The Secrecy Capacity of the MIMO Wiretap Channel

Frédérique Oggier and Babak Hassibi [*]

February 2, 2008

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 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.

1 Introduction

Security in wireless communication is a critical issue, which has recently attracted a lot of interest. By nature, wireless channels offer a shared medium, particularly favorable to eavesdropping. Among the numerous points of view from which security has been investigated, we adopt here the one of *information theoretic* security. In this context, most of the works dealing with wireless communication are based on the seminal work of Wyner [16], and its model, *the wire-tap channel*.

1.1 Information theoretic confidentiality

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 have knowledge of 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 [16]: 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 knowledge that the eavesdropper gets of w^k from its received signal z^n is modeled by

$$I(z^n; w^k) = h(w^k) - h(w^k|z^n),$$

since the mutual information measures the amount of information that z^n contains about w^k. The notion of *perfect secrecy* captures the idea that whatever are the resources available to the eavesdropper, they will not allow him to get a single bit of information. Perfect secrecy thus requires

$$I(z^n; w^k) = 0 \iff h(w^k) = h(w^k|z^n).$$

In other words, the amount of randomness is the same in w^k or in $w^k|z^n$.

The decoder computes an estimate $\hat{w}^k$ of the transmitted message w^k, and the probability P_e of decoding erroneously is given by

$$P_e = Pr(w^k \neq \hat{w}^k). \tag{1}$$

The amount of ignorance that the eavesdropper has about a message w^k is called the *equivocation rate*, and following the above discussion, it is naturally defined as:

Definition 1 *The* equivocation rate R_e *at the eavesdropper is*

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

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.

To perfect secrecy is associated 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 $\epsilon > 0$, there exists a sequence of $(2^{nR_s}, n)$ codes such that for any $n \geq n(\epsilon)$, we have*

$$P_e \leq \epsilon \tag{2}$$
$$R_s - \epsilon \leq R_e. \tag{3}$$

The first condition (2) is the standard definition of achievable rate as far as reliability is concerned. The second condition (3) 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.*

1.2 Previous work

In his seminal work [16], Wyner showed for discrete memoryless channels that the perfect secrecy capacity is actually the difference of the capacity of the two users. To prove this result, he worked 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. [7], under the same assumption.

The wire-tap channel has been adopted as a model for numerous works on information theoretic security, and in particular for those on fading channels, both for point-to-point and multi-user systems. We mainly review the prior work for point-to-point. In [5], 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. When only the legitimate channel is known, an optimal power allocation is given, using a variable rate transmission scheme. In [1], Barros et al. have characterized information theoretic security in terms of outage probability. In the case when the transmitter does not know the eavesdropper channel, they define the probability of transmitting at a secrecy rate R_S bigger than the secrecy capacity C_S (i.e. the outage probability) as the probability that the information theoretic security is compromised. They compute this probability, and also show that the probability that the secrecy capacity C_S is positive can actually be positive even if the average SNR of the legitimate channel is weaker than the one of the eavesdropper. They extend their work in [2], where they also consider the cases when Alice has either imperfect or perfect knowledge of the eavesdropper channel. Independently, Liang et al. [12] and Li et al. [10] have computed the secrecy capacity for the parallel wiretap channel with independent subchannels, and derived optimal source power allocation. The secrecy capacity of the wiretap channel with single antenna fading channel follows. Finally, the results of [12] are extended in [13], where a fading broadcast channel with confidential messages is considered, with common information for two receivers, and confidential information intended for only one receiver. The secrecy capacity is computed for the parallel broadcast channel with both independent and degraded subchannels.

In this work, we are interested in the perfect secrecy capacity of multiple antenna channels. A first study of the problem has been proposed by Hero [8]. In a different context than the wire-tap channel, he introduced the so-called constraints of low probability of detection, and low probability of intercept, considering the scenario where the transmitter and the receiver are both informed about their channel while the eavesdropper is uniformed about his. In [9], the SIMO wiretap channel has been considered. Several results on the secrecy in MIMO communication have been provided very recently. In [11], the secrecy capacity is computed for the MISO case. Furthermore, a lower bound is computed in the MIMO case. This lower bound, that is the achievability, is shown to be the expected result, namely, the difference of the two channel capacities,

3

like in the previous cases. Finally, the secrecy capacity for the MISO case has been proven independently by Khisti et al. [6], where furthermore an upper bound is given for the MIMO case, in a regime asymptotic in SNR.

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, as well as for any SNR regime. 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 (as well as in the proofs presented in [7, 5, 1, 12]). 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. [11] is tight, and this is proved by the computation of an upper bound that actually matches the lower bound.

1.3   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. Thus, our model is described by the following broadcast channel

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

where Y, V_M and Z, V_E are respectively $n_M \times 1$ and $n_E \times 1$ vectors. 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. We will denote by $\mathbf{I}_n$ the $n \times n$ identity matrix, and by $\mathbf{0}_n$ the $n \times n$ all zero matrix. We may omit the subscript if the dimension is obvious.

