Filter Design with Secrecy Constraints: The Degraded Multiple-Input Multiple-Output Gaussian Wiretap Channel

Hugo Reboredo*, Munnujahan Ara†, Miguel R. D. Rodrigues‡
Instituto de Telecomunicações
Dept. of Computer Science, University of Porto, Portugal
emails: *hugoreboredo@dcc.fc.up.pt, †munnujahan_ara@dcc.fc.up.pt, ‡mrodrigues@dcc.fc.up.pt

João Xavier
Instituto de Sistemas e Robótica
Instituto Superior Técnico, Portugal
email: 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 multiple-input multiple-output (MIMO) Gaussian channels. In particular, we consider the design of transmit and receive filters that minimize the mean-squared error (MSE) between the legitimate parties subject to a certain eavesdropper MSE level, in the situation where the eavesdropper MIMO channel is a degraded version of the main MIMO channel. We characterize the form of the optimal receive filters as well as the form of optimal transmit filter in different scenarios. We also put forth an iterative algorithm to obtain the optimal values of the transmit and receive filters. Finally, we present a set of numerical results that illustrate the conclusions.**

I. Introduction

The issues of privacy and security in wireless communication networks have taken on an increasingly important role as these networks continue to flourish worldwide. Traditionally, security is viewed as an independent feature with little or no relation to the remaining data communication tasks and, therefore, state-of-the-art cryptographic algorithms are insensitive to the physical nature of the wireless medium.

However, there has been more recently a renewed interest on information-theoretic security – widely accepted as the strictest notion of security – which calls for the use of physical-layer techniques exploiting the inherent randomness of the communications medium to guarantee both reliable and secure communication.

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 the eavesdropper observes degraded versions of the main channel messages over the wiretap channel and characterized the rate-equivocation region of the wiretap channel and its secrecy capacity. Ever since, the computation of the secrecy capacity of a range of communications channels has been an important research topic (e.g., see [4], [5], [6], [7]).

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

This paper considers secure communications from the estimation-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 dimension 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 shall extend recent results [8] on filter design with secrecy constraints from degraded parallel wiretap Gaussian channels to degraded multiple-input multiple-output Gaussian wiretap channels. Interestingly, this class of problems 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. [9], [10]). Some work on the topic of filter design in the wiretap channel scenario has also recently been presented in [11].

This paper is structured as follows: Section II defines the problem. Sections III and IV consider the design of the receive and transmit filters. Section V puts forth an iterative algorithm to compute the elements of the optimal transmit filter, and hence the receive filters. Section VI discusses the regions of validity of the operational regimes under consideration. Section VII shows various numerical results to illustrate the impact of the filter designs on both the reliability and security criteria and draws the main conclusions of this work.

II. 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, each one, the output of the main and the eavesdropper MIMO channels respectively, given by:

$$\mathbf{Y}_M = \mathbf{H}_M\mathbf{H}_T\mathbf{X} + \mathbf{N}_M \quad (1)$$

$$\mathbf{Y}_E = \mathbf{H}_E\mathbf{H}_T\mathbf{X} + \mathbf{N}_E \quad (2)$$

where $\mathbf{Y}_M$ and $\mathbf{Y}_E$ are the n_M and the n_E-dimensional vectors of receive symbols, $\mathbf{X}$ is the l-dimensional vector of independent, zero-mean and unit-variance transmit symbols. $\mathbf{N}_M$ and $\mathbf{N}_E$ are n_M and n_E-dimensional complex Gaussian

random vectors with zero mean and identity covariance matrix.

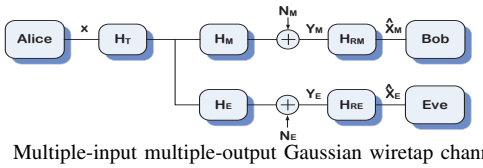

Figure 1. Multiple-input multiple-output Gaussian wiretap channel model.

