Achievable Rates in Gaussian MISO Channels with Secrecy Constraints

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

***Abstract*—A Gaussian MISO (multiple input single output) channel is considered where a transmitter is communicating to a receiver in the presence of an eavesdropper. The transmitter is equipped with multiple antennas, while the receiver and the eavesdropper each have a single antenna. The transmitter maximizes the communication rate, while concealing the message from the eavesdropper. The channel input is restricted to Gaussian signalling, with no preprocessing of information. For these channel inputs, and under different channel fading assumptions, optimal transmission strategies are found, in terms of the input covariance matrices. It is shown that, the optimal communication strategy in all cases, is beamforming.**

I. Introduction

The inherent openness of wireless communication calls for careful security considerations. Information theoretic security of wireless channels has received a great deal of attention recently, and different wireless channel models and their security limits have been extensively studied. The basic model used in these studies is introduced by Wyner [1], where he considers a wire-tap single user 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. The wire-tapping channel is assumed to be a degraded version of the channel from the sender to the legitimate receiver. This is in fact a reasonable assumption in a wired channel.

In [2], Wyner's model is generalized to a broadcast channel in which a common message is transmitted to two users while a private message is transmitted to only one of the users, and the other user should be kept as ignorant of this private message as possible. Here, the channels to the two users are not degraded versions of each other. Capacity-equivocation region for this channel is specified. When the user's channel is "more capable" compared to the eavesdropping channel, it is shown that the capacity-equivocation region is as Wyner's.

Scalar Gaussian wire-tap channel is considered in [3], and its capacity-equivocation region is characterized. Secrecy in multiple access channels (MAC) is studied in [4], [5] and [6]. In [4], a generalized MAC is considered, where the users can listen to the channel. Each user has private, as well as common information to transmit. There is no external eavesdropper, however, the private information of each user is to be kept as confidential as possible from the other user. The users listen to the channel, but their encoding functions are not affected by their eavesdropping information. The level of secrecy is measured by equivocation. When only one user has confidential information for the receiver, inner and outer bounds on the capacity-equivocation region are provided, and the secrecy capacity region is specified. In [5] as well, there is no external eavesdropper. A two user system is considered where both users communicate to the receiver, while one of them is permitted to eavesdrop on the other user. The Gaussian MAC is studied in [6]. The setting in [6] is different than [4] and [5] in that, an external eavesdropper is present, and the users do not eavesdrop on each other. A new secrecy constraint suitable for a multiple user system is defined. Using Gaussian codebooks, achievable rate-equivocation regions and their corresponding power allocation strategies are provided.

The Gaussian multiple input multiple output (MIMO) wire-tap channel is studied in [7]. An achievable scheme is proposed where the user tries to put the eavesdropper in relative disadvantage by transmitting noise in the user channel's null space. The single input multiple output (SIMO) Gaussian channel is considered in [8]. There, the existence of an equivalent scalar Gaussian channel is shown and consequently, the results of [3] are used to derive the capacity-equivocation region.

Secrecy in single input single output (SISO) fading channels is studied in [10], [11], [12], [13] and [14]. [10] investigates the outage performance. [11], [12] and [13] specify the secrecy capacity, when full channel state information is available to all the parties. [13] further finds the secrecy capacity without the eavesdropper channel state information for a special fading eavesdropper channel. In [14], only the eavesdropping channel is assumed to experience fading, and the main channel is considered to be non-fading. The eavesdropping channel fading realization is assumed to be known only to the eavesdropper. Achievable secrecy rates under Gaussian signalling are characterized.

We consider a Gaussian MISO channel under various assumptions on the channel attenuations. We first assume that the channel attenuations are constants, known to all the parties. We characterize the maximum secrecy rate achievable through Gaussian signalling, and show that the Gaussian signalling that achieves the best secrecy rate is of beamformig nature. [9] reports a similar result, as derived in this paper, however, these similar results are derived independently and concurrently. Our problem is different than [7] in that we seek the optimum Gaussian signalling, while [7] investigates the performance of one specific Gaussian strategy. The results of [8] cannot be

extended to our case, since the method used in [8] to find an equivalent scalar Gaussian channel cannot be used for a MISO Gaussian channel.

