FILTER DESIGN WITH SECRECY CONSTRAINTS: THE MULTIPLE-INPUT MULTIPLE-OUTPUT GAUSSIAN WIRETAP CHANNEL WITH ZERO FORCING RECEIVE FILTERS

Hugo Reboredo[†], *Vinay Prabhu*[‡], *Miguel R. D. Rodrigues*[§], *João Xavier*[*]

[†‡§] Instituto de Telecomunicações, Dept. of Computer Science, University of Porto, Portugal
[*] Instituto de Sistemas e Robótica, Instituto Superior Técnico, Portugal
[†] hugoreboredo@dcc.fc.up.pt, [‡] vinay@dcc.fc.up.pt, [§] mrodrigues@dcc.fc.up.pt, [*] 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. This problem involves the design of transmit and receive filters which minimize the mean-square error (MSE) between the legitimate parties, whilst assuring that the eavesdropper MSE remains above a certain level. We characterize the form of the optimal transmit filter when both the legitimate receiver and the eavesdropper employ Zero-Forcing (ZF) filters. By capitalizing on the dual problem, we also show that the original matrix optimization problem can be reduced to a simple scalar optimization problem, whose solution can be readily computed by employing a simple bisection method. Numerical results illustrate the main conclusions.

Index Terms— Multiple-Input Multiple-Output, Wiretap channel, Filter Design, ZF filters, Secrecy.

1. INTRODUCTION

Security constitutes one of the most important issues in wireless communication systems. In fact, due to the inherent broadcast nature of the wireless medium, the wireless links are much more susceptible to eavesdropping attacks, in contrast to their wire-line counterparts. The conventional security techniques rely essentially on cryptographic solutions, based on the intractability of certain functions, 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, information-theoretic security – widely accepted as the strictest notion of security – has, recently, attracted an increasing amount of interest. This calls for the use of physical-layer techniques exploiting the inherent randomness of the communications medium to guarantee both reliable communication between two legitimate parties as well as secure communication 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. Wyner characterized the rate-equivocation region of the wiretap channel and its secrecy capacity (i.e., the maximum transmission rate between the legitimate parties with the eavesdropper unable to obtain any information). Ever since, the computation of the secrecy capacity of a range of communications channels has been an important research topic (e.g., see [4]).

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, where the objective is to dimension transmit and receive filters that minimize the mean-square error (MSE) between the legitimate parties whilst guaranteeing a certain eavesdropper MSE level, subject to the use of Zero-Forcing (ZF) receive filters. 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. [5], [6]). Further work on the topic of filter design in the wiretap channel scenario can be found in [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.

Bob and Eve observe the output of the real-valued MIMO channels given, respectively, by[1]:

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

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

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

[1] We focus on real-valued MIMO channel models, but the extension to complex-valued is straightforward.

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 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 $n_E \geq m$. This is necessary to guarantee the existence of the solutions.

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 particular we consider a scenario where:

$$\mathbf{H}_{RM}\mathbf{H}_M\mathbf{H}_T = \mathbf{I} \tag{5}$$

$$\mathbf{H}_{RE}\mathbf{H}_E\mathbf{H}_T = \mathbf{I} \tag{6}$$

where $\mathbf{I}$ is the $m \times m$ identity matrix. The justification for including the ZF constraints in equations (5) and (6) is to eliminate crosstalk between the various streams. Note also that the performance of linear ZF receivers is equivalent to that of optimal Wiener receivers in the regime of high SNR. Yet, one may still argue that a eavesdropper will always adopt the optimal linear receive filter – the Wiener filter – rather than the sub-optimal ZF receive filter. Interestingly, our numerical analysis will show that a situation where the legitimate receiver and the eavesdropper employ ZF filters is always more advantageous, in terms of information leakage, for the eavesdropper than the situation where the legitimate receiver and the eavesdropper employ the optimal Wiener filter.

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:

$$\mathsf{MSE} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}\|^2\right] \tag{7}$$

The objective is to design the transmit filter that solves the optimization problem:

$$\min \mathsf{MSE}_{\mathsf{M}} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}_M\|^2\right] \tag{8}$$

subject to the security constraint:

$$\mathsf{MSE}_{\mathsf{E}} = \mathcal{E}\left[\|\mathbf{X} - \hat{\mathbf{X}}_E\|^2\right] \geq \gamma \tag{9}$$

and to the total power constraint:

$$\mathsf{tr}\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right) \leq P_{avg} \tag{10}$$

where $\mathcal{E}\left(\cdot\right)$ denotes the expectation operator and $\left(\cdot\right)^\dagger$ denotes the transpose.