The $n_M \times m$ matrix $\mathbf{H}_M$ and the $n_E \times m$ matrix $\mathbf{H}_E$ contain the deterministic gains from each main and eavesdropper channel input to each main and eavesdropper channel output, respectively. The $m \times l$ matrix $\mathbf{H}_T$ represents Alice's transmit filter.

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 $l \times n_M$ matrix $\mathbf{H}_{RM}$ and the $l \times n_E$ 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 given by:

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

The general objective is to design Alice's transmit filter and Bob's receive filter that solve the optimization problem:

$$\min \mathsf{MSE_M} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}_M\|^2\right] \tag{6}$$

subject to the constraint $\mathsf{MSE_E} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}_E\|^2\right] \geq \gamma$, with $0 \leq \gamma \leq l$ and to a total power constraint $\mathsf{tr}\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right) \leq P_{avg}$, where $\mathcal{E}\left(\cdot\right)$ denotes the expectation value and $\left(\cdot\right)^\dagger$ the Hermitian transpose.

We assume that the matrices $\mathbf{H}_M^\dagger\mathbf{H}_M$ and $\mathbf{H}_E^\dagger\mathbf{H}_E$ are positive definite. We also assume a degraded scenario where $\mathbf{H}_M^\dagger\mathbf{H}_M \succ \mathbf{H}_E^\dagger\mathbf{H}_E$. It is reasonable to make such assumption, as in the wiretap channel, the legitimate parties must have some advantage over the eavesdropper. It is important to note that this approach does not guarantee perfect information-theoretic security, as defined in [1], [2] and [3]. [1] The design of the filters based on the MSE criteria is instead, a means to provide additional security in a communications system. The rationale is based on the fact that some applications require the MSE to be below a certain level to function properly, so that this approach would impair further the performance of the eavesdropper. This setup can also be combined with existing cryptographic algorithms, in order to strengthen the security of the communications system.

III. Optimal Receive Filters

This section considers the design of the optimal receive filters. Bob and Eve use the receive filters that minimize, respectively:

$$\mathsf{MSE_M} = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RM}\mathbf{Y}_M\|^2\right] \tag{7}$$

$$\mathsf{MSE_E} = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RE}\mathbf{Y}_E\|^2\right] \tag{8}$$

The optimal receive filters, for any fixed transmit filter $\mathbf{H}_T$, correspond to the Wiener filter given by (see e.g. [12])[2]:

$$\mathbf{H}_{RM}^* = \mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\left(\mathbf{I} + \mathbf{H}_M\mathbf{H}_T\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\right)^{-1} \tag{9}$$

$$\mathbf{H}_{RE}^* = \mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\left(\mathbf{I} + \mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\right)^{-1} \tag{10}$$

In turn, the MSEs corresponding to these receive filters are given by:

$$\mathsf{MSE_M} = \mathsf{tr}\left(\left(\mathbf{I} + \mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right) \tag{11}$$

$$\mathsf{MSE_E} = \mathsf{tr}\left(\left(\mathbf{I} + \mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right) \tag{12}$$

where $\mathsf{tr}\left(\cdot\right)$ denotes the trace operator.

IV. Optimal Transmit Filter

This section considers the design of the optimal transmit filter. This constitutes a complex optimization problem. In general, it follows from the Karush-Kuhn-Tucker conditions that the solution to the optimization problem falls into three different categories: (1) power constraint active and secrecy constraint inactive; (2) power and secrecy constraints active; (3) power constraint inactive and secrecy constraint active. Consequently, rather than solve completely the optimization problem, we will concentrate on the solutions in the regimes (1) and (3). We will also put forth conditions that depend solely on the system parameters (e.g. P_{avg}, γ, $\mathbf{H}_M$, $\mathbf{H}_E$) which identify the exact regime of operation. We note in passing that the general solution is only known, to the best of our knowledge, for the parallel degraded Gaussian wiretap channel [8].

