The Secrecy Capacity of the $2 \times 2$ MIMO Wiretap Channel

Frédérique Oggier and Babak Hassibi

Abstract—We consider the MIMO wiretap channel, that is a MIMO broadcast channel where the transmitter sends some confidential information to one user which is a legitimate receiver, while the other user is an eavesdropper. Perfect secrecy is achieved when the transmitter and the legitimate receiver can communicate at some positive rate, while insuring that the eavesdropper gets zero bits of information. In this paper, we compute the secrecy capacity of a two antenna MIMO broadcast channel.

I. INTRODUCTION

Security in wireless communication is a critical issue, which has recently attracted a lot of interest. It has been investigated from several different points of view, one of them being information theoretic security. In this context, most of the works dealing with wireless communication are based on the seminal work of Wyner [14], and its model, the wire-tap channel. The wire-tap channel is a broadcast channel, where the transmitter wants to send some confidential information to a legitimate receiver, while the second user is an eavesdropper. The secrecy capacity is defined as the rate at which the transmitter can communicate with the legitimate receiver, while insuring that the eavesdropper cannot get more than a fixed amount of information, being zero in the case of perfect secrecy. Wyner showed for discrete memoryless channels that the secrecy capacity is actually the difference of the capacity of the two users. This result has been generalized to Gaussian channels by Leung et al [7]. The wire-tap channel has been adopted as a model for several works addressing the question of security in single antenna fading channels [1], [9], [5], [2], [10].

We are here interested in the secrecy capacity in the multiple antenna case. A first study of the problem (not in the wire-tap channel case) has been done by Hero [6]. Very recent results on that problem have been done by Li et al. [8], where a lower bound is computed, and by Liu et al. [11], where they consider the case of a single antenna receiver.

In this paper, we compute the secrecy capacity of a two antenna wire-tap channel. One of the difficulties in studying the MIMO wire-tap channel is that the broadcast MIMO channel is not degraded, an assumption which is crucial in the proof of the converse in the original paper by Wyner. In order to compute the secrecy capacity, we provide a proof technique for the converse, which is different than the original one, and allows us to deal with channels that are not degraded. Note that our result shows that the inner bound by Li et al. [8] is tight, and this is proved by the computation of an upper bound that actually matches the lower bound.

The paper is organized as follows. In Section II, we set up the framework and give the secrecy capacity of the $2 \times 2$ MIMO wiretap channel. In Section III, we prove an achievability result. Section IV contains the main results, namely the proof of the converse.

II. CHANNEL MODEL AND SECRECY CAPACITY

Consider the following broadcast channel:

$$Y' = H_M X + V'_M$$

$$Z' = H_E X + V'_E$$

where $X, Y', Z', V'_M, V'_E$ are $2 \times 1$ vectors, and $H_M, H_E$ are fixed $2 \times 2$ matrices, that we assume invertible. The notation that we will use throughout the paper is that the subscript $M$ refers to the main channel (the one of the legitimate receiver), while the subscript $E$ refers to the eavesdropper channel.

The transmitted signal $X$ has covariance matrix $K_X \succeq 0$, with furthermore $\text{Tr}(K_X) = P$, where $P$ denotes the power at the transmitter. The noise matrices $V'_M$ and $V'_E$ are independent circularly symmetric complex Gaussian vectors with identity covariance and independent of the transmitted signal $X$. We can thus write the channel model as

$$Y = H_M^\dagger Y' = X + H_M^\dagger V'_M = X + V_M$$

$$Z = H_E^\dagger Z' = X + H_E^\dagger V'_E = X + V_E$$

which makes the channel matrices identity. The noise covariances are now given by

$$K_M = (H_M^\dagger H_M)^{-1} \succ 0, \quad K_E = (H_E^\dagger H_E)^{-1} \succ 0.$$  

The transmitter wants to send a confidential message $W^k$ to the legitimate receiver, which is encoded into a codeword $X^n$, using a $(2^nR, R)$ code. The decoder computes an estimate $\hat{W}^k$ of the transmitted message $W^k$, and the probability $P_e$ of decoding wrongly is given by

$$P_e = Pr(W^k \neq \hat{W}^k).$$

The level of ignorance of a transmitted message $W^k$ at the eavesdropper is called the equivocation rate, defined as:

Definition 1: Let $h$ denote the differential entropy. The equivocation rate $R_e$ at the eavesdropper is

$$R_e = \frac{1}{n} h(W^k | Z^n).$$

We have $0 \leq R_e \leq h(W^k)/n$, and when $R_e$ reaches the information rate $h(W^k)/n$, then $I(Z^n | W^k) = 0$, which yields perfect secrecy.
In this work, we consider the perfect secrecy case.

**Definition 2:** A perfect secrecy rate $R_s$ is said to be achievable if for any $\epsilon > 0$, there exists a sequence of codes $(2^{nR_s}, n)$ such that for any $n \geq n(\epsilon)$, we have

$$P_e \leq \epsilon \quad R_s - \epsilon \leq R_e.$$

The secrecy capacity is defined similarly to the standard capacity:

**Definition 3:** The secrecy capacity $C_s$ is the maximum achievable perfect secrecy rate.

The contribution of this paper is to prove the following:

**Theorem 1:** The secrecy capacity $C_s$ of the $2 \times 2$ MIMO wiretap channel is given by

$$C_s = \max_{K_X} \log \det(I + K_X K_M^{-1}) - \log \det(I + K_X K_E^{-1}),$$

or alternatively

$$C_s = \max_{K_X} \log \det(I + H_M K_X H_M^*) - \log \det(I + H_E K_X H_E^*)$$

where $K_X \succeq 0$ such that $\text{Tr}(K_X) = P$.