It is important to note that this approach does not guarantee perfect information-theoretic security, in the sense of [1], [2] and [3]. [2] 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 certain maximum MSE level to function properly, so that this approach would impair further the performance of the eavesdropper by imposing a threshold on its MSE level.

3. OPTIMAL RECEIVE FILTERS

The design of the receive filters is trivial. In particular, the form of the receive filters follows immediately from the equations (5) and (6):

$$\mathbf{H}_{R_M}{}^* = \left(\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\right)^{-1}\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger \tag{11}$$

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

The MSEs in the main and eavesdropper channels are then given by:

$$\mathsf{MSE}_M = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RM}\mathbf{Y}_M\|^2\right] = \mathsf{tr}\left\{\left(\mathbf{H}_T^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\right)^{-1}\right\} \tag{13}$$

$$\mathsf{MSE}_E = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RE}\mathbf{Y}_E\|^2\right] = \mathsf{tr}\left\{\left(\mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\right)^{-1}\right\} \tag{14}$$

4. OPTIMAL TRANSMIT FILTER

In view of (13) and (14), the form of the optimal transmit filter corresponds to the solution of the optimization problem:

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

subject to the constraints:

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

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

and $\mathbf{H}_T\mathbf{H}_T^\dagger \succ 0$. Note that by considering the change of variables: $\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1} = \mathbf{Z}$, $\left(\mathbf{H}_M^\dagger\mathbf{H}_M\right)^{-1} = \mathbf{A}$ and $\left(\mathbf{H}_E^\dagger\mathbf{H}_E\right)^{-1} = \mathbf{B}$, it is possible to rewrite the optimization problem as follows:

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

subject to the constraints:

$$\mathsf{tr}\left\{\mathbf{BZ}\right\} \geq \gamma \tag{19}$$

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

and $Z \succ 0$. One recognizes immediately that this is a standard convex optimization problem. The following theorem, which stems directly from the Karush-Kuh-Tucker optimality conditions [8], defines the form of the optimal transmit filter.

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

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

$$\mathbf{H}_T{}^* = \sqrt{\frac{P_{avg}}{\mathsf{tr}\left\{\mathbf{A}^{1/2}\right\}}}\mathbf{A}^{1/4}\,, \quad \frac{\mathsf{tr}\left\{\mathbf{A}^{1/2}\right\}}{P_{avg}}\mathsf{tr}\left\{\mathbf{B}\mathbf{A}^{-1/2}\right\} > \gamma \qquad (21)$$

$$\mathbf{H}_T{}^* = \sqrt{\frac{P_{avg}}{\mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{1/2}\right\}}}\left(\mathbf{A}-\nu\mathbf{B}\right)^{1/4}\,, \quad \frac{\mathsf{tr}\left\{\mathbf{A}^{1/2}\right\}}{P_{avg}}\mathsf{tr}\left\{\mathbf{B}\mathbf{A}^{-1/2}\right\} \leq \gamma \qquad (22)$$

where the value of the Lagrange multiplier ν is such that:

$$\mathsf{tr}\left\{\mathbf{B}\left(\mathbf{A}-\nu\mathbf{B}\right)^{-1/2}\right\}\cdot\mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{1/2}\right\} = \gamma\cdot P_{avg} \quad (23)$$

Remark: The solution embodied in Theorem 1 exhibits two distinct regimes:

i) The regime where the security constraint is inactive $\left(\frac{\mathsf{tr}\left\{\mathbf{A}^{1/2}\right\}}{P_{avg}}\mathsf{tr}\left\{\mathbf{B}\mathbf{A}^{-1/2}\right\} > \gamma\right)$, which typically occurs for low available power values. In this scenario, the matrix with left singular vectors of the transmit filter diagonalizes $\left(\mathbf{H}_M^{\dagger}\mathbf{H}_M\right)^{-1}$. This solution corresponds to the solution in [5].

ii) The regime where the security constraint is active $\left(\frac{\mathsf{tr}\left\{\mathbf{A}^{1/2}\right\}}{P_{avg}}\mathsf{tr}\left\{\mathbf{B}\mathbf{A}^{-1/2}\right\} \leq \gamma\right)$, which typically occurs for high available power values. In this scenario, the matrix with the left singular vectors of the transmit filter diagonalizes $\left[\left(\mathbf{H}_M^{\dagger}\mathbf{H}_M\right)^{-1} - \nu\left(\mathbf{H}_E^{\dagger}\mathbf{H}_E\right)^{-1}\right]$. This result generalizes the result in [5].