A. Power constraint active / secrecy constraint inactive

We now consider the scenario where the power constraint is active, whilst the secrecy constraint is inactive. This situation arises typically 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.

Consequently, the solution follows by solving the optimization problem:

$$\min_{\mathbf{H}_T} \quad \mathsf{tr}\left(\left(\mathbf{I} + \mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right) \tag{13}$$

subject to the constraint

$$\mathsf{tr}\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right) = P_{avg} \tag{14}$$

To address this design problem, we shall use the fact that there exists an orthogonal matrix $\mathbf{C}$ that diagonalizes $\mathbf{H}_M^\dagger\mathbf{H}_M$, i.e.:

$$\mathbf{C}^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{C} = \mathbf{\Lambda}_M \tag{15}$$

where $\mathbf{\Lambda}_M = \mathsf{diag}(\lambda_{M1}, \lambda_{M2}, \ldots, \lambda_{Ml}) \succ 0$. We assume that the values of λ_{Mi}, $i = 1, \ldots, l$ are organized in a decreasing order, i.e., $\lambda_{M1} \geq \lambda_{M2} \cdots \geq \lambda_{Ml}$.

The solution for this optimization problem can be found in, e.g., [8] or [9].

Theorem 1: The optimal transmit filter for the degraded multiple-input multiple-output Gaussian wiretap channel with no secrecy constraints is, without loss of generality, given by:

$$\mathbf{H}_T^* = \mathbf{C}\ \mathsf{diag}(\sqrt{\sigma_i^*}) \tag{16}$$

where

$$\sigma_i^* = \sqrt{\frac{1}{\lambda \cdot \lambda_{Mi}}} - \frac{1}{\lambda_{Mi}}, \qquad \lambda_{Mi} \geq \lambda \tag{17}$$

$$\sigma_i^* = 0, \qquad \lambda_{Mi} < \lambda \tag{18}$$

with λ such that $\sum_{i=1}^{l} \sigma_i^* = P_{avg}$.

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

[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 at both receivers, in this paper.

B. Power constraint inactive / secrecy constraint active

We now consider the scenario where the secrecy constraint is active and the power constraint is inactive. This is a situation that typically arises in a regime of high available power: in fact, the use of all the available power, in such regime, would immediately violate the secrecy constraint.

Consequently, the solution follows by solving the optimization problem:

$$\min_{\mathbf{H}_T} \quad \mathsf{tr}\Big(\big(\mathbf{I}+\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\mathbf{H}_T^\dagger\big)^{-1}\Big) \tag{19}$$

subject to the constraint

$$\mathsf{tr}\Big(\big(\mathbf{I}+\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\big)^{-1}\Big)=\gamma \tag{20}$$

To address this design problem, we shall use the fact that there exists a non-singular matrix $\mathbf{C}$ that diagonalizes both $\mathbf{H}_M^\dagger\mathbf{H}_M$ and $\mathbf{H}_E^\dagger\mathbf{H}_E$ [13], i.e.:

$$\mathbf{C}^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{C}=\mathbf{\Lambda}_M \tag{21}$$

$$\mathbf{C}^\dagger\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{C}=\mathbf{\Lambda}_E \tag{22}$$

where $\mathbf{\Lambda}_M = \mathsf{diag}(\lambda_{M1},\lambda_{M2},\ldots,\lambda_{Ml}) \succ 0$, $\mathbf{\Lambda}_E = \mathsf{diag}(\lambda_{E1},\lambda_{E2},\ldots,\lambda_{El}) \succ 0$, $\mathbf{\Lambda}_M \succ \mathbf{\Lambda}_E$ because $\mathbf{H}_M^\dagger\mathbf{H}_M \succ \mathbf{H}_E^\dagger\mathbf{H}_E$. We assume that the set of ratios $\lambda_{Mi}/\lambda_{Ei}$, $i=1,\ldots,l$ are in a decreasing order, i.e., $\lambda_{M1}/\lambda_{E1}\geq\lambda_{M2}/\lambda_{E2}\geq\cdots\geq\lambda_{Ml}/\lambda_{El}$.

