Secret Communication via Multi-antenna Transmission

Zang Li, Wade Trappe, Roy Yates
Wireless Information Network Laboratory,
Rutgers University, North Brunswick, NJ 08902
Email: {*zang, trappe, ryates*}*@winlab.rutgers.edu*

***Abstract*— For a multiple antenna Gaussian broadcast channel, we look for inputs that facilitate secret transmission between authorized communication parties in the presence of passive eavesdroppers. In this work, we assume all channel information is known at the transmitter. For the general multiple antenna system, we find that the problem of optimizing over Gaussian inputs for achievable secrecy rate is not convex, making it difficult to solve. However, for the simpler case where multiple transmit antennas are deployed with only a single receive antenna used at both the intended receiver and the eavesdropper, the problem can be solved easily. The analytical solution for this case is presented.**

***Index Terms*— Information security, Multi-antenna transmission**

I. Introduction

Although conventional cryptographic security mechanisms are essential to the overall problem of security, the openness of wireless medium poses both threats and opportunities for securing transmission. The openness of the transmission medium makes eavesdropping extremely easy– anyone within communication range can listen to the traffic in the air, and possibly extract information. However, the unique properties of wireless medium might provide ways of combating such security threats. For example, due to random fading, the intended receiver will have a channel different from an eavesdroppers's when she is at a reasonable distance away. This difference can be utilized to secure the communication between the transmitter and the intended receiver. In this paper, we consider the secret wireless communication problem for multiple antenna system from an information-theoretic view.

In an information-theoretic secret communication system, a sender (Alice) wishes to reliably communicate a secret S to an intended receiver (Bob) in the presence of an eavesdropper (Eve). The secret S, a random integer from the set $\{1, 2, \ldots, 2^{nR}\}$, is transmitted in n channel uses. In this case, the secret has entropy $H(S) = nR$ bits and the secrecy communication rate is $R = H(S)/n$ bits per channel use. In these n channel uses, Alice transmits the coded signal $X^n = X_1, \ldots, X_n$; Bob receives the channel output $Y^n = Y_1, \ldots, Y_n$ and decodes $\hat{S}$ with error probability $P_e = P\left\{S \neq \hat{S}\right\}$. After Eve overhears the output $Z^n = Z_1, \ldots, Z_n$, her residual uncertainty regarding the secret message S is given by the conditional entropy $H(S|Z^n)$. This conditional entropy is generally expressed as a normalized equivocation rate $\Delta = H(S|Z^n)/H(S)$. From the perspective of confidential and reliable communication, the system performance depends on both the communication rate R and the equivocation rate Δ. In particular, the rate tuple (R_0, Δ_0) is achievable if for any $\epsilon > 0$ there exists a rate R encoder and decoder with equivocation rate Δ such that for some n,

$$P_e \leq \epsilon, \qquad R \geq R_0 - \epsilon, \qquad \Delta \geq \Delta_0 - \epsilon. \tag{1}$$

In this paper, we focus on the case $\Delta_0 = 1$, corresponding to the case where Eve's information per secret information bit regarding the secret S gained by the observation Z^n is given by

$$\begin{aligned} I(S; Z^n) &= H(S) - H(S|Z^n) \\ &= (1 - \Delta)H(S) \leq \epsilon H(S). \end{aligned} \tag{2}$$

That is, Eve learns arbitrarily little information regarding the secret S.

This model of information-theoretic secret communication started with Wyner's analysis of the discrete memoryless wiretap channel [1]. In Wyner's system, Eve hears a degraded version of Bob's received signal in that the channels are defined by a Markov chain $X \to Y \to Z$. This was generalized by Csiszár and Körner [2] to a system in which Alice transmits confidential messages to Bob at rate R as well as common messages to both Bob and Eve at rate R_0. When the rate of common messages is $R_0 = 0$, [2] defined the secrecy capacity C_{sec} as the maximum rate R, such that the tuple $(R, \Delta = 1)$ is achievable and showed that

$$C_{sec} = \max_{V \to X \to YZ} I(V; Y) - I(V; Z). \tag{3}$$

In this case, given the discrete memoryless channel (DMC) $P_{YZ|X}$, secrecy capacity is achieved by maximizing over all joint distributions $P_{V,X}(v, x)$ such that the Markov chain $V \to X \to YZ$ holds.[1]

In subsequent work, Maurer and Wolf [3] showed that the secrecy condition (2) employed by Wyner and by Csiszár and Körner could be strengthened considerably through a technique called *privacy amplification* without reducing the secret capacity C_{sec}. In this work, we follow the traditional information-theoretic definitions of security with a focus on the optimization of C_{sec} while keeping in mind that an actual system would likely employ privacy amplification[4].