Next, we assume that the eavesdropping channel experiences fading, where the realizations of the fading coefficients are not known to the transmitter. We characterize achievable secrecy rates through Gaussian signalling. We show that the optimal Gaussian signalling has a unit-rank covariance matrix, and therefore, beamforming is optimal in this case as well. However, while the beamforming vector in the non-fading case depends on both channel attenuation vectors from the transmitter to the receiver and the eavesdropper, in this case, it depends only on the channel attenuation vector from the transmitter to the receiver. As a result of the optimality of beamforming, our MISO system reduces to a SISO system. We identify conditions under which, positive secrecy rates are achievable. Our formulation is partially similar to that of [14]. [14] treats the SISO system, and we study the MISO problem, but in both cases, the main channel is constant, while the eavesdropping channel is fading and unknown to the transmitter. After we reduce the MISO system to a SISO system, our results overlap significantly with those of [14]. Here again, the results of this paper and those of [14] have been derived independently and concurrently. Our results are different than [10], [11], [12], [13] and [14], in that they all consider single antennas for all the parties, while multiple transmit antennas are considered for the transmitter here.

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

II. System model

Figure 1 shows a communication system, with a transmitter equipped with multiple transmit antennas and a receiver and an eavesdropper, each with a single antenna. The user and eavesdropper channel attenuations can be represented by $t \times 1$ vectors $\mathbf{h}$ and $\mathbf{g}$, where t is the number of transmit antennas. The received signals at the receiver and the eavesdropper at time i are

$$y_i = \mathbf{h}^\dagger \mathbf{x}_i + n_{y,i} \tag{1}$$

$$z_i = \mathbf{g}^\dagger \mathbf{x}_i + n_{z,i} \tag{2}$$

where $\mathbf{x}_i$ is the transmitted signal at time i, and without loss of generality, $n_{y,i}$ and $n_{z,i}$ are unit-variance complex circularly symmetric Gaussian random variables. $\mathbf{h}$ is known and fixed. When the eavesdropper channel is non-fading, $\mathbf{g}$ is assumed to be known and fixed too. When the eavesdropper channel experiences fading, $\mathbf{g}$ is assumed to be a vector of i.i.d. zero mean unit-variance complex circularly symmetric Gaussian random variables.

A message m of rate R, is a random integer from the set $\{1, \ldots, 2^{nR}\}$, which is transmitted in n channel uses.

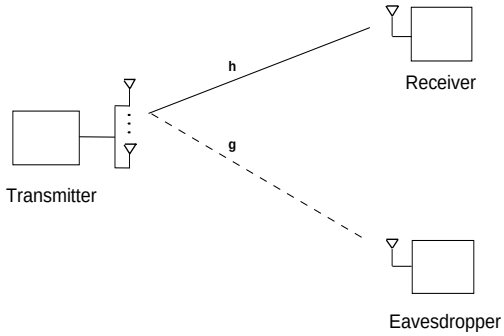

Fig. 1. A communication system with a multi-antenna transmitter, and a single-antenna receiver and eavesdropper.

The equivocation rate R_e, is the conditional entropy of the transmitted message, conditioned on the received signal at the eavesdropper. The equivocation rate is a measure of the amount of information that the eavesdropper can attain about the message, and quantifies the level of secrecy in the system. The secrecy capacity, C_S, is the largest rate R achievable with perfect secrecy, i.e., $R_e = R$.

