Secrecy Capacity of the 2-2-1 Gaussian MIMO Wire-tap Channel

Shabnam Shafiee Nan Liu Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, Maryland 20742
sshafiee@umd.edu nkancy@umd.edu ulukus@umd.edu

***Abstract*—We find the secrecy capacity of the 2-2-1 Gaussian MIMO wire-tap channel, which consists of a transmitter and a receiver with two antennas each, and an eavesdropper with a single antenna. We determine the secrecy capacity of this channel by proposing an achievable scheme and then developing a tight upper bound that meets the proposed achievable secrecy rate. We show that, for this channel, Gaussian signalling in the form of beam-forming is optimal, and no pre-processing of information is necessary.**

I. Introduction

The inherent openness of wireless communications makes it vulnerable to eavesdropping and jamming attacks. This vulnerability has to be addressed through secure communications. The eavesdropping attack was first studied by Wyner in [1], where he considers a single-user wire-tap channel. The measure of secrecy is the message equivocation rate at the wire-tapper, which is defined as the entropy of the message at the wire-tapper, given the wire-tapper's observation. Wyner models the wire-tapper's channel as a degraded version of the channel from the transmitter to the legitimate receiver, which is a reasonable assumption in a wired channel. For this channel, Wyner identifies the rate-equivocation region and therefore, the secrecy capacity. Wyner's result was extended to the Gaussian wire-tap channel in [2], and it was shown that Gaussian signalling is optimal. The secrecy capacity was found to be the difference between the capacities of the main and the eavesdropping channels.

Csiszar and Korner [3] studied the general single-transmitter, single-receiver, single-eavesdropper, discrete memoryless channel with secrecy constraints, and found an expression for the secrecy capacity, in the form of the maximization of the difference between two mutual informations involving an auxiliary random variable. The auxiliary random variable is interpreted as performing pre-processing on the information. The explicit calculation of the secrecy capacity for a given channel requires the solution of this maximization problem in terms of the joint distribution of the auxiliary random variable and the channel input.

The use of multiple transmit and receive antennas has been shown to increase the achievable rates when there are no secrecy constraints [4]. The Gaussian multiple-input multiple-output (MIMO) wire-tap channel is a special case of the single-transmitter, single-receiver, single-eavesdropper wire-tap channel. Since the Gaussian MIMO channel is not degraded in general, finding its secrecy capacity involves identifying the optimum joint distribution of the auxiliary random variable representing pre-processing and the channel input in the Csiszar-Korner formula. However, solving this optimization problem directly for non-degraded channels is difficult, forcing researchers typically to follow a two-step solution, where in the first step a feasible solution is identified (an achievable scheme), and in the second step a tight upper bound that meets this feasible solution is developed (tight converse).

The first paper studying secrecy in MIMO communications is [5], which proposes an achievable scheme, where the transmitter uses its multiple transmit antennas to transmit only in the null space of the eavesdropper's channel, thereby preventing any eavesdropping. Reference [6] studies the Gaussian single-input multiple-output (SIMO) wire-tap channel, and shows that it is equivalent to a scalar Gaussian channel, and gives the secrecy capacity using the results of [2]. An achievable scheme has been proposed for the Gaussian multiple-input single-output (MISO) wire-tap channel in [7], and independently and concurrently in [8]. In both of these papers, the achievable secrecy rate is obtained by restricting the channel input to be Gaussian, with no pre-processing of information. The secrecy rate found in [7], [8] is shown to be the secrecy capacity of the Gaussian MISO wire-tap channel in [9], [10]. Further, [9], [10] allow the eavesdropper to have multiple antennas (MISOME).

In all of the above papers, the secrecy capacity of MIMO communications is specified only in the cases where the receiver has a single antenna. The next step towards finding the secrecy capacity of the general Gaussian MIMO channel is to consider multiple antennas at the receiver. In this paper, we consider a MIMO channel where both the transmitter and the receiver have multiple antennas. Since the general problem seems to be intractable for now, we focus on a simple special case where both the transmitter and the receiver have two antennas each, and the eavesdropper has a single antenna, hence we call this channel the 2-2-1 MIMO wire-tap channel. We find the secrecy capacity of this channel in two steps: we first propose an achievable scheme, which is a Gaussian signalling scheme with no pre-processing of information, and then, we develop a tight upper bound that meets the rate achieved with our proposed signalling scheme.

Secure communications in multi-user networks, e.g., multi-

ple access channel [11]–[15], broadcast channel [16], relay channel [17], [18], interference channel [19], and two-way channel [20], and in fading channels [7], [21]–[25] have been considered recently.

We use the following notations throughout this paper: Bold face lower and upper case letters are used to represent vectors and matrices, respectively. $\mathbf{x}^T$ and $||\mathbf{x}||$ denote the transpose and the Euclidean norm of the vector $\mathbf{x}$, respectively. $\text{tr}(\mathbf{X})$ and $|\mathbf{X}|$ denote the trace and the determinant of the square matrix $\mathbf{X}$, respectively. Whether a variable is deterministic or random will be clear from the context.