We make the following assumptions:

- X is the $n \times 1$ transmitted signal, with covariance matrix $K_X \succeq \mathbf{0}_n$ satisfying the power constraint
$$
\mathrm{Tr}(K_X) = P.
$$
The power constraint holds for the whole paper, and we may sometimes omit to repeat it explicitly.

- H_M and H_E are respectively $n_M \times n$ and $n_E \times n$ fixed channel matrices such that
$$
H_M^* H_M \succ \mathbf{0}_n, \ H_E^* H_E \succ \mathbf{0}_n.
$$
They are assumed to be known at the transmitter.

- V_M, V_E are independent circularly symmetric complex Gaussian vectors with identity covariance $K_M = \mathbf{I}_{n_M}$, $K_E = \mathbf{I}_{n_E}$ and independent of the transmitted signal X.

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

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

where $\mathrm{Tr}(K_X) = P$. The paper contains the proof of the above theorem: in Section 2, we prove an achievability result which characterizes the optimal matrices $\tilde{K}_X$, while Section 3 contains the main results, namely the proof of the converse.

2 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*

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

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*

$$\max K_X \quad \log \det(\mathbf{I} + H_M K_X H_M^*) - \log \det(\mathbf{I} + H_E K_X H_E^*)$$
$$s.t. \qquad\qquad K_X \succeq \mathbf{0}, \ Tr(K_X) = P,$$

where $H_E^* H_E - H_M^* H_M$ is either indefinite or semidefinite. Then $\tilde{K}_X$ is a low rank matrix.

Proof. In order 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, namely matrices of rank $r < n$.

We thus define the following Lagrangian:

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

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

$$\nabla_{K_X}(\log\det(\mathbf{I} + H_M K_X H_M^*) - \log\det(\mathbf{I} + H_E K_X H_E^*) - \lambda\mathrm{Tr}(K_X)) = 0$$
$$\iff ((H_M^* H_M)^{-1} + K_X)^{-1} = ((H_E^* H_E)^{-1} + K_X)^{-1} + \lambda\mathbf{I}_n. \tag{4}$$

By pre-multiplying the above equation by $(K_X + (H_M^* H_M)^{-1})$ and post-multiplying it by $(K_X + (H_E^* H_E)^{-1})$, we get

$$(H_E^* H_E)^{-1} + K_X = (H_M^* H_M)^{-1} + K_X + \lambda((H_M^* H_M)^{-1} + K_X)((H_E^* H_E)^{-1} + K_X),$$

or equivalently

$$((H_E^* H_E)^{-1} - (H_M^* H_M)^{-1})\frac{1}{\lambda} = ((H_M^* H_M)^{-1} + K_X)((H_E^* H_E)^{-1} + K_X). \tag{5}$$

Now, we have by assumption that $H_M^* H_M \succ \mathbf{0}_n$ and $H_E^* H_E \succ \mathbf{0}_n$. If furthermore $K_X \succ \mathbf{0}$, then all the eigenvalues of $((H_M^* H_M)^{-1} + K_X)((H_E^* H_E)^{-1} + K_X)$ are strictly positive (see Lemma 2, in Appendix). This implies that (5) can have a solution if and only if the Hermitian matrix $((H_E^* H_E)^{-1} - (H_M^* H_M)^{-1})\frac{1}{\lambda}$ 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.

$$\blacksquare$$

3 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*

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

The proof is done in three main steps, that we briefly sketch before entering into the details.

First (subsection 3.1), we have, similarly to [7, 5] that

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

Thus, all the work consists of finding an upper bound on $I(X; Y|Z)$. We will prove the following upper bound:

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

where

$$\tilde{I}(X;Y|Z) = \log \det \left(\mathbf{I}_n + (H_M^*, \; H_E^*) \begin{pmatrix} \mathbf{I}_{n_M} & A \\ A^* & \mathbf{I}_{n_E} \end{pmatrix}^{-1} \begin{pmatrix} H_M \\ H_E \end{pmatrix} K_X \right)$$
$$- \log \det(\mathbf{I} + H_E K_X H_E^*)$$

and A is an $n_M \times n_E$ matrix which denotes the correlation between V_M and V_E. At this point of the proof, the converse can be proved for the two "simple" cases when $H_M^* H_M \succ H_E^* H_E$ and $H_E^* H_E \succ H_M^* H_M$, which are the cases when the channel is degraded.

In general, V_M and V_E are independent. However, since the secrecy capacity does not depend on A, we can assume that $\tilde{I}(X;Y|Z)$ is a function of both A and K_X for the purposes of tightening our upper bound . We show (subsection 3.2) that $\tilde{I}(X;Y|Z)$ is actually concave in K_X and convex in A. As a result, we obtain a new upper bound

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

for all A such that $\mathbf{I} - AA^* \succ \mathbf{0}_{n_E}$, thus

$$\begin{aligned} I(X;Y|Z) &\leq& \min_A \max_{K_X \succeq \mathbf{0}} \tilde{I}(X;Y|Z) \\ &=& \max_{K_X \succeq \mathbf{0}} \min_A \tilde{I}(X;Y|Z). \end{aligned}$$

Furthermore, we jointly optimize $\tilde{I}(X:Y|Z)$ over K_X and A, and compute the optimal $\tilde{A}$ in closed form expression, while showing that the optimal $\tilde{K}_X$ is on the boundary of its domain, namely, $\tilde{K}_X$ is low rank.