**III. ON THE ACHIEVABILITY**

In this section, we state the achievability part of the secrecy capacity, and further prove that the achievability is maximized by rank 1 matrices.

**Proposition 1:** The perfect secrecy rate

$$R_s = \max_{K_X} \log \det(I + K_X K_M^{-1}) - \log \det(I + K_X K_E^{-1})$$

is achievable. This has already been proven [8]. In fact, the interpretation is obvious. When $K_X$ is chosen, the difference between the resulting mutual informations to the legitimate user and eavesdropper can be secretly transmitted.

**Proposition 2:** Let $K_X$ be an optimal solution to the optimization problem

$$\max K_X \log \det(I + K_X K_M^{-1}) - \log \det(I + K_X K_E^{-1})$$

s.t.

$$K_X \succeq 0, \quad \text{Tr}(K_X) = P,$$

where $K_E - K_M$ is indefinite. Then $K_X$ is a low rank matrix.

**Proof:** In order to show that the optimal $K_X$ is low rank, we define a Lagrangian which includes the power constraint, and show that this yields no solution. From there, we conclude that the optimal solution is on the boundary of the cone of positive semi-definite matrices, i.e., it is rank 1.

We thus define the following Lagrangian:

$$\log \det(I + K_X K_M^{-1}) - \log \det(I + K_X K_E^{-1}) - \lambda \text{Tr}(K_X),$$

and look for its stationary points, that is for the solution of the following equation:

$$\nabla_{K_X} (\log \det(I + K_X K_M^{-1}) - \log \det(I + K_X K_E^{-1}) - \lambda \text{Tr}(K_X)) = 0 \\
\iff (K_M + K_X)^{-1} = (K_E + K_X)^{-1} + \lambda I.$$  \hspace{1cm} (1)

By pre-multiplying the above equation by $(K_X + K_M)$ and post-multiplying it by $(K_X + K_E)$, and vice versa, by pre-multiplying it by $(K_X + K_E)$ and post-multiplying it by $(K_X + K_M)$, we get two new equations:

$$\begin{cases} 
K_E + K_X = K_M + K_X + \lambda (K_M + K_X)(K_E + K_X) \\
K_E + K_X = K_M + K_X + \lambda (K_E + K_X)(K_M + K_X),
\end{cases}$$

so that by subtracting these two equations, one gets that solutions of (1) are included into the set of solutions of

$$\begin{align*}
0 &= (K_M + K_E)K_E - K_E K_M \\
&\quad + K_X ((K_E - K_M) + (K_M - K_E)K_X).
\end{align*}$$  \hspace{1cm} (2)

**Part 1.** We start by computing the solutions of (2), which is a Lyapunov equation in $K_X$. Clearly they are of the form $K_X' + K_X''$, where $K_X'$ is a particular solution of (2), while $K_X''$ is the solution of

$$K_X'' = \frac{-1}{2}(K_M + K_E)$$

which does not depend on $\lambda$. It is immediate to check that

$$K_X' = \frac{-1}{2}(K_M + K_E)$$

is a solution of (2). Now, consider the eigendecomposition $K_M - K_E = U\Sigma U^*$, where $U$ is a unitary matrix and $\Sigma$ is a diagonal matrix containing the eigenvalues of $K_M - K_E$. Thus, (3) can be rewritten as

$$U\Sigma U^* K_X - K_X U\Sigma U^* = 0 \iff \Sigma U^* K_X U - U^* K_X U \Sigma = 0.$$

Since $\Sigma$ is diagonal, we deduce that $U^* K_X U = D$, where $D$ is diagonal, so that

$$K_X'' = U D U^*.$$ In other words, solutions of (3) are diagonalizable in the same basis as $K_M - K_E$. Thus, we conclude that solutions of (2) are of the form

$$K_X = \frac{-1}{2}(K_M + K_E) + U D U^*.$$  \hspace{1cm} (4)

**Part 2.** Solutions of (1) are included in those of (2). We now show that none of the solutions of (2) are actually valid solutions for (1). By plugging solutions of (2) into (1),

$$K_M - \frac{1}{2}(K_M + K_E) + U D U^* - \frac{1}{2}(K_M + K_E) + U D U^* = \lambda I$$

or equivalently

$$\left(\frac{1}{2} \Sigma + D\right)^{-1} = \left(\frac{1}{2} \Sigma + D\right)^{-1} + \lambda I$$

should hold. Denote by $d_1, d_2$ respectively $\sigma_1, \sigma_2$ the diagonal coefficients of $D$ and $\Sigma$. We are left with the following system to solve:

$$\begin{cases} 
\frac{1}{\sigma_1 + 2 d_1} = -\frac{1}{\sigma_1 + 2 d_1} + \lambda \\
\frac{1}{\sigma_2 + 2 d_2} = -\frac{1}{\sigma_2 + 2 d_2} + \lambda \\
d_1 + d_2 = P + \text{Tr}(K_M + K_E)
\end{cases}$$
where the last constraint comes from \( \text{Tr}(K_X) = P \). Solving the system for \( \lambda \) yields
\[
\sigma_1(d_2^2 - \sigma_2^2/4) = \sigma_2(d_2^2 - \sigma_1^2/4),
\]
where \( d_2^2 = (P + \text{Tr}(K_M + K_E))^2 - d_2^2 \). For this solution to have real roots, we need
\[
-\sigma_1\sigma_2 \left(-4 \left( P + \text{Tr}(K_M + K_E) \right)^2 + (\sigma_1 - \sigma_2)^2 \right) \geq 0,
\]
namely
\[
(\sigma_1 - \sigma_2)^2 \geq (2P + \text{Tr}(K_M + K_E))^2 \]
\[\iff \text{Tr}((K_M - K_E)^2) - 2\text{det}(K_M - K_E) \geq 4P^2 + 2P\text{Tr}(K_M + K_E) + \text{Tr}(K_M + K_E)^2 \]
for \( \sigma_1 > 0, \sigma_2 < 0 \) and \( \sigma_1 < 0, \sigma_2 > 0 \) (the case of interest here). For the above inequality to be true, we at least need
\[
\text{Tr}((K_M - K_E)^2) - 2\text{det}(K_M - K_E) \geq 2\text{det}(K_M + K_E) + \text{Tr}((K_M + K_E)^2)
\]
which yields a contradiction.

\[\square\]

IV. PROOF OF THE CONVERSE

The goal of this section is to prove the converse, namely

**Theorem 2:** For any sequence of \((2^{nR_s}, n)\) codes with probability of error \( P_e \leq \epsilon \) and equivocation rate \( R_s - \epsilon \leq R_e \) for any \( n \geq n(\epsilon), \epsilon > 0 \), then the secrecy rate \( R_s \) satisfies
\[
R_s - \epsilon \leq \frac{1}{n}I[(X^n, Y^n | Z^n) + \delta].
\]

Thus, all the work consists of finding an upper bound on \( I(X; Y | Z) \). Clearly, it is upper bounded by taking the maximum over all input distributions \( \mathcal{P}(X) \):
\[
I(X; Y | Z) \leq \max_{\mathcal{P}(X)} I(X; Y | Z) = \max_{K_X} \hat{I}(X; Y | Z),
\]

where \( \hat{I}(X; Y | Z) \) denotes the value of \( I(X; Y | Z) \) when \( \mathcal{P}(X) \) is Gaussian, which will be proven to be the optimal strategy. At this point, the converse can be proved for the two “simple” cases when \( K_M \succ K_E \) and \( K_E \succ K_M \).

In general, \( V_M \) and \( V_E \) are independent. However, since the secrecy capacity does not depend on \( A \), the correlation between \( V_M \) and \( V_E \), for the purposes of tightening our upper bound we can assume that \( \hat{I}(X; Y | Z) \) is a function of both \( A \) and \( K_X \). We show that it is actually concave in \( K_X \) and convex in \( A \). As a result, we obtain a new upper bound
\[
I(X; Y | Z) \leq \max_{K_X} \hat{I}(X; Y | Z), \quad \text{for all } A,
\]
\[
\leq \min_A \max_{K_X} \hat{I}(X; Y | Z)
\]
\[
= \min_{K_X} \max_A \hat{I}(X; Y | Z).
\]

The last part of the proof (subsection IV-C) consists of computing the double optimization over \( A \) and \( K_X \). We find a closed form expression for the optimal \( A \), while proving that the optimal \( K_X \) has to be low rank, and finally show that the converse matches the achievability.

### A. Step 1

We start by recalling a standard result, which has already been proven in [7], [5].

**Lemma 1:** Given any sequence of \((2^{nR_s}, n)\) codes with \( P_e \leq \epsilon \) and \( R_s - \epsilon \leq R_e \) for any \( n \geq n(\epsilon), \epsilon > 0 \), the secrecy rate \( R_s \) can be upper bounded as follows:
\[
R_s - \epsilon \leq \frac{1}{n}I[(X^n, Y^n | Z^n) + \delta],
\]
for \( \epsilon, \delta > 0 \).

We thus focus now on finding an upper bound on \( I(X; Y | Z) \). Clearly
\[
I(X; Y | Z) \leq \max_{\mathcal{P}(X)} I(X; Y | Z),
\]

where \( \mathcal{P}(X) \) denotes the input distribution. Now note that
\[
I(X; Y | Z) = h(Y | Z) - h(Y | X, Z)
\]
\[
= h(Y | Z) - h(Y, Z | X) + h(Y | X, Z)
\]
\[
= h(Y | Z) - h(V_E, V_M) + h(V_E).
\]

Thus the optimization problem we have to solve is
\[
\max_{\mathcal{P}(X)} h(X + V_M, X + V_E) - h(X + V_E).
\]

We now prove that the optimal of the above optimization problem is given by choosing \( X \) Gaussian.