II. System Model

The 2-2-1 Gaussian MIMO wire-tap channel is characterized by

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}_y \tag{1}$$

$$z = \mathbf{g}^T\mathbf{x} + n_z \tag{2}$$

where $\mathbf{x}$ is the transmitted signal, and $\mathbf{y}$, z are the received signals at the legitimate user and the eavesdropper, respectively. $\mathbf{n}_y$ is a Gaussian random vector with zero-mean and identity covariance matrix, while n_z is a Gaussian random variable with zero-mean and unit-variance. $\mathbf{n}_y$, n_z are assumed to be independent. The transmitted signal satisfies an average power constraint,

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\mathbf{x}_i^T\mathbf{x}_i\right] \leq P \tag{3}$$

The secrecy capacity $C(P)$ is defined as the maximum number of bits that can be correctly transmitted to the intended receiver while the eavesdropper is essentially no better informed about the transmitted information after observing the received signal than it was before [2].

When $\mathbf{H}$ is not full-rank, by performing singular value decomposition (SVD) on $\mathbf{H}$ and obtaining an equivalent channel by rotation, it can be shown that the system is equivalent to a 2-1-1 system, whose secrecy capacity has been found in [9], [10]. Therefore, without loss of generality, for the rest of the paper, we assume that $\mathbf{H}$ is full-rank, and hence is invertible. When

$$\left\|\mathbf{H}^{-T}\mathbf{g}\right\| \leq 1 \tag{4}$$

z can be written as a noisy version of $\mathbf{y}$, i.e., $\mathbf{r}^T\mathbf{y} + n$, which means that the channel is degraded. In this case, no pre-processing of information is necessary [3], and also it can be shown that Gaussian signalling is optimal. Thus, in this paper, we concentrate on the more interesting and difficult case where $\mathbf{H}$ is full-rank and satisfies

$$\left\|\mathbf{H}^{-T}\mathbf{g}\right\| > 1 \tag{5}$$

III. An Achievable Scheme

By [3], the following secrecy rate is achievable,

$$[I(\mathbf{u};\mathbf{y}) - I(\mathbf{u};z)]^+ \tag{6}$$

where $\mathbf{u} \rightarrow \mathbf{x} \rightarrow \mathbf{y}z$. By taking $\mathbf{u} = \mathbf{x}$ and constraining the input signal $\mathbf{x}$ to be Gaussian with covariance matrix $\mathbf{S}$ such that $\text{tr}(\mathbf{S}) \leq P$, the following secrecy rate is achievable,

$$\left[\frac{1}{2}\log\left|\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T\right| - \frac{1}{2}\log(1 + \mathbf{g}^T\mathbf{S}\mathbf{g})\right]^+ \tag{7}$$

Thus, the following secrecy rate is achievable

$$\max_{\mathbf{S}\succeq\mathbf{0}:\text{tr}(\mathbf{S})\leq P} \quad \frac{1}{2}\log\left|\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T\right| - \frac{1}{2}\log(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}) \tag{8}$$

unless the maximum value in (8) is negative, in which case, the achieved secrecy rate is zero.

Ignoring the $1/2$, we may rewrite the cost function in (8) as

$$\log\left|\mathbf{I} + \mathbf{H}^T\mathbf{H}\mathbf{S}\right| - \log\left(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}\right) \tag{9}$$

We first use the following lemma to show that the $\mathbf{S}$ that maximizes (8) is unit-rank.

Lemma 1: If $\mathbf{D}$ is a 2×2 invertible matrix that satisfies

$$\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g} \geq 1 \tag{10}$$

then the optimal $\mathbf{S}$ that solves the following optimization problem

$$\max_{\mathbf{S}\succeq\mathbf{0},\text{tr}(\mathbf{S})\leq P} \quad \log|\mathbf{I} + \mathbf{D}\mathbf{S}| - \log\left(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}\right) \tag{11}$$

is unit-rank.

Proof: The KKT necessary conditions for the optimization problem in (11) are

$$\mathbf{S}^* \succeq \mathbf{0} \tag{12}$$

$$\text{tr}(\mathbf{S}^*) \leq P \tag{13}$$

$$\mathbf{C} \succeq \mathbf{0} \tag{14}$$

$$\lambda \geq 0 \tag{15}$$

$$\lambda(\text{tr}(\mathbf{S}^*) - P) = 0 \tag{16}$$

$$\mathbf{C}\mathbf{S}^* = \mathbf{0} \tag{17}$$

$$-(\mathbf{I} + \mathbf{D}\mathbf{S}^*)^{-1}\mathbf{D} + \frac{1}{1 + \mathbf{g}^T\mathbf{S}^*\mathbf{g}}\mathbf{g}\mathbf{g}^T - \mathbf{C} + \lambda\mathbf{I} = \mathbf{0} \tag{18}$$

We will prove the claim by contradiction. Assume that the optimal $\mathbf{S}$ is full-rank. Then, from (17), it follows that $\mathbf{C} = \mathbf{0}$, i.e, (18) becomes

$$(\mathbf{I} + \mathbf{D}\mathbf{S}^*)^{-1}\mathbf{D} = \frac{1}{1 + \mathbf{g}^T\mathbf{S}^*\mathbf{g}}\mathbf{g}\mathbf{g}^T + \lambda\mathbf{I} \tag{19}$$

Since $\mathbf{D}$ is invertible

$$(\mathbf{I} + \mathbf{D}\mathbf{S}^*)^{-1} = \frac{1}{1 + \mathbf{g}^T\mathbf{S}^*\mathbf{g}}\mathbf{g}\mathbf{g}^T\mathbf{D}^{-1} + \lambda\mathbf{D}^{-1} \tag{20}$$

