The Secrecy Capacity of the MIMO Wiretap Channel

Frédérique Oggier and Babak Hassibi
Department of Electrical Engineering,
California Institute of Technology,
Pasadena 91125 CA, USA.
Email:{frederique,hassibi}@systems.caltech.edu

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 perfect secrecy capacity of the multiple antenna MIMO broadcast channel, where the number of antennas is arbitrary for both the transmitter and the two receivers. Our technique involves a careful study of a Sato-like upper bound via the solution of a certain algebraic Riccati equation.**

I. Introduction

In a traditional confidentiality setting, a transmitter (Alice) wants to send some secret message to a legitimate receiver (Bob), and prevent the eavesdropper (Eve) to read the message.

From an information theoretic point of view, the communication channel involved can be modeled as a broadcast channel, following the wire-tap channel model introduced by Wyner [22]: a transmitter broadcasts its message, say $w^k \in \mathcal{W}^k$, encoded into a codeword x^n, and the two receivers (the legitimate and the illegitimate) respectively receive y^n and z^n, the output of their channel. The amount of ignorance that the eavesdropper has about a message w^k is called the *equivocation rate*, defined as:

Definition 1: The *equivocation rate* R_e is defined as

$$R_e = \frac{1}{n} h(w^k|z^n),$$

with $0 \leq R_e \leq h(w^k)/n$. Clearly, if R_e is equal to the information rate $h(w^k)/n$, then $I(z^n|w^k) = 0$, which yields *perfect secrecy*.

Associated with secrecy is a *perfect secrecy rate* R_s, which is the amount of information that can be sent not only reliably but also confidentially, with the help of a $(2^{nR_s}, n)$ code.

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

$$\begin{aligned} P_e &\leq \epsilon' & (1) \\ R_s - \epsilon &\leq R_e. & (2) \end{aligned}$$

The first condition (1), where P_e is the probability of decoding erroneously, is the standard definition of achievable rate as far as reliability is concerned. The second condition (2) guarantees secrecy, up to the equivocation rate, which we will require to be $h(w^k)/n$ to have perfect secrecy. The *secrecy capacity* is defined similarly to the standard capacity:

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

In this paper, we are interested in the secrecy capacity for the case where Alice, Bob and Eve are communicating via multiple antenna channels.

A. Previous work

In his seminal work [22], Wyner showed for discrete memoryless channels that the perfect secrecy capacity is actually the difference of the capacity of the two users, under the assumption that the channel of the eavesdropper is a degraded version of the channel of the legitimate receiver. This result has been generalized to Gaussian channels by Leung et al. [9].

In [4], Gopala et al. have shown that the secrecy capacity is also the difference of the two capacities in the case of a single antenna fading channel, under the assumption of asymptotically long coherence intervals, when the transmitter either knows both channels or only the legitimate channel. In [1], [2], Barros et al. have characterized information theoretic security in terms of outage probability. Independently, Liang et al. [12], [13] and Li et al. [10] have computed the secrecy capacity for the parallel wiretap channel with independent subchannels. The secrecy capacity of the wiretap channel with single antenna fading channel follows.

A first study involving multiple antenna channels has been proposed by Hero [5], in a different context than the wiretap channel. In [19], the SIMO wiretap channel has been considered. In [11], the secrecy capacity is computed for the MISO case. Furthermore, a lower bound is computed in the MIMO case. The secrecy capacity for the MISO case has also been proven independently by Khisti et al. [7] and Shafiee et al. [20]. In [7], the authors furthermore give an upper bound for the MIMO case, in a regime asymptotic in SNR. The secrecy capacity has been computing for the particular cases where both the transmitter and receiver have two antennas, and the eavesdropper has either one antenna [21] or two antennas [17]. Finally, Liu et al. [14], [15] computed the secrecy capacity for a Gaussian broadcast channel, where a multi-antenna transmitter sends independent confidential messages to two users.

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

The contribution of this paper is to compute the perfect secrecy capacity of the multiple antenna wire-tap channel, for any number of transmit/receive antennas. In order to compute the secrecy capacity, we provide a proof technique for the converse, which allows us to deal with channels that are not degraded. Note that our result shows that the inner bound by Li et al. [11] is tight, and this is proved by the computation of an upper bound that actually matches the lower bound. Independently of our results, Khisthi and Wornell [8] have also computed the secrecy capacity of the MIMO wiretap channel (which they refer to as MIMO-ME). An alternative derivation of our result, and that of Khisti-Wornell, has also appeared in Liu and Shamai [16].