Theorem 2: The optimal transmit filter for the degraded multiple-input multiple-output Gaussian wiretap channel with no power constraint is, without loss of generality, given by:[3]

$$\mathbf{H}_T^*=\mathbf{C}\ \mathsf{diag}(\sqrt{\sigma_i^*}) \tag{23}$$

where

$$\sigma_i^*=0, \qquad \lambda_{Mi}/\lambda_{Ei}\leq\lambda \tag{24}$$

$$\sigma_i^*=+\infty, \qquad \lambda_{Ei}/\lambda_{Mi}\geq\lambda \tag{25}$$

$$\lambda_{Mi}\cdot\mathsf{lmmse}^2(\lambda_{Mi}\sigma_i^*)=\lambda\cdot\lambda_{Ei}\cdot\mathsf{lmmse}^2(\lambda_{Ei}\sigma_i^*), \quad \lambda_{Ei}/\lambda_{Mi}<\lambda<\lambda_{Mi}/\lambda_{Ei} \tag{26}$$

with λ such that $\sum_{i=1}^l\mathsf{lmmse}(\lambda_{Ei}\sigma_i^*)=\gamma$. The linear minimum mean-squared error (LMMSE) is $\mathsf{lmmse}(x)=1/(1+x)$.

Proof: Using the generalized eigenvalue decomposition in eq. (21) and (22), it is possible to show that the original optimization problem is equivalent to the optimization problem:

$$\min_{\tilde{\mathbf{H}}_T} \quad \mathsf{tr}\Big(\big(\mathbf{I}+\mathbf{\Lambda}_M\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger\big)^{-1}\Big) \tag{27}$$

subject to the constraint:

$$\mathsf{tr}\Big(\big(\mathbf{I}+\mathbf{\Lambda}_E\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger\big)^{-1}\Big)=\gamma \tag{28}$$

where $\tilde{\mathbf{H}}_T=\mathbf{C}^{-1}\mathbf{H}_T$. Consider now any matrix $\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger$ that respects the secrecy constraint. It is possible to show, via considerable algebraic manipulation, that using the matrix $\mathsf{Diag}(\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger)$ (which is a diagonal matrix whose diagonal elements correspond to the diagonal elements of $\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger$) rather than $\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger$ will decrease the value of the objective function without violating the constraint. Consequently, we can take, without loss of generality, the optimal matrix $\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger$ to be diagonal, i.e., $\tilde{\mathbf{H}}_T\tilde{\mathbf{H}}_T^\dagger=\mathbf{\Sigma}=\mathsf{diag}(\sigma_1,\sigma_2,\ldots,\sigma_l)$, and the optimal matrix $\mathbf{H}_T\mathbf{H}_T^\dagger=\mathbf{C}\mathbf{\Sigma}\mathbf{C}^\dagger=\mathbf{C}\mathsf{diag}(\sigma_1,\sigma_2,\ldots,\sigma_l)\mathbf{C}^\dagger$. We can also take without loss of generality the optimal matrix $\mathbf{H}_T=\mathbf{C}\mathbf{\Sigma}^{1/2}=\mathbf{C}\mathsf{diag}(\sqrt{\sigma_1},\sqrt{\sigma_2},\ldots,\sqrt{\sigma_l})$. Consequently, the main channel and the eavesdropper channel MSEs reduce to $\mathsf{MSE_M}=\sum_{i=1}^l(1+\sigma_i\lambda_{Mi})^{-1}$ and $\mathsf{MSE_E}=\sum_{i=1}^l(1+\sigma_i\lambda_{Ei})^{-1}$, respectively.