Using the matrix inversion lemma [26, page 19], we have

$$\mathbf{I} + \mathbf{D}\mathbf{S}^* = \frac{1}{\lambda}\mathbf{D} - \frac{1}{\lambda^2 + \lambda^2\mathbf{g}^T\mathbf{S}^*\mathbf{g} + \lambda||\mathbf{g}||^2}\mathbf{D}\mathbf{g}\mathbf{g}^T \tag{21}$$

i.e.,

$$\mathbf{S}^* = \frac{1}{\lambda}\mathbf{I} - \frac{1}{\lambda^2 + \lambda^2\mathbf{g}^T\mathbf{S}^*\mathbf{g} + \lambda||\mathbf{g}||^2}\mathbf{g}\mathbf{g}^T - \mathbf{D}^{-1} \tag{22}$$

We multiply both sides of (22) with $\mathbf{g}^T$ on the left and $\mathbf{g}$ on the right. Let us define $\gamma = \mathbf{g}^T\mathbf{S}^*\mathbf{g}$, which is a non-negative real number. Then, we have

$$\gamma = \frac{||\mathbf{g}||^2}{\lambda} - \frac{||\mathbf{g}||^4}{\lambda^2 + \lambda^2\gamma + \lambda||\mathbf{g}||^2} - \mathbf{g}^T\mathbf{D}^{-1}\mathbf{g} \tag{23}$$

i.e., we have

$$\gamma^2 + \left(1 + \mathbf{g}^T\mathbf{D}^{-1}\mathbf{g}\right)\gamma + \mathbf{g}^T\mathbf{D}^{-1}\mathbf{g} + \frac{||\mathbf{g}||^2}{\lambda}\left(\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g} - 1\right) = 0 \tag{24}$$

Because $\mathbf{g}^T\mathbf{D}^{-1}\mathbf{g} - 1 \geq 0$, the second-order equation in (24) has no non-negative roots, i.e., it either has no real roots, or it has two negative roots. Thus, we arrive at a contradiction. Therefore, $\mathbf{C}$ cannot be equal to $\mathbf{0}$, and consequently, $\mathbf{S}$ cannot be full-rank, and it has to be unit-rank. ■

Since $\mathbf{H}^T\mathbf{H}$ is invertible and satisfies (5), $\mathbf{D} = \mathbf{H}^T\mathbf{H}$ satisfies the condition of Lemma 1. Hence, the optimal $\mathbf{S}$ for the optimization problem in (8) is unit-rank.

Given that the optimal $\mathbf{S}$ is unit-rank, it can be written as

$$\mathbf{S} = P\mathbf{q}\mathbf{q}^T \tag{25}$$

The corresponding achievable secrecy rate is

$$R = \frac{1}{2}\log\left|\mathbf{I} + P\mathbf{H}\mathbf{q}\mathbf{q}^T\mathbf{H}^T\right| - \frac{1}{2}\log(1 + P\mathbf{g}^T\mathbf{q}\mathbf{q}^T\mathbf{g}) \tag{26}$$

$$= \frac{1}{2}\log\frac{\mathbf{q}^T(\mathbf{I} + P\mathbf{H}^T\mathbf{H})\mathbf{q}}{\mathbf{q}^T(\mathbf{I} + P\mathbf{g}\mathbf{g}^T)\mathbf{q}} \tag{27}$$

where (27) is now in the Rayleigh quotient [26, page 176] form and the optimal achievable $\mathbf{q}$, which we will call $\mathbf{q}_a$, is

$$\mathbf{q}_a = \frac{\mathbf{B}^{-1/2}\mathbf{w}_a}{||\mathbf{B}^{-1/2}\mathbf{w}_a||} \tag{28}$$

where $\mathbf{w}_a$ is the eigenvector that corresponds to the largest eigenvalue of $\mathbf{B}^{-1/2}\mathbf{A}\mathbf{B}^{-1/2}$ with

$$\mathbf{A} = \mathbf{I} + P\mathbf{H}^T\mathbf{H} \tag{29}$$

$$\mathbf{B} = \mathbf{I} + P\mathbf{g}\mathbf{g}^T \tag{30}$$

In other words, $\mathbf{q}_a$ is the unit-norm eigenvector that satisfies

$$\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T\right)^{-1}\left(\mathbf{I} + P\mathbf{H}^T\mathbf{H}\right)\mathbf{q}_a = \lambda_1\mathbf{q}_a \tag{31}$$

where λ_1 is the largest eigenvalue of the matrix

$$\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T\right)^{-1/2}\left(\mathbf{I} + P\mathbf{H}^T\mathbf{H}\right)\left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T\right)^{-1/2} \tag{32}$$

Written explicitly, the achievable secrecy rate is

$$\frac{1}{2}\log\left(\frac{1 + P\mathbf{q}_a^T\mathbf{H}^T\mathbf{H}\mathbf{q}_a}{1 + P\mathbf{q}_a^T\mathbf{g}\mathbf{g}^T\mathbf{q}_a}\right) = \frac{1}{2}\log\lambda_1 \tag{33}$$

Next, we show that the secrecy rate in (33) is in fact strictly positive. By picking $\mathbf{S} = P\mathbf{g}^\perp\left(\mathbf{g}^\perp\right)^T$, where $\mathbf{g}^\perp$ is the unit-norm vector that is orthogonal to $\mathbf{g}$, an achievable secrecy rate is

$$\frac{1}{2}\log\left(1 + P\left\|\mathbf{H}\mathbf{g}^\perp\right\|^2\right) \tag{34}$$