B. The MIMO wiretap channel

We consider the MIMO wiretap channel, that is, a broadcast channel where the transmitter is equipped with n transmit antennas, while the legitimate receiver and an eavesdropper have respectively n_M and n_E receive antennas, namely:

$$\begin{aligned} Y &= H_M X + V_M \\ Z &= H_E X + V_E \end{aligned}$$

where Y, V_M and Z, V_E are resp. $n_M \times 1$ and $n_E \times 1$ vectors. We have that X is the $n \times 1$ complex transmitted signal, with covariance matrix $K_X \succeq \mathbf{0}_n$ with power constraint $\mathrm{Tr}(K_X) = P$, while H_M and H_E are respectively $n_M \times n$ and $n_E \times n$ fixed channel matrices. They are both assumed to be known at the transmitter. Along the paper we will usually consider two cases: the *definite case*, that is when $H_M^* H_M \succ H_E^* H_E$ or $H_E^* H_E \succ H_M^* H_M$, which corresponds to the degraded case, and the *indefinite case*, which is when some of the eigenvalues of $H_E^* H_E - H_M^* H_M$ are positive, and other negative or zero. The vectors V_M, V_E are independent circularly symmetric complex Gaussian with identity covariance $K_M = \mathbf{I}_{n_M}$, $K_E = \mathbf{I}_{n_E}$ and independent of the transmitted signal X.

Our main result is:

Theorem 1: The secrecy capacity C_S of the MIMO wiretap channel is given by

$$\max_{K_X \succeq \mathbf{0}} \log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*)$$

with $\mathrm{Tr}(K_X) = P$.
The paper contains the main parts of the proof of the above theorem.

II. On the Achievability

In this section, we state the achievability part of the secrecy capacity, and further prove that in the non-degraded case, the achievability is maximized by $n \times n$ matrices K_X which are low rank, that is of any rank $r < n$.

Proposition 1: The perfect secrecy rate

$$R_s = \max_{K_X \succeq \mathbf{0}} \log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*)$$

with $\mathrm{Tr}(K_X) = P$, is achievable.
This has already been proved [11]. 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 $\tilde{K}_X$ be an optimal solution to the optimization problem

$$\max_{K_X \succeq \mathbf{0}} \log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*),$$

where $\mathrm{Tr}(K_X) = P$ and $H_E^* H_E - H_M^* H_M$ is either indefinite or semidefinite. Then $\tilde{K}_X$ is a low rank matrix.

Proof: To show that the optimal $\tilde{K}_X$ is low rank, we define a Lagrangian which includes the power constraint, and show that this yields no solution. From there, we can conclude that the optimal solution is on the boundary of the cone of positive semi-definite matrices, i.e., matrices of rank $r < n$.

We thus define the following Lagrangian:

$$\begin{gathered} \log\det(\mathbf{I}_{n_M} + H_M K_X H_M^*) \\ - \log\det(\mathbf{I}_{n_E} + H_E K_X H_E^*) - \lambda \mathrm{Tr}(K_X), \end{gathered}$$

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

$$\begin{gathered} \nabla_{K_X}(\log\det(\mathbf{I} + H_M K_X H_M^*) \\ - \log\det(\mathbf{I} + H_E K_X H_E^*) - \lambda \mathrm{Tr}(K_X)) = 0 \\ \iff H_M^* H_M (\mathbf{I} + K_X H_M^* H_M)^{-1} \\ = (\mathbf{I} + H_E^* H_E K_X)^{-1} H_E^* H_E + \lambda \mathbf{I}_n. \end{gathered} \tag{3}$$

By pre-multiplying the above equation by $(\mathbf{I} + H_E^* H_E K_X)$ and post-multiplying it by $(\mathbf{I} + K_X H_M^* H_M)$, we get

$$H_M^* H_M - H_E^* H_E = \lambda(\mathbf{I} + H_E^* H_E K_X)(\mathbf{I} + K_X H_M^* H_M),$$

or equivalently, by further pre and post-multiplying by K_X,

$$\begin{gathered} K_X(H_M^* H_M - H_E^* H_E) K_X \tfrac{1}{\lambda} = \\ (K_X + K_X H_E^* H_E K_X)(K_X + K_X H_M^* H_M K_X). \end{gathered} \tag{4}$$