We shall now determine the optimal elements of the matrix $\mathbf{\Sigma}=\mathsf{diag}(\sigma_1,\sigma_2,\ldots,\sigma_l)$. Interestingly, the one-to-one mapping $\sigma_i'=(1+\lambda_{Ei}\sigma_i)^{-1}$ transforms the (apparently non-convex) optimization problem:

$$\min_{\sigma_i,i=1\ldots,l} \ \sum_{i=1}^l\frac{1}{1+\lambda_{Mi}\sigma_i} \tag{29}$$

subject to

$$\sum_{i=1}^l\frac{1}{1+\lambda_{Ei}\sigma_i}=\gamma \tag{30}$$

and $\sigma_i\geq 0,\ i=1,\ldots,l$ into a standard convex optimization problem:

$$\min_{\sigma_i',i=1\ldots,l} \ \sum_{i=1}^l\frac{\sigma_i'}{\sigma_i'\Big(1-\frac{\lambda_{Mi}}{\lambda_{Ei}}\Big)+\frac{\lambda_{Mi}}{\lambda_{Ei}}} \tag{31}$$

subject to

$$\sum_{i=1}^l\sigma_i'=\gamma \tag{32}$$

and $0\leq\sigma_i'\leq 1,\ i=1,\ldots,l$. [4] The optimal solution follows immediately from the Karush-Kuhn-Tucker optimality conditions [14].

Consequently, the solution is given by

$$\sigma_i'^*=1, \qquad \lambda_{Mi}/\lambda_{Ei}\leq\lambda \tag{33}$$

$$\sigma_i'^*=0, \qquad \lambda_{Ei}/\lambda_{Mi}\geq\lambda \tag{34}$$

$$\frac{\frac{\lambda_{Mi}}{\lambda_{Ei}}}{\left(\sigma_i'^*\Big(1-\frac{\lambda_{Mi}}{\lambda_{Ei}}\Big)+\frac{\lambda_{Mi}}{\lambda_{Ei}}\right)^2}=\lambda, \frac{\lambda_{Ei}}{\lambda_{Mi}}<\lambda<\frac{\lambda_{Mi}}{\lambda_{Ei}} \tag{35}$$

with λ such that $\sum_{i=1}^l\sigma_i'^*=\gamma$. Theorem 2 follows immediately by reversing the one-to-one mapping. ■

V. Algorithm

In this section, we put forth an algorithm capable of efficiently determining the elements of the optimal transmit filter. In particular, we concentrate solely on the regime where the power constraint is inactive whilst the secrecy constraint is active, because a computational procedure applicable to the other regime appears in [9]. The generalized eigenvalue decomposition can be computed using standard procedures [13]. In turn, the elements $\sigma_i{}^*, i=1,\ldots,l$ of the optimal transmit filter can be computed using the algorithm shown in Table 1. This algorithm, which converges in a maximum of l iterations, is based on the solution embodied in Theorem 2. The receive filters in (9) and (10) follow trivially from knowledge of the channel matrices and the transmit filter.

[3] Note that $\sigma_i^*=+\infty$ means that $\sigma_i^*\to+\infty$ is asymptotically optimal. Obviously, this part of the solution will not belong to region of validity of this regime, as discussed in section VI.

[4] It is important to note that this optimization problem is convex due to degradedness, i.e., $\lambda_{Mi}\geq\lambda_{Ei}, i=1,\ldots,l$.

VI. Operational regimes regions

We have presented the solution to the optimization problem in two operational regimes: (i) when the power constraint is active while the secrecy constraint is inactive; and (ii) when the power constraint is inactive while the secrecy constraint is active. We now establish conditions, as function of the system parameters, that identify the exact regions for the regimes of operation. Consider the first operational regime (i). It is immediate to show that this regime is valid if:

$$\gamma < \sum_{i=1}^{l} \frac{1}{1+\lambda_{Ei}\sigma_i^*} \tag{36}$$

where σ_i^* follows the solution embodied in Theorem 1, or:

$$\sigma_i^* = \frac{P_{avg} + \sum_{j=1}^{n_{act}} \frac{1}{\lambda_{Mj}}}{\sum_{j=1}^{n_{act}} \frac{1}{\sqrt{\lambda_{Mj}}}} \frac{1}{\sqrt{\lambda_{Mi}}} - \frac{1}{\lambda_{Mi}} \tag{37}$$

with n_{act} being the number of active channels. The value n_{act} is obtained from the algorithm present in [9].

