FILTER DESIGN WITH SECRECY CONSTRAINTS: ZERO-FORCING CONSTRAINT AT THE LEGITIMATE RECEIVER

Hugo Reboredo[⋆†], *Miguel R. D. Rodrigues*[⋆] *and João Xavier*[†]

[⋆†] Instituto de Telecomunicações, Dept. de Ciência de Computadores da Faculdade de Ciências da Universidade do Porto, Portugal

[⋆] Department of Electronic and Electrical Engineering, University College London, United Kingdom

[†] Instituto de Sistemas e Robótica, Instituto Superior Técnico, Portugal

Emails: [⋆†] hugoreboredo@dcc.fc.up.pt, [⋆] m.rodrigues@ee.ucl.ac.uk, [†] jxavier@isr.ist.utl.pt

ABSTRACT

This paper considers the problem of filter design with secrecy constraints, where two legitimate parties (Alice and Bob) communicate in the presence of an eavesdropper (Eve), over a Gaussian multiple-input multiple-output (MIMO) wiretap channel. In particular, this problem involves the design of the transmit and the receive filters, subject to a power constraint, which minimize the mean-squared error (MSE) between the legitimate parties whilst assuring that the eavesdropper MSE remains above a certain level. We consider a general Multiple-Input Multiple-Output (MIMO) Gaussian wiretap scenario, where a Zero-Forcing (ZF) filter is used at the legitimate receiver, whilst the eavesdropper uses an optimal linear receive filter, and characterize the receive and transmit filters in various power regimes. Finally, we present a set of numerical results that support some of the main conclusions.

1. INTRODUCTION

Security and privacy remain issues of utmost importance in wireless communications systems. In contrast to their wire-line counterparts, the wireless links are much more susceptible to eavesdropping attacks due to the inherent broadcast nature of the wireless medium.

In addiction to the traditional cryptographic algorithms (which are based on the intractability of certain functions and are insensitive to the physical nature of the wireless medium), there has been a renewed interest in information-theoretic security – widely accepted as the strictest notion of security. This involves the use of physical-layer techniques that exploit the inherent randomness of the communications medium to guarantee both reliable and secure communications in the presence of an eavesdropper.

The basis of information-theoretic security, which builds upon Shannon's notion of perfect secrecy [1], was laid by Wyner [2] and by Csiszár and Körner [3] who proved in seminal papers that there exist channel codes guaranteeing both robustness to transmission errors and a certain degree of data confidentiality. In particular, Wyner considered the wiretap channel where two legitimate users communicate over a main channel in the presence of an eavesdropper who observes degraded versions of the main channel messages over the wiretap channel. Wyner characterized the rate-equivocation region of the wiretap channel and its secrecy capacity. The computation of the secrecy capacity of a range of communications channels has thus been an important research topic (e.g. see [4], [5]).

This paper addresses the problem of secure communications from the estimation-theoretic rather than from the information-theoretic view-point. We consider the problem of filter design with secrecy constraints in the classical wiretap scenario consisting of two legitimate parties that communicate in the presence of an eavesdropper, where the objective is to conceive transmit and receive filters that minimize the mean-squared error (MSE) between the legitimate parties whilst guaranteeing a certain eavesdropper MSE level. In particular we consider the case where the legitimate receiver uses a Zero-Forcing (ZF) constraint whereas the eavesdropper uses the optimal linear receiver. This generalizes the filter design with secrecy constraint problem in [6], where both the legitimate receiver and the eavesdropper employ a ZF filter. Interestingly, this class of problems also represents a natural generalization of filter design for point-to-point communications systems which has been considered in the past by several authors (e.g. [7], [8]). Another approach to this problem is presented in [9] where the authors aim to minimize the transmit power required to guarantee a certain signal-to-interference-plus-noise ratio (SINR) for the legitimate receiver and then, use the remaining power generate artificial noise to jam the eavesdropper. Note that, due to the nature of the problem, minimizing the MSE is equivalent to maximizing the SINR [7].

This paper is structured as follows: Section 2 defines the problem. Sections 3 and 4 consider the design of the receive and transmit filters, respectively. Section 5 discusses the regions of validity of key operational regimes under consideration. Section 6 shows various numerical results to illustrate the impact of the filter designs on both the reliability and security criteria. The main conclusions of this work are drawn in section 7.