We conclude the proof (subsection 3.3) by showing that the converse matches the achievability.

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

We start by recalling a standard result, which has already been proved 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 $I(X;Y|Z)$. We provide two approaches:

1. An upper bound is given by assuming that the legitimate receiver knows both his channel and the one of the eavesdropper.

2. The same upper bound can also be obtained as follows. Clearly, $I(X;Y|Z)$ is upper bounded by taking the maximum over all input distributions $\mathcal{P}(X)$:

$$I(X;Y|Z) \leq \max_{\mathcal{P}(X)} I(X;Y|Z) = \max_{K_X \succeq \mathbf{0}} \tilde{I}(X;Y|Z),$$

where $\tilde{I}(X;Y|Z)$ denotes the value of $I(X;Y|Z)$ when $\mathcal{P}(X)$ is optimal. We will prove that the optimal distribution is Gaussian.

Proposition 3 *We have the following upper bound:*

$$I(X;Y|Z) \leq \max_{K_X \succeq \mathbf{0}} \log \det \left(\mathbf{I}_n + (H_M^*, \ H_E^*) \begin{pmatrix} \mathbf{I} & A \\ A^* & \mathbf{I} \end{pmatrix}^{-1} \begin{pmatrix} H_M \\ H_E \end{pmatrix} K_X \right)$$
$$- \log \det (\mathbf{I} + H_E K_X H_E^*),$$

where A denotes the correlation between V_M and V_E and 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. In this case, the capacity of the link between the transmitter and the legitimate receiver is that of a MIMO system, namely

$$\max_{K_X} \log \det \left(\mathbf{I}_n + (H_M^*, \ H_E^*) \begin{pmatrix} \mathbf{I}_{n_M} & A \\ A^* & \mathbf{I}_{n_E} \end{pmatrix}^{-1} \begin{pmatrix} H_M \\ H_E \end{pmatrix} K_X \right).$$

Now the channel we consider is degraded, and an upper bound is thus the difference of the two capacities, which yields the result.

We now provide the alternative proof. 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

$$
\begin{aligned}
I(X;Y|Z) &= h(Y|Z) - h(Y|X,Z) \\
&= h(Y|Z) - h(X,Y,Z) + h(X,Z) \\
&= h(Y|Z) - h(X) - h(Y,Z|X) + h(X) + h(Z|X) \\
&= h(Y|Z) - h(V_E, V_M) + h(V_E).
\end{aligned}
$$

Thus the optimization problem we have to solve is

$$\max_{\mathcal{P}(X)} h(X + V_M, X + V_E) - h(X + V_E).$$

Using Proposition 10 (see Appendix), the optimal is given by choosing X Gaussian. Thus we have that

$$
\begin{aligned}
I(X;Y|Z) &= h(Y|Z) - h(V_E, V_M) + h(V_E) \\
&= h(Y,Z) - h(Z) - h(V_E, V_M) + h(V_E),
\end{aligned}
$$

which, when X is Gaussian, is given by

$$\log \det(K_{YZ}) - \log \det(K_Z) - \log \det(K_{ME}) + \log \det(K_E)$$

where K_{YZ}, K_Z, K_{ME} and $K_E = \mathbf{I}_{n_E}$ are covariance matrices, with

$$K_{YZ} = \left(\begin{array}{cc} H_M K_X H_M^* + \mathbf{I}_{n_M} & H_M K_X H_E^* + A \\ H_E K_X H_M^* + A^* & H_E K_X H_E^* + \mathbf{I}_{n_E} \end{array} \right),$$

where A denotes the correlation between V_M and V_E, and

$$K_{ME} = \left(\begin{array}{cc} \mathbf{I}_{n_M} & A \\ A^* & \mathbf{I}_{n_E} \end{array} \right).$$

In order for K_{ME} to be well defined, A has to satisfy $\mathbf{I} - AA^* \succeq \mathbf{0}$.

Thus we have

$$\log \det \left(\left(\begin{array}{cc} \mathbf{I} & A \\ A^* & \mathbf{I} \end{array} \right) + \left(\begin{array}{c} H_M \\ H_E \end{array} \right) K_X (H_M^*, \ H_E^*) \right) - \log \det(H_E K_X H_E^* + \mathbf{I})$$
$$- \log \det(K_{ME})$$
$$= \log \det \left(\mathbf{I} + \left(\begin{array}{cc} \mathbf{I} & A \\ A^* & \mathbf{I} \end{array} \right)^{-1} \left(\begin{array}{c} H_M \\ H_E \end{array} \right) K_X (H_M^*, \ H_E^*) \right) - \log \det(H_E K_X H_E^* + \mathbf{I}),$$

where the second equality is well defined if we further require $\mathbf{I} - AA^* \succ \mathbf{0}$. The value of $I(X; Y|Z)$ when X is Gaussian is denoted by $\tilde{I}(X; Y|Z)$:

$$\tilde{I}(X; Y|Z) = \log \det \left(\mathbf{I} + (H_M^*, \ H_E^*) \left(\begin{array}{cc} \mathbf{I} & A \\ A^* & \mathbf{I} \end{array} \right)^{-1} \left(\begin{array}{c} H_M \\ H_E \end{array} \right) K_X \right) \qquad (6)$$
$$- \log \det(\mathbf{I} + H_E K_X H_E^*).$$

