ROBUST SECRET KEY CAPACITY FOR THE MIMO INDUCED SOURCE MODEL

Javier Vía

University of Cantabria, Spain
e-mail: jvia@gtas.dicom.unican.es
web: gtas.unican.es

ABSTRACT

This paper considers the problem of distilling a secret key in a Gaussian multiple-input multiple-output (MIMO) scenario with two legitimate nodes and an eavesdropper. Focusing on the realistic case without perfect knowledge of the eavesdropper channel, and following a conservative practical approach based on the maximization of the worst case secret key capacity (SKC), the problem of designing the optimal transmit covariance matrix is reformulated as a convex optimization problem. In the limiting case in which the eavesdropper channel can not be estimated, or when the estimate is highly unreliable, the optimal covariance matrix can be obtained by means of waterfilling or matched filtering like algorithms. Additionally, we illustrate the benefits of allowing time sharing between transmissions of the two legitimate nodes, and provide an efficient algorithm for obtaining the optimal transmit covariance matrices and time-sharing factor.

Index Terms— Secret Key Capacity (SKC), Induced Source Model, Multiple-Input Multiple-Output (MIMO), Robust Design, Time-Sharing, S-Procedure.

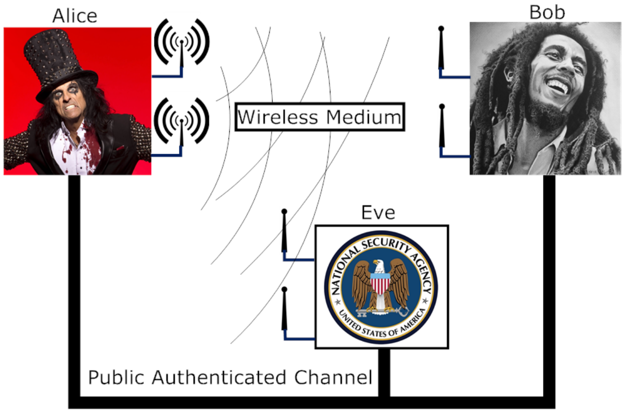

Fig. 1. Considered scenario. Alice and Bob use the wireless medium for inducing common randomness. The secret key is distilled by interchanging messages over the public authenticated channel.

1. INTRODUCTION

During the last decade, physical layer security [1, 2] has received increasing interest of the information theory, signal processing, and communications communities. Unlike traditional cryptographic approaches, this new paradigm does not rely on the assumption of attackers with limited computing power, thus providing fundamental limits for security.

While information theoretic security is a very active research area, many important results are already available, both for the secure transmission of information (secrecy capacity) [3–7], as well as for generation of secret keys (secret key capacity) [1, 8]. However, from a signal processing perspective, most of the literature is focused on secrecy capacity issues [9–11], as well as other interesting topics such as authentication [12–15] or discriminatory channel estimation [16, 17]. Thus, it is rather surprising that the signal processing approaches to secret key capacity (SKC) are really scarce [12, 18]. In particular, [18] considers a MIMO Gaussian wiretap channel, complemented by a public authenticated channel, and the transmit covariance matrix is optimized in order to maximize the SKC, with some interesting insights in the case of low and high signal to noise ratios (SNRs).

In this paper we extend the results in [18] in two different ways. First of all, we consider the realistic case in which the eavesdropper channel is not perfectly known, and following a conservative worst-case approach, we show that the robust problem can be reformulated as a convex optimization problem. Secondly, we consider the case in which both legitimate nodes are allowed to transmit, and provide an algorithm for obtaining the fraction of time and power to be allocated to each node in order to maximize the SKC. Finally, we also consider the practical cases in which the eavesdropper channel estimate is very inaccurate or not even available. In these cases, the optimal power allocation is given by a waterfilling or matched filtering like solution, which constitutes an important difference with the results obtained in [18] for low and high SNRs.