In theory, (3) is a complete characterization of the secrecy capacity C_{sec}; however, many questions remain unanswered. For example, there are no systematic methods to optimize over the auxiliary input V and the $P_{X|V}$ channel. Yet the auxiliary is often essential, how to choose it optimally remains elusive for the general cases. However, for fixed channels, some results

[1]The notation $\max_X$ where X is a random variable is a shorthand for maximization over the choice of PMF $P_X(x)$ when X is discrete or PDF $f_X(x)$ when X is continuous.

are known when the channels of Bob and Eve satisfy certain conditions. In [5], the DMC $P_{Y|X}$ is defined to be *more capable* than $P_{Z|X}$ if $I(X;Y) - I(X;Z) \geq 0$ for all inputs X. In addition, the DMC $P_{Y|X}$ is defined to be *less noisy* than $P_{Z|X}$ if $I(U;Y) - I(U;Z) \geq 0$ for all inputs U and DMCs $P_{X|U}$. It is known that less noisy implies more capable. In [2], it is shown that if Bob's channel is *more capable* than Eve's channel, then the secrecy rate C_{sec} is achieved when $V = X$. Thus, when Bob has a more capable channel,

$$C_{sec} = \max_{X} I(X;Y) - I(X;Z). \tag{4}$$

Nevertheless, it remains to find the optimal input X that achieves C_{sec} for common channels. A fundamental difficulty is that $I(X;Y)$ and $I(X;Z)$ are both concave functions in the input distribution P_X. Thus the difference $I(X;Y) - I(X;Z)$ is, in general, neither concave nor convex in P_X and may have multiple local maxima. In this case, convex optimization procedures are not guaranteed to find the optimal input distribution [6]. We do note that the case that Bob's channel is less noisy than Eve's is an exception since van Dijk [7] has shown that $P_{Y|X}$ is less noisy than $P_{Z|X}$ if and only if $I(X;Y) - I(X;Z)$ is a concave function of P_X.

Recently there has been a flurry of activity targeted at enhancing the secrecy of communication between wireless devices utilizing the fading properties of wireless channels, such as [8], [9], [10], [11]. In this paper, we are interested in multiple antenna systems. The secure communication problem for Multiple-input Multiple-output (MIMO) systems was studied in [12], where it was shown that proper exploitation of space-time diversity at the transmitter can enhance information security and information hiding capabilities. In particular, for information security, Hero showed that when the eavesdropper is uninformed about his channel, the transmitter can enforce a zero information rate to the eavesdropper while delivering a positive information rate to the intended receiver by restricting the space-time modulation to a class of complex transmit matrices whose spatial inner product is a constant matrix. The channel capacity under this perfect secrecy condition, when both the transmitter and the intended receiver have channel information, was derived. However, the restriction to an eavesdropper uninformed about his channel is quite unrealistic. The secrecy capacity of single-input multiple-output channel under Gaussian noise was studied in [13] by transforming the channel into scalar wiretap channels. Negi et al. [14], [15] studied secrecy capacity with MIMO channels when artificial noise is injected. They showed that injecting artificial noise in the nullspace of the intended receiver's channel can degrade Eve's channel and allow positive secrecy capacity even when Eve's channel was better before artificial noise injection. Practical schemes for secret transmission with MIMO using randomization were proposed in [16], [17].

In this paper, we examine what kind of input structure should we use to achieve the secrecy rate for a multiple antenna broadcast channel. Since the MIMO channel does not satisfy the more capable or less noisy conditions, it remains elusive whether an auxiliary random variable V is beneficial or not. However, $\max_X I(X;Y) - I(X;Z)$ can be considered as a lower bound to the achievable secrecy rate, and it is instructive to study this achievable secrecy rate under the MIMO scenario. To make the problem simpler, we assume Gaussian random codes are used at the transmitter and both Bob's and Eve's channels are known to Alice. The problem is formulated in Section II. A simplified version of the problem for the Multiple-Input Single-Output (MISO) case is solved in Section III.

II. Problem Formulation for MIMO

When the broadcast channels are MIMO, the outputs at Bob and Eve are modeled as

$$\mathbf{y} = H\mathbf{x} + \mathbf{w}_1, \tag{5a}$$

$$\mathbf{z} = G\mathbf{x} + \mathbf{w}_2, \tag{5b}$$

where H is the channel matrix between Alice and Bob, and G is the channel matrix between Alice and Eve. $\mathbf{w}_1$ and $\mathbf{w}_2$ are the corresponding noise.

To make the problem simpler, we assume zero mean Gaussian random codes are used at the transmitter and both Bob's and Eve's channels are known to all parties. We further assume that the noise $\mathbf{w}_1$ and $\mathbf{w}_2$ are independent Gaussian white noise with the covariance matrix normalized to identity matrix. The distribution of the input $\mathbf{x}$ is characterized by its covariance matrix $Q = E[\mathbf{x}\mathbf{x}^\dagger]$. The mutual information between the transmitter and the receiver with channel matrix H under this MIMO model was shown to be $\log\det(I_r + HQH^\dagger)$ in [18], where I_r is the identity matrix with size r, the number of receiving antennas. Therefore, to maximize the achievable secrecy rate $R_s(Q) = I(X;Y) - I(X;Z)$, we need to

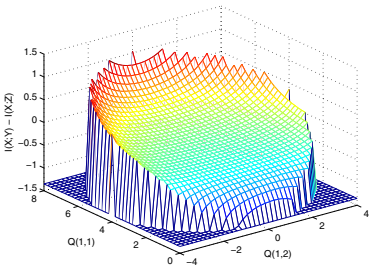
$$\begin{aligned} \text{maximize} \quad & \log\det(I_r + HQH^\dagger) - \log\det(I_r + GQG^\dagger) \\ \text{subject to} \quad & \mathrm{tr}(Q) \leq P, \;\; Q \succeq 0, \; Q = Q^\dagger, \end{aligned} \tag{6}$$

with the optimization variable Q, where $\succeq 0$ implies positive semidefiniteness. The channel input is required to satisfy the transmission power constraint P. Here we assume Bob and Eve have the same number of antennas, which we will extend in later work.