Now if $K_X \succ \mathbf{0}$, then all the eigenvalues of $(K_X + K_X H_E^* H_E K_X)(K_X + K_X H_M^* H_M K_X)$ are strictly positive (Lemma 1 below). This implies that (4) can have a solution if and only if the Hermitian matrix $K_X(H_M^* H_M - H_E^* H_E) K_X \frac{1}{\lambda}$ is positive definite. This means that either $H_M^* H_M \succ H_E^* H_E$ and $\lambda > 0$, or $H_M^* H_M \prec H_E^* H_E$ and $\lambda < 0$. This gives a contradiction if $H_M^* H_M - H_E^* H_E$ is either indefinite or semidefinite, implying that $\tilde{K_X}$ has to be low rank. ■

Lemma 1: If $A = A^* \succ \mathbf{0}$ and $B = B^* \succ \mathbf{0}$, then the matrix AB has all positive eigenvalues.

Proof: Since $A \succ \mathbf{0}$, we can write $A = A^{1/2}(A^*)^{1/2}$ with $A^{1/2}$ invertible. Therefore,

$$AB = A^{1/2}((A^*)^{1/2} B A^{1/2}) A^{-1/2},$$

has the same eigenvalues as the matrix $(A^*)^{1/2} B A^{1/2}$, which is positive definite. ■

III. 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 $n \geq n(\epsilon, \epsilon')$, $\epsilon, \epsilon' > 0$, then the secrecy rate R_s satisfies

$$R_s \leq \max_{K_X \succeq \mathbf{0}} \log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*),$$

with $\mathrm{Tr}(K_X) = P$.

A. Bound on $I(X;Y|Z)$ and result for the degraded case

We start by recalling a standard result [9], [4].

Lemma 2: Given any sequence of $(2^{nR_s}, n)$ codes with $P_e \le \epsilon$ and $R_s - \epsilon \le R_e$ for any $n \ge n(\epsilon)$, $\epsilon > 0$, the secrecy rate R_s can be upper bounded as follows:

$$R_s - \epsilon \le \frac{1}{n}[I((X^n, Y^n|Z^n) + \delta], \ \epsilon, \delta > 0.$$

We thus focus on finding an upper bound on $I(X;Y|Z)$.

Proposition 3: We have the following upper bound:

$$I(X;Y|Z) \le \max_{K_X \succeq \mathbf{0}} \tilde{I}(X;Y|Z)$$

where $\tilde{I}(X;Y|Z)$ is given by

$$\log\det\left(\mathbf{I} + (H_M^* \ \ H_E^*)\begin{pmatrix}\mathbf{I} & A\\ A^* & \mathbf{I}\end{pmatrix}^{-1}\begin{pmatrix}H_M\\ H_E\end{pmatrix}K_X\right) - \log\det(\mathbf{I} + H_E K_X H_E^*). \tag{5}$$

and A denotes the correlation between V_M and V_E, which satisfies $\mathbf{I} - AA^* \succ \mathbf{0}$.

Proof: An upper bound on $I(X;Y|Z)$ is obtained by assuming that the legitimate receiver knows both its channel and the one of the eavesdropper, so that the capacity of the link between the transmitter and the legitimate receiver is that of a MIMO system, namely

$$\max_{K_X}\log\det\left[\mathbf{I}_n + [H_M^* \ \ H_E^*]\begin{bmatrix}\mathbf{I}_{n_M} & A\\ A^* & \mathbf{I}_{n_E}\end{bmatrix}^{-1}\begin{bmatrix}H_M\\ H_E\end{bmatrix}K_X\right]$$

where A has to satisfy $\mathbf{I} - AA^* \succ \mathbf{0}$. Now the channel we consider is degraded, and an upper bound is thus the difference of the two capacities, which yields the result. ■

We can now conclude the proof of the converse for the "simple" cases when $H_M^*H_M \succ H_E^*H_E$ or $H_E^*H_E \succ H_M^*H_M$.

Proposition 4: 1) If $H_M^*H_M \succ H_E^*H_E$, we have that

$$I(X;Y|Z) \le \max_{K_X \succeq \mathbf{0}} \log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*).$$

2) Vice versa, if $H_E^*H_E \succ H_M^*H_M$, then $I(X;Y|Z) = 0$.

