On the Gaussian MIMO Wiretap Channel

Ashish Khisti and Gregory Wornell
EECS Department, MIT,
Cambridge, MA 02139,
{khisti,gww}@mit.edu

Ami Wiesel and Yonina Eldar
EE Department, IIT,
Haifa, Israel 32000,
{amiw@tx,yonina@ee}.technion.ac.il

***Abstract*—**
Wyner's wiretap channel is generalized to the case when the sender, the receiver and the eavesdropper have multiple antennas. We consider two cases: the deterministic case and the fading case. In the deterministic case, the channel matrices of the intended receiver and the eavesdropper are fixed and known to all the nodes. In the fading case, the channel matrices experience block fading and the sender has only the intended receiver's channel state information (CSI) and statistical knowledge of the eavesdropper's channel. For the deterministic case, a scheme based on the generalized-singular-value-decomposition (GSVD) of the channel matrices is proposed and shown to achieve the secrecy capacity in the high signal-to-noise-ratio (SNR) limit. When the intended receiver has only one antenna (MISO case) the secrecy-capacity is characterized for any SNR. Next, a suboptimal "artificial noise" based scheme is considered. Its performance is characterized and observed to be nearly optimal in the high SNR regime for the MISO case. This scheme extends naturally to the fading case and results are reported for the MISO case. For the independent Rayleigh fading distribution as we simultaneously increase the number of antennas at the sender and the eavesdropper, the secrecy capacity approaches zero if and only if the ratio of the number of eavesdropper antennas to transmitter antennas is at least two.

I. Introduction

The wiretap channel introduced by Wyner [1] has potential applications in secret-key distribution over wireless links. In this paper, we study the Gaussian wiretap channel when the sender, the intended receiver and the eavesdropper have multiple antennas. Note that unlike the scalar case [2], our channel of interest is a non-degraded broadcast channel. A first natural attempt to characterize the secrecy capacity is to apply a result by Csiszár and Körner [3] who characterized the secrecy capacity for the non-degraded discrete memoryless wiretap channel (with transition probability $p(Y_r, Y_e|X)$)

$$C_s = \max_{p(U),X=f(U)} I(U;Y_r) - I(U;Y_e), \qquad (1)$$

where U is an auxiliary random variable over a certain alphabet and $f(\cdot)$ is a stochastic mapping from U to X. While the secrecy capacity (1) naturally extends to the continuous alphabet case, the optimal choice of U and $f(\cdot)$ are not clear a priori.

In the present paper, we develop an upper bound on the MIMO wiretap secrecy capacity, that enables us to characterize the secrecy capacity in the high signal-to-noise-ratio (SNR) limit for the general MIMO wiretap channel and at any SNR for the special case when the intended receiver has only one antenna (the MISO case). Perhaps more interestingly, the optimal capacity achieving scheme admits a geometrical interpretation. Suppose $H_r \in \mathbb{C}^{n_r \times n_t}$ and $H_e \in \mathbb{C}^{n_e \times n_t}$ denote the channel matrices of the intended receiver and the eavesdropper. An optimal strategy is to perform a generalized-singular-value-decomposition (GSVD) of the pencil (H_r, H_e) (see e.g., [4], [5]) to reduce the system into a set of parallel channels and then use an independent Gaussian wiretap codebook on the resulting channels. In the case of the MISO channel, the optimal scheme (at any SNR) is to beamform along the direction of the generalized eigenvector of the pencil $(I_t + PH_r^H H_r, I_t + PH_e^H H_e)$, where P denotes the SNR.

While the capacity achieving schemes require that the transmitter exploit the knowledge of both H_r and H_e, the knowledge of H_e may not be available to the transmitter in practice. Motivated by this consideration, we study an 'artificial noise" (AN) based scheme that does not require the knowledge of H_e. The proposed scheme performs a singular value decomposition of H_r, transmits information along the directions corresponding to non-zero singular values of H_r, and transmits artificial noise in the null space of H_r. We characterize the achievable rate and the associated loss with respect to the high SNR secrecy capacity. Somewhat surprisingly, the AN scheme is nearly optimal for the MISO case in the high SNR limit. Our analysis provides new insights into the artificial noise based scheme which was studied in [6] via monte-carlo simulations.

The AN scheme extends naturally to the block fading channels when only the intended receiver's channel state information (CSI) is known to the sender and statistical knowledge of the eavesdropper's channel is available. We provide an achievable rate expression for the MISO case. More interestingly, in the i.i.d. block Rayleigh fading MISO model, as we increase the number of antennas at the sender and the eavesdropper while keeping their ratio fixed, the secrecy capacity approaches zero if and only if the ratio of the number of eavesdropper antennas to transmitter antennas is at least two.