$\blacksquare$

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*

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

2. Vice versa, if $H_E^* H_E \succ H_M^* H_M$, we have that

$$I(X; Y|Z) = 0.$$

Proof.   Let us first compute another way of writing $\tilde{I}(X; Y|Z)$, as defined in (6). Note the following factorization:

$$\left(\begin{array}{cc} \mathbf{I}_{n_M} & A \\ A^* & \mathbf{I}_{n_E} \end{array} \right) = \left(\begin{array}{cc} \mathbf{I} & A \\ \mathbf{0} & \mathbf{I} \end{array} \right) \left(\begin{array}{cc} \mathbf{I} - AA^* & \mathbf{0} \\ \mathbf{0} & \mathbf{I} \end{array} \right) \left(\begin{array}{cc} \mathbf{I} & \mathbf{0} \\ A^* & \mathbf{I} \end{array} \right)$$

9

so that

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

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

$$
\begin{aligned}
\tilde{I}(X;Y|Z) &= \log \det(\mathbf{I} + ((H_M^* - H_E^* A^*)(\mathbf{I} - AA^*)^{-1}(H_M - AH_E) + H_E^* H_E)K_X) \\
&\quad - \log \det(\mathbf{I} + H_E K_X H_E^*). \quad\quad\quad (7)
\end{aligned}
$$

1. Since the secrecy capacity does not depend on the noise correlation A, and that
$$I(X;Y|Z) \leq \max_{K_X} \tilde{I}(X;Y|Z),$$
for all A such that $\mathbf{I} - AA^* \succ \mathbf{0}$, we are free to take $A^* = H_E(H_M^* H_M)^{-1} H_M^*$. Indeed, such A does *not* depend on a choice of K_X, and since $H_M^* H_M \succ H_E^* H_E$, A satisfies

$$\mathbf{I} - AA^* = \mathbf{I} - H_M(H_M^* H_M)^{-1} H_E^* H_E (H_M^* H_M)^{-1} H_M^* \succ \mathbf{0}.$$

Finally, we are left to show that by replacing A^* with $H_E(H_M^* H_M)^{-1} H_M^*$ in $\tilde{I}(X;Y|Z)$ indeed yields $\log \det(\mathbf{I} + H_M K_X H_M^*) - \log \det(\mathbf{I} + H_E K_X H_E^*)$. Consider thus $\tilde{I}(X;Y|Z)$ as defined in (7). It is enough to show that

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

We have that

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

using the matrix inversion lemma, so that

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

and finally

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

10

2. Similarly if $H_E^* H_E \succ H_M^* H_M$, we are free to choose $A^* = H_E(H_E^* H_E)^{-1} H_M^*$, which satisfies

$$\mathbf{I} - AA^* = \mathbf{I} - H_M(H_E^* H_E)^{-1} H_M^* \succ \mathbf{0}.$$

Since $H_M^* - H_E^* A^* = \mathbf{0}$, we see from (7) that

$$\tilde{I}(X;Y|Z) = 0.$$

■

The cases described in the lemma can be understood as a simple generalization of the scalar case, since those are the degraded cases. When $H_M^* H_M \succ H_E^* H_E$, 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 case when $H_M^* H_M - H_E^* H_E$ is indefinite, which is the non-degraded case, and thus the interesting case to understand.

3.2 Minimization over A and maximization over K_X

We have shown in Proposition 3 that

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

Since this is true for all A such that $\mathbf{I} - AA^* \succ \mathbf{0}$, we further have that

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

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 (6) 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

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

Proof. Recall from (6) that $\tilde{I}(X;Y|Z)$ is given by

$$\log \det \left(\mathbf{I}_n + (H_M^*, \ H_E^*) \left(\begin{array}{cc} \mathbf{I}_{n_M} & A \\ A^* & \mathbf{I}_{n_E} \end{array} \right)^{-1} \left(\begin{array}{c} H_M \\ H_E \end{array} \right) K_X \right) - \log \det(\mathbf{I} + H_E K_X H_E^*).$$

1. **Convexity in A.** Set

$$C := \begin{pmatrix} \mathbf{I} & A \\ A^* & \mathbf{I} \end{pmatrix}, \; D := \begin{pmatrix} H_M \\ H_E \end{pmatrix} K_X(H_M^*, \; H_E^*).$$

Now $\tilde{I}(X;Y|Z)$ is of the form $\log\det(\mathbf{I}_{n_M+n_E}+C^{-1}D)$, plus some constant term, where $D \succeq \mathbf{0}$. It is known that $\log\det(C)$ is concave in C [3, p.74]), thus $\log\det(C^{-1}) = -\log\det(C)$ is convex in C, which implies that $\log\det(\mathbf{I}+C^{-1}D)$ is convex. Furthermore, it is convex in any block of C, thus convex in A. Finally, the set of A such that $\mathbf{I} - AA^* \succ \mathbf{0}$ is convex.