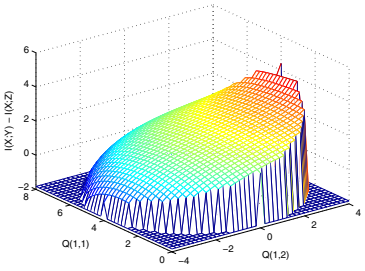
The objective function of the above optimization problem is not convex. This can be easily seen by noting that $\log\det(I_r + HQH^\dagger)$ is a concave function of Q. So, the objective function is a difference of two concave functions. For Q's that make the second term of the objective function zero, the objective function is concave, while for Q's that make the first term of the objective function zero, the objective function is convex. For a simple 2×2 MIMO case, we plot the $I(X;Y) - I(X;Z)$ as a function of $Q(1,1)$ and $Q(1,2)$ for two random channel realizations (assumed real here to allow plotting $Q(1,2)$) in Figure 1, with the power constraint satisfied with equality. From the figure, it is clear that maximizing $I(X;Y) - I(X;Z)$ is not easy even for this simple example, and a simple Newton method could be trapped in a local maximum.

By introducing an auxiliary variable t, we can reformulate the problem as

$$\begin{aligned} \text{maximize} \quad & t - \log\det(I_r + GQG^\dagger) \\ \text{subject to} \quad & \log\det(I_r + HQH^\dagger)) \geq t \\ & \mathrm{tr}(Q) \leq P, \;\; Q \succeq 0, \; Q = Q^\dagger. \end{aligned} \tag{7}$$



(a)



(b)

Fig. 1. $I(X;Y) - I(X;Z)$ for 2×2 random generated MIMO systems as a function of the covariance matrix coefficients $Q(1,1)$ and $Q(1,2)$, with the power constraint satisfied with equality.

This is a convex maximization problem over a convex constraint set. There is rich research on solving the convex maximization problem (referred to as concave minimization in most references) numerically, as described in detail in [19], but their applicability is not straightforward to our problem due to the complex function format used here.

III. A Simple Case: MISO

Although problem (6) is non-convex, and thus hard when H and G are of arbitrary size, the problem can be simplified for the MISO case, where both receivers at Bob and Eve have only a single antenna. Denote n to be the number of transmit antennas, then H and G are $1 \times n$ vectors in this case. To avoid confusion, we use row vectors $\mathbf{h}$ and $\mathbf{g}$ of size $1 \times n$ to denote the channel realization, and rewrite the channel model as

$$y = \mathbf{h}\mathbf{x} + w_1, \tag{8a}$$
$$z = \mathbf{g}\mathbf{x} + w_2. \tag{8b}$$

Both the noise and the outputs are scalar now. We can further simplify the model by a coordinate transform. Suppose we have a unitary matrix R of size $n \times n$, with property

$$RR^\dagger = R^\dagger R = I_n. \tag{9}$$

Then (8) is equivalent to

$$y = \mathbf{h}RR^\dagger\mathbf{x} + w_1 = \tilde{\mathbf{h}}\tilde{\mathbf{x}} + w_1, \tag{10a}$$
$$z = \mathbf{g}RR^\dagger\mathbf{x} + w_2 = \tilde{\mathbf{g}}\tilde{\mathbf{x}} + w_2, \tag{10b}$$

where $\tilde{\mathbf{x}}$, $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ are the vector representations of $\mathbf{x}$, $\mathbf{h}$ and $\mathbf{g}$ in the transformed space spanned by R. Since R is invertible, it is clear that $I(\mathbf{x};y) = I(\tilde{\mathbf{x}};y)$ and $I(\mathbf{x};z) = I(\tilde{\mathbf{x}};z)$.