Proof: Let us introduce two other ways of writing $\tilde{I}(X;Y|Z)$ (see (5)). Let us first compute a UDL factorization:

$$\begin{bmatrix}\mathbf{I}_{n_M} & A\\ A^* & \mathbf{I}_{n_E}\end{bmatrix} = \begin{bmatrix}\mathbf{I} & A\\ \mathbf{0} & \mathbf{I}\end{bmatrix}\begin{bmatrix}\mathbf{I} - AA^* & \mathbf{0}\\ \mathbf{0} & \mathbf{I}\end{bmatrix}\begin{bmatrix}\mathbf{I} & \mathbf{0}\\ A^* & \mathbf{I}\end{bmatrix}$$

so that

$$\begin{bmatrix}\mathbf{I} & A\\ A^* & \mathbf{I}\end{bmatrix}^{-1} = \begin{bmatrix}\mathbf{I} & \mathbf{0}\\ -A^* & \mathbf{I}\end{bmatrix}\begin{bmatrix}(\mathbf{I} - AA^*)^{-1} & \mathbf{0}\\ \mathbf{0} & \mathbf{I}\end{bmatrix}\begin{bmatrix}\mathbf{I} & -A\\ \mathbf{0} & \mathbf{I}\end{bmatrix}$$

and we have that

$$(H_M^* \ \ H_E^*)\begin{pmatrix}\mathbf{I} & A\\ A^* & \mathbf{I}\end{pmatrix}^{-1}\begin{pmatrix}H_M\\ H_E\end{pmatrix} = (H_M^* - H_E^*A^*)(\mathbf{I} - AA^*)^{-1}(H_M - AH_E) + H_E^*H_E.$$

Thus a first equivalent formula for $\tilde{I}(X;Y|Z)$ is given by

$$\log\det(\mathbf{I} + ((H_M^* - H_E^*A^*)(\mathbf{I} - AA^*)^{-1}(H_M - AH_E) + H_E^*H_E)K_X) - \log\det(\mathbf{I} + H_E K_X H_E^*). \tag{6}$$

By considering now a LDU factorization, we get

$$\begin{bmatrix}\mathbf{I} & A\\ A^* & \mathbf{I}\end{bmatrix} = \begin{bmatrix}\mathbf{I} & \mathbf{0}\\ A^* & \mathbf{I}\end{bmatrix}\begin{bmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & \mathbf{I} - A^*A\end{bmatrix}\begin{bmatrix}\mathbf{I} & A\\ \mathbf{0} & \mathbf{I}\end{bmatrix},$$

$$\begin{bmatrix}\mathbf{I} & A\\ A^* & \mathbf{I}\end{bmatrix}^{-1} = \begin{bmatrix}\mathbf{I} & -A\\ \mathbf{0} & \mathbf{I}\end{bmatrix}\begin{bmatrix}\mathbf{I} & \mathbf{0}\\ \mathbf{0} & (\mathbf{I} - A^*A)^{-1}\end{bmatrix}\begin{bmatrix}\mathbf{I} & \mathbf{0}\\ -A^* & \mathbf{I}\end{bmatrix}$$

so that

$$(H_M^* \ \ H_E^*)\begin{pmatrix}\mathbf{I} & A\\ A^* & \mathbf{I}\end{pmatrix}^{-1}\begin{pmatrix}H_M\\ H_E\end{pmatrix} = H_M^*H_M + (-H_M^*A + H_E^*)(\mathbf{I} - A^*A)^{-1}(-A^*H_M + H_E)$$

and a second equivalent formula for $\tilde{I}(X;Y|Z)$ is given by

$$\log\det(\mathbf{I} + H_M^*H_M K_X + (-H_M^*A + H_E^*)(\mathbf{I} - A^*A)^{-1}(-A^*H_M + H_E)K_X) - \log\det(\mathbf{I} + H_E K_X H_E^*). \tag{7}$$

Since the secrecy capacity does not depend on A, and that

$$I(X;Y|Z) \le \max_{K_X} \tilde{I}(X;Y|Z),$$

for all A such that $\mathbf{I} - AA^* \succ \mathbf{0}$, we are now free to take any such A which does not depend on a choice of K_X.