Consider now the regime (ii). It is also immediate to show that this regime is valid if:

$$P_{avg} \geq \sum_{i=1}^{l} \sigma_i^* (\mathbf{C}^\dagger \mathbf{C})_{ii} \tag{38}$$

where σ_i^* follows the solution embodied in Theorem 2, or:

$$\sigma_i^* = \frac{\sqrt{\lambda_{Mi}}\left(\sum_{j=1}^{n_{act}} \frac{\lambda_{Mj}}{\lambda_{Ej}-\lambda_{Mj}} + \gamma - n_{inact}\right) - \sum_{j=1}^{n_{act}} \frac{\sqrt{\lambda_{Mj}\lambda_{Ej}}}{\lambda_{Ej}-\lambda_{Mj}} \lambda_{Ei}}{\sqrt{\lambda_{Ei}}\lambda_{Mi} \sum_{j=1}^{n_{act}} \frac{\sqrt{\lambda_{Mj}\lambda_{Ej}}}{\lambda_{Ej}-\lambda_{Mj}} - \sqrt{\lambda_{Mi}}\lambda_{Ei}\left(\sum_{j=1}^{n_{act}} \frac{\lambda_{Mj}}{\lambda_{Ej}-\lambda_{Mj}} + \gamma - n_{inact}\right)} \tag{39}$$

with $\mathbf{C}$ being the matrix that diagonalizes both channels, n_{act} the number of active channels and n_{inact} the number of inactive channels. We can obtain n_{act} and n_{inact} from the algorithm depicted in Table 1. Note that (36) and (37) can be used to determine a maximum value for the secrecy constraint, $\gamma_{max_{reg1}}$, below which we operate under regime (i), or equivalently, a maximum value for the power constraint, $P_{avg_{max}}$, below which we operate under the same regime. Likewise, (38) and (39) can be used to determine a minimum value for the secrecy constraint, $\gamma_{min_{reg3}}$, above which we operate under regime (ii), or equivalently, a minimum value for the power constraint, $P_{avg_{min}}$, above which we operate in the same regime. This is further explored in the next section.

VII. Results and conclusions

We shall now present a set of numerical results to provide further insight into the problem of filter design with secrecy constraints. We consider a 2×2 MIMO Gaussian wiretap channel where the main and the eavesdropper channel matrices are, respectively, given by:

$$\mathbf{H}_M = \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix} \quad , \quad \mathbf{H}_E = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix} \tag{40}$$

Note that this represents a degraded scenario because $\mathbf{H}_M^\dagger \mathbf{H}_M \succ \mathbf{H}_E^\dagger \mathbf{H}_E$.

Figure 2 illustrates the optimal values of the elements of the transmit filter, $\sigma_i^*, i = 1, 2$ *vs.* the secrecy constraint γ, with $P_{avg} = 1$. This figure clearly depicts the three regimes of operation. It is interesting to note that, in the first operational regime, the optimal σ_i^* are constant because the solution is independent from the value of the secrecy constraint γ. In the second regime, the optimal σ_i^* will depend on γ, and the values are such that both the secrecy and the power constraint are met with equality. In the third regime, where the power constraint is not active, the optimal σ_i^* also depend on γ. In fact, as the secrecy constraint increases, the values σ_i^* decrease, and hence the injected power into de channel decreases too, otherwise one would violate the secrecy constraint. Note also that we identify the secrecy constraint threshold values $\gamma_{max_{reg1}}$ and $\gamma_{min_{reg3}}$, below and above which, one operates in the first and third regimes, respectively.