2. PROBLEM STATEMENT

We consider a communications scenario where a legitimate user, say Alice, communicates with another legitimate user, say Bob, in the presence of an eavesdropper, Eve (see Figure 1). Bob and Eve observe the output of the multiple-input multiple-output (MIMO) channels given, respectively, by:

This work was supported by Fundação para a Ciência e Tecnologia through the research project PTDC/EEA-TEL/100854/2008.

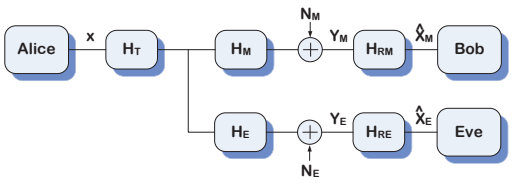

Fig. 1. MIMO Gaussian wiretap channel model.

$$\mathbf{Y}_M = \mathbf{H}_M\mathbf{H}_T\mathbf{X} + \mathbf{N}_M \tag{1}$$

$$\mathbf{Y}_E = \mathbf{H}_E\mathbf{H}_T\mathbf{X} + \mathbf{N}_E \tag{2}$$

where $\mathbf{Y}_M$ and $\mathbf{Y}_E$ are the n_M and the n_E-dimensional vectors of receive symbols, $\mathbf{X}$ is a m-dimensional vector of independent, zero-mean and unit-variance transmit symbols, and $\mathbf{N}_M$ and $\mathbf{N}_E$ are n_M and n_E-dimensional complex Gaussian random vectors with zero mean and identity covariance matrix. The $n_M \times m$ matrix $\mathbf{H}_M$ and the $n_E \times m$ matrix $\mathbf{H}_E$ contain the gains from each main and eavesdropper channel input to each main and eavesdropper channel output, respectively. The $m \times m$ matrix $\mathbf{H}_T$ represents Alice's transmit filter. We assume that $\mathbf{H}_M\mathbf{H}_T$ and $\mathbf{H}_E\mathbf{H}_T$ are full column rank, which implies that $n_M \geq m$ and $n_E \geq m$. We also assume that Alice, Bob and Eve have perfect knowledge about the channel matrices $\mathbf{H}_M$ and $\mathbf{H}_E$. This is often a common assumption in the physical layer security literature (see e.g. [4]).

Bob's and Eve's estimate of the vector of input symbols are given by:

$$\hat{\mathbf{X}}_M = \mathbf{H}_{RM}\mathbf{Y}_M \tag{3}$$

$$\hat{\mathbf{X}}_E = \mathbf{H}_{RE}\mathbf{Y}_E \tag{4}$$

where the $m \times n_M$ matrix $\mathbf{H}_{RM}$ and the $m \times n_E$ matrix $\mathbf{H}_{RE}$ represent Bob's and Eve's receive filters, respectively.

In this setting, we take as a performance metric the MSE between the estimate of the input vector and the true input vector. The objective is to design the transmit filter that solves the optimization problem:

$$\min \quad \mathsf{MSE_M} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}_M\|^2\right] \tag{5}$$

subject to the security constraint:

$$\mathsf{MSE_E} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}_E\|^2\right] \geq \gamma \tag{6}$$

and to the total power constraint:

$$\mathsf{tr}\left\{\mathbf{H}_T\mathbf{H}_T^\dagger\right\} \leq P_{avg} \tag{7}$$

for particular receiver filter choices, where $\|\cdot\|^2$ denotes the l_2-norm, $\mathcal{E}(\cdot)$ denotes the expectation operator, $(\cdot)^\dagger$ denotes the Hermitian transpose operator and $\mathsf{tr}\{\cdot\}$ denotes the trace operator.

It is important to note that this approach does not guarantee perfect information-theoretic security, in the sense of [1], [2] and [3][1]. The design of the filters based on the MSE criteria is, instead, a means to provide additional confusion in a communications system. The rationale is based on the fact that some applications require a MSE below a certain level to function properly, so that this approach would impair further the performance of the eavesdropper by imposing a threshold on its MSE level. This setup can also be combined with existing cryptographic algorithms, in order to strengthen the security of the communications system.

[1]We consider this aspect in greater detail in section 6, where we analyze the mutual information in the eavesdropper channel.