Case 1. If $H_M^*H_M \succ H_E^*H_E$, we will now show that there always exists a matrix A such that $H_M^*A = H_E^*$ and $\mathbf{I} - AA^* \succ \mathbf{0}$. Note that using (7), we then get

$$\tilde{I}(X;Y|Z) = \log\det(\mathbf{I} + H_M^*H_M K_X) - \log\det(\mathbf{I} + H_E^*H_E K_X).$$

Now $H_M^*H_M \succ H_E^*H_E$ implies that $H_M H_M^* = H_E^*H_E + X^*X$, for some $X^*X \succ \mathbf{0}$. Now this means [6] that there exists a unitary matrix Θ such that $[H_E^* \ \ X^*] = [H_M^* \ \ \mathbf{0}]\ \Theta$. Partitioning Θ, we get

$$[H_E^* \ \ X^*] = [H_M^* \ \ \mathbf{0}]\begin{bmatrix}\Theta_{11} & \Theta_{12}\\ \Theta_{21} & \Theta_{22}\end{bmatrix}$$

from which it follows that $H_E^* = H_M^*\Theta_{11}$. Note that we can take $A = \Theta_{11}$, since $\Theta_{11}^*\Theta_{11} \prec \mathbf{I}$ as it is a sub-block of a unitary matrix, and using the fact that $X^*X \succ \mathbf{0}$.

Case 2. This is similar when $H_E^*H_E \succ H_M^*H_M$. ■

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

We are now left with the interesting case when $H_M^*H_M - H_E^*H_E$ is indefinite, which is the non-degraded case.

B. Minimization over A and maximization over K_X

Since Proposition 3 is true for all A such that $\mathbf{I} - AA^* \succ \mathbf{0}$, we get

$$I(X;Y|Z) \le \min_A \max_{K_X} \tilde{I}(X;Y,Z).$$

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 (5) 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 $\mathrm{Tr}(K_X)=P$, $K_X\succeq\mathbf{0}$, $\mathbf{I}-AA^*\succ\mathbf{0}$.
This proof is skipped here by lack of space (see [18]).

We next compute the minimization over A. Note that we can write $\tilde{I}(X;Y|Z)$ in the following alternative way:

$$\begin{gathered}\log\det(H_MK_XH_M^*+\mathbf{I}_{n_M}-\\ (H_MK_XH_E^*+A)(H_EK_XH_E^*+\mathbf{I})^{-1}(H_EK_XH_M^*+A^*))\\ -\log\det(\mathbf{I}_{n_M}-AA^*).\end{gathered}\tag{8}$$

Proposition 6: Let $\tilde{A}^*$ be a local minima of $\tilde{I}(X;Y|Z)$. Then

$$\tilde{A}^*=(H_EV\ \ QW)(H_MV\ \ PW)^{-1},$$

where W is an $(n_M+n_E-n)\times m$ matrix, $0\le m\le n_M$, $(P^T\ \ Q^T)^T$ is orthogonal to $(-H_M^*\ \ H_E^*)$, P,Q of dimension resp. $n_M\times(n_M+n_E-n)$, $n_E\times(n_M+n_E-n)$, and V is a $n\times(n_M-m)$ matrix, such that

$$\left(\begin{array}{c}H_MV\\ H_EV\end{array}\right)$$

is an invariant subspace of M, as defined in (9).

Proof: Let M_1,M_2,M_3,X be square complex matrices. Set $f(X)=M_1-(X+M_2)M_3(X^*+M_2^*)$. We have that

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

Using this formula, we compute that $\nabla_{A^*}\tilde{I}(X;Y|Z)=0$ iff

$$\begin{gathered}f(A)(A^*+H_EK_XH_M^*)^{-1}(H_EK_XH_E^*+\mathbf{I})=\\ (\mathbf{I}-AA^*)(A^*)^{-1},\end{gathered}$$

where $f(A)$ is given by

$$\begin{gathered}H_MK_XH_M^*+\mathbf{I}\\ -(H_MK_XH_E^*+A)(H_EK_XH_E^*+\mathbf{I})^{-1}(H_EK_XH_M^*+A^*).\end{gathered}$$

We get a nonsymmetric algebraic Ricatti equation given by

$$\begin{gathered}A^*(H_MK_XH_M^*{+}\mathbf{I})^{-1}H_MK_XH_E^*A^*{+}A^*(H_MK_XH_M^*{+}\mathbf{I})^{-1}{+}\\ [-H_EK_XH_E^*{-}\mathbf{I}{+}H_EK_XH_M^*(H_MK_XH_M^*{+}\mathbf{I})^{-1}H_MK_XH_E^*]A^*\\ +H_EK_XH_M^*(H_MK_XH_M^*+\mathbf{I})^{-1}=0.\end{gathered}$$