**Proposition 3:** Let \( A, B \) be circularly symmetric complex jointly Gaussian random vectors with strictly positive definite covariance matrices. Let \( X \) be a random vector independent of \( A \) and \( B \), and \( S \) be a positive definite matrix. The optimal solution to
\[
\max_{\mathcal{P}(X)} h(X + A, X + B) - h(X + B)
\]
\[\text{s.t. } \text{Tr}(K_X) = P \]
is Gaussian.

**Proof:** First note that
\[
\frac{1}{\sqrt{2}} \begin{pmatrix} I & -I \\ I & I \end{pmatrix} \begin{pmatrix} X + A \\ X + B \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}(A - B) \\ \sqrt{2}X + \frac{1}{\sqrt{2}}(A + B) \end{pmatrix}.
\]

Since multiplication by a unitary matrix does not change the entropy,
\[
h(X + A, X + B)
\]
\[
= h\left(\sqrt{2}X + \frac{1}{\sqrt{2}}(A + B), \frac{1}{\sqrt{2}}(A - B)\right)
\]
\[
h\left(\sqrt{2}X + \frac{1}{\sqrt{2}}(A + B), \frac{1}{\sqrt{2}}(A - B)\right) + h\left(\frac{1}{\sqrt{2}}(A - B)\right)
\]
\[
= h(\sqrt{2}X + U) + h\left(\frac{1}{\sqrt{2}}(A - B)\right)
\]
where \( U \) is Gaussian with covariance matrix \( K_U \) given by
\[
\frac{1}{2}E[(X + B)(A + B)^*] - \frac{1}{2}E[(A + B)(A - B)^*] - E[(A - B)(A - B)^*]^{-1}E[(A - B)(A + B)^*],
\]
using conditional Gaussian distribution.
To maximize
\[ h(X + A, X + B) - h(X + B), \]
we thus need to maximize
\[ h(\sqrt{2}X + U) - h(X + B), \]
or equivalently
\[ h(X + U') - h(X + B) \]
where \( U' = U/\sqrt{2} \) is Gaussian, independent of \( X \). The optimal distribution of such expression has been shown to be Gaussian by Liu and Viswanath [12] in the case of real Gaussian vectors. Their result can be readily extended to the circularly symmetric complex Gaussian case. 

Finally, a straightforward computation shows that by replacing \( A \) with \( K_M \) in \( \tilde{I}(X; Y|Z) \) yields
\[
\log \det(I + K_X K_M^{-1}) - \log \det(I + K_X K_E^{-1}).
\]

Similarly if \( K_M \succ K_E \), we are free to choose \( A = K_E \), which satisfies (5), so that the second term dominates the first, and the optimal \( K_X \) is 0.

The cases described in the lemma can be understood as a simple generalization of the scalar case, since those are the degraded cases. When \( K_E \succ K_M \), both links to the legitimate receiver are better, and the capacity is given by the difference of the two capacities, while if \( K_M \succ K_E \), then both links to the eavesdropper are better, and thus no positive secrecy capacity can be achieved.

We are now left with the case when \( K_M - K_E \) is indefinite, which is the non-degraded case, and thus the interesting case.

\[ B. \text{ Step 2} \]

We have shown in Proposition 4 that
\[ I(X; Y|Z) \leq \max_{K_X} \tilde{I}(X; Y|Z). \]

Since this is true for all \( A \), we further have that
\[ I(X; Y|Z) \leq \min_{A} \text{max}_{K_X} \tilde{I}(X; Y|Z). \]

To understand this double optimization, we start by analyzing the function \( \tilde{I}(X; Y, Z) \).

Proposition 5: The function \( \tilde{I}(X; Y, Z) \) defined in (4) is concave in \( K_X \) and convex in \( A \). Consequently,
\[ \min_{A} \max_{K_X} \tilde{I}(X; Y|Z) = \max_{K_X} \min_{A} \tilde{I}(X; Y|Z) \]

where \( K_X \) and \( A \) respectively satisfy
\[ \text{Tr}(K_X) = P, K_X \succeq 0, K_M - A K_E^{-1} A^* \succeq 0. \]

Proof: We start by rewriting \( \tilde{I}(X; Y, Z) \):
\[
\tilde{I}(X; Y, Z) = \\
\log \det(K_Y Z) - \log \det(K_Z) - \log \det(K_M) + \log \det(K_E) \\
= \log \det \left( K_M + \left( \begin{array}{c} K_X \\ A \\ A^* \end{array} \right) \right) \\
- \log \det \left( K_X + K_E \right) - \log \det \left( K_M \right) + \log \det \left( K_E \right) \\
= \log \det \left( I + \left( \begin{array}{c} K_M \\ A \\ A^* \end{array} \right) \right) \\
- \log \det \left( K_X + K_E \right) + \log \det \left( K_E \right).
\]

An alternative way of writing \( \tilde{I}(X; Y|Z) \) is then
\[
\log \det \left( I + \left( \begin{array}{c} K_M \\ A \\ A^* \end{array} \right) \right) \\
- \log \det \left( I + K_E^{-1} K_X \right).
\]

Convexity in \( A \). Set
\[
C := \left( \begin{array}{c} K_M \\ A \\ A^* \end{array} \right) \left( \begin{array}{c} K_M \\ A \\ A^* \end{array} \right)^{-1}.
\]

Now \( \tilde{I}(X; Y|Z) \) is of the form \( \log \det(I + CB) \), plus some constant term, where \( B \succeq 0 \). It can thus be shown that \( \tilde{I}(X; Y|Z) \) is convex in \( C \) (the same kind of proof that shows
that log det($K_X$) is concave holds [3, p.74]). Furthermore, it is convex in any block of $C$, thus convex in $A$. Also, the set of $A$ such that $K_M - AK_E^{-1}A^* \succ 0$ is convex.