II. Channel Model

With the exception of Section VII, we focus on the *deterministic* Gaussian channel model

$$\begin{aligned} \mathbf{y}_r(t) &= H_r\mathbf{x}(t) + \mathbf{z}_r(t) \\ \mathbf{y}_e(t) &= H_e\mathbf{x}(t) + \mathbf{z}_e(t), \end{aligned} \qquad t = 1, 2, \ldots, N \qquad (2)$$

This work was supported in part by NSF under Grant No. CCF-0515109.

1-4244-1429-6/07/$25.00 ©2007 IEEE

where $H_r \in \mathbb{C}^{n_r \times n_t}$ and $H_e \in \mathbb{C}^{n_e \times n_t}$ are the deterministic channel matrices of the intended receiver and the eavesdropper. Note that in our model, the number of antennas at the transmitter, the intended receiver and the eavesdropper is denoted by n_t, n_r and n_e respectively. We assume that the noise vectors $\mathbf{z}_r(t)$ and $\mathbf{z}_e(t)$ have i.i.d. $\mathcal{CN}(0,1)$ components, and are independently sampled for each t. The input signal must satisfy an average power constraint $E[||\mathbf{X}||^2] \leq P$. A secrecy rate R is achievable if there exist a sequence of $(N, 2^{NR})$ codes such that for W uniformly distributed in the set $[1, 2, \ldots, 2^{NR}]$, the error probability at intended receiver approaches zero and the equivocation at the eavesdropper $\frac{1}{N}H(W|\mathbf{Y}_e^N)$ approaches $\frac{1}{N}H(W)$ as $N \to \infty$.

Throughout this paper, unless otherwise stated, we use the following notation: for a matrix M, M^H will denote the hermitian conjugate while $M^\dagger$ will denote its pseudo-inverse. The matrix $O_{p\times q}$ denotes a matrix of dimension $p \times q$ while all entries are zeros, while $\mathbf{0}_t$ denotes a zero column vector of length t. The matrix I_p denotes the $p \times p$ identity matrix. For convenience we will designate I_{n_r}, I_{n_t} and I_{n_e} by I_r, I_t and I_e respectively.

III. Upper Bound On Secrecy Capacity

We develop an expression for the upper bound on the secrecy capacity of the MIMO channel (2) which will be used to establish several results in the subsequent sections.

We define two sets: $\mathcal{K}_P \triangleq \{K_P | \mathrm{Tr}(K_P) \leq P, K_P \geq 0\}$ is the set of feasible input covariance matrices and $\mathcal{K}_\Phi \triangleq \left\{ K_\Phi \;\middle|\; K_\Phi = \begin{bmatrix} I_r & \Phi \\ \Phi^H & I_e \end{bmatrix}, K_\Phi \geq 0 \right\}$ is the set of admissible noise covariance matrices.

Theorem 1: An upper bound on the secrecy capacity for the MIMO channel model (2) is

$$R^+ = \min_{K_\Phi \in \mathcal{K}_\Phi} \max_{K_P \in \mathcal{K}_P} R^+(K_P, K_\Phi) = \max_{K_P \in \mathcal{K}_P} \min_{K_\Phi \in \mathcal{K}_\Phi} R^+(K_P, K_\Phi), \tag{3}$$

where $R^+(K_P, K_\Phi) \triangleq I(\mathbf{X}; \mathbf{Y}_r | \mathbf{Y}_e)$ is evaluated for $\mathbf{X} \sim \mathcal{CN}(0, K_P)$ and for a joint distribution of $(\mathbf{Z}_r, \mathbf{Z}_e)$, such that the vector $[\mathbf{Z}_r^H \mid \mathbf{Z}_e^H]^H \sim \mathcal{CN}(0, K_\Phi)$.