III. Non-fading eavesdropper channel

Assume that $\mathbf{g}$ in (2) is fixed and known. From [2], the secrecy capacity of this system is

$$C_S = \max_{\mathbf{u} \to \mathbf{x} \to yz} I(\mathbf{u}; y) - I(\mathbf{u}; z) \tag{3}$$

Ideally, one should solve (3) for the optimal joint distribution of $\mathbf{u}$ and $\mathbf{x}$. We restrict ourselves to the potentially sub-optimal assumption that $\mathbf{x} = \mathbf{u}$, under which, the following rate is achievable with perfect secrecy

$$R_S = \max_{p(\mathbf{x})} \quad I(\mathbf{x}; y) - I(\mathbf{x}; z) \tag{4}$$

R_S would have been equivalent to the secrecy capacity C_S, if the main channel was "more capable" than the eavesdropping channel [2]. $p(\mathbf{x})$ must be chosen to maximize (4), but we restrict ourselves to the class of Gaussian pdfs. Our aim is to characterize the best achievable secrecy rates, under this restriction, and the input power constraint. This is in fact one further potentially sub-optimal assumption that we make, as, Gaussian signalling maximizes both terms on the right hand side of (4), but does not necessarily maximize the difference. Note that in the scalar Gaussian channel studied in [3], the two assumptions of $\mathbf{x} = \mathbf{u}$ and $\mathbf{x}$ being Gaussian are not sub-optimal, as the eavesdropping channel is a degraded version of the main channel.

The optimization problem of interest is now

$$R_S = \log(1 + \mathbf{h}^\dagger \mathbf{\Sigma} \mathbf{h}) - \log(1 + \mathbf{g}^\dagger \mathbf{\Sigma} \mathbf{g}) \tag{5}$$

where $\mathbf{\Sigma}$ is the covariance matrix for the channel input vector $\mathbf{x}$, and is constrained such that $\text{tr}(\mathbf{\Sigma}) \leq P$. There is no $\frac{1}{2}$ coefficient before the $\log$ terms, as, complex Gaussian vectors are involved. It remains to identify the covariance matrix $\mathbf{\Sigma}$

that maximizes R_S. This is equivalent to finding the $\mathbf{\Sigma}$ that maximizes

$$\rho(\mathbf{\Sigma}) = \frac{1+\mathbf{h}^\dagger\mathbf{\Sigma}\mathbf{h}}{1+\mathbf{g}^\dagger\mathbf{\Sigma}\mathbf{g}} \tag{6}$$

or, the pair $(\mathbf{V}, \mathbf{\Lambda})$ that maximizes

$$\rho(\mathbf{\Sigma}) = \frac{1+\mathbf{a}^\dagger\mathbf{\Lambda}\mathbf{a}}{1+\mathbf{b}^\dagger\mathbf{\Lambda}\mathbf{b}} \tag{7}$$

where $\mathbf{\Sigma} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^\dagger$ is the eigenvalue decomposition for $\mathbf{\Sigma}$, $\mathbf{a} = \mathbf{V}^\dagger\mathbf{h}$ and $\mathbf{b} = \mathbf{V}^\dagger\mathbf{g}$. We first show that $\mathbf{\Lambda}$ should have only one non-zero component, equal to P, and therefore, the optimal $\mathbf{\Sigma}$ should be unit rank.

The optimization function can be rewritten as

$$\rho(\mathbf{\Sigma}) = \frac{1+\mathbf{a}^\dagger\mathbf{\Lambda}\mathbf{a}}{1+\mathbf{b}^\dagger\mathbf{\Lambda}\mathbf{b}} = \frac{1+\sum_{i=1}^t a_i^2\lambda_i}{1+\sum_{i=1}^t b_i^2\lambda_i} \tag{8}$$

For a fixed $\mathbf{V}$, we show that either all eigenvalues are zero, or there is only one nonzero eigenvalue equal to P, depending on the parameters a_i and b_i.

1) If

$$a_i^2 < b_i^2, \qquad i = 1, \ldots, t \tag{9}$$

then for all values of $\mathbf{\Lambda}$, $\rho(\mathbf{\Sigma}) \leq 1$. Its maximum value $\rho(\mathbf{\Sigma}) = 1$ happens when $\mathbf{\Lambda} = 0$ and the user stays quiet. This situation can be interpreted as the case were the eavesdropping channel is strictly better than the user channel, and therefore, it is not possible to transmit information at any positive rate with perfect secrecy $R_e = R$. The corresponding rate-equivocation region in this case is empty.