2. **Concavity in K_X.** Recall from (7) that

$$\begin{aligned} &\tilde{I}(X;Y|Z) \\ = \; &\log\det(\mathbf{I} + ((H_M^* - H_E^* A^*)(\mathbf{I} - AA^*)^{-1}(H_M - AH_E) + H_E^* H_E)K_X) \\ &- \log\det(\mathbf{I} + H_E K_X H_E^*). \end{aligned}$$

Set

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

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

$$\log\det(\mathbf{I}_n + BK_X) - \log\det(\mathbf{I}_n + H_E^* H_E K_X), \tag{8}$$

with $B \succeq H_E^* H_E$.

If we compute the gradient of (8) with respect to K_X, we get that

$$(B^{-1} + K_X)^{-1} - ((H_E^* H_E)^{-1} + K_X)^{-1} \succeq \mathbf{0}, \tag{9}$$

since $B \succeq H_E^* H_E$. Recall that

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

so that the derivative of $F := ((H_E^* H_E)^{-1} + K_X)^{-1}$ is a $n^2 \times n^2$ matrix given by

$$\begin{aligned} &\begin{pmatrix} -FF_{11} & -FF_{12} & \dots & -FF_{1n} \\ -FF_{21} & -FF_{22} & \dots & -FF_{2n} \\ \vdots & & & \vdots \\ -FF_{n1} & -FF_{n2} & & -FF_{nn} \end{pmatrix} \\ = \; &-((H_E^* H_E)^{-1} + K_X)^{-1} \otimes ((H_E^* H_E)^{-1} + K_X)^{-1}. \end{aligned}$$

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

$$((H_E^* H_E)^{-1}+K_X)^{-1}\otimes((H_E^* H_E)^{-1}+K_X)^{-1} \preceq (B^{-1}+K_X)^{-1}\otimes(B^{-1}+K_X)^{-1},$$

which is true by (9).

12

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

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

∎

From the previous steps of the proof, we now know that

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

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

$$\tilde{I}(X;Y,Z) = \log\det(K_{YZ}) - \log\det(K_Z) - \log\det(K_{ME}).$$

By simplifying the Schur complement of $\det(K_{YZ})$ with $\det(K_Z) = \det(K_X + K_E)$, we get that $\tilde{I}(X;Y|Z)$ is given by

$$\log\det(H_M K_X H_M^* + \mathbf{I}_{n_M} - (H_M K_X H_E^* + A)(H_E K_X H_E^* + \mathbf{I})^{-1}(H_E K_X H_M^* + A^*))$$
$$- \log\det(\mathbf{I}_{n_M} - AA^*). \tag{10}$$

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

$$\tilde{A}^* = (H_E(H_M^* H_M)^{-1} H_M^* V, H_E(H_E^* H_E)^{-1} H_M^* W)(V,W)^{-1},$$

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

$$\begin{pmatrix} V \\ H_E(H_M^* H_M)^{-1} H_M^* V \end{pmatrix}$$

is an invariant subspace of the matrix M, as defined in (11). In particular, if $m = n_M$, then $\tilde{A}^* = H_E(H_E^* H_E)^{-1} H_M^*$. Similarly, if $m = 0$, then $\tilde{A}^* = H_E(H_M^* H_M)^{-1} H_M^*$.

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

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

Using this formula, we compute that

$$\nabla_{A^*} \tilde{I}(X;Y|Z) = 0 \iff f(A)(A^* + H_E K_X H_M^*)^{-1}(H_E K_X H_E^* + \mathbf{I}) = (\mathbf{I} - AA^*)(A^*)^{-1},$$

where

$$f(A) = H_M K_X H_M^* + \mathbf{I} - (H_M K_X H_E^* + A)(H_E K_X H_E^* + \mathbf{I})^{-1}(H_E K_X H_M^* + A^*).$$

This yields the following nonsymmetric algebraic Ricatti equation

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

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

$$+ H_E K_X H_M^*(H_M K_X H_M^* + \mathbf{I})^{-1} = 0.$$

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

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

is to look for invariant subspaces of

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

Here we have that M is given by

$$\begin{pmatrix} -(H_M K_X H_M^* + \mathbf{I})^{-1} & -(H_M K_X H_M^* + \mathbf{I})^{-1} H_M K_X H_E^* \\ H_E K_X H_M^*(H_M K_X H_M^* + \mathbf{I})^{-1} & -H_E K_X H_E^* - \mathbf{I} + H_E K_X H_M^*(H_M K_X H_M^* + \mathbf{I})^{-1} H_M K_X H_E^* \end{pmatrix}. \tag{11}$$

Set

$$F = \begin{pmatrix} H_M K_X H_M^* + \mathbf{I}_{n_M} & 0 \\ 0 & \mathbf{I}_{n_E} \end{pmatrix}.$$

