Design of Filters For Reliable and Secure Communications Conditional Mean Estimation at the Eavesdropper

Hugo Reboredo, Miguel R. D. Rodrigues
Instituto de Telecomunicações
Dept. of Computer Science, University of Porto, Portugal
emails: {hugoreboredo,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 analyze the penalty in terms of MSE in the eavesdropper channel due to the assumption that optimal linear receive filters are used, while the eavesdropper employs nonlinear conditional mean estimation instead. This penalty is also shown to be negligible in regions of operational interest. We present a set of numerical results to illustrate the main conclusions.**

I. Introduction

Due to the inherent broadcast nature of the wireless medium, security and privacy protection remains an issue of utmost importance in wireless communications. Aside from traditional cryptographic algorithms, insensitive to the physical nature of the wireless medium, information-theoretic security – widely accepted as the strictest notion of security – have regained increasing attention in recent years. This 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] and [7]).

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, the aim is to characterize the impact incurred on performance when the eavesdropper uses the optimal nonlinear receive filter whilst the transmitter assumes that the eavesdropper uses the optimal linear filter. 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. [8], [9]). Further work on the topic of filter design in the wiretap channel scenario can also be found in [10] and [11].

This paper is structured as follows: Section II defines the problem. Sections III and IV briefly present the optimal solution for the linear receive and transmit filters. Section V shows various numerical results to illustrate the primary outcomes of this paper. Section VI summarizes the primary contributions of the manuscript 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. 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.

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

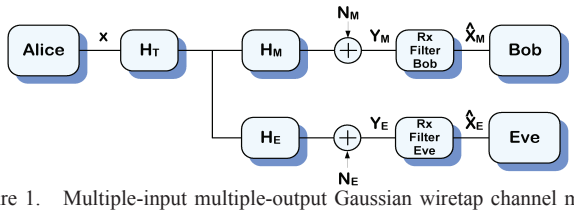

Figure 1. Multiple-input multiple-output Gaussian wiretap channel model.

It is assumed that 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 linear 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.

The design of the filters based on the MSE criteria constitutes 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. Even though this approach does not guarantee perfect information-theoretic security, as defined in [1], [2] and [3], the work presented in [11] analyzes the mutual information in the eavesdropper channel, showing that 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.

One can in fact argue that the eavesdropper will not use the optimal linear receive filter, but rather the optimal nonlinear receive filter to process the information, which corresponds to conditional mean estimation:

$$\hat{\mathbf{X}}_E = \mathcal{E}\left\{\mathbf{X} \mid \mathbf{Y}_E = \mathbf{y}_E\right\} = \frac{\int \mathbf{x} \;\; P_{\mathbf{X}}\left(\mathbf{X} = \mathbf{x}\right) \;\; P_{\mathbf{Y}_E|\mathbf{X}}\left(\mathbf{y}_E \mid \mathbf{X} = \mathbf{x}\right) d\mathbf{x}}{\int P_{\mathbf{X}}\left(\mathbf{X} = \mathbf{x}\right) \;\; P_{\mathbf{Y}_E|\mathbf{X}}\left(\mathbf{y}_E \mid \mathbf{X} = \mathbf{x}\right) d\mathbf{x}} \tag{7}$$

As such, the goal of this work is to assess the penalty incurred by the use of conditional mean estimation by the eavesdropper, when the transmitter assumes that both the receivers use the optimal linear filter. Surprisingly, it will be shown that the penalty is negligible in regions of operational interest.

III. Optimal Linear Receive Filters

This section considers the design of the optimal receive filters. In order to characterize the optimal linear transmit filter, we assume that Bob and Eve use the linear receive filters that minimize, respectively:

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

and

$$\mathsf{MSE_E} = \mathcal{E}\left[\|\mathbf{X} - \mathbf{H}_{RE}\mathbf{Y}_E\|^2\right] \tag{9}$$

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

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

$$\mathbf{H}_{RE}^* = \mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\left(\mathbf{I} + \mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\mathbf{H}_E^\dagger\right)^{-1} \tag{11}$$

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

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

$$\mathsf{MSE_E} = \mathsf{tr}\left(\left(\mathbf{I} + \mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right) \tag{13}$$

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

As mentioned in the previous section, the fact that the eavesdropper can use more sophisticated nonlinear techniques in order to estimate Alice's information will be studied in this paper.

IV. Optimal Linear Transmit Filter

We briefly lay out the optimal solution previously presented in [11]. In general, it follows from the Karush-Kuhn-Tucker conditions that, with respect to the transmit filter, 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 also present 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 [10].