Proof Outline: We only sketch the main steps of the proof, which will be provided in [7]. First, following Wyner [1], an upper bound on secrecy capacity for any memoryless channel is $R_I^+ = \max_{p(\mathbf{X}) \in \mathcal{P}} I(\mathbf{X}; \mathbf{Y}_r | \mathbf{Y}_e)$, where $\mathcal{P}$ is the set of all feasible input distributions. We further tighten this bound by evaluating it for the worst-case joint distribution of $(\mathbf{Z}_r, \mathbf{Z}_e)$ in $\mathcal{K}_\Phi$ i.e., $R_{II}^+ = \min_{K_\Phi \in \mathcal{K}_\Phi} \max_{p(\mathbf{X}) \in \mathcal{P}} I(\mathbf{X}; \mathbf{Y}_r | \mathbf{Y}_e)$. Next it can be verified that for each K_Φ, the optimal $p(\mathbf{X})$ is Gaussian and hence it suffices to restrict the set $\mathcal{P}$ to Gaussian distributions. The resulting upper bound $R^+ = \min_{K_\Phi \in \mathcal{K}_\Phi} \max_{K_P \in \mathcal{K}_P} R^+(K_P, K_\Phi)$ provides the first half of (3). Furthermore, one can show using standard methods that $R^+(K_P, K_\Phi)$ is a convex function in K_Φ for each fixed K_P and concave in K_P for each fixed K_Φ. Since the sets $\mathcal{K}_\Phi$ and $\mathcal{K}_P$ are convex and compact, the minimax theorem establishes the existence of a saddle point and the order of maximization and minimization can be switched. ■

The following alternative representation of the upper bound in (3) is more convenient in our subsequent proofs.

Corollary 1: An upper bound on the secrecy capacity is

$$R^+ = \min_{K_\Phi \in \mathcal{K}_\Phi} \min_{F \in \mathbb{C}^{n_r \times n_e}} \max_{K_P \in \mathcal{K}_P} \log \frac{|I_r + FF^H - \Phi F^H - F\Phi^H + M|}{|K_\Phi|}, \quad \text{where} \quad M = (H_r - FH_e) K_P (H_r - FH_e)^H. \tag{4}$$

IV. GSVD based scheme

To provide our achievable scheme, it is convenient to introduce the GSVD (generalized singular value decomposition [4], [5]) of the pair (H_r, H_e). Intuitively, this transform decomposes the system into a set of parallel independent channels, which can then be encoded separately. This is analogous to the case of no eavesdropper, where the singular value decomposition (SVD) reduces the system into a set of parallel channels. The GSVD, unlike the SVD, is not unitary, and hence there is an associated power loss.

Definition 1 (GSVD): Given $H_r \in \mathbb{C}^{n_r \times n_t}$ and $H_e \in \mathbb{C}^{n_e \times n_t}$ there exist unitary matrices $\Psi_r \in \mathbb{C}^{n_r \times n_r}$, $\Psi_e \in \mathbb{C}^{n_e \times n_e}$ and $\Psi_t \in \mathbb{C}^{n_t \times n_t}$ and a non-singular lower-triangular[1] matrix $\Omega \in \mathbb{C}^{k \times k}$ with $k = \mathrm{rank}\{[H_r^H \mid H_e^H]^H\}$ such that

$$\Psi_r^H H_r \Psi_t = \Sigma_r [\Omega^{-1}, O_{k \times n_t - k}], \quad \Psi_e^H H_e \Psi_t = \Sigma_e [\Omega^{-1}, O_{k \times n_t - k}], \tag{5}$$

where Σ_r and Σ_e have the form

$$\Sigma_r = \begin{pmatrix} O_a & & \\ & D_r & \\ & & I_p \end{pmatrix}, \quad \Sigma_e = \begin{pmatrix} I_{k-p-s} & & \\ & D_e & \\ & & O_b \end{pmatrix}, \tag{6}$$

with $p = \dim(\mathrm{Null}(H_r)^\perp \cap \mathrm{Null}(H_e))$ and $s = \mathrm{rank}(H_r) - p$. The matrices O_a and O_b denote zero matrices with dimensions $(n_r - p - s \times k - p - s)$ and $(n_e + p - k \times p)$ and can be possibly void if either dimension is zero. Furthermore the matrices $D_r = \mathrm{diag}\{r_1, r_2, \ldots, r_s\}$ and $D_e = \mathrm{diag}\{e_1, e_2, \ldots, e_s\}$ are diagonal matrices such that $0 < r_1 \leq r_2, \ldots, \leq r_s < 1$ and $1 > e_1 \geq e_2 \ldots \geq e_s > 0$ and $r_j^2 + e_j^2 = 1$, for all $1 \leq j \leq s$. The (non-trivial) generalized singular values are defined as $\sigma_j = \frac{r_j}{e_j}$ with $0 < \sigma_1 \leq \sigma_2 \leq \ldots \leq \sigma_s < \infty$.