One way of solving an algebraic Riccati [3] of the form

$$\mathbf{0}=M_{21}+M_{22}A^*-A^*M_{11}-A^*M_{12}A^*,$$

is to look for invariant subspaces of

$$M=\left(\begin{array}{cc}M_{11}&M_{12}\\ M_{21}&M_{22}\end{array}\right).$$

Here we have that M is given by

$$\begin{array}{rcl}M_{11}&=&-(H_MK_XH_M^*+\mathbf{I})^{-1}\\ M_{12}&=&-(H_MK_XH_M^*+\mathbf{I})^{-1}H_MK_XH_E^*\\ M_{21}&=&H_EK_XH_M^*(H_MK_XH_M^*+\mathbf{I})^{-1}\\ M_{22}&=&-H_EK_XH_E^*-\mathbf{I}+\\ &&H_EK_XH_M^*(H_MK_XH_M^*+\mathbf{I})^{-1}H_MK_XH_E^*.\end{array}\tag{9}$$

Set

$$F=\left(\begin{array}{cc}H_MK_XH_M^*+\mathbf{I}_{n_M}&0\\ 0&\mathbf{I}_{n_E}\end{array}\right).$$

It is easy to see that $F(M+\mathbf{I})$ is given by

$$\left[\begin{array}{c}-H_M\\ -H_E+H_EK_XH_M^*(H_MK_XH_M^*+\mathbf{I})^{-1}H_M\end{array}\right]K_X[-H_M^*\ \ H_E^*]$$

which implies that -1 is an eigenvalue of M. Thus a first invariant subspace is given by the eigenspace associated to -1, which is the kernel of $M+\mathbf{I}$, or in other words, the subspace $(P^T\ \ Q^T)^T$ orthogonal to $(-K_XH_M^*\ \ K_XH_E^*)$.

We further rewrite M as

$$\begin{gathered}\left(\begin{array}{c}-H_M(K_XH_M^*H_M+\mathbf{I})^{-1}\\ -H_E+H_E(K_XH_M^*H_M+\mathbf{I})^{-1}K_XH_M^*H_M\end{array}\right).\\ (-K_XH_M^*\ \ K_XH_E^*)-\mathbf{I}\\ =\left(\begin{array}{c}-H_M\\ -H_E\end{array}\right)(K_XH_M^*H_M+\mathbf{I})^{-1}(-K_XH_M^*\ \ K_XH_E^*)-\mathbf{I}.\end{gathered}$$

Thus, a Jordan basis of M is given by

$$\left(\begin{array}{cc}H_M&P\\ H_E&Q\end{array}\right)$$

with $(P^T\ \ Q^T)^T$ orthogonal to $(-H_M^*\ \ H_E^*)$.

Finally, solutions of the Ricatti equation are given [3], in the general case, by:

$$\tilde{A}^*=(H_EV\ \ QW)(H_MV\ \ PW)^{-1},$$

where W is an $n_M\times m$ matrix, $0\le m\le n_M$, and V is a $n_M\times n_M-m$ matrix, such that

$$\left(\begin{array}{c}H_MV\\ H_EV\end{array}\right)$$

is an invariant subspace of M. Note that W can be chosen arbitrary since $(P^T,Q^T)^T$ is the eigenspace associated to -1. ■

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

$$\begin{array}{ll}\max K_X&\min_A\tilde{I}(X;Y|Z)\\ &\text{s.t. }\ K_X\succeq\mathbf{0},\ \mathrm{Tr}(K_X)=P,\end{array}$$

where $\tilde{A}^*=(H_EV\ \ QW)(H_MV\ \ PW)^{-1}$ is the optimal solution for the minimization over A. Then $\tilde{K}_X$ is low rank.

Proof: Note that $\tilde{I}(X;Y|Z)$ can be written

$$\log\det(\mathbf{I}+BK_X)-\log\det(\mathbf{I}+H_EK_XH_E^*),$$

where

$$B:=(H_M^*-H_E^*A^*)(\mathbf{I}-AA^*)^{-1}(H_M-AH_E)+H_E^*H_E.$$

We now show that $B-H_E^*H_E$ is low rank by showing that $(H_M^*-H_E^*A^*)$ is low rank. Indeed, we have that $A^*=(H_EV\ \ QW)(H_MV\ \ PW)^{-1}$. Therefore,

$$\begin{gathered}H_M^*-H_E^*A^*=(H_M^*\ \ -H_E^*)\left(\begin{array}{c}\mathbf{I}\\ A^*\end{array}\right)\\ =(H_M^*\ \ -H_E^*)\left(\begin{array}{cc}H_MV&PW\\ H_EV&QW\end{array}\right)(H_MV\ \ PW)^{-1}\end{gathered}$$

which, since $(P^T \;\; Q^T)^T$ is orthogonal to $(H_M^* \;\; -H_E^*)$ yields

$$H_M^* - H_E^* A^* = ((H_M^* H_M - H_E^* H_E)V \;\; \mathbf{0})(H_M V \;\; PW)^{-1},$$

which, as desired, is low rank.