3. RECEIVE FILTERS DESIGN

We now consider the design of the receive filters. The legitimate receiver uses the receive filter that, for any fixed transmit filter, minimizes the MSE given by:

$$\mathsf{MSE_M} = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RM}\mathbf{Y}_M\|^2\right] \tag{8}$$

subject to the ZF constraint:

$$\mathbf{H}_{RM}\mathbf{H}_M\mathbf{H}_T = \mathbf{I} \tag{9}$$

where $\mathbf{I}$ is the $m \times m$ identity matrix. The legitimate receiver receive filter is then given by:

$$\mathbf{H}_{RM}^* = \left(\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\right)^{-1}\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger \tag{10}$$

On the other hand, the eavesdropper uses the receive filter that, for any fixed transmit filter, minimizes the MSE given by:

$$\mathsf{MSE_E} = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RE}\mathbf{Y}_E\|^2\right] \tag{11}$$

The eavesdropper receive filter is then given by [10][2]:

$$\mathbf{H}_{RE}^* = \mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\left(\mathbf{I} + \mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\right)^{-1} \tag{12}$$

Hence, upon substitution of (10) and (12) into (8) and (11), respectively, it follows that the MSEs associated with the receive filter designs are given by:

$$\mathsf{MSE}_M = \mathsf{tr}\left\{\left(\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\right)^{-1}\right\} \tag{13}$$

and

$$\mathsf{MSE_E} = \mathsf{tr}\left\{\left(\mathbf{I} + \mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right\} \tag{14}$$

4. TRANSMIT FILTER DESIGN

We now consider the design of the optimal linear transmit filter. This, in view of (13) and (14), corresponds to the solution of the optimization problem given by:

$$\min_{\mathbf{H}_T} \quad \mathsf{tr}\left\{\left(\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\right)^{-1}\right\} \tag{15}$$

subject to the secrecy constraint:

$$\mathsf{tr}\left\{\left(\mathbf{I} + \mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right\} \geq \gamma \tag{16}$$

and to the power constraint:

$$\mathsf{tr}\left\{\mathbf{H}_T\mathbf{H}_T^\dagger\right\} \leq P_{avg} \tag{17}$$

[2]We recognize the fact that more sophisticated nonlinear techniques could be used in order to estimate Alice's information, but we restrict our attention to the use of linear filters by the eavesdropper, in this paper.

with $\mathbf{H}_T\mathbf{H}_T^\dagger \succ 0$. By considering the change of variable $\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1} = \mathbf{Z}$, $\left(\mathbf{H}_M^\dagger\mathbf{H}_M\right)^{-1} = \mathbf{A}$ and $\left(\mathbf{H}_E^\dagger\mathbf{H}_E\right) = \mathbf{B}$, together with the Woodbury matrix identity, it is also possible to rewrite the optimization problem as follows:

$$\min_{\mathbf{Z}} \ \mathsf{tr}\left\{\mathbf{AZ}\right\} \tag{18}$$

subject to the constraints:

$$\mathsf{tr}\left\{\mathbf{I}\right\} - \mathsf{tr}\left\{\mathbf{B}\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\right\} \geq \gamma \tag{19}$$

$$\mathsf{tr}\left\{\mathbf{Z}^{-1}\right\} \leq P_{avg} \tag{20}$$

and $\mathbf{Z} \succ 0$. One recognizes immediately that this is a standard convex optimization problem, so that the solution follows from the Karush-Kuhn-Tucker conditions given by:

$$\mathbf{A} - \nu\left[\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\mathbf{B}\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\right] - \mu\mathbf{Z}^{-2} = 0 \tag{21}$$

$$\nu\left\{\left[\mathsf{tr}\left\{\mathbf{I}\right\} - \mathsf{tr}\left\{\mathbf{B}\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\right\}\right] - \gamma\right\} = 0, \quad \nu \geq 0 \tag{22}$$

$$\mu\left[P_{avg} - \mathsf{tr}\left\{\mathbf{Z}^{-1}\right\}\right] = 0, \quad \mu \geq 0 \tag{23}$$

$$\mathbf{Z} \succ 0 \tag{24}$$

$$\mathsf{tr}\left\{\mathbf{I}\right\} - \mathsf{tr}\left\{\mathbf{B}\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\right\} \geq \gamma \tag{25}$$

$$\mathsf{tr}\left\{\mathbf{Z}^{-1}\right\} \leq P_{avg} \tag{26}$$

where ν ans μ are the Lagrange multipliers associated with the secrecy and the power constraints, respectively.