Theorem 2: The high SNR secrecy capacity of the MIMO wiretap channel is given by the following: If $\mathrm{Null}(H_r)^\perp \cap \mathrm{Null}(H_e) = \{\cdot\}$,

$$\lim_{P \to \infty} C^{\mathrm{MIMO}}(P) = \sum_{j: \sigma_j \geq 1} \log \sigma_j^2, \tag{7}$$

else, let $p = \dim\{\mathrm{Null}(H_e) \cap \mathrm{Null}(H_r)^\perp\} > 0$ then

$$C^{\mathrm{MIMO}}(P) = \sum_{j: \sigma_j \geq 1} \log \sigma_j^2 + \log \left| I_r + \frac{P}{p} H_r H_e^\perp H_r^H \right| + o(1), \tag{8}$$

where $o(1) \to 0$ as $P \to \infty$ and $H_e^\perp \in \mathbb{C}^{n_t \times n_t}$ is the projection matrix onto $\mathrm{Null}(H_e)$.

[1]The gsvd$(\cdot)$ command in MATLAB does not enforce a lower triangular structure on Ω but instead sets $\Psi_t = I_{n_t}$. However, it can be easily modified for our definition by performing the LQ decomposition of Ω^{-1}.

Remark 1: The dimension of the subspace $\mathcal{S}_d = \text{Null}(H_r)^\perp \cap \text{Null}(H_e)$ can be viewed as the number of degrees of freedom of the MIMO wiretap channel. Note that the secrecy capacity can be positive even when there are no available degrees of freedom. This distinction between zero capacity and having no degrees of freedom will also appear in the fading case, when the sender only has the intended receiver's CSI.

Remark 2: The result in Theorem 2 can also be used to establish the necessary and sufficient condition that the secrecy capacity is zero. In particular, for any $P > 0$, $C^{\text{MIMO}}(P) = 0$ if and only if (a) $\text{Null}(H_r)^\perp \cap \text{Null}(H_e) = \{\cdot\}$ and (b) $\sigma_j \leq 1$ for $j = 1, 2, \ldots, s$. Note that this remark provides a generalization of the condition for the scalar Gaussian case that the secrecy capacity is zero if and only if the eavesdropper's channel is noisier than the intended receiver's channel.

Remark 3: In the absence of an eavesdropper, i.e., when $H_e = O_{n_e \times n_t}$, our capacity expression reduces to $C^{\text{MIMO}}(P) = \log\left|I_r + \frac{P}{p} H_r H_r^H\right| + o(1)$, which is simply the high SNR MIMO capacity.

To establish the main ideas in the proof of Theorem 2 it is instructive to consider the case when H_e has a full column rank. The proof of the case when H_e does not have a full column rank is along the same lines, but requires us to exploit the lower triangular structure of Ω to explicitly characterize $H_r H_e^\perp$ via the GSVD and is provided in the full version [7].

Proof (Full rank case): When H_e has a full column rank, note that $p = 0$, $k = n_t$ and the expressions for Σ_r and Σ_e simplify as

$$\Sigma_r = \begin{pmatrix} O_{n_r - s \times n_t - s} & \\ & D_r \end{pmatrix}, \Sigma_e = \begin{pmatrix} I_{n_t - s} & \\ & D_e \\ & O_{n_e - n_t \times s} \end{pmatrix}. \tag{9}$$

It can be readily verified that

$$H_r H_e^\dagger = \Psi_r \begin{pmatrix} O_{n_r - s \times n_t - s} & O_{n_r - s \times s} & O_{n_r - s \times n_e - n_t} \\ O_{s \times n_t - s} & \Sigma & O_{s \times n_e - n_t} \end{pmatrix} \Psi_e^H \tag{10}$$

with $\Sigma = D_r D_e^{-1} = \text{diag}\{\sigma_1, \ldots, \sigma_s\}$. Note that the non-zero singular values of $H_r H_e^\dagger$ are also the generalized singular values of (H_r, H_e).

Achievability: To establish the achievability, we identify a particular choice of $\mathbf{U}$ and $\mathbf{X}$ in (1). Select random variables $U_\tau, U_{\tau+1}, \ldots, U_s$ i.i.d. $\mathcal{CN}(0, \alpha P)$ where τ is the smallest value of j such that $\sigma_j > 1$ and select $\alpha = \frac{1}{(s-\tau+1)||\Omega||_2^2}$ in order to satisfy $E[||\mathbf{X}||^2] \leq P$. Set $\mathbf{U} = [0, \ldots, 0, U_\tau, U_{\tau+1}, \ldots, U_s]^H$ and

$$\mathbf{X} = \Psi_t^H \Omega \begin{bmatrix} \mathbf{0}_{n_t - s} \\ \mathbf{U} \end{bmatrix}. \tag{11}$$