Since $\mathbf{H}$ is full rank, $\mathbf{H}\mathbf{g}^\perp \neq \mathbf{0}$, i.e., the secrecy rate in (34) is strictly positive. Since the secrecy rate in (33) is the maximum over all $\mathbf{S}$ satisfying $\text{tr}(\mathbf{S}) \leq P$, we conclude that

$$\frac{1}{2}\log\lambda_1 \geq \frac{1}{2}\log\left(1 + P\left\|\mathbf{H}\mathbf{g}^\perp\right\|^2\right) > 0 \tag{35}$$

which also means that

$$\lambda_1 > 1 \tag{36}$$

IV. A Tight Upper Bound

The following theorem provides an upper bound on the secrecy capacity of the wire-tap channel described in (1) and (2).

Theorem 1: An upper bound on the secrecy capacity of the wire-tap channel described in (1) and (2) is

$$\max_{\mathbf{S}\succeq\mathbf{0},\text{tr}(\mathbf{S})\leq P} U(\mathbf{S}, \mathbf{a}) \tag{37}$$

for any $\mathbf{a}$ with $||\mathbf{a}|| < 1$, where $U(\mathbf{S}, \mathbf{a})$ is defined as

$$U(\mathbf{S}, \mathbf{a}) = \frac{1}{2}\log\frac{\left|\mathbf{I} + \mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{(1 + \mathbf{g}^T\mathbf{S}\mathbf{g})} \tag{38}$$

with $\mathbf{N}$ defined as

$$\mathbf{N} = \begin{bmatrix}\mathbf{I} & \mathbf{a} \\ \mathbf{a}^T & 1\end{bmatrix} \tag{39}$$

and $\bar{\mathbf{H}}$ defined as

$$\bar{\mathbf{H}} = \begin{bmatrix}\mathbf{H} \\ \mathbf{g}^T\end{bmatrix} \tag{40}$$

The proof of Theorem 1 is provided in the Appendix. Intuitively, this upper bound is obtained by considering the secrecy capacity of a new channel where the legitimate receiver also has access to the eavesdropper's signal. Since the legitimate user is more capable in the new channel, the secrecy capacity of the new channel will serve as an upper bound on the secrecy capacity of the original channel. The new channel is degraded, and therefore the secrecy capacity is easier to obtain.

The vector $\mathbf{a}$ introduced in Theorem 1 is the correlation between the Gaussian noises at the legitimate user and the eavesdropper, i.e., $\mathbf{a} = E[\mathbf{n}_y n_z]$. We note that $\mathbf{a}$ thus defined has to satisfy $||\mathbf{a}|| \leq 1$ for $\mathbf{N}$ in (39) to be positive semi-definite. Introducing correlation between $\mathbf{n}_y$ and n_z does not change the secrecy capacity of the channel, but changes the upper bound in (37). In fact, (37) remains a valid upper bound for any $\mathbf{a}$, with $||\mathbf{a}|| < 1$. Thus, we will smartly pick an $\mathbf{a}$ vector, and show that the upper bound with this $\mathbf{a}$ vector is in fact tight, to establish the secrecy capacity.

We rewrite $U(\mathbf{S}, \mathbf{a})$ as

$$U(\mathbf{S}, \mathbf{a}) = \frac{1}{2}\log\frac{\left|\mathbf{I} + \bar{\mathbf{H}}^T\mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\right|}{(1 + \mathbf{g}^T\mathbf{S}\mathbf{g})} \tag{41}$$

By the definition of $\mathbf{N}$ in (39), we have

$$\mathbf{N}^{-1} = \begin{bmatrix}\mathbf{I} + \frac{1}{k}\mathbf{a}\mathbf{a}^T & -\frac{1}{k}\mathbf{a} \\ -\frac{1}{k}\mathbf{a}^T & \frac{1}{k}\end{bmatrix} \tag{42}$$

where $k = 1 - ||\mathbf{a}||^2$. Then,

$$\bar{\mathbf{H}}^T \mathbf{N}^{-1} \bar{\mathbf{H}} = \mathbf{H}^T \mathbf{H} + \frac{1}{k} \left(\mathbf{H}^T \mathbf{a} - \mathbf{g} \right) \left(\mathbf{H}^T \mathbf{a} - \mathbf{g} \right)^T \quad (43)$$

Let us define $\mathbf{A}(\mathbf{a})$ as

$$\mathbf{A}(\mathbf{a}) = \bar{\mathbf{H}}^T \mathbf{N}^{-1} \bar{\mathbf{H}} = \mathbf{H}^T \mathbf{H} + \frac{1}{k} \left(\mathbf{H}^T \mathbf{a} - \mathbf{g} \right) \left(\mathbf{H}^T \mathbf{a} - \mathbf{g} \right)^T \quad (44)$$

Then, $U(\mathbf{S}, \mathbf{a})$ in (41) is written as

$$U(\mathbf{S}, \mathbf{a}) = \frac{1}{2} \log |\mathbf{I} + \mathbf{A}(\mathbf{a})\mathbf{S}| - \frac{1}{2} \log \left(1 + \mathbf{g}^T \mathbf{S} \mathbf{g} \right) \quad (45)$$

Let us also define $\mathbf{q}_a^\perp$ to be the unit-norm vector that is orthogonal to $\mathbf{q}_a$, which is defined in (28).