2) If for some $1 \leq i \leq t$, $a_i^2 > b_i^2$, and there is unused power, increasing λ_i will increase $\rho(\mathbf{\Sigma})$. Therefore, if at least for one i, $a_i^2 > b_i^2$, the user should use all the available power. To show that the power should be used in only one direction, consider any two indices i and j, $1 \leq i, j \leq t$. Assume that $\lambda_i + \lambda_j = P_{ij} \leq P$. Fixing all other eigenvalues, the optimization function can be written as

$$\rho(\mathbf{\Sigma}) = \frac{a + b\lambda_i}{c + d\lambda_i} \tag{10}$$

where

$$a = 1 + \sum_{l=1, l\neq i,j}^{t} a_l^2\lambda_l + a_j^2 P_{ij} \tag{11}$$

$$b = a_i^2 - a_j^2 \tag{12}$$

$$c = 1 + \sum_{l=1, l\neq i,j}^{t} b_l^2\lambda_l + b_j^2 P_{ij} \tag{13}$$

$$d = b_i^2 - b_j^2 \tag{14}$$

Depending on the sign of $bc - ad$, this function is either monotonically increasing or monotonically decreasing in λ_i. Therefore, in the optimal solution, for any two indices i and j, $1 \leq i, j \leq t$, we should have either $(0, \lambda_i + \lambda_j)$ or $(\lambda_i + \lambda_j, 0)$ instead of (λ_i, λ_j). We conclude that there is only one nonzero eigenvalue, which is equal to P.

Since $\mathbf{\Sigma}$ is unit rank, it can be written as $\mathbf{\Sigma} = P\mathbf{q}\mathbf{q}^\dagger$ where $\mathbf{q}$ is constrained to be a unit-norm vector, i.e., $\mathbf{q}^\dagger\mathbf{q} = 1$. Then, we can write the optimization problem as

$$\rho(\mathbf{q}) = \frac{\mathbf{q}^\dagger\mathbf{q} + P(\mathbf{q}^\dagger\mathbf{h})^2}{\mathbf{q}^\dagger\mathbf{q} + P(\mathbf{q}^\dagger\mathbf{g})^2} = \frac{\mathbf{q}^\dagger(\mathbf{I} + P\mathbf{h}\mathbf{h}^\dagger)\mathbf{q}}{\mathbf{q}^\dagger(\mathbf{I} + P\mathbf{g}\mathbf{g}^\dagger)\mathbf{q}} = \frac{\mathbf{q}^\dagger\mathbf{A}\mathbf{q}}{\mathbf{q}^\dagger\mathbf{B}\mathbf{q}} \tag{15}$$

where

$$\mathbf{A} = \mathbf{I} + P\mathbf{h}\mathbf{h}^\dagger \tag{16}$$

$$\mathbf{B} = \mathbf{I} + P\mathbf{g}\mathbf{g}^\dagger \tag{17}$$

Now, $\rho(\mathbf{q})$ is insensitive to the scaling of $\mathbf{q}$, therefore, we can ignore the constraint on $\mathbf{q}$, find the general solution, and then scale it to have the unit-norm solution for the original problem. The problem in (15) is equivalent to

$$\rho(\mathbf{w}) = \frac{\mathbf{w}^\dagger\mathbf{B}^{-1/2}\mathbf{A}\mathbf{B}^{-1/2}\mathbf{w}}{\mathbf{w}^\dagger\mathbf{w}} \tag{18}$$

where $\mathbf{w} = \mathbf{B}^{1/2}\mathbf{q}$. The problem in (18) is a Rayleigh quotient [16] and is maximized when $\mathbf{w}$ is any scaled version of the eigenvector of $\mathbf{Z}$ corresponding to its largest eigenvalue, where

$$\mathbf{Z} = (\mathbf{I} + P\mathbf{g}\mathbf{g}^\dagger)^{-1/2}(\mathbf{I} + P\mathbf{h}\mathbf{h}^\dagger)(\mathbf{I} + P\mathbf{g}\mathbf{g}^\dagger)^{-1/2} \tag{19}$$