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:

$$\min_{\mathbf{H}_T} \;\; \mathsf{tr}\left(\left(\mathbf{I} + \mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\mathbf{H}_T^\dagger\right)^{-1}\right) \tag{14}$$

subject to the constraint

$$\mathsf{tr}\big(\mathbf{H}_T\mathbf{H}_T^\dagger\big) = P_{avg} \tag{15}$$

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.:

$$\mathbf{C}^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{C} = \mathbf{\Lambda}_M \tag{16}$$

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., $\lambda_{M1} \geq \lambda_{M2} \cdots \geq \lambda_{Ml}$.

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:

$$\mathbf{H}_T^* = \mathbf{C}\ \mathsf{diag}(\sqrt{\sigma_i^*}) \tag{17}$$

where

$$\sigma_i^* = \sqrt{\frac{1}{\lambda \cdot \lambda_{Mi}}} - \frac{1}{\lambda_{Mi}}, \qquad \lambda_{Mi} \geq \lambda \tag{18}$$

$$\sigma_i^* = 0, \qquad \lambda_{Mi} < \lambda \tag{19}$$

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

Proof: See [10] or [8]. ■

It is immediate to show that this regime is valid if:

$$\gamma < \sum_{i=1}^{l} \frac{1}{1 + \lambda_{Ei}\sigma_i^*} \tag{20}$$

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

$$\sigma_i^* = \frac{P_{avg} + \sum_{j=1}^{n_{act}} \frac{1}{\lambda_{Mj}}}{\sum_{j=1}^{n_{act}} \frac{1}{\sqrt{\lambda_{Mj}}}} \frac{1}{\sqrt{\lambda_{Mi}}} - \frac{1}{\lambda_{Mi}} \tag{21}$$

with n_{act} being the number of active channels. The value n_{act} is obtained from the algorithm present in [8].

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:

$$\min_{\mathbf{H}_T} \quad \mathsf{tr}\Big(\big(\mathbf{I} + \mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{H}_T\mathbf{H}_T^\dagger\big)^{-1}\Big) \tag{22}$$

subject to the constraint

$$\mathsf{tr}\Big(\big(\mathbf{I} + \mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{H}_T\mathbf{H}_T^\dagger\big)^{-1}\Big) = \gamma \tag{23}$$

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.:

$$\mathbf{C}^\dagger\mathbf{H}_M^\dagger\mathbf{H}_M\mathbf{C} = \mathbf{\Lambda}_M \tag{24}$$

$$\mathbf{C}^\dagger\mathbf{H}_E^\dagger\mathbf{H}_E\mathbf{C} = \mathbf{\Lambda}_E \tag{25}$$

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:

$$\mathbf{H}_T^* = \mathbf{C}\ \mathsf{diag}(\sqrt{\sigma_i^*}) \tag{26}$$

where

$$\sigma_i^* = 0, \qquad \lambda_{Mi}/\lambda_{Ei} \leq \lambda \tag{27}$$

$$\sigma_i^* = +\infty, \qquad \lambda_{Ei}/\lambda_{Mi} \geq \lambda \tag{28}$$

[1]

$$\lambda_{Mi} \cdot \mathsf{lmmse}^2(\lambda_{Mi}\sigma_i^*) = \lambda \cdot \lambda_{Ei} \cdot \mathsf{lmmse}^2(\lambda_{Ei}\sigma_i^*), \qquad \lambda_{Ei}/\lambda_{Mi} < \lambda < \lambda_{Mi}/\lambda_{Ei} \tag{29}$$

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: See [11]. ■

It is immediate to show that this regime is valid if:

$$P_{avg} \geq \sum_{i=1}^{l} \sigma_i^* (\mathbf{C}^\dagger\mathbf{C})_{ii} \tag{30}$$

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

$$\sigma_i^* = \frac{\sqrt{\lambda_{Mi}}\Big(\sum_{j=1}^{n_{act}} \frac{\lambda_{Mj}}{\lambda_{Ej}-\lambda_{Mj}} + \gamma - n_{inact}\Big) - \sum_{j=1}^{n_{act}} \frac{\sqrt{\lambda_{Mj}\lambda_{Ej}}}{\lambda_{Ej}-\lambda_{Mj}}\lambda_{Ei}}{\sqrt{\lambda_{Ei}}\lambda_{Mi} \sum_{j=1}^{n_{act}} \frac{\sqrt{\lambda_{Mj}\lambda_{Ej}}}{\lambda_{Ej}-\lambda_{Mj}} - \sqrt{\lambda_{Mi}}\lambda_{Ei}\Big(\sum_{j=1}^{n_{act}} \frac{\lambda_{Mj}}{\lambda_{Ej}-\lambda_{Mj}} + \gamma - n_{inact}\Big)} \tag{31}$$

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 present in [11].