With these choice of parameters, we have

$$\mathbf{Y}_r = \Psi_r \begin{bmatrix} \mathbf{0}_{n_r - s} \\ D_r \mathbf{U} \end{bmatrix} + \mathbf{Z}_r, \quad \mathbf{Y}_e = \Psi_e \begin{bmatrix} \mathbf{0}_{n_t - s} \\ D_e \mathbf{U} \\ \mathbf{0}_{n_e - n_t} \end{bmatrix} + \mathbf{Z}_e. \tag{12}$$

Since Ψ_r and Ψ_e are unitary,

$$I(\mathbf{U}; \mathbf{Y}_r) - I(\mathbf{U}; \mathbf{Y}_e) = \sum_{j=\tau}^{s} \log \frac{1 + \alpha P r_j^2}{1 + \alpha P e_j^2} = \sum_{j=\tau}^{s} \log \sigma_j^2 - o(1), \tag{13}$$

where $o(1) \to 0$ as $P \to \infty$.

Converse: We select a specific choice of F and Φ in the upper bound expression in (4): select $F = H_r H_e^\dagger$ which gives $M = 0$ and (4) reduces to

$$R^+ = \min_{K_\Phi \in \mathcal{K}_\Phi} \log \frac{|I_r + FF^H - \Phi F^H - F\Phi^H|}{|I_r - \Phi\Phi^H|}, \quad F = H_r H_e^\dagger. \tag{14}$$

Recall that from (10) we can write $F = \Psi_r \Sigma_F \Psi_e^H$ and select $\Phi = \Psi_r \Delta_\phi \Psi_e^H$, where

$$\Delta_\phi = \begin{pmatrix} O_{n_r - s \times n_t - s} & O_{n_r - s \times s} & O_{n_r - s \times n_e - n_t} \\ O_{s \times n_t - s} & \Delta & O_{s \times n_e - n_t} \end{pmatrix}$$

and Δ is diagonal with $\Delta_{ii} = \min\left(\sigma_i, \frac{1}{\sigma_i}\right), \quad i = 1, 2, \ldots, s$. Our choice for Φ is clearly feasible and furthermore substituting in (14)

$$R^+ = \log \frac{|I_s + \Sigma^2 - 2\Sigma\Delta|}{|I_s - \Delta^2|} = \sum_{j:\sigma_j > 1} \log \sigma_j^2. \tag{15}$$

This establishes the converse for the full rank case. ■

V. MISO Case

We refer to the case when $n_r = 1$ as the MISO case. In this case, we characterize the secrecy capacity at any SNR. To emphasize this special case, we will denote the intended receiver's channel vector $\mathbf{h}_r^H$, i.e., (2) specializes to

$$\begin{aligned} y_r &= \mathbf{h}_r^H \mathbf{x} + z_r \\ \mathbf{y}_e &= H_e \mathbf{x} + \mathbf{z}_e. \end{aligned} \tag{16}$$

Theorem 3: The secrecy capacity of the channel (16) is given by:

$$C^{\text{MISO}}(P) = \left[\log \lambda_{\max}(I_t + P\mathbf{h}_r \mathbf{h}_r^H, I_t + P H_e^H H_e)\right]^+, \tag{17}$$

where $\lambda_{\max}(\cdot, \cdot)$ denotes the largest generalized eigenvalue of the pencil $(I + P\mathbf{h}_r\mathbf{h}_r^H, I + P H_e^H H_e)$. The capacity is obtained by beamforming along the direction of the generalized eigenvector of this pencil and using a scalar Gaussian wiretap code.

Achievability: The achievability follows by evaluating (1) for $\mathbf{X} = \mathbf{v}U$, where $U \sim \mathcal{CN}(0, P)$ and $\mathbf{v}$ is a generalized eigenvector of the pencil $(I + P\mathbf{h}_r\mathbf{h}_r^H, I + P H_e^H H_e)$ corresponding to $\lambda_{\max}(\cdot, \cdot)$.

Converse: In the MISO special case, the upper bound in Corollary 1 reduces to

$$\begin{aligned} R^+ &= \min_{\Phi, \theta} \max_{K_p} \log \frac{1 + ||\theta||^2 - 2\theta^H \Phi + M}{1 - ||\Phi||^2} \\ &= \min_{\Phi, \theta} \log \frac{1 + ||\theta||^2 - 2\theta^H \Phi + P||\mathbf{h}_r - H_e^H \theta||^2}{1 - ||\Phi||^2}, \end{aligned} \tag{18}$$

where the second equality follows from the fact that the maximum over K_p is attained for $K_p \propto (\mathbf{h}_r - H_e^H\theta)(\mathbf{h}_r - H_e^H\theta)^H$. For $\lambda_{\max}(\cdot,\cdot) > 1$, evaluating (18) for $\Phi = \frac{1}{\mathbf{h}_r^H\mathbf{v}} H_e\mathbf{v}$ and $\theta = \lambda_{\max}(\cdot,\cdot)\Phi$, we have that $R^+ \leq \log\lambda_{\max}(\cdot,\cdot)$ as required.