**Concavity in $K_X$.** Note first that

$$
\begin{pmatrix}
K_M & A \\
A^* & K_E
\end{pmatrix} = 
\begin{pmatrix}
I & AK_E^{-1} \\
0 & I
\end{pmatrix}
\begin{pmatrix}
K_M - AK_E^{-1}A^* & 0 \\
0 & K_E
\end{pmatrix} 
\begin{pmatrix}
I & 0 \\
K_E^{-1}A^* & I
\end{pmatrix}.
$$

Set

$$B := (I, I) \begin{pmatrix}
K_M & A \\
A^* & K_E
\end{pmatrix}^{-1} \begin{pmatrix}
I \\
I
\end{pmatrix}.$$

We have that $B \succ K_E^{-1}$, since

$$
\begin{pmatrix}
K_M - AK_E^{-1}A^* & 0 \\
0 & K_E
\end{pmatrix}^{-1} \begin{pmatrix}
I & 0 \\
K_E^{-1}A^* & I
\end{pmatrix} = (I - K_E^{-1}A^*)(K_M - AK_E^{-1}A^*)^{-1}(I - AK_E^{-1}) + K_E^{-1}.
$$

We now have that $\tilde{I}(X;Y|Z)$ is given by

$$\log \det (I + BK_X) - \log \det (I + K_E^{-1}K_X) = \log \det (I + B K_X) - \log \det (I + K_E^{-1}K_X).
$$

By computing the gradient of (6) with respect to $K_X$, we get that

$$(B^{-1} + K_X)^{-1} - (K_E + K_X)^{-1} \succ 0,$$

since $B \succ K_E^{-1}$. Recall that

$$\frac{\partial(X^{-1})_{kl}}{\partial X_{ij}} = -(X^{-1})_{kl}(X^{-1})_{ji},$$

so that the derivative of $F := (K_E + K_X)^{-1}$ is a $4 \times 4$ matrix given by

$$
\begin{pmatrix}
-F F_{11} & -F F_{12} \\
-F F_{21} & -F F_{22}
\end{pmatrix} = - (K_E + K_X)^{-1} \otimes (K_E + K_X)^{-1}.
$$

To check the concavity in $K_X$, we are thus left to check that

$$(K_E + K_X)^{-1} \otimes (K_E + K_X)^{-1} \prec (B^{-1} + K_X)^{-1} \otimes (B^{-1} + K_X)^{-1},$$

which is true since $B \succ K_E^{-1}$ implies

$$(B^{-1} + K_X)^{-1} \succ (K_E + K_X)^{-1}.$$

Since we have shown above that $\tilde{I}(X;Y|Z)$ is concave in $K_X$ and convex in $A$, we have that

$$\min_{A} \max_{K_X} \tilde{I}(X;Y|Z) = \max_{K_X} \min_{A} \tilde{I}(X;Y|Z).$$

### C. Step 3

From the two previous proof steps, we now know that

$$I(X;Y|Z) \leq \max_{K_X} \min_{A} \tilde{I}(X;Y|Z).$$

This last step consists of computing the double optimization over $A$ and $K_X$, and show that the optimal $A$ yields the converse.

**Proposition 6:** Let $A^*$ be given by

$$A^* = \begin{pmatrix}
v_3 & K_E & v_1 \\
v_4 & w_2 & w_1
\end{pmatrix} \begin{pmatrix}
0 & 0 \\
0 & 0
\end{pmatrix}^{-1},
$$

where $w_1, w_2$ are arbitrary and $(v_1, v_2, v_3, v_4)^T$ is an eigenvector of the matrix $M$, as defined in (8). Then $A^*$ is a local minima of $\tilde{I}(X;Y|Z)$.

**Proof:** Let $M_1, M_2, M_3, X$ be square complex matrices. Set

$$f(X) = M_1 - (X + M_2) M_3 (X^* + M_2^*).$$

It can be shown that its gradient is

$$\nabla_X \log \det (f(X)) = - f(X)^{-1} (X + M_2) M_3.$$

Using this formula, we compute that

$$\nabla_A \tilde{I}(X;Y|Z) = 0 \iff f(A) (A^* + K_X)^{-1} (K_X + K_E) = g(A) (A^*)^{-1} K_E
$$

where

$$f(A) = K_X + K_M - (K_X + A)(K_X + K_E)^{-1} (K_X + A^*)$$

and

$$g(A) = K_M - AK_E^{-1} A^*.$$ 

This yields the following nonsymmetric Riccati equation:

$$A^*(K_X + K_M)^{-1} K_X K_E^{-1} A^* + [(K_X + K_E K_E^{-1} + K_X (K_X + K_M)^{-1} K_X K_E^{-1}) A^*
+ A^* [(K_X + K_M)^{-1} K_M] + K_X (K_X + K_M)^{-1} K_M = 0.$$