2. PROBLEM FORMULATION AND GENERAL SOLUTION

We adopt the system model in [18] (see Figure 1), where a couple of legitimate multiantenna nodes (Alice and Bob) try to distill a secret key unknown to a multiantenna eavesdropper (Eve). The three nodes have access to both the wireless medium, and an ideal (infinite rate, error free) authenticated public channel, which is used by Alice and Bob as a feedback channel for distilling a secret key. In particular, the secret-key agreement protocol consists of the following two phases:

1. Alice transmits over the wireless medium, which results in a set of observations at Bob (the received signals Y) and Alice (the transmitted signals X), as well as in a set of signals Z received by Eve.

This work was supported by the Spanish Government, Ministerio de Ciencia e Innovación (MICINN), under projects COSIMA (TEC2010-19545-C04-03) and COMONSENS (CSD2008-00010, CONSOLIDER-INGENIO 2010 Program)

2. Based on their observations, Alice and Bob interchange a set of messages F_A, F_B over the public channel, with the aim of distilling a secret key K unknown to Eve. Formally, the final goal consists in having a key satisfying the following requirements [1,18]:

   - *Reliability*: Alice and Bob obtain the same key, i.e., if we denote K_A and K_B as the keys distilled by Alice and Bob, we need to ensure $\lim_{n\to\infty} P(K_A \neq K_B) = 0$, where $P(\cdot)$ denotes probability, and n represents the number of uses of the wireless medium.
   - *Strong Secrecy*: We need to ensure that Eve can not extract any useful information about the secret key, from the observed signals and messages. Formally, $\lim_{n\to\infty} \mathbb{I}(K; Z, F_A, F_B) = 0$, where $\mathbb{I}(\cdot;\cdot)$ denotes mutual information.
   - *Uniformity*: The entropy of the secret key has to be maximized, i.e., $\lim_{n\to\infty} |\mathbb{H}(K) - nR| = 0$, where $\mathbb{H}(\cdot)$ denotes entropy, n is the number of channel uses, and R is the secret key generation rate.

We must note here that we are focusing on a simplified model in which the over the air signals do not depend on the messages transmitted through the public channel. This more general setup, which is beyond the scope of this paper, is known as the channel model for secret key agreement [1], and it represents an interesting information theoretic open problem. Thus, the problem considered in this paper can be referred to as an induced source model for secret key agreement, and the obtained results can be seen as a lower bound for the achievable rate in the channel model.

Let us start by writing the signals received by Bob and Eve as

$$\mathbf{y} = \mathbf{H}_{AB}\mathbf{x} + \mathbf{n}_B, \qquad \mathbf{z} = \mathbf{H}_{AE}\mathbf{x} + \mathbf{n}_E, \tag{1}$$

where $\mathbf{H}_{AB} \in \mathbb{C}^{N_B \times N_A}$ and $\mathbf{H}_{AE} \in \mathbb{C}^{N_E \times N_A}$ represent, respectively, the MIMO channel matrices from Alice to Bob and Eve. Analogously, $\mathbf{n}_B$ and $\mathbf{n}_E$ are two independent circularly symmetric complex Gaussian noise vectors with zero mean and identity covariance matrices $E[\mathbf{n}_B\mathbf{n}_B^H] = \mathbf{I}_{N_B}$, $E[\mathbf{n}_E\mathbf{n}_E^H] = \mathbf{I}_{N_E}$. Obviously, N_A, N_B and N_E represent the number of antennas at Alice, Bob and Eve.

Under the previous assumptions,[1] and for a fixed covariance matrix $\mathbf{K}_A = E[\mathbf{x}\mathbf{x}^H]$, the secret key capacity is achieved with Gaussian signaling and is given by [1,18]

$$R_{AB} = C(\mathbf{R}_{AB} + \mathbf{R}_{AE}, \mathbf{K}_A) - C(\mathbf{R}_{AE}, \mathbf{K}_A), \tag{2}$$