Now, from Proposition 2, we know that either $B \succ H_E^* H_E$ and $\lambda > 0$, or $B \prec H_E^* H_E$ and $\lambda < 0$. This is a contradiction since $B \succeq H_E^* H_E$, yielding that $\tilde{K}_X$ is low rank. ■

Proposition 8: The rank of $\tilde{K}_X$ being $r < n$, that is $K_X = U_X U_X^*$ with U_X an $n \times r$ matrix, the optimal solution to

$$\min_A \tilde{I}(X; Y|Z)$$

is given by

$$A^* = (H_E(K_X H_M^* H_M + \mathbf{I})^{-1} U_X V \;\; QW)$$
$$(H_M(K_X H_M^* H_M + \mathbf{I})^{-1} U_X V \;\; PW)^{-1}.$$

Proof: The Jordan decomposition of M is now given by

$$M \begin{pmatrix} H_M & P \\ H_E & Q \end{pmatrix} = \begin{pmatrix} H_M & P \\ H_E & Q \end{pmatrix} \begin{pmatrix} J & \mathbf{0} \\ \mathbf{0} & -\mathbf{I} \end{pmatrix}$$

where

$$J = (\mathbf{I} + K_X H_M^* H_M)^{-1} (K_X H_M^* \;\; -K_X H_E^*) \begin{pmatrix} H_M \\ H_E \end{pmatrix} - \mathbf{I}.$$

Let us now look more carefully at J. We first notice that when K_X is low rank, -1 is an eigenvalue. This is clear since

$$J + \mathbf{I} = (\mathbf{I} + K_X H_M^* H_M)^{-1} K_X (H_M^* \;\; -H_E^*) \begin{pmatrix} H_M \\ H_E \end{pmatrix}$$

and $\det(K_X) = 0$. Furthermore, since $K_X = U_X U_X^*$, we have

$$J = (\mathbf{I} + K_X H_M^* H_M)^{-1} U_X U_X^* (H_M^* \;\; -H_E^*) \begin{pmatrix} H_M \\ H_E \end{pmatrix} - \mathbf{I}$$

and clearly $(\mathbf{I} + K_X H_M^* H_M)^{-1} U_X$ is an invariant subspace of J. A Jordan basis is thus given by

$$P' = \left(\; (\mathbf{I} + K_X H_M^* H_M)^{-1} U_X \quad Q' \; \right)$$

where Q' is the eigenspace associated to -1. This thus gives us a more precise Jordan basis for M (as defined in (9)), namely

$$\begin{bmatrix} H_M P' & P \\ H_E P' & Q \end{bmatrix} = \begin{bmatrix} H_M(K_X H_M^* H_M + \mathbf{I})^{-1} U_X & H_M Q' & P \\ H_E(K_X H_M^* H_M + \mathbf{I})^{-1} U_X & H_E Q' & Q \end{bmatrix}.$$

From this Jordan basis of M, we have that

$$A^* = (H_E(K_X H_M^* H_M + \mathbf{I})^{-1} U_X V \;\; QW)$$
$$(H_M(K_X H_M^* H_M + \mathbf{I})^{-1} U_X V \;\; PW)^{-1}$$

is a solution of the Ricatti equation, where W is any $n_M \times (n_M - r)$ matrix, and V is any $r \times r$ matrix. ■

C. The converse matches the achievability

We can now conclude.

Proposition 9: Let

$$A^* = (H_E(K_X H_M^* H_M + \mathbf{I})^{-1} U_X V \;\; QW)$$
$$(H_M(K_X H_M^* H_M + \mathbf{I})^{-1} U_X V \;\; PW)^{-1}$$

be a solution of the Ricatti equation. Then

$$\tilde{I}(X; Y|Z) = \log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*).$$

Furthermore, there exists V, W such that $\mathbf{I} - AA^* \succ \mathbf{0}$. Now that the matrix A^* is known explicitly, this can be checked by computation, which is omitted here by lack of space (see [18]).

