g_2P_e) \quad (24)$$

$$R_{F,E} \approx N_a\log\left(\frac{N_b}{N_a}\right) - N_a\log\left(\frac{N_e}{N_a}\right) \quad (25)$$

$$R_{F,J} \approx N_e\log(1+4(P_a+g_2P_e)) - N_e\log(1+4g_2P_e). \quad (26)$$

The above expressions reinforce the belief that $R_{F,E} \le R_{A,E}$, and $R_{A,J} \le R_{F,J}$ which is always true for any antenna and power regime.

IV. STRATEGIC GAME

In this section we construct the zero-sum game model of the wiretap game by building upon the rate results derived in the previous section. Define the payoff to Alice as the achievable MIMO *secrecy rate* between her and Bob as defined in (5). Modeling the strategic interactions between Alice and Eve as a

strictly competitive simultaneous-move game leads to a zero-sum formulation, where Alice tries to maximize her payoff and Eve attempts to minimize it. We can define the following strategy sets X, Y for the players: Alice chooses between transmitting with full power for data (*F*) or devoting some power to jam Eve (*A*), described as $X = \{F, A\}$. On the other hand, Eve must decide between eavesdropping (*E*) or jamming Bob (*J*) at every channel use, represented by $Y = \{E, J\}$.

		Eve	
		Eavesdrop (E)	*Jam Bob (J)*
Alice	*Full Power (F)*	$R_{F,E}$	$R_{F,J}$
	Artificial Noise (A)	$R_{A,E}$	$R_{A,J}$

Fig. 2. Strategic form payoff matrix of the MIMO wiretap game.

A. Pure-strategy Equilibria

If we assume that both Alice and Eve move simultaneously without knowledge of the action taken by the other, the *strategic form* of the game can be represented by the 2×2 payoff matrix $\mathbf{R}$ in Fig. 2. In the sequel, for ease of exposition we assume $R_{F,E} \leq R_{F,J}$ holds even in the finite antenna regime, which is seen to be true for the specific examples simulated in Section V. The sequential or dynamic version of this game was considered by the authors in [26], and led to a different set of solution concepts, namely subgame-perfect and sequential equilibria.

Proposition 1: A single pure-strategy saddle-point or Nash Equilibrium (NE) with the outcome either as $R_{A,E}$ or $R_{F,J}$ exists in the proposed MIMO wiretap game, if and only if $R_{A,E} \leq R_{A,J}$.

Proof: Consider the game where Alice plays A and Eve plays J. From (16) it is trivial to see that Alice can unilaterally increase her payoff by devoting all her power to transmitting information, i.e., Alice has an incentive to switch to (F, J) since $R_{F,J}$ weakly dominates $R_{A,J}$. Subsequently, Eve has an incentive to switch from (F, J) to (F, E) if $R_{F,E} < R_{F,J}$, otherwise $R_{F,J}$ is the NE. However, if Eve switches from (F, J) to (F, E), Alice will prefer to switch to (A, E), since by definition $R_{A,E} \geq R_{F,E}$. Therefore the existence of a saddle-point in the pure strategy $R_{A,E}$ or $R_{F,J}$, depends on either $R_{A,E} \leq R_{A,J}$ or $R_{F,J} \leq R_{F,E}$ being true.

B. Mixed-strategy Equilibria

Proposition 1 establishes that there is no single strategy choice that is always optimal for either player depending upon the comparison between $R_{A,E}, R_{A,J}$ and $R_{F,J}, R_{F,E}$. Therefore, since the minimax theorem guarantees that any finite zero-sum game has a saddle-point in randomized strategies [**?**], in such a scenario Alice and Eve must randomize over $X \times Y$, i.e., adopt mixed strategies.

Let $\mathbf{p} = (p, 1-p)$ and $\mathbf{q} = (q, 1-q)$ represent the probabilities with which Alice and Eve randomize over their strategy sets $X = \{F, A\}$ and $Y = \{E, J\}$, respectively. Alice obtains her optimal strategy by solving

$$\max_{p} \min_{q} \mathbf{p}^T \mathbf{R} \mathbf{q}, \tag{27}$$

while Eve optimizes the corresponding minimax problem. For the payoff matrix $\mathbf{R}$ in Fig. 2, the optimal mixed strategies and expected value of the game can be easily derived as

$$\begin{aligned} (p*, 1-p*) &= (R_{A,J} - R_{A,E}, R_{F,E} - R_{F,J})/D \\ (q*, 1-q*) &= (R_{A,J} - R_{F,J}, R_{F,E} - R_{A,E})/D \\ v(p*, q*) &= (R_{F,E}R_{A,J} - R_{F,J}R_{A,E})/D, \end{aligned} \tag{28}$$

where $D = R_{F,E} + R_{A,J} - R_{F,J} - R_{A,E}$.