It is clear from the Karush-Kuhn-Tucker conditions that there are three operational regimes: i) the scenario where the transmitter can use all the available power without violating the secrecy constraint (there is not enough available power to violate the secrecy constraint), so that the secrecy constraint is not active ($\nu = 0$) and the power constraint is active ($\mu > 0$); ii) the scenario where both the secrecy and power constraints are active ($\nu > 0$ and $\mu > 0$); and iii) the scenario where the transmitter cannot use all the available power without violating the secrecy constraint, so that the secrecy constraint is active ($\nu > 0$) and the power constraint is inactive ($\mu = 0$).

It is difficult to extract a characterization of the optimal filter design from the Karush-Kuhn-Tucker conditions above in the general scenario. Consequently, we concentrate on scenarios i) and iii) only.

4.1. Power constraint active / secrecy constraint inactive

Let us consider the scenario where the power constraint is active, whilst the secrecy constraint is inactive. This situation typically arises – for a certain fixed γ – in a regime of low available power, due to the fact that the power, injected into the channel, is not enough to meet or violate the secrecy constraint.

The following Theorem, which stems directly from the Karush-Kuhn-Tucker optimality conditions above, defines the form of the optimal transmit filter, in such a regime.

Theorem 1 *An optimal transmit filter is, without loss of generality, given by:*

$$\mathbf{H}_T^* = \alpha\left(\mathbf{H}_M^\dagger\mathbf{H}_M\right)^{-\frac{1}{4}} \tag{27}$$

where $\alpha = \sqrt{\dfrac{P_{avg}}{\mathsf{tr}\left\{\left(\mathbf{H}_M^\dagger\mathbf{H}_M\right)^{-\frac{1}{2}}\right\}}}$.

Proof 1 *This Theorem follows from the Karush-Kuhn-Tucker conditions by using the fact that $\nu = 0$, so that we can rewrite* (21) *as follows:*

$$\mathbf{A} - \mu\mathbf{Z}^{-2} = 0 \tag{28}$$

Note that in this regime, the left singular vectors of $\mathbf{H}_T^*$ correspond to the matrix with the right singular vectors of $\mathbf{H}_M$, so that the transmit filter diagonalizes the main channel. This solution corresponds to the solution in [7].

4.2. Power constraint inactive / secrecy constraint active

Let us now consider the scenario where the power constraint is inactive, whilst the secrecy constraint is active. This is a situation that typically arises – for a certain fixed γ – in a regime of high available power; in fact, the use of all the available power would immediately violate the secrecy constraint.

The following theorem, which also stems directly from the Karush-Kuhn-Tucker optimality conditions above, defines the form of the optimal transmit filter, in such a regime. In particular, we use the fact that there exists a non-singular $m \times m$ matrix $\mathbf{C}$ that diagonalizes both $\mathbf{H}_M^\dagger\mathbf{H}_M$ and $\mathbf{H}_E^\dagger\mathbf{H}_E$ simultaneously [11], i.e.:

$$\mathbf{C}^\dagger\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{C} = \mathbf{\Lambda}_E$$

$$\mathbf{C}^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{C} = \mathbf{\Lambda}_M$$

such that:

$$\mathbf{H}_E^\dagger\mathbf{H}_E = \mathbf{C}^{-\dagger}\mathbf{\Lambda}_E\mathbf{C}^{-1}$$

$$\left(\mathbf{H}_M^\dagger\mathbf{H}_M\right)^{-1} = \mathbf{C}\mathbf{\Lambda}_M^{-1}\mathbf{C}^\dagger$$

where, the $m \times m$ matrices $\mathbf{\Lambda}_M$, $\mathbf{\Lambda}_M^{-1}$ and $\mathbf{\Lambda}_E$ are diagonal matrices.

Theorem 2 *An optimal transmit filter is, without loss of generality, given by:*

$$\mathbf{H}_T^* = \mathbf{C}\left(\alpha\mathbf{\Lambda}_M^{\frac{1}{2}}\mathbf{\Lambda}_E^{\frac{1}{2}} - \mathbf{\Lambda}_E\right)^{-\frac{1}{2}} \tag{29}$$

where $\alpha = \dfrac{\mathsf{tr}\left\{\mathbf{\Lambda}_E^{\frac{1}{2}}\mathbf{\Lambda}_M^{-\frac{1}{2}}\right\}}{\mathsf{tr}\{\mathbf{I}\}-\gamma}$.