Figure 3 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, with $P_{avg} = 1$. The three operational regimes are, once more, very evident. Below $\gamma_{max_{reg1}}$,the optimal solution corresponds to the minimum mean squared error in the main channel that is possible to obtain given the available power only. We can verify that the available power is not sufficient to meet or violate the secrecy constraint, in this region. In-between $\gamma_{max_{reg1}}$ and $\gamma_{min_{reg3}}$, the optimal solution (which has not been derived in this paper

Table 1

Input :

• Number of sub-channels l; set of values $\lambda_{Mi}, i = 1, \ldots, l$; set of values $\lambda_{Ei}, i = 1, \ldots, l$; secrecy constraint γ.

Output:

• Set of optimal values ${\sigma_i}^*$, $i = 1, \ldots, l$; number of finite active sub-channels n_{act} $(0 < {\sigma_i}^* < +\infty)$; number of inactive sub-channels n_{inact} $({\sigma_i}^* = 0)$.

1 • **Set** $n = l$; **set** $n_{inact} = 0$.

2 • **Set** $\lambda = \lambda_{Mn}/\lambda_{En}$.

3 **if** $\sqrt{\frac{1}{\lambda}} \sum_{i=1}^{n} \frac{\sqrt{\lambda_{Mi}\lambda_{Ei}}}{\lambda_{Ei}-\lambda_{Mi}} - \sum_{i=1}^{n} \frac{\lambda_{Mi}}{\lambda_{Ei}-\lambda_{Mi}} + n_{inact} \leq \gamma$ **then**

• **Set** ${\sigma_n}^* = 0$; **set** $n = n - 1$; **set** $n_{inact} = n_{inact} + 1$; **go to** step 2.

else

• **Set** $\lambda = \left(\sum_{i=1}^{n} \frac{\sqrt{\lambda_{Mi}\lambda_{Ei}}}{\lambda_{Ei}-\lambda_{Mi}} \Big/ \sum_{i=1}^{n} \frac{\lambda_{Mi}}{\lambda_{Ei}-\lambda_{Mi}} + \gamma - n_{inact}\right)^2$;

if $\lambda \leq \left(\lambda_{Mn}/\lambda_{En}\right)^{-1}$ **then**

• **Set** ${\sigma_n}^* = +\infty$; **set** $n = n - 1$; **go to** step 2.

else

• **Set** $n_{act} = n$;

4 • **Set** ${\sigma_i}^* = \frac{\sqrt{\frac{\lambda_{Mi}}{\lambda \cdot \lambda_{Ei}}} - 1}{\lambda_{Mi} - \sqrt{\frac{\lambda_{Mi}}{\lambda \cdot \lambda_{Ei}}} \lambda_{Ei}}$, $i = 1, 2, ..., n_{act}$;

The number of finite active sub-channels (where $0 < {\sigma_n}^* < +\infty$) is n_{act}, the number of inactive sub-channels (where ${\sigma_i}^* = 0$) is n_{inact}.

and was obtained through numerical methods) minimizes the MSE in the main channel while meeting the power and the secrecy constraint with equality. Above $\gamma_{min_{reg3}}$, the optimal solution corresponds to the minimum mean squared error in the main channel, that is possible to obtain, given the secrecy constraint only. It is also important to verify that, since we are considering the degraded case, the mean squared error in the main channel will always be lower than the one in the eavesdropper channel.

