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

\[ P_e \leq \epsilon' \quad (1) \]
\[ R_s - \epsilon \leq R_e \quad (2) \]

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.
The vectors \( K \) and the indefinite case \( H \) of the transmitter. Along the paper we will usually consider two covariance matrix \( K \). This has already been proved [11]. In fact, the interpretation 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:

\[
\begin{align*}
Y &= H_M X + V_M \\
Z &= H_E X + V_E
\end{align*}
\]

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 \( K_X \succeq 0_n \), with power constraint \( \text{Tr}(K_X) = P \), 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 \( H_M^* H_M > H_E^* H_E \) or \( H_E^* H_E > H_M^* H_M \), 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 \( K_V = I_{n_M}, K_E = I_{n_E} \) 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

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

with \( \text{Tr}(K_X) = P \).

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

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

with \( \text{Tr}(K_X) = P \), 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 \( \hat{K}_X \) be an optimal solution to the optimization problem

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

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

**Proof:** To show that the optimal \( \hat{K}_X \) 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:

\[
\log \det(I_{n_M} + H_M K_X H_M^*) - \log \det(I_{n_E} + H_E K_X H_E^*) - \lambda \text{Tr}(K_X),
\]

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

\[
\nabla_{K_X} \log \det(I_{n_M} + H_M K_X H_M^*) - \log \det(I_{n_E} + H_E K_X H_E^*) - \lambda \text{Tr}(K_X) = 0
\]

\[
\leftrightarrow H_M^* H_M (I + K_X H_M^* H_M) = \frac{1}{\lambda} H_E^* H_E (I + H_E K_X H_E^*)^{-1}
\]

Pre-multiplying the above equation by \( (I + H_E K_X H_E^*) \) and post-multiplying it by \( (I + K_X H_M^* H_M) \), we get

\[
H_M^* H_M - H_E^* H_E = \lambda (I + H_E K_X H_E^*) (I + K_X H_M^* H_M),
\]

or equivalently, by further pre and post-multiplying by \( K_X \),

\[
K_X (H_M^* H_M - H_E^* H_E) K_X \frac{1}{\lambda} = (K_X + K_X H_E^* H_E K_X) (K_X + K_X H_M^* H_M K_X).
\]

Now if \( K_X \succ 0 \), 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 \( H_M^* H_M \succeq H_E^* H_E \) and \( \lambda > 0 \), or \( H_M^* H_M \prec H_E^* H_E \) and \( \lambda < 0 \). This gives a contradiction if \( H_M^* H_M \prec H_E^* H_E \) is either indefinite or semidefinite, implying that \( K_X \) has to be low rank.

**Lemma 1:** If \( A = A^* > 0 \) and \( B = B^* > 0 \), then the matrix \( AB \) has all positive eigenvalues.

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

\[
AB = A^{1/2}((A^*)^{1/2}BA^{1/2})A^{-1/2},
\]

has the same eigenvalues as the matrix \( (A^*)^{1/2}BA^{1/2} \), 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

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

with \( \text{Tr}(K_X) = P \).
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 $(2^nR, n)$ codes with $P_e \leq \epsilon$ and $R_x - \epsilon \leq R_e$ for any $n \geq n_0(\epsilon), \epsilon > 0$, the secrecy rate $R_x$ can be upper bounded as follows:

$$R_x - \epsilon \leq \frac{1}{n}\{I((X^n, Y^n)|Z^n) + \delta\}, \delta > 0.$$ 

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

**Proposition 3:** We have the following upper bound:

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

where $I(X;Y|Z)$ is given by

$$\log \det \left( I + (H_M^* H_E^T) \left[ A^* I \right]^{-1} \left( H^*_M H_E^T \right) K_X \right)$$

and $A$ denotes the correlation between $V_M$ and $V_E$, which satisfies $I - AA^* > 0$.

**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

$$\max K_X \log \det \left[ I + [H^*_M H_E^T] \left[ A^* I \right]^{-1} \left( H^*_M H_E^T \right) K_X \right]$$

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

We can now conclude the proof of the converse for the “simple” cases when $H_M^* H_M > H_E^* H_E$ or $H_E^* H_E > H_M^* H_M$.

**Proposition 4:**

1. If $H_M^* H_M > H_E^* H_E$, we have that

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

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

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

$$[I_{n_M} A]_{A^* I_{n_E}} = \left[ \begin{array}{c} I \ A \ A^* I \end{array} \right] \left[ \begin{array}{c} I - AA^* I \end{array} \right] \left[ \begin{array}{c} I \ 0 \ 0 \ I \end{array} \right]$$

so that

$$\left[ \begin{array}{c} I \ A \ A^* I \end{array} \right]^{-1} = \left[ \begin{array}{c} I \ 0 \ 0 \ I \end{array} \right] \left[ I - AA^* \right]^{-1} \left[ \begin{array}{c} I \ 0 \ 0 \ I \end{array} \right]$$

and we have that

$$H^*_M H_E^T \left( \begin{array}{c} I \ A \ \ A^* I \end{array} \right)^{-1} \left( H^*_M H_E^T \right) =$$

$$(H^*_M - H^*_E A^*(I - AA^*)^{-1}(H_M - AH_E) + H_E^* H_E).$$

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

$$\log \det( I + (H^*_M - H^*_E A^*)(I - AA^*)^{-1}(H_M - AH_E) + H_E^* H_E K_X ) - \log \det(I + H_E K_X H_E^T).$$