where $\mathbf{R}_{AB} = \mathbf{H}_{AB}^H\mathbf{H}_{AB}$, $\mathbf{R}_{AE} = \mathbf{H}_{AE}^H\mathbf{H}_{AE}$, and $C(\mathbf{R}, \mathbf{K}) = \log|\mathbf{I} + \mathbf{R}\mathbf{K}|$ is the conventional Shannon's capacity. Analogously to [18], here we consider the problem of designing the covariance matrix $\mathbf{K}_A$ for maximizing the secret key capacity. However, we do not assume perfect knowledge of the eavesdropper channel, which we model as

$$\mathbf{H}_{AE} = \hat{\mathbf{H}}_{AE} + \mathbf{\Delta}_{\mathbf{H}_{AE}}, \tag{3}$$

where $\hat{\mathbf{H}}_{AE}$ represents the estimated channel, and $\mathbf{\Delta}_{\mathbf{H}_{AE}}$ is an error term which is assumed to be bounded as $\|\mathbf{\Delta}_{\mathbf{H}_{AE}}\|^2_{\mathbf{W}_A} = \mathrm{tr}(\mathbf{\Delta}_{\mathbf{H}_{AE}}\mathbf{W}_A\mathbf{\Delta}_{\mathbf{H}_{AE}}^H) \leq 1$, with $\mathbf{W}_A$ a fixed positive semidefinite ($\mathbf{W}_A \succeq \mathbf{0}$) weighting matrix. Although the information theoretical analysis of the scenario without CSI has received increasing attention, there are still several open questions that do not seem easy to answer, and the practical application of approaches based on the compound wiretap channel [19] are not completely clear. Here, we follow a practical conservative approach based on ensuring that the eavesdropper channel is degraded with respect to the estimated worst case "channel". In particular, we consider the optimization problem

$$\begin{aligned} \underset{\mathbf{K}_A, \mathbf{R}_{AE}}{\text{maximize}} \quad & C(\mathbf{R}_{AB} + \mathbf{R}_{AE}, \mathbf{K}_A) - C(\mathbf{R}_{AE}, \mathbf{K}_A) \\ \text{subject to} \quad & \mathbf{R}_{AE} \succeq \mathbf{H}_{AE}^H\mathbf{H}_{AE} \quad \forall \|\mathbf{H}_{AE} - \hat{\mathbf{H}}_{AE}\|_{\mathbf{W}_A} \leq 1, \\ & \mathbf{K}_A \in \mathcal{S}_{\mathbf{K}_A}, \end{aligned} \tag{4}$$

where the convex set $\mathcal{S}_{\mathbf{K}_A}$ represents the set of feasible transmit covariance matrices. In particular, we will focus on the case of a total power constraint,[2] that is $\mathcal{S}_{\mathbf{K}_A} = \{\mathbf{K}_A | \mathbf{K}_A \succeq \mathbf{0}, \mathrm{tr}(\mathbf{K}_A) \leq P\}$, where P is the total power budget, and $\mathrm{tr}(\mathbf{K}_A)$ denotes the trace of matrix $\mathbf{K}_A$.

2.1. Reformulation as a Convex Optimization Problem

The optimization problem in (4) presents two main difficulties: 1) The cost function is not (simultaneously) concave on $\mathbf{K}_A$ and $\mathbf{R}_{AE}$; and 2) the infinite constraints introduced by the robustness requirement can not be directly handled. Fortunately, the following theorem ensures that (4) can be reformulated as a convex optimization problem

Theorem 1 *The problem in* (4) *is equivalent to the convex optimization problem (with* $\mathbf{S}_{AE} = \mathbf{R}_{AE}^{-1}$*)*