We pick $\mathbf{a}$ to be of the form

$$\mathbf{a} = \mathbf{H}^{-T} \left(\alpha \mathbf{q}_a^\perp + \mathbf{g} \right) \quad (46)$$

for any real number α that makes $||\mathbf{a}|| < 1$. $\alpha = 0$ results in $\mathbf{a} = \mathbf{H}^{-T}\mathbf{g}$, which is a vector with norm greater than 1, and therefore, is not permissible. Then, with this selection of $\mathbf{a}$, $\mathbf{A}(\mathbf{a})$ in (44) can be written as

$$\mathbf{A}(\mathbf{a}) = \mathbf{H}^T \mathbf{H} + \theta(\alpha) \mathbf{q}_a^\perp \left(\mathbf{q}_a^\perp \right)^T \quad (47)$$

where $\theta(\alpha)$ is defined as

$$\theta(\alpha) = \frac{\alpha^2}{1 - \mathbf{a}^T \mathbf{a}} \quad (48)$$

$$= \frac{\alpha^2}{1 - \left(\mathbf{H}^{-T} \left(\alpha \mathbf{q}_a^\perp + \mathbf{g} \right) \right)^T \left(\mathbf{H}^{-T} \left(\alpha \mathbf{q}_a^\perp + \mathbf{g} \right) \right)} \quad (49)$$

Then, we have

$$\frac{1}{\theta(\alpha)} = - \left(\mathbf{q}_a^\perp \right)^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp - \frac{2 \mathbf{g}^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp}{\alpha} - \frac{\mathbf{g}^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{g} - 1}{\alpha^2} \quad (50)$$

This is a second-order polynomial in terms of $1/\alpha$, and it is easy to see that $1/\alpha^*$ maximizes $\theta(\alpha)$, with

$$\frac{1}{\alpha^*} = \frac{\mathbf{g}^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp}{1 - \mathbf{g}^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{g}} \quad (51)$$

Finally, we call the $\mathbf{a}$ vector that we pick $\mathbf{a}^*$, which is given as

$$\mathbf{a}^* = \mathbf{H}^{-T} \left(\alpha^* \mathbf{q}_a^\perp + \mathbf{g} \right) \quad (52)$$

First, we will prove that $\mathbf{a}^*$ has norm no greater than 1. Let us define $\mathbf{a}_0$ to be

$$\mathbf{a}_0 = \frac{\mathbf{g}^T \mathbf{q}_a}{||\mathbf{H}\mathbf{q}_a||^2} \mathbf{H} \mathbf{q}_a \quad (53)$$

$\mathbf{a}_0$ satisfies the form of $\mathbf{a}$ in (46) because $\mathbf{H}^T \mathbf{a}_0 - \mathbf{g}$ is orthogonal to $\mathbf{q}_a$, hence, it is along the direction of $\mathbf{q}_a^\perp$. Therefore, $\mathbf{a}_0$ must correspond to an α, which we call α_0. It can be seen that

$$||\mathbf{a}_0|| = \frac{\left| \mathbf{g}^T \mathbf{q}_a \right|}{||\mathbf{H}\mathbf{q}_a||} < 1 \quad (54)$$

because of (36) and the fact that $\mathbf{q}_a$ satisfies (33), i.e.,

$$1 < \lambda_1 = \frac{1 + P||\mathbf{H}\mathbf{q}_a||^2}{1 + P(\mathbf{g}^T \mathbf{q}_a)^2} \quad (55)$$

Hence, $||\mathbf{a}_0|| < 1$ means that $\alpha_0 \neq 0$ and furthermore, we have

$$\theta(\alpha_0) = \frac{\alpha_0^2}{1 - \mathbf{a}_0^T \mathbf{a}_0} > 0 \quad (56)$$

Therefore, we have

$$\frac{1}{\theta(\alpha^*)} \overset{(a)}{\geq} \frac{1}{\theta(\alpha_0)} > 0 \quad (57)$$

where (a) follows because α^* maximizes $\frac{1}{\theta(\alpha^*)}$. Finally, (57) implies $||\mathbf{a}^*|| < 1$ because of (48).

Next, we will show that the optimal $\mathbf{S}$ for $\max U(\mathbf{S}, \mathbf{a}^*)$ in (37) is unit-rank. Since the upper bound and achievable scheme differ only in replacing $\mathbf{A}(\mathbf{a}^*)$ with $\mathbf{H}^T\mathbf{H}$, as shown in (8) and (45), we will use Lemma 1 again to show the optimality of unit-rank $\mathbf{S}$ in (37). Since $\mathbf{H}^T\mathbf{H}$ is invertible and $\theta(\alpha^*) > 0$, matrix $\mathbf{A}(\mathbf{a}^*)$, in the form of (47), is invertible. In addition, in order to use Lemma 1, we need $\mathbf{g}^T \mathbf{A}(\mathbf{a}^*)^{-1} \mathbf{g} \geq 1$. In the following, we will show that $\mathbf{g}^T \mathbf{A}(\mathbf{a}^*)^{-1} \mathbf{g} = 1$. Using the matrix inversion lemma [26, page 19] on (47), we have

$$\mathbf{A}(\mathbf{a}^*)^{-1} = \left(\mathbf{H}^T \mathbf{H} \right)^{-1} - \frac{1}{\frac{1}{\theta(\alpha^*)} + \left(\mathbf{q}_a^\perp \right)^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp} \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp \left(\mathbf{q}_a^\perp \right)^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \quad (58)$$