It is also of interest to analyze the mutual information between the input vector and the eavesdropper output vector, 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, assuming that the input is Gaussian and considering four different scenarios: (1) the optimal transmit filter ; (2) the transmit filter $\mathbf{H}_T$ that minimizes the mean squared error in the main channel, but does not take in account any secrecy constraint; (3) the transmit filter $\mathbf{H}_T$ being a multiple of the identity matrix, and the $\mathrm{tr}\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right)$ equal to the power used by the optimal transmit filter; and (4) the transmit filter $\mathbf{H}_T$ being a multiple of the identity matrix, and $\mathrm{tr}\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right) = P_{avg}$. 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 four cases. In particular, by imposing a minimum 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.

To conclude, we 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, the design have been shown to limit the amount of mutual information leaked to the eavesdropper, in comparison to other designs. To the best of our knowledge, the general solution to the optimization problem is not known.

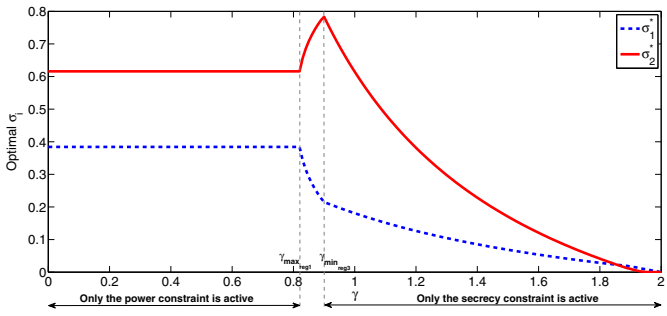

Figure 2. Optimal values of the elements of the transmit filter, $\sigma_i^*, i = 1, 2$, *vs*. secrecy constraint γ, with $P_{avg} = 1$.

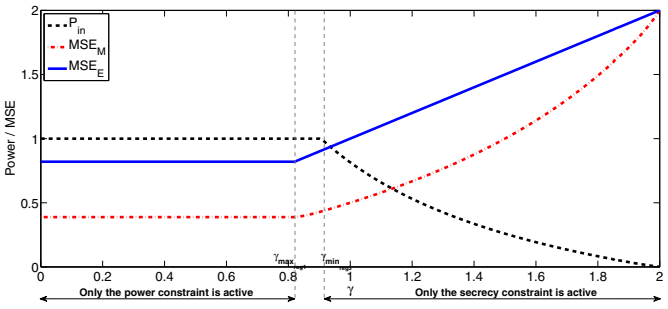

Figure 3. Main and Eavesdropper channel MSEs *vs*. secrecy constraint and input power *vs*. secrecy constraint, with $P_{avg} = 1$.

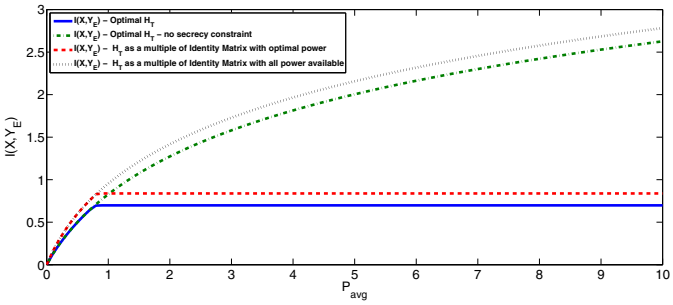

Figure 4. Eavesdropper mutual information *vs*. available power for four different transmit filters, with $\gamma = 1$.

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.

[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] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

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

[6] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," in *IEEE International Symposium on Information Theory*, Jun. 2007.

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

[8] M. R. D. Rodrigues and P. D. M. Almeida, "Filter design with secrecy constraints: The degraded parallel gaussian wiretap channel," in *IEEE Global Communications Conference*, Dec. 2008.

[9] 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.

[10] F. Pérez-Cruz, M. R. D. Rodrigues, and S. Verdu, "Optimal precoding for digital subscriber lines," in *IEEE International Conference on Communications*, May 2008.

[11] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect csi," arXiv:1009.2274v1 [cs.IT], 2010. [Online]. Available: http://arxiv.org/abs/1009.2274v1

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

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

[14] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.