$$\begin{aligned} \underset{\substack{\mathbf{K}_A, \mathbf{S}_{AE}, \mathbf{M}_A \\ \mathbf{G}_A, s_A}}{\text{maximize}} \quad & \log|\mathbf{I}_{N_A} + \mathbf{M}_A\mathbf{R}_{AB}| \\ \text{subject to} \quad & \begin{bmatrix} \mathbf{S}_{AE} + \mathbf{K}_A & \mathbf{K}_A \\ \mathbf{K}_A & \mathbf{K}_A - \mathbf{M}_A \end{bmatrix} \succeq \mathbf{0}, \\ & \begin{bmatrix} \mathbf{G}_A & -\hat{\mathbf{H}}_{AE}\mathbf{S}_{AE} \\ -\mathbf{S}_{AE}\hat{\mathbf{H}}_{AE}^H & s_A\mathbf{W}_A - \mathbf{S}_{AE} \end{bmatrix} \succeq \mathbf{0}, \\ & \mathbf{G}_A = (1 - s_A)\mathbf{I}_{N_E} - \hat{\mathbf{H}}_{AE}\mathbf{S}_{AE}\hat{\mathbf{H}}_{AE}^H, \\ & s_A \geq 0, \quad \mathbf{K}_A \succeq \mathbf{0}, \quad \mathrm{tr}(\mathbf{K}_A) \leq P. \end{aligned} \tag{5}$$

The proof is omitted due to the lack of space. However, its main ingredients consist in the application of the matrix inversion lemma (Sherman-Morrison-Woodbury formula) [20], the monotonicity of the objective function with respect to $\mathbf{R}_{AE}$, and the S-procedure [21].

2.2. Time Sharing Solutions

Until now, and analogously to [18], we have focused on a scenario in which only Alice transmits over the air. However, as illustrated in Fig. 4, we should consider a more general setting in which a fraction (α) of the time is allocated for Alice's transmissions, while Bob transmits in the remaining fraction $(1 - \alpha)$ of time. The only scenario in which the optimal solution consists in allocating all the time to the same node (Alice or Bob) is given in the following lemma, whose proof reduces to realize that in the single antenna case with reciprocal channels, the secret key capacities are monotonically decreasing functions of the energy of the channel to the eavesdropper.

[1] We omit here the problem of designing practical codes for secret key agreement, which is beyond the scope of this paper. The interested reader can find details in [1,8].

[2] Our general results can be easily extended to other practical cases such as per antenna or peak power constraints.

Algorithm 1 Time Sharing for Robust SKC (Golden Section)

```
Input: $\mathbf{R}_{AB}, \mathbf{R}_{BA}, \mathbf{R}_{AE}, \mathbf{R}_{BE}, \mathbf{W}_A, \mathbf{W}_B$ and precision $\gamma$.
Output: Optimal covariance matrices $\mathbf{K}_A$ and $\mathbf{K}_B$, and time sharing factor $\alpha$.
Initialize: $\phi = 1 + \frac{1-\sqrt{5}}{2}$, and $M = \frac{\log \gamma}{\log(1-\phi)}$.
Evaluate (by solving (7)) $R(\alpha)$ at $\alpha_{\min} = 0$, $\alpha_1 = \phi$, $\alpha_2 = 1 - \phi$, and $\alpha_{\max} = 1$.
for $t = 1, \dots, M$ do
    if the maximum evaluated $R(\alpha)$ is at $\alpha_2$ or $\alpha_{\max}$ then
        Set the new lower bound $\alpha_{\min} = \alpha_1$, and update $\alpha_1 = \alpha_2$.
        New evaluation point $\alpha_2 = \alpha_{\min} + (1-\phi)(\alpha_{\max} - \alpha_{\min})$.
    else
        Set the new upper bound $\alpha_{\min} = \alpha_2$, and update $\alpha_2 = \alpha_1$.
        New evaluation point $\alpha_1 = \alpha_{\min} + \phi(\alpha_{\max} - \alpha_{\min})$.
    end if
    Evaluate $R(\alpha)$ at the new evaluation point, and obtain $\mathbf{K}_A$ and $\mathbf{K}_B$ by solving (7).
end for
```

Lemma 1 *In the case of single antenna nodes ($N_A = N_B = N_E = 1$), reciprocal channels, and a total power constraint, the optimal solution consists in allocating all the time to the same node.*