Remark 4: In the MISO case, beamforming is optimal at any SNR, and regardless of the number of eavesdropping antennas. However the beamforming direction depends on both $\mathbf{h}_r$ and H_e. In the high SNR regime the optimal direction approaches zero-forcing i.e., $H_e^\perp\mathbf{h}_r$ (whenever it is non-zero). In the low SNR regime, it approaches an eigenvector corresponding to the largest eigenvalue of $\mathbf{h}_r\mathbf{h}_r^H - H_e^H H_e$, and not the "matched-filtering" direction of $\mathbf{h}_r$.

We conclude with some Corollaries to Theorem 3.

Corollary 2: In the high SNR regime, the MISO secrecy capacity is given by:

$$C^{\text{MISO}}(P) = \begin{cases} \log\left(P||H_e^\perp\mathbf{h}_r||^2\right)] + o(1), & H_e^\perp\mathbf{h}_r \neq \mathbf{0}_{n_t}, \\ [\log\lambda_{\max}(\mathbf{h}_r\mathbf{h}_r^H, H_e^H H_e)]^+ + o(1) & \text{otherwise}, \end{cases} \tag{19}$$

where $o(1) \to 0$ as $P \to \infty$.

Corollary 3: In the low SNR regime, we have

$$\lim_{P\to 0} \frac{C^{\text{MISO}}(P)}{P} = \left[\lambda_{\max}(\mathbf{h}_r\mathbf{h}_r^H - H_e^H H_e)\right]^+. \tag{20}$$

VI. Artificial Noise based Scheme

The capacity achieving schemes in Theorem 2 and 3 use the knowledge of H_e for selecting the transmit directions. We study a suboptimal scheme where the transmit directions are chosen without the knowledge of H_e. The knowledge of H_e is used in selecting the rate however. This scheme readily generalizes to the ergodic fading channel model treated in the next section, where only the CSI of the intended receiver is available.

Our proposed scheme is as follows. Let $H_r = U_r\Upsilon V_r^H$ be the compact singular value decomposition of H_r i.e., with $d = \text{rank}(H_r)$, $\Upsilon \in R_+^{d\times d}$, while $U_r \in \mathbb{C}^{n_r\times d}$ and $V \in \mathbb{C}^{n_t\times d}$ have unitary columns. Let $V = [V_r \mid V_n]$ be a $n_t \times n_t$ unitary matrix and denote its columns by $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{n_t}$. Let $B_1, B_2, \ldots, B_{n_t}$ be i.i.d. $\mathcal{CN}(0, P_t)$ random variables with $P_t = P/n_t$. We set $U = (B_1, B_2, \ldots, B_d)$ and set

$$\mathbf{X} = \sum_{j=1}^{n_t} B_j\mathbf{v}_j. \tag{21}$$

Note that we can interpret the symbols $B_1, B_2, \ldots, B_d$ as information symbols, while the symbols $B_{d+1}, \ldots, B_{n_t}$ as "artificial noise".

Remark 5: The proposed scheme (21) has been studied in [6] in the context of MISO fading channels where the term artificial-noise has been coined. Their study is however based on monte-carlo simulations. To our knowledge, the present work is the first one to provide an analytical study of this scheme. By comparing the achievable rate for this scheme and with the secrecy capacity in Theorem 2, we can develop some new insights into these schemes.

We first establish an achievable rate for the artificial noise scheme by evaluating (1) for our choices of $\mathbf{U}$ and $\mathbf{X}$ in (21).

Proposition 1: Let $H_r = U_r\Upsilon V_r^H$ be the compact SVD representation of H_r. The achievable rate corresponding to the AN scheme is

$$R_{AN}(P) = \log\left|I_r + P_t H_r H_r^H\right| + \log\left|V_r^H\left(I_t + P_t H_e^H H_e\right)^{-1} V_r\right|, \tag{22}$$

where $P_t = P/n_t$.

Note that the expression in (22) captures the intuitive fact that the eavesdropper "projects" the received signal into the subspace of V_r. We next do a high SNR analysis of (22) to compare it with the capacity in Theorem 2.