To simplify the model, we can choose R in the following way

1) The first column is $\mathbf{r}_1 = \mathbf{h}^\dagger/||\mathbf{h}||$,
2) The second column $\mathbf{r}_2$ is orthogonal to $\mathbf{r}_1$, and lies in the space spanned by $\mathbf{h}$ and $\mathbf{g}$. Mathematically, this means

$$\mathbf{r}_2 = \frac{(\mathbf{g} - (\mathbf{g}\mathbf{r}_1)\mathbf{r}_1^\dagger)^\dagger}{||\mathbf{g} - (\mathbf{g}\mathbf{r}_1)\mathbf{r}_1^\dagger||} = \frac{(\mathbf{g} - ||\mathbf{g}||\alpha\mathbf{r}_1^\dagger)^\dagger}{||\mathbf{g}||\sqrt{1-\alpha^\dagger\alpha}}, \tag{11}$$

where α is the normalized correlation coefficient, defined as

$$\alpha = \frac{\mathbf{g}\mathbf{h}^\dagger}{||\mathbf{g}|| \cdot ||\mathbf{h}||}.$$

(It is assumed that $\mathbf{h}$ and $\mathbf{g}$ are not in the same direction here, since in that situation, the channel is just reduced to a scalar Gaussian broadcast channel).

3) The rest of the rows are an arbitrarily chosen orthonormal basis set for the remaining $n-2$ dimensions, and are orthogonal to the first two rows.

With this selection of R, we have

$$\tilde{\mathbf{h}} = \mathbf{h}R = ||\mathbf{h}|| \cdot [1, 0, \cdots, 0], \tag{12}$$
$$\tilde{\mathbf{g}} = \mathbf{g}R = ||\mathbf{g}|| \cdot [\alpha, \sqrt{1-\alpha^\dagger\alpha}, \cdots, 0]. \tag{13}$$

Since $\tilde{\mathbf{h}}$ and $\tilde{\mathbf{g}}$ both have zero components in the subspace spanned by $\{\mathbf{r}_3, \cdots, \mathbf{r}_n\}$, no power should be put into those dimensions. So we can focus only on the subspace spanned by the first two rows of R. This reduces the MISO channel model to

$$\begin{bmatrix} y \\ z \end{bmatrix} = \begin{bmatrix} ||\mathbf{h}|| & 0 \\ ||\mathbf{g}||\alpha & ||\mathbf{g}||\sqrt{1-\alpha^\dagger\alpha} \end{bmatrix} \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix} + \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \tag{14}$$

From now on, we will refer

$$\tilde{\mathbf{x}} = \begin{bmatrix} \tilde{x}_1 \\ \tilde{x}_2 \end{bmatrix}, \ \tilde{\mathbf{h}} = ||\mathbf{h}|| \begin{bmatrix} 1 & 0 \end{bmatrix}, \ \tilde{\mathbf{g}} = ||\mathbf{g}|| \begin{bmatrix} \alpha & \sqrt{1-\alpha^\dagger\alpha} \end{bmatrix}.$$

Our goal is to find the covariance matrix $Q = E[\tilde{\mathbf{x}}\tilde{\mathbf{x}}^\dagger]$ that maximizes the secrecy rate $I(\tilde{\mathbf{x}};y) - I(\tilde{\mathbf{x}};z)$ under the power constraint $tr(Q) \le P$. Once we find Q, we can easily transfer it back to the original space using the transformation matrix R.

A. Analytical Solution

For the transformed model (14), we have

$$R_s(Q) = I(\tilde{\mathbf{x}};y) - I(\tilde{\mathbf{x}};z) \tag{15}$$
$$= \log(1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger) - \log(1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger) \tag{16}$$
$$= \log\frac{1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger}{1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger}. \tag{17}$$

So, maximizing $R_s(Q)$ is equivalent to maximizing $(1 + \tilde{\mathbf{h}}Q\tilde{\mathbf{h}}^\dagger)/(1 + \tilde{\mathbf{g}}Q\tilde{\mathbf{g}}^\dagger)$. Since the matrix Q is Hermitian and positive semidefinite, it can be written as $Q = \sum_{i=1}^{2} \lambda_i u_i u_i^\dagger$, where u_i are orthogonal unit vectors and $\lambda_i \ge 0$ for $i = 1, 2$. Also,

since the optimal solution always uses up all available power (this point is more clear from the alternative method in Section III-B), we let $tr(Q) = P$, which yields $\sum_i \lambda_i = P$. Then, we can write

$$1 + \tilde{\mathbf{h}} Q \tilde{\mathbf{h}}^\dagger = \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger u_i + \sum_{i=1}^{2} \lambda_i \tilde{\mathbf{h}} u_i u_i^\dagger \tilde{\mathbf{h}}^\dagger \tag{18}$$

$$= \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger I_2 u_i + \sum_{i=1}^{2} \lambda_i u_i^\dagger \tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}} u_i \tag{19}$$

$$= \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i, \tag{20}$$

where we utilized the fact that for MISO $\tilde{\mathbf{h}} u_i$ is a scalar so that $\tilde{\mathbf{h}} u_i u_i^\dagger \tilde{\mathbf{h}}^\dagger = u_i^\dagger \tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}} u_i$. Similarly, we can write

$$1 + \tilde{\mathbf{g}} Q \tilde{\mathbf{g}}^\dagger = \sum_{i=1}^{2} \frac{\lambda_i}{P} u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i. \tag{21}$$

Thus,

$$\frac{1 + \tilde{\mathbf{h}} Q \tilde{\mathbf{h}}^\dagger}{1 + \tilde{\mathbf{g}} Q \tilde{\mathbf{g}}^\dagger} = \frac{\sum_{i=1}^{2} \lambda_i u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i}{\sum_{i=1}^{2} \lambda_i u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i}. \tag{22}$$