Also, from (50) and (51), $1/\theta(\alpha^*)$ is equal to

$$\frac{1}{\theta(\alpha^*)} = - \left(\mathbf{q}_a^\perp \right)^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp + \frac{\left(\mathbf{g}^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{q}_a^\perp \right)^2}{\mathbf{g}^T \left(\mathbf{H}^T \mathbf{H} \right)^{-1} \mathbf{g} - 1} \quad (59)$$

$$= - \left(\mathbf{q}_a^\perp \right)^T \left(\mathbf{H}^T \mathbf{H} - \mathbf{g}\mathbf{g}^T \right)^{-1} \mathbf{q}_a^\perp \quad (60)$$

Now, using straightforward algebra, starting from (58) and (59), it is easy to verify that $\mathbf{g}^T \mathbf{A}(\mathbf{a}^*)^{-1} \mathbf{g} = 1$. Thus, $\mathbf{D} = \mathbf{A}(\mathbf{a}^*)$ satisfies the conditions of Lemma 1, and therefore, $\arg\max U(\mathbf{S}, \mathbf{a}^*)$ is unit-rank.

Thus, for the selected $\mathbf{a}^*$, the optimization in the upper bound in (37) over $\mathbf{S} \succeq \mathbf{0}$ reduces to an optimization over $\mathbf{q}$, as $\mathbf{S} = P\mathbf{q}\mathbf{q}^T$,

$$\max_{\mathbf{S} \succeq \mathbf{0}, \mathrm{tr}(\mathbf{S}) \leq P} U(\mathbf{S}, \mathbf{a}^*) = \max_{\mathbf{q}} \frac{1}{2} \log \frac{\mathbf{q}^T \left(\mathbf{I} + P\mathbf{H}^T\mathbf{H} + P\theta(\alpha^*) \mathbf{q}_a^\perp \left(\mathbf{q}_a^\perp \right)^T \right) \mathbf{q}}{\mathbf{q}^T \left(\mathbf{I} + P\mathbf{g}\mathbf{g}^T \right) \mathbf{q}} \quad (61)$$

where (61) is again in the Rayleigh quotient [26, page 176] form. With $\mathbf{B}$ defined as in (30), the solution to this optimiza-

tion problem is the largest eigenvalue of the matrix

$$\mathbf{B}^{-1/2}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T\right)\mathbf{B}^{-1/2} \quad (62)$$

which is the largest eigenvalue of the matrix

$$\mathbf{B}^{-1}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T\right) \quad (63)$$

since the two matrices are related by a similarity transformation. Note that

$$\begin{aligned}\mathbf{B}^{-1}&\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T\right)\mathbf{q}_a\\ &=\mathbf{B}^{-1}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}\right)\mathbf{q}_a=\lambda_1\mathbf{q}_a \quad (64)\end{aligned}$$

where the last equality of (64) follows from (31).

Let us define vector $\mathbf{q}_1$ as

$$\mathbf{q}_1=-\theta(\alpha^*)\left(\mathbf{H}^T\mathbf{H}-\mathbf{g}\mathbf{g}^T\right)^{-1}\mathbf{q}_a^{\perp} \quad (65)$$

Note that

$$\mathbf{q}_1^T\mathbf{q}_a^{\perp}=-\theta(\alpha^*)\left(\mathbf{q}_a^{\perp}\right)^T\left(\mathbf{H}^T\mathbf{H}-\mathbf{g}\mathbf{g}^T\right)^{-1}\mathbf{q}_a^{\perp}=1 \quad (66)$$

where the last equality follows from (60). Also, (65) implies that

$$\mathbf{H}^T\mathbf{H}\mathbf{q}_1=\mathbf{g}\mathbf{g}^T\mathbf{q}_1-\theta(\alpha^*)\mathbf{q}_a^{\perp} \quad (67)$$

Then, we have

$$\begin{aligned}&\mathbf{B}^{-1}\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\left(\mathbf{q}_a^{\perp}\right)^T\right)\mathbf{q}_1\\ &=\mathbf{B}^{-1}\left(\left(\mathbf{I}+P\mathbf{H}^T\mathbf{H}\right)\mathbf{q}_1+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\right) \quad (68)\\ &=\mathbf{B}^{-1}\left(\mathbf{q}_1+P\mathbf{g}\mathbf{g}^T\mathbf{q}_1-P\theta(\alpha^*)\mathbf{q}_a^{\perp}+P\theta(\alpha^*)\mathbf{q}_a^{\perp}\right) \quad (69)\\ &=\mathbf{B}^{-1}(\mathbf{I}+P\mathbf{g}\mathbf{g}^T)\mathbf{q}_1 \quad (70)\\ &=\mathbf{q}_1 \quad (71)\end{aligned}$$

where (68) follows from (66), and (69) follows from (67). This means that the eigenvalues of the matrix in (63), and also the eigenvalues of the matrix in (62), are λ_1 and 1. Since $\lambda_1>1$, as shown in (36), the resulting maximum value in (61) is $\frac{1}{2}\log\lambda_1$. Hence, the upper bound on the secrecy capacity, i.e.,$\max_{\mathbf{S}\succeq\mathbf{0},\mathrm{tr}(\mathbf{S})\leq P}U(\mathbf{S},\mathbf{a}^*)$, is $\frac{1}{2}\log\lambda_1$, which is equal to the lower bound on the secrecy capacity shown in (33).