We have that $F(M + \mathbf{I}_{n_M + n_E})$ is given by

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

It is easy to see that

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

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 orthogonal to $(-K_X H_M^*, K_X H_E^*)$:

$$Ker(M + \mathbf{I}) = \begin{pmatrix} U_1 \\ H_E(H_E^* H_E)^{-1} H_M^* U_1 \end{pmatrix},$$

for any U_1. Let us now look for the second invariant subspace. We first rewrite M as

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

14

We now show that
$$\begin{pmatrix} U_2 \\ H_E(H_M^* H_M)^{-1} H_M^* U_2 \end{pmatrix},$$
is an invariant subspace for any U_2. Indeed, we have that

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

since

$$
-H_E(\mathbf{I} - K_X H_M^*(H_M K_X H_M^* + \mathbf{I})^{-1} H_M)
$$
$$
= -H_E((H_M^* H_M)^{-1} H_M^*(H_M K_X H_M^* + \mathbf{I}) - K_X H_M^*)(H_M K_X H_M^* + \mathbf{I})^{-1} H_M
$$
$$
= -H_E(H_M^* H_M)^{-1} H_M^*(H_M K_X H_M^* + \mathbf{I})^{-1} H_M.
$$

Thus, a Jordan basis of M is given by

$$\begin{pmatrix} \mathbf{I}_{n_M} & \mathbf{I}_{n_E} \\ H_E(H_M^* H_M)^{-1} H_M^* & H_E(H_E^* H_E)^{-1} H_M^* \end{pmatrix}.$$

Finally, solutions of the Ricatti equation are given by [4]

$$\tilde{A}^* = (H_E(H_M^* H_M)^{-1} H_M^* V, H_E(H_E^* H_E)^{-1} H_M^* W)(V, W)^{-1},$$

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

$$\begin{pmatrix} V \\ H_E(H_M^* H_M)^{-1} H_M^* V \end{pmatrix}$$

is an invariant subspace of M. Note that W can be chosen arbitrary since $(\mathbf{I}, H_E(H_E^* H_E)^{-1} H_M^*)$ is the eigenspace associated to -1.

∎

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

$$
\max K_X \qquad \min_A \tilde{I}(X;Y|Z)
$$
$$
s.t. \quad K_X \succeq \mathbf{0}, \ Tr(K_X) = P,
$$

where $\tilde{A}^* = (H_E(H_M^* H_M)^{-1} H_M^* V, H_E(H_E^* H_E)^{-1} W)(V, W)^{-1}$ is the optimal solution for the minimization over A. Then $\tilde{K}_X$ is a low rank matrix.

Proof. We have seen in (8) that $\tilde{I}(X;Y|Z)$ can be written

$$\log \det(\mathbf{I} + B K_X) - \log \det(\mathbf{I} + H_E K_X H_E^*),$$

15

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

Using the matrix inversion lemma, we have that

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

so that

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

Now

$$(H_E^* H_E)^{-1}(H_M^* - H_E^* A^*)$$
$$= (H_E^* H_E)^{-1}[H_M^* - H_E^*(H_E(H_M^* H_M)^{-1}H_M^* V, H_E(H_E^* H_E)^{-1}W)(V, W)^{-1}]$$
$$= [(H_E^* H_E)^{-1}H_M^*(V, W) - ((H_M^* H_M)^{-1}H_M^* V, (H_E^* H_E)^{-1}W)](V, W)^{-1}$$
$$= (((H_E^* H_E)^{-1} - (H_M^* H_M)^{-1})H_M^* V, \mathbf{0})(V, W)^{-1}$$

thus $(H_E^* H_E)^{-1}(H_M^* - H_E^* A^*)$ is low rank and consequently $B^{-1} - (H_E^* H_E)^{-1}$ is.

Now, from Proposition 2, we know that either $B^{-1} \prec (H_E^* H_E)^{-1}$ and $\lambda > 0$, or $B^{-1} \succ (H_E^* H_E)^{-1}$ and $\lambda < 0$. This gives a contradiction since $B^{-1} \preceq (H_E^* H_E)^{-1}$, implying that $\tilde{K}_X$ has to be low rank.

$\blacksquare$

Proposition 8 *Knowing that the rank of $\tilde{K}_X$ is $r < n$, the optimal solution to*

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

is given by

$$A^* = (H_E(H_M^* H_M)^{-1}H_M^* BH_M U_X V, H_E(H_E^* H_E)^{-1}H_M^* W)(BH_M U_X V, W)^{-1}$$

where $K_X = U_X U_X^*$ and $B = (H_M K_X H_M^* + \mathbf{I})^{-1}$.