By considering now a LDU factorization, we get

$$\left[ \begin{array}{c} I \ A \ A^* I \end{array} \right]^{-1} = \left[ \begin{array}{c} I \ 0 \ 0 \ I \end{array} \right] \left[ I - AA^* \right]^{-1} \left[ \begin{array}{c} I \ 0 \ 0 \ I \end{array} \right]$$

so that

$$H^*_M H_E^T \left( \begin{array}{c} I \ A \ \ A^* I \end{array} \right)^{-1} \left( H^*_M H_E^T \right) = H^*_M H_M +$$

$$(H^*_M A + H^*_E^T(I - AA^*)^{-1}(-A^* H_M + H_E))$$

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

$$\log \det( I + H^*_M H_M K_X ) - \log \det(I + H_E K_X H_E^T).$$

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

$$I(X;Y|Z) \leq \max_{K_X \succeq 0} I(X;Y|Z),$$

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

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

$$I(X;Y|Z) = \log \det(I + H^*_M H_M K_X) - \log \det(I + H_E K_X H_E^T).$$

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

$$[H_M^* X^*] = [H_M^* 0] \left[ \begin{array}{c} \Theta_{11} \ \Theta_{12} \ \Theta_{21} \ \Theta_{22} \end{array} \right]$$

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

**Case 2.** This is similar when $H_E^* H_E > H_M^* H_M$.

The cases described in the lemma can be understood as a simple generalization of the scalar case, since those are the degraded cases. When $H_M^* H_M > H_E^* H_E$, all links to the legitimate receiver are better, and the capacity is given by the difference of the two capacities, while if $H_E^* H_E > H_M^* H_M$, 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 $I - AA^* > 0$, we get

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

To understand this double optimization, we start by analyzing the function $I(X;Y,Z)$. 
**Proposition 5:** The function \( I(X; Y, Z) \) defined in (5) is concave in \( K_X \) and convex in \( A \). Consequently,

\[
\min_A \max_{K_X} I(X; Y|Z) = \max_{K_X} \min_A I(X; Y|Z)
\]

where \( \text{Tr}(K_X) = P, K_X \succeq 0, I - AA^* \succ 0 \).

This proof is skipped here by lack of space (see [18]).

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

\[
\log \det(H_M K_X H_M^* + I_{n_M} - (H_M K_X H_M^* + A)(H_E K_X H_E^* + I)^{-1}(H_E K_X H_M^* + A^*)) - \log \det(I_{n_M} - AA^*).
\]

(8)

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

\[
\hat{A}^* = (H_E V \ Q W)(H_M V \ PW)^{-1},
\]

where \( W \) is an \((n_M + n_E - n) \times m\) matrix, \( 0 \leq m \leq n_M, \) \((P^T \ Q^T)^T \) 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

\[
\begin{pmatrix}
H_M V \\
H_E V
\end{pmatrix}
\]

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 \( \nabla_A \hat{I}(X; Y|Z) = 0 \) iff

\[
f(A)(A^* + H_E K_X H_M^* - I) = (I - AA^*)(A^*)^{-1},
\]

where \( f(A) \) is given by

\[
-H_M K_X H_M^* + I - (H_M K_X H_M^* + A)(H_E K_X H_E^* + I)^{-1}(H_E K_X H_M^* + A^*).
\]

We get a nonsymmetric algebraic Riccati equation given by

\[
A^*(H_M K_X H_M^* + I)^{-1}H_M K_X H_M^* A^* + A^*(H_M K_X H_M^* + I)^{-1}H_M K_X H_E^* A^* + \cdots
\]

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

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

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 given by

\[
\begin{align*}
M_{11} &= -(H_M K_X H_M^* + I)^{-1} \\
M_{12} &= -(H_M K_X H_M^* + I)^{-1}H_M K_X H_E^* \\
M_{21} &= H_E K_X H_M^* (H_M K_X H_M^* + I)^{-1} \\
M_{22} &= -H_E K_X H_E^* + I + H_E K_X H_M^* (H_M K_X H_M^* + I)^{-1}H_M K_X H_E^*.
\end{align*}
\]

(9)

Set

\[
F = \begin{pmatrix}H_M K_X H_M^* + I_{n_M} & 0 \\0 & I_{n_E}\end{pmatrix}.
\]

It is easy to see that \( F(M + I) \) is given by

\[
\begin{pmatrix}
-H_M & -H_E + H_E K_X H_M^* (H_M K_X H_M^* + I)^{-1}H_M \\
-H_E & H_E (H_M K_X H_M^* + I)^{-1}K_X H_E^* - I
\end{pmatrix}.
\]