Calling this vector $\mathbf{w}^*$, the solution of the original optimization problem is

$$\mathbf{q}^* = \frac{(\mathbf{I} + P\mathbf{g}\mathbf{g}^\dagger)^{-1/2}\mathbf{w}^*}{\|(\mathbf{I} + P\mathbf{g}\mathbf{g}^\dagger)^{-1/2}\mathbf{w}^*\|} \tag{20}$$

It is well-known that the capacity achieving transmission strategy in a peaceful MISO channel without secrecy constraints, is to beamform in the direction of the main channel $\mathbf{h}$ [15]. The above result shows that, with the addition of an eavesdropping channel, and the resulting secrecy constraints, the optimal strategy is still beamforming, but the beamforming direction $\mathbf{q}^*$, is "adjusted" to be as orthogonal to the eavesdropping channel direction as possible, while being as close to the main channel direction as possible.

IV. Fading eavesdropper channel

We study two situations regarding the availability of the eavesdropper's channel state information. First, we assume that the channel state information of the eavesdropper is also available, similar to the setting used in [11], [12]. This can also be motivated by the assumption that the eavesdropper can be an idle user in a broadcast channel [2], [4], therefore, its channel information can be common knowledge just like the receiver channel information. Later, we make the more natural assumption that, only statistical information about the channel state of the eavesdropper is available.

If the eavesdropping channel state information is available, the transmitter can design a communication strategy for a set of parallel constant sub-channels corresponding to the set of possible fading levels of the eavesdropping

channels, and also choose a power allocation strategy over those sub-channels [11]. The communication/equivocation rates at the receiver/eavesdropper, are the average communication/equivocation rates of the sub-channels [11], [12], therefore, the user can choose the optimal strategy over each sub-channel independently. The focus of this paper is on characterizing the optimal strategies at each sub-channel. It is left as future work to determine the optimal power allocation strategies. Each sub-channel is equivalent to the non-fading MISO channel studied in the previous section.

Now, assume that there is only statistical information about the channel state of the eavesdropper. Again, the transmitter can design a communication strategy for a set of parallel constant sub-channels corresponding to the set of possible fading levels of the main channel, together with a power allocation strategy over those sub-channels. Again, we focus on characterizing the optimal strategies at each sub-channel and leave the optimal power allocation strategies for future work. Toward that end, assume that the channel of the intended receiver is constant, while the eavesdropper's channel is complex Gaussian fading. From [2], the ergodic secrecy capacity of this system is

$$C_S = \max_{\mathbf{u}\to\mathbf{x}\to y\mathbf{g}z} I(\mathbf{u};y) - I(\mathbf{u};\mathbf{g}z) \tag{21}$$

$$= \max_{\mathbf{u}\to\mathbf{x}\to y\mathbf{g}z} I(\mathbf{u};y) - I(\mathbf{u};z|\mathbf{g}) \tag{22}$$

Letting $\mathbf{x}=\mathbf{u}$, the following rate is achievable with perfect secrecy

$$R_S = \max_{p(\mathbf{x})} \quad I(\mathbf{x};y) - I(\mathbf{x};z|\mathbf{g}) \tag{23}$$

As before, we restrict ourselves to Gaussian, potentially sub-optimal $\mathbf{x}$, and characterize the best achievable secrecy rates. The optimization problem of interest is therefore

$$R_S(\mathbf{\Sigma}) = \log(1+\mathbf{h}^\dagger\mathbf{\Sigma}\mathbf{h}) - E_{\mathbf{g}}\left[\log(1+\mathbf{g}^\dagger\mathbf{\Sigma}\mathbf{g})\right] \tag{24}$$

where $\mathbf{\Sigma}$ is the covariance matrix for the channel input vector $\mathbf{x}$, and is constrained such that $\text{tr}(\mathbf{\Sigma}) \le P$, where P is the available input power. Let the eigenvalue decomposition for the input covariance matrix be $\mathbf{\Sigma} = \mathbf{V}\mathbf{\Lambda}\mathbf{V}^\dagger$. The goal is to solve (24) for the maximizing $\mathbf{\Sigma}$, or equivalently, to solve for $\mathbf{V}$ and $\mathbf{\Lambda}$. The optimization function $R_S(\mathbf{\Sigma})$ can be rewritten as