Proof 2 *This Theorem also follows from the Karush-Kuhn-Tucker conditions above by using the fact that $\mu = 0$, so that we can rewrite* (21) *as follows:*

$$\mathbf{A} - \nu\left[\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\mathbf{B}\left(\mathbf{Z}+\mathbf{B}\right)^{-1}\right] = 0 \tag{30}$$

5. A NOTE ON THE VALIDITY OF THE OPERATIONAL REGIMES

It is now relevant to establish conditions, which are a function of the system parameters, that identify the exact regions of validity of the operational regimes unveiled and investigated in the previous section.

5.1. Power constraint active / secrecy constraint inactive

It is easy to show that this regime is valid if, for a fixed set of system parameters, P_{avg}, γ, $\mathbf{H}_M$ and $\mathbf{H}_E$, the following condition holds:

$$\mathsf{tr}\left\{\mathbf{I}\right\} - \mathsf{tr}\left\{\mathbf{H}_E^{\dagger}\mathbf{H}_E\left[\left(\mathbf{H}_T^{*}\mathbf{H}_T^{*\dagger}\right)^{-1} + \mathbf{H}_E^{\dagger}\mathbf{H}_E\right]^{-1}\right\} \geq \gamma \quad (31)$$

where $\mathbf{H}_T^{*}$ follows the solution embodied in Theorem 1, given by:

$$\mathbf{H}_T^{*} = \sqrt{\frac{P_{avg}}{\mathsf{tr}\left\{\left(\mathbf{H}_M^{\dagger}\mathbf{H}_M\right)^{-\frac{1}{2}}\right\}}}\left(\mathbf{H}_M^{\dagger}\mathbf{H}_M\right)^{-\frac{1}{4}} \quad (32)$$

Note that (31) and (32) can be used to determine a threshold secrecy constraint, $\gamma_{max_{reg1}}$, below which we operate under this regime, or equivalently, a threshold power constraint, $P_{avg_{maxR1}}$, below which we operate under this same regime. The threshold secrecy constraint is given by:

$$\gamma_{max_{reg1}} = \mathsf{tr}\{\mathbf{I}\} - \mathsf{tr}\left\{\mathbf{H}_E^{\dagger}\mathbf{H}_E\left[\frac{\mathsf{tr}\left\{\left(\mathbf{H}_M^{\dagger}\mathbf{H}_M\right)^{-\frac{1}{2}}\right\}}{P_{avg}}\left(\mathbf{H}_M^{\dagger}\mathbf{H}_M\right)^{\frac{1}{2}} + \mathbf{H}_E^{\dagger}\mathbf{H}_E\right]^{-1}\right\} \quad (33)$$

5.2. Power constraint inactive / secrecy constraint active

It is also straightforward to show that this regime is valid if, for a fixed set of system parameters, P_{avg}, γ, $\mathbf{H}_M$ and $\mathbf{H}_E$, the following condition holds:

$$\mathsf{tr}\left\{\mathbf{H}_T^{*}\mathbf{H}_T^{*\dagger}\right\} \leq P_{avg} \quad (34)$$

where $\mathbf{H}_T^{*}$ follows the solution embodied in Theorem 2, given by:

$$\mathbf{H}_T^{*} = \mathbf{C}\left(\frac{\mathsf{tr}\left\{\mathbf{\Lambda}_E^{\frac{1}{2}}\mathbf{\Lambda}_M^{-\frac{1}{2}}\right\}}{\mathsf{tr}\left\{\mathbf{I}\right\} - \gamma}\mathbf{\Lambda}_M^{\frac{1}{2}}\mathbf{\Lambda}_E^{\frac{1}{2}} - \mathbf{\Lambda}_E\right)^{-\frac{1}{2}} \quad (35)$$