Proof. The Jordan decomposition of M is now given by

$$M \begin{pmatrix} \mathbf{I} & \mathbf{I} \\ H_E(H_M^* H_M)^{-1}H_M^* & H_E(H_E^* H_E)^{-1}H_M^* \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{I} \\ H_E(H_M^* H_M)^{-1}H_M^* & H_E(H_E^* H_E)^{-1}H_M^* \end{pmatrix} \begin{pmatrix} J & \mathbf{0} \\ \mathbf{0} & -\mathbf{I} \end{pmatrix}.$$

where

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

Let us now look more carefully at J. We first show that when K_X is low rank, -1 is an eigenvalue. Indeed, we have

$$-(H_M K_X H_M^* + \mathbf{I})^{-1}(H_M K_X H_E^* H_E (H_M^* H_M)^{-1} H_M^* + \mathbf{I}) + \mathbf{I}$$
$$= -(H_M K_X H_M^* + \mathbf{I})^{-1} H_M K_X (H_E^* H_E (H_M^* H_M)^{-1} - \mathbf{I}) H_M^*.$$

This is enough to show that -1 is an eigenvalue since $\det(K_X) = 0$ by assumption that K_X is low rank. The above computation also tells us that

$$-(H_M K_X H_M^* + \mathbf{I})^{-1}(H_M K_X H_E^* H_E (H_M^* H_M)^{-1} H_M^* + \mathbf{I})$$
$$= -(H_M K_X H_M^* + \mathbf{I})^{-1} H_M K_X (H_E^* H_E (H_M^* H_M)^{-1} - \mathbf{I}) H_M^* - \mathbf{I}.$$

Since K_X is low rank, it can be factorized as $K_X = U_X U_X^*$ where U_X is a $n \times r$ matrix, if $r < n$ denotes the rank of K_X. Clearly, $(H_M K_X H_M^* + \mathbf{I})^{-1} H_M U_X$ is an invariant subspace of J. A Jordan basis is thus given by

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

where Q is the eigenspace associated to -1. Set $B := (H_M K_X H_M^* + \mathbf{I})^{-1}$. This thus gives us a more precise Jordan basis for M (as defined in (11)), namely

$$\begin{pmatrix} P & \mathbf{I} \\ H_E (H_M^* H_M)^{-1} H_M^* P & H_E (H_E^* H_E)^{-1} H_M^* \end{pmatrix} =$$
$$\begin{pmatrix} B H_M U_X & Q & \mathbf{I} \\ H_E (H_M^* H_M)^{-1} H_M^* B H_M U_X & H_E (H_M^* H_M)^{-1} H_M^* Q & H_E (H_E^* H_E)^{-1} H_M^* \end{pmatrix}.$$

In this decomposition, the third block is the eigenspace of -1 of dimension n_M which is always present. The middle block also corresponds to an eigenspace of -1, of dimension $n_M - r$, this one appearing only when K_X drops rank. The first block is an invariant subspace, corresponding to the r eigenvalues of M that are different from -1.

From this Jordan basis of M, we have that

$$A^* = (H_E (H_M^* H_M)^{-1} H_M^* B H_M U_X V, H_E (H_E^* H_E)^{-1} H_M^* W)(B H_M U_X V, W)^{-1}$$

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.

■

3.3   The converse matches the achievability

So far, we have solved the optimization problem

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

by computing the optimal $\tilde{A}$ in a closed form expression, and by showing that the optimal $\tilde{K}_X$ is low rank. We are now ready to conclude the proof, by proving that the optimal A makes the converse match the achievability.

Proposition 9 *Set $B = (H_M K_X H_M^* + \mathbf{I})^{-1}$ and let*

$$A^* = (H_E(H_M^* H_M)^{-1} H_M^* B H_M U_X V, H_E(H_E^* H_E)^{-1} H_M^* W)(B H_M U_X V, W)^{-1}$$

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 $\mathbf{I} - AA^* \succ \mathbf{0}$.

Proof. Recall from (6) that a way of writing $\tilde{I}(X;Y|Z)$ is

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

where

$$\begin{pmatrix} \mathbf{I} & A \\ A^* & \mathbf{I} \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ A^* & \mathbf{I} \end{pmatrix} \begin{pmatrix} \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} - A^* A \end{pmatrix} \begin{pmatrix} \mathbf{I} & A \\ \mathbf{0} & \mathbf{I} \end{pmatrix}.$$

Thus

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

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

$$\tilde{I}(X;Y|Z) = \log \det(\mathbf{I} + H_M^* H_M K_X + (-H_M^* A + H_E^*)(\mathbf{I} - A^* A)^{-1}(-A^* H_M + H_E)K_X)$$
$$- \log \det(\mathbf{I} + H_E K_X H_E^*).$$

We now show that K_X is in the kernel of $-A^* H_M + H_E$. We have that

$$
\begin{aligned}
(B H_M U_X V, W)^{-1} H_M K_X &= (H_M U_X V, B^{-1} W)^{-1} B^{-1} H_M K_X \\
&= (H_M U_X V, B^{-1} W)^{-1} H_M U_X U_X^* (H_M^* H_M K_X + \mathbf{I}) \\
&= \begin{pmatrix} V^{-1} U_X^* (H_M^* H_M K_X + \mathbf{I}) \\ \mathbf{0} \end{pmatrix},
\end{aligned}
$$

so that

$$
\begin{aligned}
A^* H_M K_X &= H_E(H_M^* H_M)^{-1} H_M^* B H_M U_X U_X^* (H_M^* H_M K_X + \mathbf{I}) \\
&= H_E(H_M^* H_M)^{-1} H_M^* B B^{-1} H_M K_X \\
&= H_E K_X,
\end{aligned}
$$