In the general case, we must solve the following optimization problem

$$\begin{array}{ll} \underset{\alpha}{\text{maximize}} & R(\alpha) \\ \text{subject to} & 0 \leq \alpha \leq 1, \end{array} \tag{6}$$

where the overall secret key rate $R(\alpha)$ is the optimal value of the following convex optimization problem

$$\begin{array}{ll} \text{maximize} & \alpha R_{AB} + (1-\alpha) R_{BA} \\ \text{subject to} & R_{AB} \leq \log\left|\mathbf{I}_{N_A} + \mathbf{M}_A \mathbf{R}_{AB}\right|, \\ & R_{BA} \leq \log\left|\mathbf{I}_{N_B} + \mathbf{M}_B \mathbf{R}_{BA}\right|, \\ & \begin{bmatrix} \mathbf{S}_{CE} + \mathbf{K}_C & \mathbf{K}_C \\ \mathbf{K}_C & \mathbf{K}_C - \mathbf{M}_C \end{bmatrix} \succeq \mathbf{0}, \quad C = A, B, \\ & \begin{bmatrix} \mathbf{G}_C & -\hat{\mathbf{H}}_{CE}\mathbf{S}_{CE} \\ -\mathbf{S}_{CE}\hat{\mathbf{H}}_{CE}^H & s_C \mathbf{W}_C - \mathbf{S}_{CE} \end{bmatrix} \succeq \mathbf{0}, \quad C = A, B, \\ & \mathbf{G}_C = (1 - s_C)\mathbf{I}_{N_E} - \hat{\mathbf{H}}_{CE}\mathbf{S}_{CE}\hat{\mathbf{H}}_{CE}^H, \quad C = A, B, \\ & \mathbf{K}_C \succeq \mathbf{0}, \quad s_C \geq 0, \quad C = A, B, \\ & \alpha \text{tr}(\mathbf{K}_A) + (1-\alpha)\text{tr}(\mathbf{K}_B) \leq P, \end{array} \tag{7}$$

where the optimization variables are R_{AB}, $\mathbf{K}_A$, $\mathbf{S}_{AE}$, $\mathbf{M}_A$, $\mathbf{G}_A$, s_A, R_{BA}, $\mathbf{K}_B$, $\mathbf{S}_{BE}$, $\mathbf{M}_B$, $\mathbf{G}_B$, s_B, and where R_{AB} and R_{BA} represent, respectively, the secret key rates from Alice to Bob, and from Bob to Alice.

The following lemma, whose proof is based on standard convexity arguments, establishes a key property of the function $R(\alpha)$.

Lemma 2 *The function $R(\alpha)$ is concave in $0 \leq \alpha \leq 1$, and its maximum can be efficiently found by means of the golden section algorithm.*

Finally, the application of the golden section algorithm [22] provides the overall procedure summarized in Algorithm 1.

3. IMPORTANT PARTICULAR CASES

In this section we focus on two particularly important cases, which consider scenarios with very limited (if any) knowledge about the eavesdropper channel. We analyze the case with Alice's transmissions, but the extension to the time-sharing case is trivial. Additionally, here we focus on the case with a spherical uncertainty region of radius ϵ, i.e. $\mathbf{W}_A = \epsilon^{-2}\mathbf{I}_{N_A}$.

3.1. Centered Eavesdropper Channel

Let us start by considering the case with $\hat{\mathbf{H}}_{AE} = \mathbf{0}$, which is reasonable when the channel (or even the presence) of the eavesdropper can not be estimated, but we can ensure that it is bounded as $\|\mathbf{H}_{AE}\| \leq \epsilon$. In this case, it is easy to prove that the worst case matrix $\mathbf{R}_{AE} = \mathbf{H}_{AE}^H\mathbf{H}_{AE}$ is $\mathbf{R}_{AE} = \epsilon^2\mathbf{I}_{N_A}$, and therefore, a straightforward analysis of the Karush-Kuhn-Tucker (KKT) conditions [23] provides the following result.