Similarly to the previous regime, (34) and (35) can be used to determine a threshold secrecy constraint, $\gamma_{min_{reg3}}$, above which we operate under this regime, or equivalently, a threshold power constraint, $P_{avg_{minR3}}$, above which we operate in the same regime. The threshold power constraint is given by:

$$P_{avg_{min}} = \mathsf{tr}\left\{\mathbf{C}\left(\frac{\mathsf{tr}\left\{\mathbf{\Lambda}_E^{\frac{1}{2}}\mathbf{\Lambda}_M^{-\frac{1}{2}}\right\}}{\mathsf{tr}\left\{\mathbf{I}\right\} - \gamma}\mathbf{\Lambda}_M^{\frac{1}{2}}\mathbf{\Lambda}_E^{\frac{1}{2}} - \mathbf{\Lambda}_E\right)^{-1}\mathbf{C}^{\dagger}\right\} \quad (36)$$

6. NUMERICAL RESULTS

We shall now present a set of numerical results in order to provide further insight into this problem. We consider, for simplicity, a 2×2 MIMO Gaussian wiretap channel where the main and the eavesdropper channel matrices are given by:

$$\mathbf{H}_M = \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix} \qquad and \qquad \mathbf{H}_E = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}$$

Figure 2 shows the values of the MSEs in the main and in the eavesdropper channels and the injected power into the channels *vs*. the secrecy constraint, for $P_{avg} = 1$. The three operational regimes are evident. Below $\gamma_{max_{reg1}}$,the solution minimizes the MSE in the main channel subject to the power constraint only. We can indeed verify that the available power is not sufficient to meet or violate the secrecy constraint. In-between $\gamma_{max_{reg1}}$ and $\gamma_{min_{reg3}}$,the optimal solution[3] minimizes the MSE in the main channel while meeting the power and the secrecy constraint with equality. Above $\gamma_{min_{reg3}}$, the optimal solution minimizes MSE in the main channel subject to the secrecy constraint only. Note that it is not possible to use all the available power, otherwise the secrecy constraint would be violated. Figure 3 shows the values of the MSEs in the main and eavesdropper channel along with the injected power *vs* the available power, for $\gamma = 1$. We easily identify, once more, the three regimes of operation. For $P_{avg} < P_{avg_{maxR1}}$ the optimal design follows the solution embodied in Theorem 1. For $P_{avg} > P_{avg_{minR3}}$ the optimal design follows the solution embodied in Theorem 2. For $P_{avg_{maxR1}} < P_{avg} < P_{avg_{minR3}}$ the optimal design satisfies the power and the secrecy constraints with equality.

It is also of interest to analyze the mutual information between the input vector and the output vectors achieved by our design. Figure 4 depicts the mutual information between the input $\mathbf{X}$ and the eavesdropper output $\mathbf{Y_E}$ *vs*. the available power, by assuming that the input follows a Gaussian distribution. We consider three distinct designs: (1) the optimal transmit filter achieved by our design; (2) the transmit filter that minimizes the mean squared error in the main channel, but does not take in account any secrecy constraint; and (3) a transmit filter which is a multiple of the identity matrix, and such that $\mathsf{tr}\left\{\mathbf{H}_T\mathbf{H}_T^{\dagger}\right\} = P_{avg}$ – note that this represents isotropic signalling. It is very interesting to verify that, even without directly minimizing the mutual information in the eavesdropper channel, which corresponds to the information-theoretic security criteria *par excellence*, our optimal solution results in the lowest mutual information of these three cases. In particular, by imposing a threshold on the MSE in the eavesdropper channel one will, not only impair the eavesdropper performance, but also limit the amount of information that is leaked.

7. CONCLUSIONS

We have considered the problem of filter design with secrecy constraints in the classical wiretap scenario, where the objective is to design transmit and receive filters that minimize the

[3]The solution in this regime, which has not been derived, was obtained through numerical methods.

MSE between the legitimate parties whilst guaranteeing that the eavesdropper MSE remains above a certain threshold. In particular we considered the case where the legitimate receiver uses a Zero Forcing receive filter while the eavesdropper utilizes the optimum linear receive filter. We characterized the form of the receive and transmit filters in particular operational regimes, together with a set of numerical results to illustrate the performance. We also note that the design of filters that minimize the MSE between the legitimate parties whilst guaranteeing a minimum MSE at the eavesdropper, subject to a power constraint, appears to be a viable option to provide reliability and a certain additional degree of security. In particular, our designs have been shown to limit the amount of mutual information leaked to the eavesdropper, in comparison to other designs.