Theorem 4: Suppose that H_r and H_e are such that $\text{rank}(H_r) = n_r$ and $\text{rank}(H_e) = \min(n_e, n_t)$. The achievable rate for the AN scheme in the high SNR limit is given as follows: If $\text{rank}(H_e) = n_t$, we have that

$$\lim_{P\to\infty} R_{\text{AN}}(P) = \sum_{j=1}^{s} \log\sigma_j^2, \tag{23}$$

otherwise if $\text{rank}(H_e) = n_e < n_t$ and $H_r H_e^\perp \neq O_{n_r\times n_t}$, then

$$R_{\text{AN}}(P) = \log\left|I_r + \frac{P}{n_t} H_r H_e^\perp H_r^H\right| + \sum_{j=1}^{s} \log\sigma_j^2 + o(1), \tag{24}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_s$ are the (non-trivial) generalized singular values of the pair (H_r, H_e) and $o(1) \to 0$ as $P \to \infty$.

The proof follows from a Taylor series expansion of (22). Note that one can also obtain qualitatively similar results when $\text{rank}(H_r) = n_t$. The technical constraint that the matrices be either full row rank or full column rank is satisfied with probability 1 if the entries of H_r and H_e are sampled from i.i.d. $\mathcal{CN}(0,1)$ distribution.

Remark 6: The expressions (23) and (24) for the achievable rate for the AN scheme in Theorem 4 can be easily compared with the corresponding expressions for the secrecy capacity in Theorem 2. The suboptimality of the artificial noise scheme is due to the fact that (23) and (24) include singular values which take value in $(0,1)$ and contribute negatively to the summation.

The AN scheme is nearly optimal for the MISO case.

Corollary 4: In the high SNR limit, the loss incurred by the AN scheme for the MISO case (16) is,

$$\lim_{P\to\infty} C^{\text{MISO}}(P) - R_{\text{AN}}^{\text{MISO}}(P) = \begin{cases} 0, & \text{rank}(H_e) = n_t, \\ \log n_t, & H_e^\perp\mathbf{h}_r \neq \mathbf{0}_{n_t}. \end{cases} \tag{25}$$

Remark 7: We provide example plots that compare the performance of $R_{AN}(P)$ with the capacity in Figure 1. In this example, we have randomly selected (real valued) $\mathbf{h}_r^T = [-0.5465, -0.8468, -0.2463]$, and $H_e = \begin{bmatrix} 0.6630 & -0.1199 & -0.5955 \\ -0.8542 & -0.0653 & -0.1497 \end{bmatrix}$ in the left plot and $H_e = \begin{bmatrix} 0.6630 & -0.1199 & -0.5955 \\ -0.8542 & -0.0653 & -0.1497 \\ -1.2013 & 0.4853 & -0.4348 \end{bmatrix}$ in the right plot. The

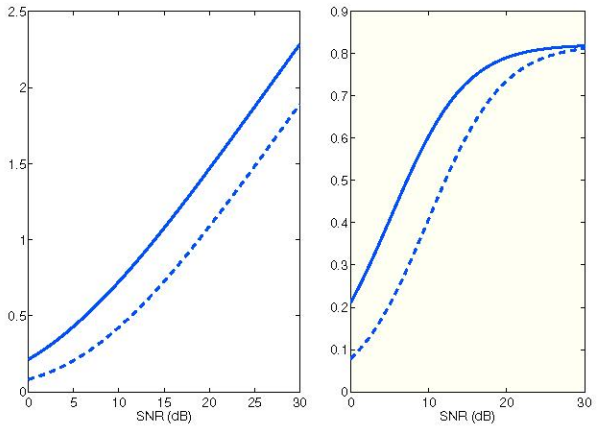

Fig. 1. Comparison of achievable secrecy rate for the artificial noise based scheme with the secrecy capacity. The dotted line is the rate for the AN scheme while the solid line is the capacity. The choices of the channel matrices are specified in the Remark 7.

right plot corresponds to the full rank case, while the left plot corresponds to the case when $H_e^{\perp}\mathbf{h}_r \neq 0$. The actual values of $\mathbf{h}_r$ and H_e do not affect the qualitative nature of the plots.

Remark 8: Corollary 4 reveals a rather unexpected fact that the knowledge of the eavesdropper's channel for beamforming does not provide dramatic gains at least in the high SNR limit. In particular, the AN scheme provides a rate of $C^{\mathrm{MISO}}(P/n_t)$ in the high SNR regime. Thus the price for not knowing the eavesdropper's channel is a multiplicative increase in the power. In this sense, the artificial noise scheme simulates transmission along the direction of optimal eigenvector by using additional power.