One way of solving an algebraic Riccati [4] of the form

$$0 = M_2 + M_2 A^* - A^* M_1 - A^* M_1 A^*,$$

is to look for invariant subspaces of

$$M = \begin{pmatrix}
M_{11} & M_{12} \\
M_{21} & M_{22}
\end{pmatrix}.$$

Here, we have that $M$ is defined by

$$M_{11} = -(K_X + K_M)^{-1} K_M$$

$$M_{12} = -(K_X + K_M)^{-1} K_X K_E^{-1}$$

$$M_{21} = K_X (K_X + K_M)^{-1} K_M$$

$$M_{22} = -(K_X + K_E) K_E^{-1} + K_X (K_X + K_M)^{-1} K_X K_E^{-1}$$

Let

$$F = \begin{pmatrix}
K_X + K_M & 0 \\
0 & (K_X + K_M) K_X^{-1}
\end{pmatrix},$$

$$G = \begin{pmatrix}
I & 0 \\
0 & K_E K_X^{-1}
\end{pmatrix}.$$ 

It is easy to see that

$$F (M + I) G = \begin{pmatrix}
K_X & -I \\
K_M & -K_M K_X^{-1}
\end{pmatrix},$$
which implies that $-1$ is an eigenvalue of $M$. Thus a first invariant subspace is given by the eigenspace associated to $-1$, given by the kernel of

$$M + I = F^{-1}\left(\begin{array}{c} K_X \\ K_M \end{array}\right) (I, -K_X^1)G^{-1}.$$ 

The kernel of $M + I$ is immediately checked to be

$$G\left(\begin{array}{c} K_X^{-1}U_1 \\ U_1 \end{array}\right) = \left(\begin{array}{c} K_X^{-1}U_1 \\ K_EK_X^{-1}U_1 \end{array}\right) = \left(\begin{array}{c} K_X^{-1}U_1 \\ K_EK_X^{-1}U_1 \end{array}\right),$$

for any $U_1$. Thus the first invariant subspace is of the form $(w_1, w_2, (w_1, w_2)K_E)^T$. Since $A^*$ is a $2 \times 2$ matrix, the second invariant subspace also has to be an eigenvector of $M$, which yields the result (see [4] for an explanation on how to find $A^*$ from the two invariant subspaces).

**Proposition 7:** Let $\tilde{K}_X$ be an optimal solution to the optimization problem

$$\max K_X \quad \min A \quad \tilde{I}(X;Y|Z)$$

s.t. $K_X \succeq 0$, $\text{Tr}(K_X) = P,$

where $A^*$ is the optimal solution for the minimization over $A$ as defined in (7). Then $\tilde{K}_X$ is a low rank matrix.

**Proof:** We know from (6) that

$$\tilde{I}(X;Y|Z) = \log \det(I + BK_X) - \log \det(I + K_E^{-1}K_X),$$

where

$$B = (I - K_E^{-1}A^*)(K_M - AK_E^{-1}A^*)^{-1}(I - AK_E^{-1}) + K_E^{-1}.$$ 

From Proposition 2, optimal $K_X$ are of the form

$$K_X = -\frac{1}{2}(B^{-1} + K_E) + UD^*U,$$

where $B^{-1} - K_E = U\Sigma U^*$, $D$ is diagonal and

$$\left(\frac{1}{2}\Sigma + D\right)^{-1} = \left(\frac{1}{2}\Sigma + D\right)^{-1} - \lambda I,$$

for some positive $\lambda$. Using the matrix inversion lemma,

$$B^{-1} - K_E = K_E - (K_E - A^*)(K_M + K_E - A^* - A)^{-1}(K_E - A),$$

so that $B^{-1} - K_E$ is given by

$$-(K_E - A^*)(K_M + K_E - A^* - A)^{-1}(K_E - A) = U\Sigma U^*.$$ 

Now $K_E - A^*$ is given by

$$K_E \left(\begin{array}{c} v_1 \\ v_2 \\ w_1 \\ w_2 \end{array}\right) - \left(\begin{array}{c} v_3 \\ v_4 \end{array}\right) K_E \left(\begin{array}{c} w_1 \\ w_2 \end{array}\right) = \left(\begin{array}{c} v_1 \\ v_2 \\ w_1 \\ w_2 \end{array}\right) - \left(\begin{array}{c} v_3 \\ v_4 \end{array}\right) 0$$

$$\left(\begin{array}{c} v_1 \\ v_2 \\ w_1 \\ w_2 \end{array}\right)^{-1}$$

thus $K_E - A^*$ is low rank and consequently $B^{-1} - K_E$ is.

The diagonal matrix $\Sigma$ then has at least one coefficient which is zero. Now Equation (9) is equivalent to

$$\frac{1}{\sigma_i/2 + d_i} = \frac{1}{-\sigma_i/2 + d_i} + \lambda, \quad i = 1, 2,$$

where $\Sigma = \text{diag}(\sigma_1, \sigma_2)$. Let us denote by $\sigma_j$ the diagonal coefficient which is zero. Then the $j$th equation yields

$$\frac{1}{d_j} = \frac{1}{d_j} + \lambda \Rightarrow \lambda = 0$$

and finally $\sigma_1 = \sigma_2 = 0$ which is a contradiction.