Denote $a_i = u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i$ and $b_i = u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i$, then maximizing $R_s(Q)$ is equivalent to

$$\text{maximize } M \text{ such that } \frac{\sum_i \lambda_i a_i}{\sum_i \lambda_i b_i} \geq M. \tag{23}$$

Since $\lambda_i \geq 0$, $a_i \geq 0$, and $b_i \geq 0$, the above problem can be rewritten as $\sum_i \lambda_i (a_i - M b_i) \geq 0$. The largest M that satisfies the constraint is

$$M^* = \max_i \frac{a_i}{b_i}, \tag{24}$$

and the corresponding λ_i are

$$\lambda_j = \begin{cases} P & j = \arg\max_i \frac{a_i}{b_i}, \\ 0 & \text{otherwise.} \end{cases} \tag{25}$$

Moreover,

$$\max_i \frac{a_i}{b_i} = \max_u \frac{u_i^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) u_i}{u_i^\dagger (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}) u_i}, \tag{26}$$

which can be converted to a well known Rayleigh quotient problem. To see this, note that $I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}$ is Hermitian and positive definite, so it can be factorized as $I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}} = VD^2V^\dagger$ where V is unitary and contains the eigenvectors of the matrix, and D is diagonal and contains the square roots of the associated eigenvalues. Since the eigenvalues are nonzero, we can define a new vector related to u by an invertible transformation: $v = DV^\dagger u$. Then the optimization problem becomes

$$\max_v \frac{v^\dagger D^{-1} V^\dagger (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) V D^{-1} v}{v^\dagger v}. \tag{27}$$

The optimal solution v^* is just the eigenvector corresponding to the largest eigenvalue of the matrix $D^{-1}V^\dagger(I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}})VD^{-1}$. This may then be transformed back to obtain the optimal normalized solution u^*. The resulting optimal covariance matrix is simply $Q^* = Pu^*u^{*\dagger}$. We note that the solution u^* is also the generalized eigenvector corresponding to the largest generalized eigenvalue of the two matrices $I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}$ and $I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}}$. In other words, it is the eigenvector with the largest eigenvalue of the matrix

$$A = (I_2 + P\tilde{\mathbf{g}}^\dagger \tilde{\mathbf{g}})^{-1} (I_2 + P\tilde{\mathbf{h}}^\dagger \tilde{\mathbf{h}}) \tag{28}$$

$$= \begin{bmatrix} P||\mathbf{g}||^2 \alpha^\dagger \alpha + 1 & P||\hat{\mathbf{g}}||^2 \alpha^\dagger \sqrt{1 - \alpha^\dagger \alpha} \\ P||\mathbf{g}||^2 \alpha \sqrt{1 - \alpha^\dagger \alpha} & P||\mathbf{g}||^2 (1 - \alpha^\dagger \alpha) + 1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} P||\hat{\mathbf{h}}||^2 + 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{29}$$

B. Alternative View

The method in previous subsection gives an analytical solution to our problem. An alternative view might provide more insight to this problem, as we will explain in this section.

We can expand (14) to the following

$$y = ||\mathbf{h}|| \tilde{x}_1 + w_1, \tag{30a}$$

$$z = ||\mathbf{g}|| \left(\alpha \tilde{x}_1 + \sqrt{1 - \alpha^\dagger \alpha}\, \tilde{x}_2 \right) + w_2. \tag{30b}$$

Then we can write the achievable secrecy rate as

$$R_s(Q) = I(\tilde{\mathbf{x}}; y) - I(\tilde{\mathbf{x}}; z) \tag{31}$$

$$= H(y) - H(y|\tilde{\mathbf{x}}) - (H(z) - H(z|\tilde{\mathbf{x}})) \tag{32}$$

$$= H(y) - H(z) \tag{33}$$

$$= \log(2\pi e P_y) - \log(2\pi e P_z), \tag{34}$$

where the last step uses the assumption that $\tilde{\mathbf{x}}$ is a zero mean Gaussian random variable. P_y and P_z are the output powers at Bob and Eve respectively. Denote P_1 and P_2 as the power of $\tilde{x}_1$ and $\tilde{x}_2$, then we have

$$P_y = E[yy^\dagger] = ||\mathbf{h}||^2 P_1 + 1, \tag{35}$$

$$P_z = E[zz^\dagger] = ||\mathbf{g}||^2 \left(\alpha \alpha^\dagger P_1 + (1 - \alpha^\dagger \alpha) P_2 + \gamma \right) + 1, \tag{36}$$

with

$$\gamma = \alpha \sqrt{1 - \alpha^\dagger \alpha} E[\tilde{x}_1 \tilde{x}_2^\dagger] + \alpha^\dagger \sqrt{1 - \alpha^\dagger \alpha} E[\tilde{x}_1^\dagger \tilde{x}_2]. \tag{37}$$