$$R_S(\mathbf{V},\mathbf{\Lambda}) = \log(1+\mathbf{h}^\dagger\mathbf{V}\mathbf{\Lambda}\mathbf{V}^\dagger\mathbf{h}) - E_{\mathbf{g}}\left[\log(1+\mathbf{g}^\dagger\mathbf{V}\mathbf{\Lambda}\mathbf{V}^\dagger\mathbf{g})\right] \tag{25}$$

where $\mathbf{\Lambda}$ is diagonal, and the constraints are $\mathbf{V}\mathbf{V}^\dagger = \boldsymbol{I}$ and $\text{tr}(\mathbf{\Lambda}) \le P$. Following [15], since $\mathbf{V}$ is unitary, and $\mathbf{g}$ is a vector of i.i.d. zero-mean complex circularly symmetric Gaussian random variables, $\mathbf{V}^\dagger\mathbf{g}$ will have the same distribution as $\mathbf{g}$, and can be replaced by $\mathbf{g}$ in the expectation. Therefore,

$$R_S(\mathbf{V},\mathbf{\Lambda}) = \log(1+\mathbf{h}^\dagger\mathbf{V}\mathbf{\Lambda}\mathbf{V}^\dagger\mathbf{h}) - E_{\mathbf{g}}\left[\log(1+\mathbf{g}^\dagger\mathbf{\Lambda}\mathbf{g})\right] \tag{26}$$

We will first solve for the optimal $\mathbf{V}$, which affects only the first term on the right hand side of (26).

Define $\mathbf{a} = \mathbf{V}^\dagger\mathbf{h}$. The constraint on $\mathbf{V}$ can be replaced by the following constraint on $\mathbf{a}$

$$\mathbf{a}^\dagger\mathbf{a} = \mathbf{h}^\dagger\mathbf{V}\mathbf{V}^\dagger\mathbf{h} = \mathbf{h}^\dagger\mathbf{h} \tag{27}$$

The choice of $\mathbf{V}$ affects (26) only through the product term $\mathbf{a} = \mathbf{V}^\dagger\mathbf{h}$. For any $\mathbf{a}$, one can find a matrix $\mathbf{V}$ that satisfies $\mathbf{a} = \mathbf{V}^\dagger\mathbf{h}$, which is in fact a rotation matrix that maps $\mathbf{h}$ onto $\mathbf{a}$. Therefore, instead of solving for the best $\mathbf{V}$, one can solve for the best $\mathbf{a}$ in

$$R_S(\mathbf{V},\mathbf{\Lambda}) = \log(1+\mathbf{a}^\dagger\mathbf{\Lambda}\mathbf{a}) - E_{\mathbf{g}}\left[\log(1+\mathbf{g}^\dagger\mathbf{\Lambda}\mathbf{g})\right] \tag{28}$$

for any given matrix $\mathbf{\Lambda}$. Without loss of generality, assume that the diagonal elements of $\mathbf{\Lambda}$ are in decreasing order, i.e., $\lambda_1 \ge \lambda_2 \ge \ldots \ge \lambda_t$. The optimal choice of $\mathbf{a}$ will then be such that

$$\mathbf{a}^\dagger\mathbf{\Lambda}\mathbf{a} = \sum_{i=1}^{t}\lambda_i a_i^2 \tag{29}$$

is maximized. Given the constraint on $\mathbf{a}$ in (27), $\sum_{i=1}^t a_i^2 = \mathbf{h}^\dagger\mathbf{h}$, and since λ_1 is larger than all other λ_i, in order to maximize the weighted sum $\sum_{i=1}^t \lambda_i a_i^2$, we should have

$$a_1^2 = \mathbf{h}^\dagger\mathbf{h} \tag{30}$$

$$a_i = 0, \qquad i > 1 \tag{31}$$

This in turn shows that, the optimal unitary matrix $\mathbf{V}$, has the unit-norm vector $\frac{\mathbf{h}}{\|\mathbf{h}\|}$ as its first column, and $t-1$ arbitrary normal vectors orthogonal to $\mathbf{h}$, as the rest of its columns.