**Let us now fix some notations. Since $K_X$ is low rank with power constraint $\text{Tr}(K_X) = P$, it can be written $K_X = U^*AU$, with

$$A = \left(\begin{array}{c} 0 \\ 0 \end{array}\right), \quad U = \left(\begin{array}{c} u_{11} \\ u_{12} \\ u_{21} \\ u_{22} \end{array}\right).$$**

We further use

$$K_M = \left(\begin{array}{cc} (K_M)_{11} & (K_M)_{12} \\ (K_M)_{21} & (K_M)_{22} \end{array}\right), \quad K_E = \left(\begin{array}{cc} (K_E)_{11} & (K_E)_{12} \\ (K_E)_{21} & (K_E)_{22} \end{array}\right).$$

**Proposition 8:** Consider the function $\tilde{I}(X;Y|Z)$ where $K_X \succeq 0$ is low rank, such that $\text{Tr}(K_X) = P$. Consider furthermore the following vector space, $L$, generated by the vector

$$\left(\begin{array}{c} u_{21}(u_{11}(K_M)_{12} + u_{12}(K_M)_{22}) \\ -u_{21}(u_{11}(K_M)_{11} + u_{12}(K_M)_{21}) \end{array}\right) \frac{\text{det}(U)^2}{\text{det}(K_M)u_{12}u_{21}}.$$ 

Pick one vector $v = (v_1, v_2, v_3, v_4)$ in $L$, and set

$$A^* = \left(\begin{array}{cc} v_3 \\ v_4 \end{array}\right) K_E \left(\begin{array}{c} w_1 \\ w_2 \end{array}\right) \left(\begin{array}{c} v_3 \\ v_4 \end{array}\right) \left(\begin{array}{c} w_1 \\ w_2 \end{array}\right)^{-1}.$$**

Then $A^*$ is local minima of $\tilde{I}(X;Y|Z)$.

**Proof:** Since $K_X = U^*AU$, $M$ (see (8)) can be rewritten as

$$M_{11} = -U^*(\Lambda + UK_MU^*)^{-1}UK_M,$$

$$M_{12} = -U^*(\Lambda + UK_MU^*)^{-1}AK_E^{-1},$$

$$M_{21} = U^*(\Lambda + UK_MU^*)^{-1}UK_M,$$

$$M_{22} = -U^*UK_E^{-1} - I + U^*(\Lambda(U + K_M)^{-1}AK_E^{-1}).$$

Let

$$F = \left(\begin{array}{cc} -U^*UK_MU^* \\ 0 \end{array}\right), \quad G = \left(\begin{array}{cc} I \\ 0 \\ K_E \end{array}\right).$$

It can be checked that $F(M + I)G$ is given by

$$F(M + I)G = \left(\begin{array}{c} 0 \\ -Pu_{12}u_{21}c_1 \\ -Pu_{12}u_{22}c_1 \end{array}\right) (1, u_{22}/u_{21}, 0, 0),$$

where $c_1 = \text{det}(U)\text{det}(K_M)/\text{det}(K_X + K_M)$.

This implies that $-1$ is an eigenvalue of $M$ with multiplicity 3. Thus a first invariant subspace is given by the eigenspace associated to $-1$. Since

$$M = F^{-1}\left(\begin{array}{c} 0 \\ -Pu_{12}u_{21}c_1 \\ -Pu_{12}u_{22}c_1 \end{array}\right) (1, u_{22}/u_{21}, 0, 0)G^{-1} - I_4.$$
with \((1, u_{22}/u_{21}, 0, 0)G^{-1}\) given by
\[
\begin{pmatrix}
1 - \frac{u_{22}}{u_{21}} & \frac{1}{\det(K_E)}((K_E)_{22} - (K_E)_{21} \frac{u_{22}}{u_{21}})
\end{pmatrix},
\]
the kernel of \(M + I\) can be seen to be
\[
\begin{pmatrix}
K_E^{-1} & -u_{22} \\
\vdots & \\
I_2 & u_{21} \\
\end{pmatrix},
\]
Let us now look for the second invariant subspace, given by the eigenspace of the eigenvalue different from -1. It can be checked to be generated by
\[
\begin{pmatrix}
\frac{1}{u_{21}}(u_{11}(K_M)_{12} + u_{12}(K_M)_{22}) & -u_{22} \\
\vdots & \\
\frac{1}{u_{21}}(u_{11}(K_M)_{11} + u_{12}(K_M)_{21}) & u_{21} \\
\frac{u_{12}}{u_{11}} & \frac{u_{11}}{u_{12}} \\
\frac{u_{12}}{u_{11}} & \frac{u_{11}}{u_{12}} \\
\frac{u_{12}}{u_{11}} & \frac{u_{11}}{u_{12}} \\
\frac{u_{12}}{u_{11}} & \frac{u_{11}}{u_{12}} \\
\end{pmatrix}
\]
This concludes the proof, since once the invariant subspaces of \(M\) are found, the solutions of the Riccati equation are given [4] by picking any two columns \(v = (v_1, v_2, v_3, v_4)\)
\[
(1, u_{22}/u_{21}, 0, 0) \gamma K \gamma^{-1} = (K_M - A^*)^{1}(1, -v_1/v_2).
\]

We thus need \(A\) such that
\[
\det(I - K_E^{-1}(-K_X + (K_X + A^*)(K_X + K_M)^{-1})),
\]
and in particular \(A\) satisfying (12) is suitable.