V. Conclusion

We determined the secrecy capacity of the 2-2-1 Gaussian MIMO wire-tap channel. First, we proposed a lower bound by evaluating the Csiszar-Korner formula based on Gaussian signalling and no pre-processing of information. A closed form solution for the resulting secrecy rate does not exist. However, in our 2-2-1 case, we have shown that the optimal transmission scheme is unit-rank, i.e., beam-forming is optimal.

Then, we showed the optimality of the proposed achievable scheme by constructing a tight upper bound that meets it. The upper bound is developed by considering the secrecy capacity of a channel where the eavesdropper's signal is given to the legitimate receiver. Even though this upper bound is well-defined for a general MIMO wire-tap channel, explicit evaluation and tightening of this upper bound has been possible by restricting ourselves to the 2-2-1 case. As in the lower-bound, and by selecting a certain correlation structure for the additive noises, we have shown that beam-forming is optimal for the upper bound as well. Furthermore, we have shown that the optimal beam-forming directions in the lower and upper bounds are the same. Finally, we have shown that the two bounds meet yielding the secrecy capacity.

The results presented in this paper are a non-trivial step towards the solution of the general MIMO wire-tap problem. Whether our techniques can be useful in determining the secrecy capacity of larger MIMO systems is unclear.

Acknowledgment

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

VI. Appendix

Proof of Theorem 1: A proof of similar results is presented for the case of m-1-n system, $m,n\geq 1$, in [10, Lemmas 1, 2]. Our proof utilizes [10, Lemma 1], which generalizes to the case of multiple antennas at the legitimate receiver easily, and extends [10, Lemma 2] to the case where there are two antennas at the legitimate receiver.

An upper bound on the secrecy capacity of the wire-tap channel described in (1) and (2) is [10, Lemma 1]

$$\max_{p(\mathbf{x}):E[\mathbf{x}^T\mathbf{x}]\leq P} I(\mathbf{x};\mathbf{y}|z) \quad (72)$$

Since we have

$$I(\mathbf{x};\mathbf{y}|z)=I(\mathbf{x};\mathbf{y},z)-I(\mathbf{x};z) \quad (73)$$

intuitively, the upper bound is obtained by considering the secrecy capacity of a new channel where the legitimate receiver also has access to the eavesdropper's signal. Since the legitimate user is more capable in the new channel, the secrecy capacity of the new channel will serve as an upper bound on the secrecy capacity of the original channel. The new channel is degraded, and therefore the secrecy capacity formula is (73), obtained by setting $\mathbf{u}=\mathbf{x}$ as shown in [3].

In evaluating the right-hand side of (72), we introduce correlation between $\mathbf{n}_y$ and n_z, i.e., let us define $\mathbf{a}$ to be

$$\mathbf{a}=E[\mathbf{n}_y n_z] \quad (74)$$

We note that $\mathbf{a}$ thus defined has to satisfy $||\mathbf{a}||\leq 1$. To avoid irregular cases, we will only consider $\mathbf{a}$ such that $||\mathbf{a}||<1$. We also note that $\mathbf{a}$ does not affect the secrecy capacity of the original channel, but it affects the upper bound in (72). Thus, (72) remains an upper bound for any $\mathbf{a}$ with $||\mathbf{a}||<1$.

We evaluate $I(\mathbf{x};\mathbf{y}|z)$ as follows,

$$\begin{aligned}I(\mathbf{x};\mathbf{y}|z)&=h(\mathbf{y}|z)-h(\mathbf{y}|z,\mathbf{x}) \quad (75)\\ &=h(\mathbf{y}|z)-h(\mathbf{n}_y|n_z) \quad (76)\end{aligned}$$

Due to the Gaussianity of the noise,

$$h(\mathbf{n}_y|n_z)=h(\mathbf{n}_y,n_z)-h(n_z)=\frac{1}{2}\log(2\pi e)^2|\mathbf{N}| \quad (77)$$

where $\mathbf{N}$ is defined as in (39). Let us define $\mathbf{S}$ as

$$\mathbf{S} = E[\mathbf{x}\mathbf{x}^T] \tag{78}$$

then

$$E[\mathbf{y}z] = E\left[(\mathbf{H}\mathbf{x} + \mathbf{n}_y)\left(\mathbf{x}^T\mathbf{g} + n_z\right)\right] = \mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a} \tag{79}$$

$$E[z^2] = 1 + \mathbf{g}^T\mathbf{S}\mathbf{g} \tag{80}$$

$$E[\mathbf{y}\mathbf{y}^T] = \mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T \tag{81}$$

The linear minimum mean squared error (LMMSE) estimator of $\mathbf{y}$ using z is

$$\hat{\mathbf{y}} = \frac{\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} z \tag{82}$$

and the resulting covariance matrix of the estimation error is

$$\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T - \frac{1}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} \left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)^T \tag{83}$$

Hence,

$$\begin{aligned}
&h(\mathbf{y}|z) \\
&= h\left(\mathbf{y} - \frac{\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} z \middle| z\right) && (84)\\
&\le h\left(\mathbf{y} - \frac{\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} z\right) && (85)\\
&\le \frac{1}{2}\log(2\pi e)^2 \\
&\quad \left|\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T \frac{1}{1 + \mathbf{g}^T\mathbf{S}\mathbf{g}} \left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)^T\right| && (86)
\end{aligned}$$