5. COMPUTATIONAL PROCEDURE

The computation of the optimal transmit filter embodied in Theorem 1 requires finding the solution of the non-linear equation in (23), in order to determine the value of the Lagrange multiplier ν. We shall now put forth a simpler procedure to design the optimal transmit filter based on the dual of the optimization problem.

Consider the Lagrangian of the optimization problem in (18) – (20):

$$\mathfrak{L}\left(\mathbf{Z},\nu,\mu\right) = \mathsf{tr}\left(\mathbf{A}\mathbf{Z}\right) + \nu\left(\gamma - \mathsf{tr}\left(\mathbf{B}\mathbf{Z}\right)\right) + \mu\left(\mathsf{tr}\left(\mathbf{Z}^{-1}\right) - P_{avg}\right) \qquad (24)$$

Consider also the dual function of the optimization problem in (18) – (20):

$$\mathfrak{L}\left(\nu,\mu\right) = \inf_{\mathbf{Z}>0}\mathfrak{L}\left(\mathbf{Z},\nu,\mu\right) \qquad (25)$$

where $\nu \geq 0$ and $\mu \geq 0$. It is straightforward to show that the dual function reduces to:

$$\mathfrak{L}\left(\nu,\mu\right) = 2\sqrt{\mu}\ \mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{\frac{1}{2}}\right\} - \mu P_{avg} + \nu\gamma \quad , \ \left(\mathbf{A}-\nu\mathbf{B}\right) \geq 0$$
$$\mathfrak{L}\left(\nu,\mu\right) = -\infty \quad , \ \text{otherwise}$$

The dual problem of the optimization problem in (18) - (20) is now given by:

$$\max \quad 2\sqrt{\mu}\ \mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{\frac{1}{2}}\right\} - \mu P_{avg} + \nu\gamma \qquad (26)$$

subject to:

$$\nu \geq 0 \qquad (27)$$
$$\mu \geq 0 \qquad (28)$$
$$\left(\mathbf{A}-\nu\mathbf{B}\right) \geq 0 \qquad (29)$$

We can employ a two step procedure to express the solution: i) optimization over μ for a fixed ν; ii) optimization over ν for the optimal μ. It is straightforward to show that the optimal value of μ is given by:

$$\mu = \frac{1}{{P_{avg}}^2}\left(\mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{\frac{1}{2}}\right\}\right)^2 \qquad (30)$$

Consequently, the dual optimization problem reduces to:

$$\max \frac{1}{P_{avg}}\left(\mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{\frac{1}{2}}\right\}\right)^2 + \nu\gamma \qquad (31)$$

subject to:

$$\nu \geq 0 \qquad (32)$$
$$\left(\mathbf{A}-\nu\mathbf{B}\right) \geq 0 \qquad (33)$$

or, equivalently,

$$\max \frac{1}{P_{avg}}\left(\mathsf{tr}\left\{\left(\mathbf{A}-\nu\mathbf{B}\right)^{\frac{1}{2}}\right\}\right)^2 + \nu\gamma \qquad (34)$$

subject to:

$$0 \leq \nu \leq \lambda_{min}\left(\mathbf{B}^{-\frac{1}{2}}\mathbf{A}\mathbf{B}^{-\frac{1}{2}}\right) \qquad (35)$$

This is due to the fact that the positive semidefinite constraint $\left(\mathbf{A}-\nu\mathbf{B}\right) \geq 0$ is equivalent to the constraint $\nu \leq \lambda_{min}\left(\mathbf{B}^{-\frac{1}{2}}\mathbf{A}\mathbf{B}^{-\frac{1}{2}}\right)$, where $\lambda_{min}\left(\mathbf{M}\right)$ denotes the minimum eigenvalue of the positive definite matrix $\mathbf{M}$.

The solution to the optimization problem (34) – (35) can be computed in a straightforward manner using, for example, the bisection method [9].