Given the optimal $\mathbf{V}$ as characterized above, it remains to find the optimal $\mathbf{\Lambda}$. The best achievable rate R_S can be written as a function of $\lambda_1,\ldots,\lambda_t$ only

$$R_S(\mathbf{\Lambda}) = \log(1+\lambda_1\|\mathbf{h}\|^2) - E_{\mathbf{g}}\left[\log\left(1+\sum_{i=1}^{t}\lambda_i\|g_i\|^2\right)\right] \tag{32}$$

where g_i, $i=1,\ldots,t$ are the i.i.d. random variables in $\mathbf{g}$. Observe that the choice of λ_i, $i>1$ only affects the second term on the right hand side of (32). For any fixed λ_1, given that λ_i and g_i^2 are all non-negative, the second term on the right hand side of (32) is increasing in λ_i, while the first term is fixed. Therefore, in order to maximize $R_S(\mathbf{\Lambda})$, the user is better off choosing $\lambda_i = 0$ for all $i>1$, as the power constraint is $\text{tr}(\mathbf{\Sigma}) = \text{tr}(\mathbf{\Lambda}) = \sum_{i=1}^t \lambda_i \le P$. This, together with (30) and (31), shows that the optimal user strategy is to transmit in the direction of $\mathbf{h}$. This beamforming in the direction of $\mathbf{h}$ is in fact expected and intuitive, since we only have information about the main channel vector $\mathbf{h}$. This also happens to be the throughput maximizing direction in the peaceful channel without secrecy constraints as mentioned at the end of the previous section.

The secrecy rate R_S can now be written as a function of λ_1 only

$$R_S(\lambda_1) = \log(1+\lambda_1\|\mathbf{h}\|^2) - E_g\left[\log(1+\lambda_1\|g\|^2)\right] \tag{33}$$

where the random variable g has the same distribution as any g_i, $i = 1, \ldots, t$, and the power constraint is $\lambda_1 \leq P$.

We now characterize the best choice of λ_1 which maximizes R_S. Since there is only one parameter λ_1 to be determined, we drop the subscript and replace λ_1 by λ. First, observe that both the first and the second terms on the right hand side of (33) grow with λ. Let $\gamma = \|g\|^2$. Since g is complex circularly symmetric Gaussian, γ will have an exponential distribution with pdf

$$p_\gamma(\gamma) = \frac{1}{\alpha} e^{\frac{-\gamma}{\alpha}} \tag{34}$$

where $\alpha = 2\sigma^2$, and σ^2 is the variance of the Gaussian random variables corresponding to the real and imaginary parts of g. The parameter α characterizes the mean and the standard deviation of the exponential random variable γ. Rewriting the optimization function in terms of γ, we will have

$$R_S(\lambda) = \log(1 + \lambda \|\mathbf{h}\|^2) - E_\gamma \left[\log(1 + \lambda\gamma)\right] \tag{35}$$

We now discuss the behavior of $R_S(\lambda)$ as a function of λ. First, it can be observed that, since the function $f(x) = \log(1 + ax)$ is concave, using Jensen's inequality [17], we will have

$$E_\gamma \left[\log(1 + \lambda\gamma)\right] \leq \log(1 + \lambda E_\gamma \left[\gamma\right]) \tag{36}$$

which shows that, by choosing the right input covariance matrix, positive secrecy rate is achievable if the combined effect of all t components of $\mathbf{h}$ is better than a single component of $\mathbf{g}$, which can occur even if $\mathbf{h}$ is much worse than $\mathbf{g}$ componentwise.

Numerical simulation of $R_S(\lambda)$ as a function of λ shows that, depending on the relative quality of the main and the eavesdropping channels, for some values of $\|\mathbf{h}\|^2$ and α, $R_S(\lambda)$ increases with λ, therefore, the user should use all its available power, and should beamform in the direction of $\mathbf{h}$. However, for some other values of $\|\mathbf{h}\|^2$ and α, $R_S(\lambda)$ can decrease with λ. After the reduction of our system to a SISO system, the results reported here overlap with those reported in [14].