V. SIMULATION RESULTS

We present some examples that show the achieved secrecy rates for various array sizes and target performance levels. All displayed results are calculated based on an average of 3000 independent trials. For simplicity, the power allocated for artificial interference and the number of data streams is set to some pre-determined value in all scenarios tested. The background noise power was assumed to be the same for both Bob and Eve: $\sigma_b^2 = \sigma_e^2 = 1$. Eve's channel gains are set to $\sqrt{g_1} = 0.5, \sqrt{g_2} = 1.2$ to model the situation where the adversary is closer to Bob than to Alice. Since $R_{A,J}$ and $R_{F,J}$ approach zero as Eve's jamming power increases asymptotically, we constrain the ratio of the transmit powers as $0 < P_e/P_a \leqslant 10$ to avoid the trivial solution of Eve choosing to jam all the time.

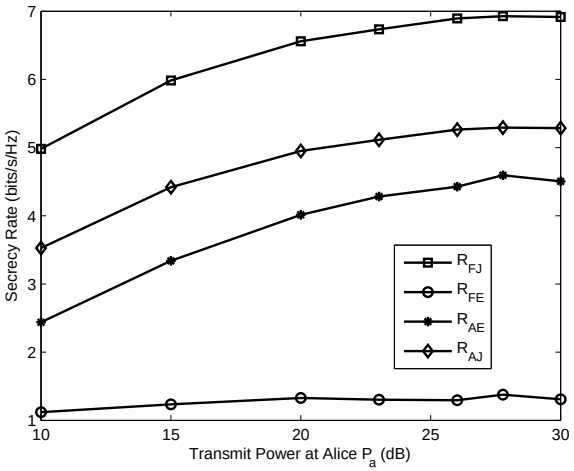

Fig. 3. $N_a = N_e = 4, N_b = 3, d = 2$.

For the strategic game where Eve is provided with a fixed proportion of Alice's transmit power $P_e = 0.25P_a$, and $N_a = N_e = 4, N_b = 3, d = 2$, the resultant pure-strategy saddle-point was observed to be $R_{A,E}$ as P_a varies. Since Eve's jamming power is less than or comparable to P_a in this case, the best she can do is to always eavesdrop, with Alice's optimal strategy being to always transmit artificial noise.

Next, we test the scenario where $N_a = N_e = 8, N_b = 6, d = 4$. If Eve's jamming power is increased relative to P_a, for e.g. if $P_e = 4P_a$, then a saddle-point in mixed strategies results in the strategic game as shown in Fig. 4. Randomizing over her strategies clearly leads to a larger payoff for Alice as Eve's jamming power increases.

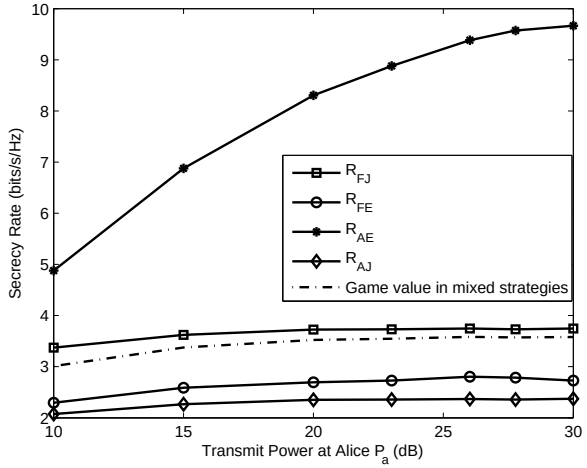

Fig. 4. $P_e = 4P_a$, $N_a = N_e = 8, N_b = 6, d = 4$.

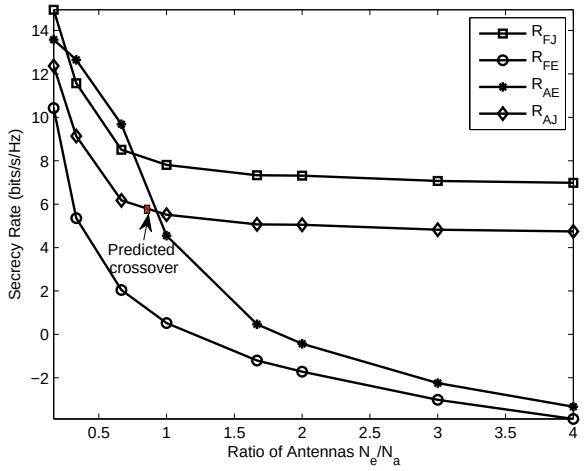

Fig. 5. Payoff versus antenna ratio N_e/N_a for fixed transmit powers $P_a = 100, P_e = 75$, and $N_a = 6, N_b = 3, d = 2$.