V. Results

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:

$$\mathbf{H}_M = \begin{bmatrix} 4 & -1 \\ 1 & 2 \end{bmatrix} \quad , \quad \mathbf{H}_E = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix} \tag{32}$$

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

As discussed earlier, we are specifically concerned with the impact that the use of the optimal nonlinear conditional mean estimator by the eavesdropper has in the secrecy measure, given that the transmitter, Alice, designs the linear transmit filter by assuming that both Bob and Eve use the optimal linear receive filter. We will consider the situations where the input to the wiretap channel is both BPSK and 16-PAM. Figure 2 shows the values of the MSEs in the main

[1] 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.

and in the eavesdropper channels (considering the different input signals) and the injected power into the channels *vs*. the secrecy constraint, with $P_{avg} = 1$. We can observe that designing the transmit filters with the assumption that the eavesdropper is using an optimal linear receive filter can, in fact, induce a penalty in the achieved secrecy, when the eavesdropper uses the conditional mean estimator and the input is not Gaussian (note that for Gaussian signals the conditional mean estimator is the optimal linear receive filter). However, and interestingly, as the solution evolves to higher values of the secrecy constraint γ, which constitutes our area of greatest operational interest, the penalty that we pay by assuming that the eavesdropper uses Wiener receive filters vanishes, so that for high values of γ the eavesdropper does not have any real advantage in using the conditional mean estimator. This is due to the fact that the power injected in the channel approaches zero as the values of γ increases, in order to meet the secrecy constraint.

Finally, we analyze the mutual information between the input vector and the eavesdropper output vector, achieved by this design. Figure 3 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, without the 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 $\mathrm{tr}\left(\mathbf{H}_T\mathbf{H}_T^\dagger\right) = P_{avg}$. As discussed in [11] we verify that, even without directly minimizing the mutual information in the eavesdropper channel, which corresponds to the information-theoretic security criteria *par excellence*, the optimal solution results in the lowest mutual information of these four cases.

VI. Conclusions

To conclude, we verify that the penalty for optimizing the transmit filter, considering linear receive filters, while the eavesdropper employs in reality conditional mean estimation is shown to be negligible for high values of γ. 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, the design have been shown to limit the amount of mutual information leaked to the eavesdropper, in comparison to other designs.

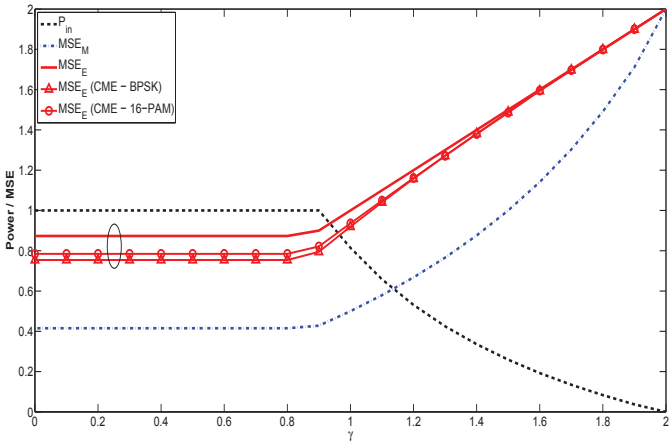

Figure 2. Main and Eavesdropper channel MSEs *vs*. secrecy constraint and input power *vs*. secrecy constraint for various input signals, with $P_{avg} = 1$.

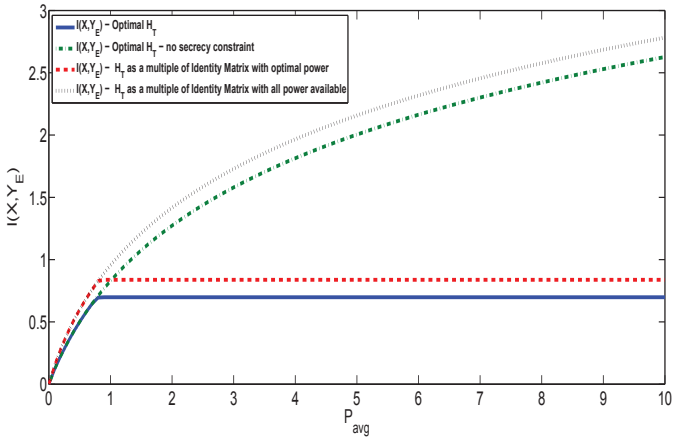

Figure 3. Eavesdropper mutual information *vs*. available power for four different transmit filters, with $\gamma = 1$.

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] 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.

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

[10] 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.

[11] 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.

[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.