Define ρ be the normalized correlation coefficient

$$\rho = \frac{E[\tilde{x}_1 \tilde{x}_2^\dagger]}{\sqrt{P_1 P_2}},$$

then

$$\gamma = \alpha \sqrt{1 - \alpha^\dagger \alpha} \rho \sqrt{P_1 P_2} + \alpha^\dagger \sqrt{1 - \alpha^\dagger \alpha} \rho^\dagger \sqrt{P_1 P_2} \tag{38}$$

$$= (\alpha \rho + \alpha^\dagger \rho^\dagger) \sqrt{(1 - \alpha^\dagger \alpha) P_1 P_2} \tag{39}$$

$$= 2\Re(\alpha \rho) \sqrt{(1 - \alpha^\dagger \alpha) P_1 P_2}. \tag{40}$$

Now our problem is converted to finding the optimal $\{P_1, P_2, \rho\}$ (which determines Q), to maximize $I(\tilde{\mathbf{x}}; y) - I(\tilde{\mathbf{x}}; z)$ with the power constraint $P_1 + P_2 \leq P$.

An important observation here is that the optimization over the correlation coefficient ρ can be separated from the optimization over the power allocation. For a given power allocation $\{P_1, P_2\}$, to maximize $R_s(Q)$, we should minimize $H(z)$, which is equivalent to minimizing P_z, and in turn minimizing γ. From (40), we conclude that we should choose ρ to minimize $\Re(\alpha\rho)$, and meanwhile satisfy the constraint $\rho\rho^\dagger \leq 1$. Let α_r and α_i denote the real and imaginary part of α respectively, and similarly for ρ_r and ρ_i, then ρ_r and ρ_i is the solution to the following optimization problem:

$$\begin{aligned} &\text{minimize} && \alpha_r\rho_r - \alpha_i\rho_i, \\ &\text{subject to} && \rho_r^2 + \rho_i^2 \leq 1. \end{aligned} \tag{41}$$

This is a convex optimization problem that can be easily solved with the Lagrangian method, and the optimal solution is $\rho^* = -\alpha^\dagger/||\alpha||$.

With $\rho = \rho^*$, we obtain

$$\gamma = -2||\alpha||\sqrt{(1-\alpha^\dagger\alpha)P_1P_2}, \tag{42}$$

$$\sigma_z^2 = ||\mathbf{g}||^2\left(\sqrt{\alpha^\dagger\alpha P_1} - \sqrt{(1-\alpha^\dagger\alpha)P_2}\right)^2 + 1. \tag{43}$$

Substituting (35) and (43) back to (34), we obtain

$$R_s(P_1, P_2) = \log(P_y) - \log(P_z) \tag{44}$$

$$= \log\left(\frac{||\mathbf{h}||^2P_1 + 1}{||\mathbf{g}||^2\left(\sqrt{\alpha^\dagger\alpha P_1} - \sqrt{(1-\alpha^\dagger\alpha)P_2}\right)^2 + 1}\right). \tag{45}$$

Now, we can choose P_1 and P_2 to maximize the above secrecy rate with the power constraint. Note that the denominator is minimized when $\sqrt{\alpha^\dagger\alpha P_1} = \sqrt{(1-\alpha^\dagger\alpha)P_2}$, which implies that $\tilde{x}_1$ and $\tilde{x}_2$ cancel each other completely at the eavesdropper's receiver so that she essentially gets no information on the input. We call this zero-forcing at Eve, and when it happens, we have

$$P_2 = \frac{\alpha^\dagger\alpha}{1-\alpha^\dagger\alpha}P_1. \tag{46}$$

Thus, for a given P_1, if $P - P_1 \geq \frac{\alpha^\dagger\alpha}{1-\alpha^\dagger\alpha}P_1$, which means $P_1 \leq (1-\alpha^\dagger\alpha)P$, we should choose $P_2 = \frac{\alpha^\dagger\alpha}{1-\alpha^\dagger\alpha}P_1$ to maximize $R_s(P_1, P_2)$. When $P_1 > (1-\alpha^\dagger\alpha)P$, due to the power constraint, zero-forcing is not possible. To maximize $R_s(P_1, P_2)$, we should do the canceling as much as possible, which means $P_2 = P - P_1$. With this analysis, we can remove P_2 from the parameter list and obtain that

for $P_1 \leq (1-\alpha^\dagger\alpha)P$

$$R_s(P_1) = \log(||\mathbf{h}||^2P_1 + 1), \tag{47}$$

and for $(1-\alpha^\dagger\alpha)P \leq P_1 \leq P$

$$R_s(P_1) = \log\left(\frac{||\mathbf{h}||^2P_1 + 1}{||\mathbf{g}||^2 f(P_1)^2 + 1}\right) \tag{48}$$

where

$$f(P_1) = \sqrt{\alpha^\dagger\alpha P_1} - \sqrt{(1-\alpha^\dagger\alpha)(P-P_1)}.$$