The optimal values of μ in (30) and ν then define the optimal transmit filter as follows:

$$\mathbf{Z}^* = \sqrt{\mu}\left(\mathbf{A}-\nu\mathbf{B}\right)^{-\frac{1}{2}} \qquad (36)$$

In turn, the optimal transmit filter defines the ZF receive filters through (11) and (12).

6. NUMERICAL RESULTS

We shall now present a set of numerical results in order 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 given by:

$$\mathbf{H}_M = \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix} \ , \ \mathbf{H}_E = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix} \tag{37}$$

Figure 1 depicts the values of the MSEs in the main and in the eavesdropper channels and the input power to the channels *vs*. the secrecy constraint with $P_{avg} = 1$. Note that the solution clearly depicts the two operational regimes unveiled in Theorem 1: i) the regime where the power constraint is active but the security constraint is inactive (for smaller values of γ); and ii) the regime where the power and security constraints are active (for larger values of γ). We also include the results for the scenario where the legitimate receiver and eavesdropper use the optimal linear Wiener filters in Figure 1 (see also [10]). Interestingly, in the relevant regime of large γ, the use of ZF filters rather than Wiener filters leads to a better MSE in the main channel without the violation of the security constraint. This is due to the fact that the transmitter can use all of the available power in such a scenario, in order to drive the MSE to a lower value.

Yet, the use of all the available power also leads to a higher eavesdropper mutual information leakage, as shown in Figure 2. This situation, which is absent in the Wiener filters scenario, also provides a rationale for the eavesdropper to use a ZF filter rather than the optimal linear one to improve the information leakage.

7. CONCLUSIONS

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 communications systems. By concentrating on a scenario where legitimate receiver and eavesdropper receiver employ linear ZF filters, as opposed to the optimal linear Wiener filters [10], it is possible to characterize the form of the optimal transmit filter as well as derive considerable operational insight.

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.

[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] Y. Liang, H. V. Poor, and S. Shamai, "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[5] D. P. Palomar, *A unified framework for communications through MIMO channels*, Ph.d. dissertation, Technical Univ. Catalonia (UPC), 2003.

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

[7] 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.

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

[9] R.L. Burden and J.D. Faires, *Numerical Analysis (8th edition)*, Brooks-Cole Publishers, Belmont, CA, 2004.

[10] H. Reboredo, M. Ara, M. R. D. Rodrigues, and J. Xavier, "Filter design with secrecy constraints: The degraded multiple-input multiple-output gaussian wiretap channel," Submitted to VTC2011-Spring, 2010, http://paginas.fe.up.pt/~ee00104/VTC2011paper.pdf.

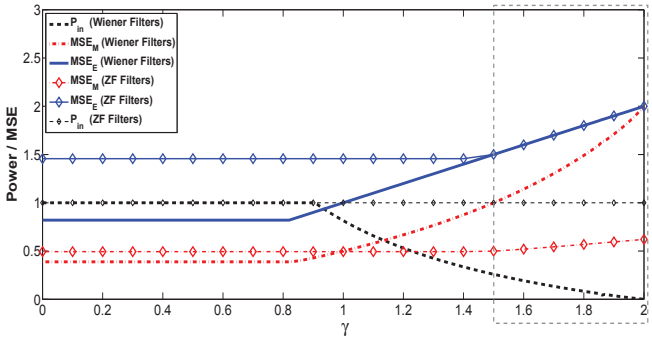

Fig. 1. Main and Eavesdropper channel MSEs *vs*. secrecy constraint and input power *vs*. secrecy constraint.

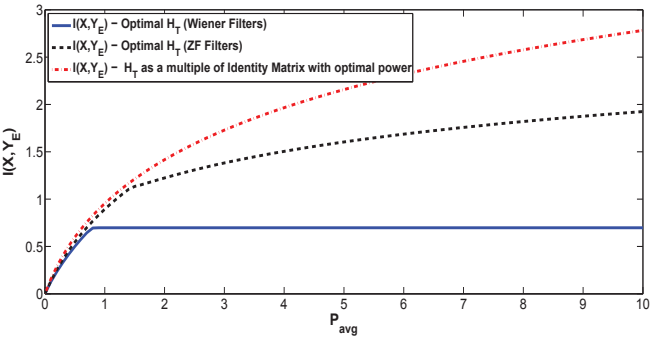

Fig. 2. Eavesdropper mutual information *vs*. available power, with $\gamma = 1$.The input is assumed to be real Gaussian with mean zero and identity covariance matrix.