For the case of equal transmit powers $P_e = P_a = 100$, the outcomes of the strategic game as the ratio of eavesdropper to transmitter antennas varies is shown in Fig. 5. We observe that a similar threshold in terms of N_e/N_a exists (roughly at $N_e/N_a \approx 0.9$) to distinguish between a pure-strategy saddle-point and a mixed-strategy equilibrium. The theoretical crossover point of $N_e \approx 5$ for rates $R_{A,E}$ and $R_{A,J}$ is obtained by numerically evaluating the expressions in (12).

VI. CONCLUSION

This paper formulated the interactions between a transmitter and a dual-threat adversary capable of either eavesdropping or jamming as a zero-sum game with the MIMO secrecy rate as the payoff. We investigated the conditions for the existence of both pure and mixed-strategy Nash equilibria. It was shown that the jamming power or number of antennas available to the eavesdropper relative to the legitimate transmitter determines the eventual equilibrium outcome of the game.

REFERENCES

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

[2] S. L. Y. Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Intl Symp. on Inf. Theory*, pp. 524-528, July 2008.

[4] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, June 2009.

[5] A. Khisti and G. Wornell, "Secure transmission with multiple antennas II: the MIMOME wiretap channel", submitted to *IEEE Trans. Inf. Theory*, Aug. 2008. [Online]. Available: http://www.rle.mit.edu/sia/.

[6] W. E. Stark and R. J. McEliece, "On the capacity of channels with block memory," *IEEE Trans. Inf. Theory*, vol. 34, no. 3, pp. 322-324, Mar. 1988.

[7] M. Medard, "Capacity of correlated jamming channels," in *Proc. 35th Allerton Conf.*, pp. 1043-1052, 1997.

[8] A. Kashyap, 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.

[9] A. Bayesteh, M. Ansari, and A. K. Khandani, "Effect of jamming on the capacity of MIMO channels, in *Proc. 42nd Allerton Conf.*, pp. 401-410, Oct. 2004.

[10] S. Shafiee and S. Ulukus, "Mutual information games in multi-user channels with correlated jamming," submitted for publication, 2006. [Online]. Available: http://arxiv.org/abs/cs.IT/0601110.

[11] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," *IEEE Trans. Inform. Forensics Security*, vol. 3, no. 2, pp. 290-303, June 2008.

[12] S. Wei and R. Kannan, "Jamming and counter-measure strategies in parallel gaussian fading channels with channel state information," in *Proc. IEEE MILCOM*, San Diego, Nov. 2008.

[13] G. T. Amariucai, "Physical security in wireless networks: Intelligent jamming and eavesdropping," Ph.D. dissertation, LSU, 2009.

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

[15] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, pp. 2437-2440, Taipei, Apr. 2009.

[16] A. Mukherjee and A. L. Swindlehurst, "Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels," in *Proc. IEEE SPAWC*, pp. 344-348, Perugia, June 2009.

[17] X. Zhou and M. R. McKay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation", in *Proc. Int. Conf. on Sig. Proc. and Commun. Syst.*, Omaha, NE, Sept. 2009.

[18] E. Telatar, "Capacity of multi-antenna Gaussian channels," *European Trans. Telecommun.*, vol. 10, no. 6, pp. 585-596, 1999.

[19] A. M. Tulino and S. Verdu, "Random matrix theory and wireless communications," *Foundations and Trends in Communications and Information Theory*, vol. 1, no. 1, pp. 1-163, 2004.

[20] G. Alfano, A. M. Tulino, A. Lozano, and S. Verdu, "Eigenvalue statistics of finite-dimensional random matrices for MIMO wireless communication", in *Proc. IEEE ICC*, pp. 4125-4129, Istanbul, Turkey, June 2006.

[21] B. Hochwald, T.Marzetta and B. Hassibi, "Space-time autocoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2761-2781, Nov. 2001.

[22] A. Lozano and A. M. Tulino, "Capacity of multiple-transmit multiple-receive antenna architectures," *IEEE Trans. Inf. Theory*, vol. 48, no. 12, pp. 3117-3128, Dec. 2002.

[23] A. L. Moustakas, S. H. Simon, and A. M. Sengupta, "MIMO capacity through correlated channels in the presence of correlated interferers and noise: A (not so) large N analysis," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2545-2561, Oct. 2003.

[24] D. Fudenberg and J. Tirole, *Game Theory*. MIT Press, 1991.

[25] R. Myerson, *Game Theory: Analysis of Conflict*. Harvard University Press, 1997.

[26] A. Mukherjee and A. L. Swindlehurst, "Equilibrium outcomes of dynamic games in MIMO channels with active eavesdroppers," in *Proc. IEEE ICC*, Cape Town, South Africa, May 2010.