IV. Conclusion

In this paper, we considered the problem of computing the perfect secrecy capacity of a multiple antenna channel, based on a generalization of the wire-tap channel to a MIMO broadcast wire-tap channel. We proved that for an arbitrary number of transmit/receive antennas, the perfect secrecy capacity is the difference of the two capacities, the one of the legitimate user minus the one of the eavesdropper, after a suitable optimization over the transmitter's input covariance matrix.

Acknowledgement

This work was supported in part by NSF grant CCF-0729203, by Caltech's Lee Center for Advanced Networking and by a grant from the David and Lucille Packard Foundation.

References

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

[2] M. Bloch, J. Barros, M. R. D. Rodrigues, S. W. McLaughlin, "Wireless Information-Theoretic Security - Part I: Theoretical Aspects". Submitted to *IEEE Transactions on Information Theory*, Special Issue on Information-Theoretic Security, November 2006

[3] G. Freiling, "A Survey on Nonsymmetric Ricatti Equations", *Lin. Algebra and its Appl.*, 251-252, 2002.

[4] P. Gopala, L. Lai, and H. El Gamal, "On the Secrecy Capacity of Fading Channels", submitted to *IEEE Transactions on Inf. Theory*, Oct. 2006

[5] A. O. Hero, "Secure Space-Time Communication," , *IEEE Trans. on Info Theory*, Vol. 49, No. 12, pp. 1-16, Dec. 2003.

[6] T. Kailath, A.H. Sayed and B. Hassibi, "Linear Estimation", Prentice-Hall, 2000.

[7] A. Khisti, G. Wornell, A. Wiesel, Y. Eldar, "On the Gaussian MIMO Wiretap Channel", in *IEEE Int. Symposium on Inf. Theory*, Nice, 2007.

[8] A. Khisti, G. Wornell, "Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel", Submitted, August 2007.

[9] S.K. Leung-Yan-Cheong, M.E. Hellman, "The Gaussian Wire-Tap Channel", *IEEE Trans. on Information Theory*, vol. 24, July 1978.

[10] Z. Li, R. Yates, W. Trappe,"Secrecy capacity of independent parallel channels", in *Allerton conference*, 2006.

[11] Z. Li, W. Trappe, R. Yates, "Secret communication via multi-antenna transmission", in *Conference on Information Sciences and Systems (CISS)*, March 2007.

[12] Y. Liang, H. V. Poor, "Secure Communication over Fading Channels", in *Proc. of Allerton*, 2006.

[13] Y. Liang, H. V. Poor, Shlomo Shamai (Shitz), "Secure Communication over Fading Channels", Submitted to *IEEE Transactions on Inf. Theory*, Special Issue on Information Theoretic Security, November 2006

[14] R. Liu, H. V. Poor, "Multiple Antenna Secure Broadcast over Wireless Networks", *First International Workshop on Information Theory for Sensor Networks, Santa Fe*, 2007.

[15] R. Liu, H. V. Poor, "Secrecy Capacity Region of a Multi-Antenna Gaussian Broadcast Channel with Confidential Messages", submitted to *IEEE Transactions on Information Theory*, (arXiv:0709.4671)

[16] T. Liu, Shlomo Shamai (Shitz), "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel", submitted to *IEEE Trans. on Information Theory*, (arxiv.org/pdf/0710/4105.pdf).

[17] F. Oggier, B. Hassibi, "The Secrecy Capacity of the 2x2 MIMO Wiretap Channel", in *Allerton Conference*, September 2007.

[18] F. Oggier, B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel", submitted.

[19] P. Parada, R. Blahut,"Secrecy capacity of SIMO and slow fading channels," in *IEEE Int. Symposium on Inf. Theory*, Adelaide, 2005.

[20] S. Shafiee, S. Ulukus, "Achievable Rates in Gaussian MISO Channels with Secrecy Constraints", in *IEEE Int. Symp. on Inf. Theory*, Nice, 2007.

[21] S. Shafiee, N. Liu and S. Ulukus, Towards the Secrecy Capacity of the Gaussian MIMO Wire-tap Channel: The 2-2-1 Channel, submitted to *IEEE Trans. on Information Theory*, September 2007.

[22] A.D. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, October 1975.