Therefore,

$$\begin{aligned}
&I(\mathbf{x}; \mathbf{y}|z) \\
&\le \frac{1}{2}\log \frac{\left|\mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T - \frac{1}{1+\mathbf{g}^T\mathbf{S}\mathbf{g}} \left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)\left(\mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a}\right)^T\right|}{|\mathbf{N}|} && (87)\\
&= \frac{1}{2}\log \frac{\left|\begin{bmatrix} \mathbf{I} + \mathbf{H}\mathbf{S}\mathbf{H}^T & \mathbf{H}\mathbf{S}\mathbf{g} + \mathbf{a} \\ \mathbf{g}^T\mathbf{S}\mathbf{H}^T + \mathbf{a}^T & 1 + \mathbf{g}^T\mathbf{S}\mathbf{g} \end{bmatrix}\right|}{\left(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}\right)|\mathbf{N}|} && (88)\\
&= \frac{1}{2}\log \frac{\left|\mathbf{N} + \bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{\left(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}\right)|\mathbf{N}|} && (89)\\
&= \frac{1}{2}\log \frac{\left|\mathbf{I} + \mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{\left(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}\right)} && (90)
\end{aligned}$$

where $\bar{\mathbf{H}}$ is defined as in (40). Thus, we have

$$\begin{aligned}
&\max_{p(\mathbf{x}): E[\mathbf{x}^T\mathbf{x}] \le P} \quad I(\mathbf{x}; \mathbf{y}|z) \\
&\qquad \le \max_{\mathbf{S} \succeq \mathbf{0}, \mathrm{tr}(\mathbf{S}) \le P} \quad \frac{1}{2}\log \frac{\left|\mathbf{I} + \mathbf{N}^{-1}\bar{\mathbf{H}}\mathbf{S}\bar{\mathbf{H}}^T\right|}{\left(1 + \mathbf{g}^T\mathbf{S}\mathbf{g}\right)} && (91)
\end{aligned}$$

Therefore, an upper bound on the secrecy capacity of the wiretap channel described in (1) and (2) is

$$\max_{\mathbf{S} \succeq \mathbf{0}, \mathrm{tr}(\mathbf{S}) \le P} U(\mathbf{S}, \mathbf{a}) \tag{92}$$

for any $\mathbf{a}$ with $||\mathbf{a}|| < 1$, with $U(\mathbf{S}, \mathbf{a})$ defined in (38).

REFERENCES

[1] A. D. Wyner. The wire-tap channel. *Bell Syst. Tech. J.*, 54(8):2–10, October 1975.

[2] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. on Information Theory*, 24(4):451–456, July 1978.

[3] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Information Theory*, 24(3):339–348, May 1978.

[4] I. E. Telatar. Capacity of multi-antenna Gaussian channels. *European Trans. Telecommunications*, 10:585–595, November 1999.

[5] R. Negi and S. Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, Toulouse, France, May 2006.

[6] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005.

[7] S. Shafiee and S. Ulukus. Achievable rates in Gaussian MISO channels with secrecy constraints. In *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[8] Z. Li, W. Trappe, and R. D. Yates. Secret communication via multi-antenna transmission. In *41st Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[9] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar. On the Gaussian MIMO wiretap channel. In *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[10] A. Khisti and G. Wornell. Secure transmission with multiple antennas: The MISOME wiretap channel. *Submitted to IEEE Trans. on Information Theory*.

[11] Y. Liang and H. V. Poor. Generalized multiple access channels with confidential messages. *Submitted to IEEE Trans. on Information Theory*.

[12] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.

[13] E. Tekin and A. Yener. Achievable rates for the general Gaussian multiple access wire-tap channel with collective secrecy. In *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2006.

[14] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *Submitted to IEEE Trans. on Information Theory*.

[15] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *IEEE Information Theory Workshop on Frontiers in Coding Theory*, Lake Tahoe, CA, September 2007.

[16] R. Liu and H. V. Poor. Multiple antenna secure broadcast over wireless networks. In *First International Workshop on Information Theory for Sensor Networks*, Santa Fe, NM, June 2007.

[17] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *Submitted to IEEE Trans. on Information Theory*.

[18] Y. Oohama. Relay channels with confidential messages. *Submitted to IEEE Trans. on Information Theory, Special Issue on Information Theoretic Security*.

[19] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *Submitted to IEEE Trans. on Information Theory, Special Issue on Information Theoretic Security*.

[20] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *Submitted to IEEE Trans. on Information Theory*.

[21] J. Barros and M. R. D. Rodrigues. Secrecy capacity of wireless channels. In *IEEE International Symposium on Information Theory*, Seattle, WA, July 2006.

[22] Y. Liang, H. V. Poor, and S. Shamai. Secure communication over fading channels. *Submitted to IEEE Trans. on Information Theory, Special Issue on Information Theoretic Security*.

[23] Z. Li, R. D. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *44th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, September 2006.

[24] P. K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *Submitted to IEEE Trans. on Information Theory*.

[25] Z. Li, R. D. Yates, and W. Trappe. Secure communication with a fading eavesdropper channel. In *IEEE International Symposium on Information Theory*, Nice, France, June 2007.

[26] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1999.