VII. Fading Channels

In this section we extend the model (2) to allow $H_r(t)$ and $H_e(t)$ to vary with time. We assume that the realization of $H_r(t)$ is known to the sender (and the receiver), while only the statistical characterization of $H_e(t)$ is available. The eavesdropper has access to both $H_e(t)$ and $H_r(t)$.

We study achievable rates for the block fading channel model i.e., the channel matrices $H_r(t)$ and $H_e(t)$ are constant for a duration of T symbols and change independently across coherence periods. In the limit of large coherence periods, the variable rate coding scheme in [8] can be naturally combined with the artificial noise based scheme. In what follows, we state our results only for the MISO case, but the extensions to the MIMO case are analogous.

Proposition 2: In the limit of large coherence period i.e., $T \to \infty$, an achievable rate for the MISO fading channel is given by

$$R_{AN}(P) = \max_{\{P(\mathbf{h}_r)\in\mathcal{P}\}} E[R_-(\mathbf{h}_r, H_e, P(\mathbf{h}_r))], \qquad (26)$$

where $\mathcal{P}$ is the set of all feasible power allocations that satisfy the average power constraint, and

$$R_-(\mathbf{h}_r, H_e, P(\mathbf{h}_r)) \triangleq \left[\log\lambda_{\max}\left(\frac{P(\mathbf{h}_r)}{n_t}\mathbf{h}_r\mathbf{h}_r^H, I + \frac{P(\mathbf{h}_r)}{n_t}H_e^H H_e\right) + \log\left(1+\frac{n_t}{P(\mathbf{h}_r)||\mathbf{h}_r||^2}\right)\right]^+. \qquad (27)$$

Furthermore in the high SNR regime if $n_e \geq n_t$, we have

$$\lim_{P\to\infty} R_{AN}(P) = E[[\log\lambda_{\max}(\mathbf{h}_r\mathbf{h}_r^H, H_e^H H_e)]^+].$$

and if $n_e < n_t$,

$$\lim_{P\to\infty}\left\{R_{AN}(P) - \log\frac{P}{n_t}\right\} = E[\log||H_e^{\perp}\mathbf{h}_r||^2].$$

The achievable rate in (27) depends only on the statistical distribution of $\mathbf{h}_r$ and H_e and naturally the secrecy capacity decreases as we increase n_e with n_t fixed.

Theorem 5: Suppose that $\mathbf{h}_r$ and H_e are sampled *independently* from a Rayleigh fading distribution. Consider the limit that $n_r \to \infty$ and $n_e \to \infty$ with $\frac{n_r}{n_e} = \beta$, held fixed. For any $\beta > 2$, the secrecy capacity approaches zero at any SNR. Conversely, for any $\beta < 2$ and sufficiently large SNR, the achievable rate for the artificial noise based scheme is positive.

Remark 9: Note that the rate $R_-(\mathbf{h}_r, H_e, P(\mathbf{h}_r))$ in (27) is non-negative. Accordingly, for any finite value of n_e the secrecy capacity is non-zero. However for any fixed n_t, as $n_e \to \infty$, observe that $R_-(\mathbf{h}_r, H_e, P(\mathbf{h}_r)) \to 0$ almost surely. Theorem 5 states that if we allow n_t to increase simultaneously with n_r then the ratio of n_t/n_r must be at least 1/2 for the secrecy capacity to remain positive as $n_e \to \infty$.

Remark 10: The requirement that $n_t > \frac{1}{2}n_e$ for the MISO secrecy capacity to be positive admits a simple intuitive explanation. In the artificial noise scheme, the sender will beamform to the intended receiver and transmit artificial noise in the remaining $n_t - 1$ directions. The eavesdropper will need $n_t - 1$ antennas to cancel the artificial noise and an additional n_t antennas to do receiver beamforming to enjoy the same signal strength as the intended receiver. Thus a total of $2n_t - 1$ will be required for the eavesdropper to be better than the intended receiver.

References

[1] A. D. Wyner, "The Wiretap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–87, 1975.
[2] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451–56, 1978.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339–348, 1978.
[4] C. Paige and M. A. Saunders, "Towards a generalized singular value decomposition," *SIAM J. Numer. Anal*, vol. 18, pp. 398–405, 1981.
[5] G. Golub and C. F. V. Loan, *Matrix Computations (3rd ed)*. Johns Hopkins University Press, 1996.
[6] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Vehicular Tech. Conf*, 2005.
[7] A. Khisti and G. W. Wornell, "Secure Transmission with Multiple Antennas," *In Preparation*.
[8] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, submitted, Oct., 2006.