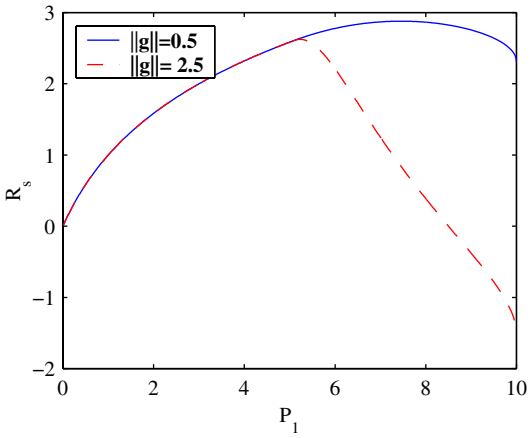


Fig. 2. Change of $R_s(P_1)$ with P_1 at different Eve's channel gains. $\alpha = 0.7$. $P = 10$, $||\mathbf{h}|| = 1$.

Note that the first segment of $R_s(P_1)$ increases with P_1, which means it has the maximum at $P_1 = (1-\alpha^\dagger\alpha)P$. This corresponds to the best secrecy rate with zero-forcing, and can be consider as the lower bound to our achievable secrecy rate. However, zero-forcing rate is constant regardless of Eve's actual channel gain, so it might not be the optimal P_1, as we can see from Figure 2. For the same $\alpha = 0.7$, when Eve's channel gain is relatively large, the zero-forcing rate (corresponding to the intersection of the two curves) is very good, while when Eve's channel gain is relatively small, it is not the best achievable secrecy rate.

It is easy to see that the power constraint should always be satisfied with equality, since the optimal P_1 satisfies $P_1 \geq (1-\alpha^\dagger\alpha)P$. Also, we only need to maximize the second segment of $R_s(P_1)$ over its corresponding range of P_1. However, the function format is complicated, and an analytical optimal solution of P_1 is hard to obtain in this way.

This view gives some insight on how coding should be performed for secrecy reason. Note that $\rho^*\rho^{*\dagger} = 1$ suggests that $\tilde{x}_2 = c\tilde{x}_1$, where c is some optimally chosen constant. In other words, $\tilde{x}_2$ is linearly correlated with $\tilde{x}_1$ in such a way that they cancel each other to some optimal extent at Eve. When (46) holds, the two inputs completely cancel each other, and the mutual information between z and the input $\tilde{\mathbf{x}}$ is zero. If we consider $\tilde{x}_1$ as the information bearing signal, and $\tilde{x}_2$ as a jamming signal, then our problem is a little similar to the correlated jamming case described in [20], except that we have a different objective function and the jammer and the user are cooperative.

IV. Numerical Evaluation

We now evaluate the achievable secrecy rate $R_s^* = \max_Q \log(1+\mathbf{h}Q\mathbf{h}^\dagger) - \log(1+\mathbf{g}Q\mathbf{g}^\dagger)$, and see how it varies with the MISO channel realizations $\mathbf{h}$ and $\mathbf{g}$ pictorially. For a fixed power budget P, R_s^* is determined by $||\mathbf{h}||$, $||\mathbf{g}||$ and α. In evaluation, we fix $||\mathbf{h}|| = 1$, and vary $||\mathbf{g}||$ and α. For simplicity, we consider only the real channel here so that α is real. It does not matter if α is positive or negative, since ρ^* will always compensate that factor, so we only evaluate the secrecy rate with positive α. The results are shown in Figure 3.

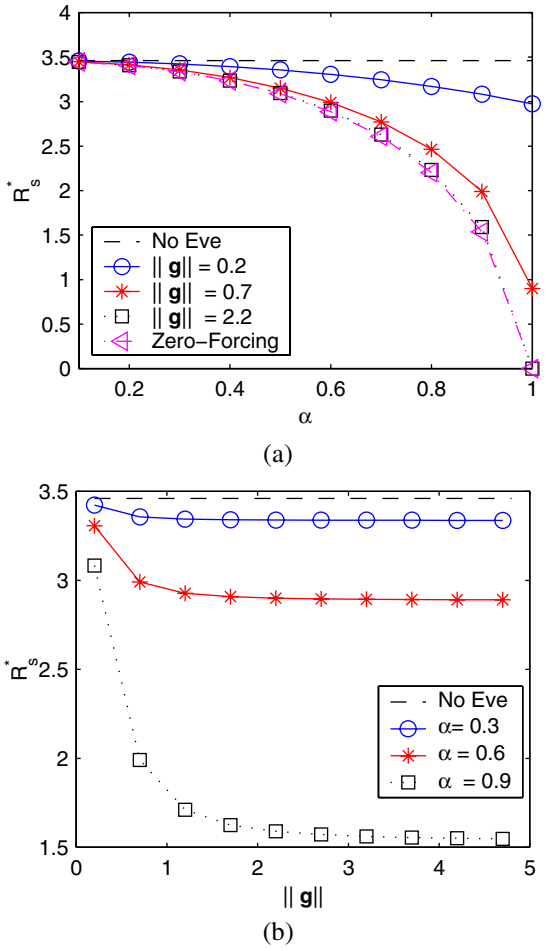


Fig. 3. Change of R_s^* with the normalized channel correlation coefficient α and Eve's channel gain α. $P = 10$, $||\mathbf{h}|| = 1$.