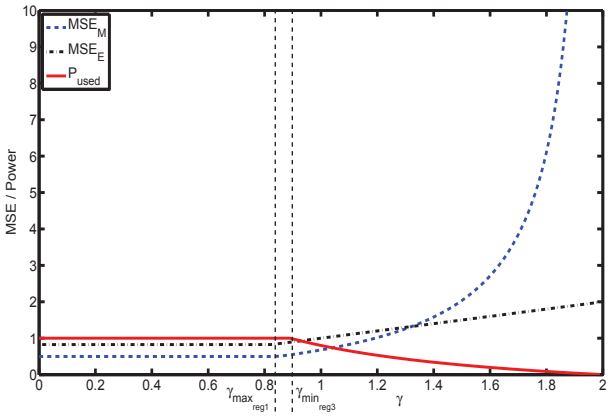

Fig. 2. Main and eavesdropper channel MSEs *vs.* secrecy constraint and input power *vs.* secrecy constraint, for optimal filter design ($P_{avg} = 1$).

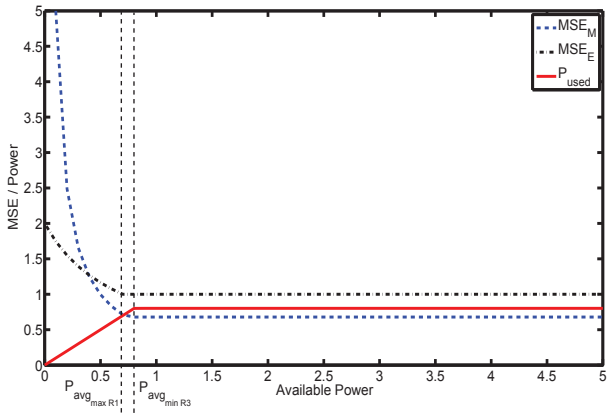

Fig. 3. Main and eavesdropper channel MSEs *vs.* available power and input power *vs.* available power, for optimal filter design ($\gamma = 1$).

8. REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

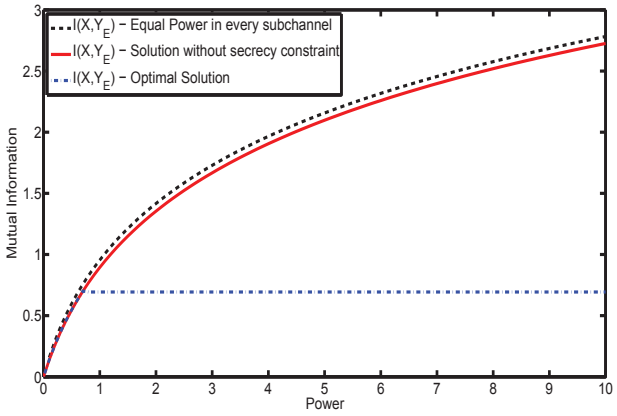

Fig. 4. Eavesdropper Mutual Information *vs.* available power for three different transmit filter designs ($\gamma = 1$).

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–349, May 1978.

[4] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE International Symposium on Information Theory*, Jul. 2006.

[5] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *IEEE International Symposium on Information Theory*, Jul. 2008.

[6] H. Reboredo, V. Prabhu, M. R. D. Rodrigues, and J. Xavier, "Filter design with secrecy constraints: The multiple-input multiple-output Gaussian wiretap channel with zero forcing receive filters," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, may 2011, pp. 3440 –3443.

[7] D. P. Palomar, J. M. Cioffi, and M. A. Lagunas, "Joint tx-rx beamforming design for multicarrier MIMO channels: A unified framework for convex optimization," *IEEE Transactions on Signal Processing*, vol. 51, no. 9, pp. 2381–2401, Sep. 2003.

[8] F. Pérez-Cruz, M. Rodrigues, and S. Verdú, "MIMO Gaussian Channels With Arbitrary Inputs: Optimal Precoding and Power Allocation," *Information Theory, IEEE Transactions on*, vol. 56, no. 3, pp. 1070 –1084, march 2010.

[9] A. Mukherjee and A. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect csi," *Signal Processing, IEEE Transactions on*, vol. 59, no. 1, pp. 351 –361, jan. 2011.

[10] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs, N.J.: Prentice-Hall, 1993.

[11] G. H. Golub and C. F. V. Loan, *Matrix Computations, 3 ed.* Baltimore, M.D.: Johns Hopkins University Press, 1996.