Part 2. Equation (12) is equivalent to
\[
(K_M - A^*)^{1}(1, -v_1/v_2) = (K_M - A^*)(1, -v_1/v_2),
\]
(13)
(Clearly this has no solution if \(K_M - A\) is invertible). In order to prove the equivalence, set

\[
F := (K_X + K_M)^{-1},\quad K_X = F^{-1} - K_M.
\]

Using the change of variables, (12) can be rewritten as
\[
(-K_M + A^*)F(-K_M + A) = K_M - A - A^* + A^*K_M^{-1} A = (K_M - A^*)F(K_M - A)
\]
which proves the claim.

We now show that \(\gamma(1, -v_1/v_2)\), \(\gamma\) a scalar, actually belongs to the kernel of \(K_M^{-1} - (K_X + K_M)^{-1}\). Vectors of the form
\[
\gamma(1, -v_1/v_2)
\]
can equivalently be rewritten as
\[
\gamma K \gamma^{-1} = (K_M - A^*)^{1}(1, -v_1/v_2).
\]

Thus \(\gamma(1, -v_1/v_2)\) belongs to the kernel of \(K_M^{-1} - (K_X + K_M)^{-1}\) if
\[
\gamma(1, -v_1/v_2) = (K_X + K_M)^{-1}K_M \gamma(1, -v_1/v_2),
\]
that is
\[
\gamma(1, -v_1/v_2) = (K_X + K_M)^{-1}K_M \gamma(1, -v_1/v_2).
\]
This concludes the proof, since \(K_X = U^*A^*U\), where

\[
\Lambda = \begin{pmatrix}
0 & 0 \\
0 & P
\end{pmatrix},
\]
\[
U = \begin{pmatrix}
11 & 12 \\
21 & 22
\end{pmatrix}.
\]

Part 4. We are now left to prove that if \(\det(I + K_X K_M^{-1}) > \det(I + K_X K_M^{-1})\), then \(A^*\) satisfies \(K_M - A^* \geq 0\) or equivalently
\[
\begin{pmatrix}
v_1 & v_2 \\
v_1 & v_2
\end{pmatrix} K_M \begin{pmatrix}
w_1 & w_2 \\
w_1 & w_2
\end{pmatrix} > 0.
\]
On the one hand we have that
\[
\begin{pmatrix}
v_3 & v_4 \\
w_3 & w_4
\end{pmatrix} K_M \begin{pmatrix}
w_1 & w_2 \\
w_1 & w_2
\end{pmatrix} = 0.
\]
and for it to be positive, we need

\[
\begin{pmatrix}
  u_{12} & u_{22} \\
  u_{21} & u_{22}
\end{pmatrix}K_M^{-1}
\begin{pmatrix}
  u_{21} \\
  u_{22}
\end{pmatrix} > 0.
\]

Since \( K_M - AK_E^{-1}A^* \) is of the form

\[
\begin{pmatrix}
  \phi & \psi \\
  w_1 & w_2
\end{pmatrix}
\begin{pmatrix}
  u_{12} & u_{21} \\
  u_{21} & u_{22}
\end{pmatrix}K_M - K_E
\begin{pmatrix}
  w_1 \\
  w_2
\end{pmatrix},
\]

where \( \phi > 0 \) has been defined in (14), we have that \( \det(K_M - AK_E^{-1}A^*) \) is a quadratic form given by

\[
\begin{pmatrix}
  w_{12}^* & w_{21}^* \end{pmatrix} \left( K_M - K_E - \psi \psi^* \right) \begin{pmatrix}
  w_{12} \\
  w_{21}
\end{pmatrix}.
\]

Thus if \( \phi(K_M - K_E - \psi \psi^*) \) is positive (semi)definite or indefinite, there always exist \( w_1, w_2 \) such that

\[
\begin{pmatrix}
  w_{12}^* & w_{21}^* \end{pmatrix} \left( K_M - K_E - \psi \psi^* \right) \begin{pmatrix}
  w_{12} \\
  w_{21}
\end{pmatrix} > 0.
\]

If \( \phi(K_M - K_E - \psi \psi^*) \) is negative definite, then take \( w_1 = w_2 = 0 \).  \hfill \blacksquare

V. CONCLUSION

In this paper, we computed the secrecy capacity of the 2 × 2 MIMO wire-tap channel. In order to do so, we introduced new proof techniques to deal with non-degraded channels. Many of the proof steps are actually quite general and apply for channel matrices of arbitrary dimension. However, others are specific to the 2 × 2 case. While this paper was under revision, we have actually generalized the result for MIMO systems with an arbitrary number of transmit and receive antennas [13].

\begin{thebibliography}{9}
\bibitem{11} Y. Li, H. V. Poor, “Secure Communication over Fading Channels”, in the proceedings of Allerton 2006.
\bibitem{12} Y. Li, H. V. Poor, Shlomo Shamai (Shitz), “Secure Communication over Fading Channels”, Submitted to IEEE Trans. on Inf. Theory, Special Issue on Information Theoretic Security, November 2006.
\bibitem{15} F. Oggier, B. Hassibi, “The Secrecy Capacity of the MIMO Wiretap Channel”, in preparation.
\end{thebibliography}