Based on the above observation, and as it is also discussed in [6], [7] and [14], the user is not always better off using all its available power. This raises the concern that the achievable scheme provided here, is potentially suboptimal. The source of the sub-optimality could be either the assumption that $\mathbf{x} = \mathbf{u}$ in (22), or later restricting $\mathbf{x}$ to be Gaussian. In [6], [7] and [14], the first assumption is targeted, and "preprocessing" of information at the transmitter is allowed, in the form of additionally injecting independent Gaussian noise by the user, or so called, "noise forwarding". Higher secrecy rates are then achieved, which shows that in fact, letting $\mathbf{x} = \mathbf{u}$ is sub-optimal. Note that, even though these techniques improve upon the achievable secrecy rates, they are yet potentially sub-optimal, and the problem of finding the optimal communication strategy remains open.

V. Conclusion

In this paper, we considered a Gaussian MISO channel with an eavesdropper. We considered both cases when the eavesdropper channel is non-fading and fading. We restricted the signalling to be Gaussian with no preprocessing of information, which is potentially sub-optimal. In both non-fading and fading cases, we showed that the optimal communication strategy that achieves the highest secrecy rate, is of beamforming type, and that the beamforming direction depends on the available channel state information. In the fading case, as the optimal Gaussian strategy is not always using the available transmit power, some sort of preprocessing, at least in the form of "noise injection" with the unused power, seems necessary to achieve a higher secrecy rate.

Acknowledgment

This work was supported by NSF Grants CCR 03-11311, CCF 04-47613, and CCF 05-14846.

References

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, 54(8):1355–1387, October 1975.

[2] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory*, 24(4):451–456, July 1978.

[4] Y. Liang and H. V. Poor, "Generalized Multiple Access Channels with Confidential Messages," *IEEE Transactions on Information Theory*, submitted April 2006.

[5] R. Liu, I. Maric, R. D. Yates and P. Spasojevic, "The Discrete Memoryless Multiple Access Channel with Confidential Messages," *IEEE International Symposium on Information Theory, Seattle*, July 2006.

[6] E. Tekin and A. Yener, "Achievable Rates for the General Gaussian Multiple Access Wire-tap Channel with Collective Secrecy," *44th Annual Allerton Conference on Communication, Control, and Computing, Monticello*, September 2006.

[7] R. Negi and S. Goel, "Secret Communication Using Artificial Noise," *IEEE Vehicular Technology Conference, Dallas*, September 2005, volume 3: 1906–1910.

[8] P. Parada and R. Blahut, "Secrecy Capacity of SIMO and Slow Fading Channels," *IEEE International Symposium on Information Theory, Adelaide*, September 2005, pp. 2152-2155.

[9] Z. Li, W. Trappe and R. Yates, "Secret Communication via Multi-antenna Transmission," *41st Conference on Information Sciences and Systems, Baltimore*, March 2007.

[10] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *IEEE International Symposium on Information Theory, Seattle*, July 2006.

[11] Y. Liang, H. V. Poor and S. Shamai, "Secure Communication over Fading Channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, submitted November 2006.

[12] Z. Li, R. D. Yates and W. Trappe, "Secrecy Capacity of Independent Parallel Channels," *44th Annual Allerton Conference on Communication, Control, and Computing, Monticello*, September 2006.

[13] P. K. Gopala, L. Lai, H. El Gamal, "On the Secrecy Capacity of Fading Channels," *IEEE Transactions on Information Theory*, submitted October 2006.

[14] Z. Li, R. Yates and W. Trappe, "Secure Communication with a Fading Eavesdropper Channel," to appear, *IEEE International Symposium on Information Theory*, June 2007.

[15] I. E. Telatar, "Capacity of Multi-antenna Gaussian Channels," *European Transactions on Telecommunications*, 10(6):585–596, November 1999.

[16] R. A. Horn and C. R. Johnson, *Matrix Analysis*, Cambridge University Press, 1987.

[17] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, John Wiely & Sons, 1991.