and thus $A^* H_M K_X = H_E K_X$, so that we get

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

18

We now have that

$$\mathbf{I} - AA^* \succ \mathbf{0}$$

$$\Longleftrightarrow$$

$$\begin{pmatrix} V^*U_X^*H_M^*B^* \\ W^* \end{pmatrix} (BH_MU_XV, W) -$$

$$\begin{pmatrix} V^*U_X^*H_M^*B^*H_M(H_M^*H_M)^{-1}H_E^* \\ W^*H_M(H_E^*H_E)^{-1}H_E^* \end{pmatrix} (H_E(H_M^*H_M)^{-1}H_M^*BH_MU_XV, H_E(H_E^*H_E)^{-1}H_M^*W) \succeq \mathbf{0}$$

$$\Longleftrightarrow$$

$$\begin{pmatrix} V^*U_X^*H_M^*B(\mathbf{I} - H_M(H_M^*H_M)^{-1}H_E^*H_E(H_M^*H_M)^{-1}H_M^*)BH_MU_XV & \mathbf{0} \\ \mathbf{0} & W^*(\mathbf{I} - H_M(H_E^*H_E)^{-1}H_M^*)W \end{pmatrix} \succ \mathbf{0},$$

since

$$V^*U_X^*H_M^*B^*W - V^*U_X^*H_M^*B^*H_M(H_M^*H_M)^{-1}H_M^*W$$
$$= V^*U_X^*[H_M^*B^* - H_M^*B^*H_M(H_M^*H_M)^{-1}H_M^*]W = \mathbf{0}.$$

To conclude the proof, notice that we have

$$\mathbf{I} - H_M(H_M^*H_M)^{-1}H_E^*H_E(H_M^*H_M)^{-1}H_M^* \preceq \mathbf{0} \iff H_M^*H_M \preceq H_E^*H_E$$

and

$$\mathbf{I} - H_M(H_E^*H_E)^{-1}H_M^* \preceq \mathbf{0} \iff H_E^*H_E \prec H_M^*H_M.$$

Thus if $H_M^*H_M - H_E^*H_E$ is indefinite, there exists V and W such that the above matrix is positive definite.

$\blacksquare$

4 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.

Appendix

Proposition 10 *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*

$$\max \mathcal{P}(X) \quad h(X + A, X + B) - h(X + B)$$
$$s.t. \qquad Tr(K_X) = P$$

is Gaussian.

Proof. First note that

$$\frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I} & -\mathbf{I} \\ \mathbf{I} & \mathbf{I} \end{pmatrix} \begin{pmatrix} X+A \\ X+B \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}}(A-B) \\ \sqrt{2}X + \frac{1}{\sqrt{2}}(A+B) \end{pmatrix}.$$

Since multiplication by a unitary matrix does not change the entropy,

$$\begin{aligned}
&h(X+A, X+B) \\
&= h\left(\sqrt{2}X + \frac{1}{\sqrt{2}}(A+B), \frac{1}{\sqrt{2}}(A-B)\right) \\
&= h\left(\sqrt{2}X + \frac{1}{\sqrt{2}}(A+B) \Big| \frac{1}{\sqrt{2}}(A-B)\right) \\
&\quad + h\left(\frac{1}{\sqrt{2}}(A-B)\right) \\
&= h(\sqrt{2}X + U) + h\left(\frac{1}{\sqrt{2}}(A-B)\right)
\end{aligned}$$

where U is Gaussian with covariance matrix K_U given by

$$\begin{aligned}
&\tfrac{1}{2}E[(A+B)(A+B)^*] - \tfrac{1}{2}E[(A+B)(A-B)^*] \cdot \\
&\quad E[(A-B)(A-B)^*]^{-1}E[(A-B)(A+B)^*],
\end{aligned}$$

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 [15] in the case of real Gaussian vectors. Their result can be readily extended to the circularly symmetric complex Gaussian case.

∎

Lemma 2 *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,

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

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

∎

References

[1] J. Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels", *IEEE International Symposium on Information Theory*, Seattle, July 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] S. Boyd and L. Vandenberghe, "Convex Optimization", Cambridge University Press, 2004.

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

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

[6] A. Khisti, G. Wornell, A. Wiesel, Y. Eldar, "On the Gaussian MIMO Wiretap Channel", in *Proc. of IEEE International Symposium on Information Theory*, Nice, 2007.

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

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

[9] P. Parada, R. Blahut,"Secrecy capacity of SIMO and slow fading channels," in *Proc. of IEEE International Symposium on Information Theory*, Adelaide, 2005.

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

[11] Z. Li, W. Trappe, R. Yates, "Secret communication via multi-antenna transmission", in the proceedings of *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 Information Theory*, Special Issue on Information Theoretic Security, November 2006

[14] R. Liu, H. V. Poor, "Multiple Antenna Secure Broadcast over Wireless Networks", to appear in the Proceedings of the First International Workshop on Information Theory for Sensor Networks, Santa Fe, NM, June 2007.

[15] T. Liu, P. Viswanath, "An Extremal Inequality Motivated by Multiterminal Information Theoretic Problems", to appear in *IEEE Transactions on Information Theory*.

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