Thus, a Jordan basis of \( M \) is given by

\[
\begin{pmatrix}H_M & P \\H_E & Q\end{pmatrix}
\]

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:

\[
\hat{A}^* = (H_E V \ Q W)(H_M V \ PW)^{-1},
\]

where \( W \) is an \( n_M \times m \) matrix, \( 0 \leq m \leq n_M, \) and \( V \) is a \( n_M \times n_M - m \) matrix, such that

\[
\begin{pmatrix}H_M V \\
H_E V
\end{pmatrix}
\]

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 \( K_X \) be an optimal solution to the optimization problem

\[
\max_{K_X} K_X \quad \min_A I(X; Y|Z) \quad \text{s.t.} \quad K_X \succeq 0, \text{Tr}(K_X) = P,
\]

where \( \hat{A}^* = (H_E V \ Q W)(H_M V \ PW)^{-1} \) is the optimal solution for the minimization over \( A \). Then \( K_X \) is low rank.

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

\[
\log \det(I + BK_X) - \log \det(I + H_E K_X H_E^*),
\]

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

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 \( A^* = (H_E V \ Q W)(H_M V \ PW)^{-1} \). Therefore,

\[
H_M - H_E A^* = (H_M - H_E^*) \begin{pmatrix}I \\ A^*\end{pmatrix}
\]

\[
= (H_M^* - H_E^*) \begin{pmatrix}H_M V \\
H_E V \ Q W\end{pmatrix}(H_M V \ PW)^{-1}
\]
which, since \((P^T Q^T)^T\) is orthogonal to \((H_M^* - H_E^2)\) yields
\[
H_M - H_E A^* = \left((H_M H_M - H_E^2 E)V \ 0\right)(H_M V \ PW)^{-1},
\]
which, as desired, is low rank.

Now, from Proposition 2, we know that either \(B > H_E^2 E\) and \(\lambda > 0\), or \(B < H_E^2 E\) and \(\lambda < 0\). This is a contradiction since \(B \geq H_E^2 E\), yielding that \(K_X\) is low rank.

Proposition 8: The rank of \(K_X\) being \(r < n\), that is \(K_X = U_X U_X^*\) with \(U_X\) an \(n \times r\) matrix, the optimal solution to
\[
\min_A \bar{I}(X; Y|Z)
\]
is given by
\[
A^* = (H_E(K_X H_M H_M + I)^{-1} U_X V \ QW)
\]
\[
(H_M (K_X H_M H_M + I)^{-1} U_X V \ PW)^{-1}.
\]

Proof: The Jordan decomposition of \(M\) is now given by
\[
M \left( \begin{array}{cc} H_M & P \\ H_E & Q \end{array} \right) = \left( \begin{array}{cc} H_M & 0 \\ H_E & -I \end{array} \right)
\]
where
\[
J = (I + K_X H_M H_M)^{-1} K_X (H_M^* - H_E^2) \left( \begin{array}{cc} H_M \\ H_E \end{array} \right) - I.
\]

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
\[
J + I = (I + K_X H_M H_M)^{-1} K_X (H_M^* - H_E^2) \left( \begin{array}{cc} H_M \\ H_E \end{array} \right)
\]
and \(\det(K_X) = 0\). Furthermore, since \(K_X = U_X U_X^*\), we have
\[
J = (I + K_X H_M H_M)^{-1} U_X U_X^* (H_M^* - H_E^2) \left( \begin{array}{cc} H_M \\ H_E \end{array} \right) - I
\]
and clearly \((I + K_X H_M H_M)^{-1} U_X\) is an invariant subspace of \(J\). A Jordan basis is thus given by
\[
P' = \left( \begin{array}{c} I + K_X H_M H_M^{-1} U_X \ Q' \end{array} \right)
\]
where \(Q'\) is the eigenspace associated to \(-1\). This thus gives us a more precise Jordan basis for \(M\) (as defined in (9)), namely
\[
\left[ \begin{array}{cc} H_M P' \\ H_E P' \end{array} \right] = \left[ \begin{array}{cc} H_M (K_X H_M H_M + I)^{-1} U_X H_M Q' \\ H_E (K_X H_M H_M + I)^{-1} U_X H_E Q' \end{array} \right].
\]

From this Jordan basis of \(M\), we have that
\[
A^* = (H_E(K_X H_M H_M + I)^{-1} U_X V \ QW)
\]
\[
(H_M (K_X H_M H_M + I)^{-1} U_X V \ PW)^{-1}
\]
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
\[
A^* = (H_E(K_X H_M H_M + I)^{-1} U_X V \ QW)
\]
\[
(H_M (K_X H_M H_M + I)^{-1} U_X V \ PW)^{-1}
\]
be a solution of the Ricatti equation. Then
\[
\bar{I}(X; Y|Z) = \log \det(I + H_M K_X H_M^2) - \log \det(I + H_E K_X H_E^2).
\]
Furthermore, there exists \(V, W\) such that \(A = AA^* > 0\).

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