We note that Eve's channel gain $||\mathbf{g}||$ has a significant effect on the secrecy rate only when it is worse than Bob's channel. When $||\mathbf{g}|| > ||\mathbf{h}||$, zero-forcing strategy is close to optimal, and $||\mathbf{g}||$ becomes almost irrelevant. Actually, the curves in Figure 3(b) converges to the corresponding zeros-forcing rates as $||\mathbf{g}||$ increases. As expected, the larger α, the more correlated the two channels are, the lower the secrecy rate. α plays the critical role on the achievable secrecy rate when $||\mathbf{g}|| > ||\mathbf{h}||$. Increasing α results in a sharp drop of the secrecy rate, and $\alpha = 1$ shuts down the secure communication completely when $||\mathbf{g}|| > ||\mathbf{h}||$. On the other hand, we note that when α is small, the rate loss relative to the normal capacity without eavesdroppers is small. Moreover, as long as the normalized channel correlation $\alpha \neq 1$, we can get a positive secrecy rate no matter how strong Eve's channel is. Since $\alpha = 1$ means Eve's channel is a scaled version of Bob's channel, the chance of this to happen is small in a fading environment with multiple antennas. Also, the more number of transmit antennas, the more likely that the correlation of the two channels is small. Therefore, multiple transmit antennas provide more freedom, and in turn allow secret communication even when Eve's channel is much better.

V. Conclusions and Future Work

In this paper, we studied the achievable secrecy rate for a MIMO system, and the optimal input structure to achieve this rate. For the general multiple input multiple output case, the problem is not convex and is hard to solve. However, for the MISO case, the problem can be reformulated, and can be solved easily. An analytical solution is derived for this simple case and the implication of the results are discussed in this paper. We note that, in practice, Eve's channel is in general not known and is time varying. However, in cases where Eve's general statistics are known, we may wish to look at more general notions for the secrecy relationship between Alice, Bob and Eve, and we are currently examining such formulations as part of our ongoing effort.

References

[1] A. Wyner. The wire-tap channel. *Bell. Syst. Tech. J.*, 54(8):1355–1387, January 1975.

[2] I. Csiszár and J. Körner. Broadcast channels with confidental messages. *IEEE Trans. on Inf. Theory*, 24(3):339–348, May 1978.

[3] Ueli M. Maurer and Stefan Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In *EUROCRYPT*, pages 351–368, 2000.

[4] C. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. on Information Theory*, 41:1915–1923, 1995.

[5] J. Körner and K. Marton. Comparison of two noisy channels. In I. Csiszár and P. Elias, editors, *Topics In Information Theory*, pages 411–423. Colloquia Mathematica Societatis Janos Bolyai, Amsterdam, The Netherlands: North Holland, 1977.

[6] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[7] M. Van Dijk. On a special class of broadcast channels with confidential messages. *IEEE Trans. Information Theory*, 43(2):712 – 714, March 1997.

[8] Z. Li, R. Yates, and W. Trappe. Secrecy capacity of independent parallel channels. In *Forty-Fourth Annual Allerton Conference on Communications, Control and Computing*, Sept 2006.

[9] P.K. Gopala, L. Lai, and H. El-Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Information Theory*. submitted 2006.

[10] Y. Liang, V.H. Poor, and S. Shamai(shitz). Secure communication over fading channels. *IEEE Trans. Information Theory*, submitted 2006.

[11] Z. Li, R. Yates, and W. Trappe. Secure communication with a fading eavesdropper channel. In *IEEE Int. Symp. Inf. Theory*, submitted 2007.

[12] A. O. Hero. Secure space-time communication. *Information Theory, IEEE Transactions on*, 49(12):3235 – 3249, Dec 2003.

[13] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *IEEE Int. Symp. Inf. Theory*, pages 2152 – 2155, Sept 2005.

[14] R. Negi and S. Goel. Secret communication using artificial noise. In *Proc. IEEE Vehicular Tech. Conf*, Fall 2005.

[15] R. Goel and R. Negi. Secret communication in presence of colluding eavesdroppers. In *Proc. IEEE Military Communication (MILCOM)*, 2005.

[16] X. Li and E. P. Ratazzi. MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks. In *Proc. IEEE Military Communications Conference (MILCOM'2005)*, 2005. Atlantic City, NJ.

[17] X. Li, M. Chen, and E. P. Ratazzi. Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy. In *The 6th IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC'05)*, 2005. The Italian Academy at Columbia University, New York.

[18] I.E. Telatar. Capacity of multi-antenna gaussian channels. *European Transactions on Telecommunications*, 10(6), Nov/Dec 1999.

[19] R. Horst and H. Tuy. *Global Optimization: Deterministic Approaches*. Berlin: Springer-Verlag, 3rd edition, 1996.

[20] M. Medard. Capacity of correlated jamming channels. In *Thirty-fifth Annual Allerton Conference on Communications, Control and Computing*, Sept 1997.