Lemma 3 *When the only knowledge about the eavesdropper channel is given by the uncertainty region $\|\mathbf{H}_{AE}\| \leq \epsilon$, the optimal transmit covariance matrix is given by $\mathbf{K}_A = \mathbf{U}\boldsymbol{\Lambda}\mathbf{U}^H$, where $\mathbf{U}$ are the eigenmodes of the channel $\mathbf{H}_{AB}$, i.e., it is obtained from the eigenvalue decomposition $\mathbf{R}_{AB} = \mathbf{H}_{AB}^H\mathbf{H}_{AB} = \mathbf{U}\boldsymbol{\Sigma}\mathbf{U}_H$, and the transmission powers in $\boldsymbol{\Lambda} = \text{diag}(\lambda_1, \dots, \lambda_{N_A})$ are given by a waterfilling like algorithm*

$$\lambda_k = \left[\frac{\frac{\sigma_k}{\mu} - 1}{\sigma_k + \epsilon^2}\right]_+, \tag{8}$$

where $\boldsymbol{\Sigma} = \text{diag}(\sigma_1, \dots, \sigma_{N_A})$, $[\cdot]_+ = \max(\cdot, 0)$, and the water-level μ is chosen to satisfy $\text{tr}(\mathbf{K}_A) = P$.

3.2. Large Uncertainty Sets

For very large uncertainty sets ($\epsilon \gg \max(\|\hat{\mathbf{H}}_{AE}\|, \|\hat{\mathbf{H}}_{AB}\|)$), we can particularize the results of the previous subsection, which yields the following result.

Lemma 4 *For $\epsilon \gg \max(\|\hat{\mathbf{H}}_{AE}\|, \|\hat{\mathbf{H}}_{AB}\|)$, the optimal transmit covariance matrix is given by the following matched-filtering like solution*

$$\mathbf{K}_A = \frac{P}{\text{tr}(\mathbf{R}_{AB})}\mathbf{R}_{AB}. \tag{9}$$

The proof of the previous lemma is simply based on the analysis of (8) for very large ϵ. Interestingly, the obtained result significatively differs from the case with perfect CSI and very low SNR, which was analyzed in [18], proving that the optimal solution reduces to "ignore" the eavesdropper channel and beamforming on the principal mode of the channel $\mathbf{H}_{AB}$. Instead of that, our result indicates that for large uncertainty sets, all the modes of the legitimate channel must be excited.

4. NUMERICAL EXAMPLES

Our main findings are illustrated in this section by means of some numerical results. In all the cases, the channels $\mathbf{H}_{AB}$ and $\mathbf{H}_{AE}$ have been randomly generated from a standard Rayleigh distribution, and we have considered spherical uncertainty sets with radius ϵ. In the first example, we show the results obtained by solving the convex optimization problem in (5). In particular, we consider $N_A = 4$ antennas, and show the averaged results of 300 independent experiments. Figs. 2 and 3 show the results for the cases with $N_B = N_E = 2$ and $N_B = N_E = 4$, where we can see that the uncertainty in the eavesdropper channel reduces the degrees of freedom (slope of the

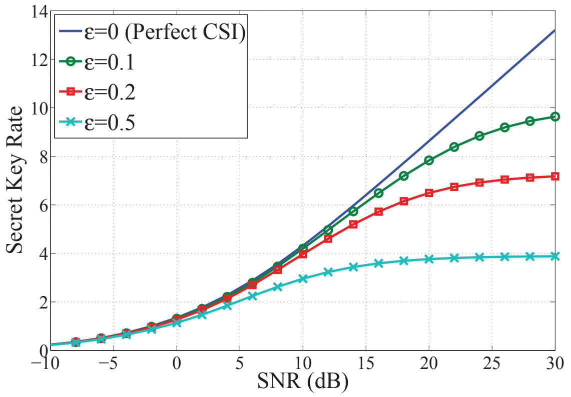

Fig. 2. Performance analysis of the robust solution obtained from (5). $N_A = 4$, $N_B = N_E = 2$.

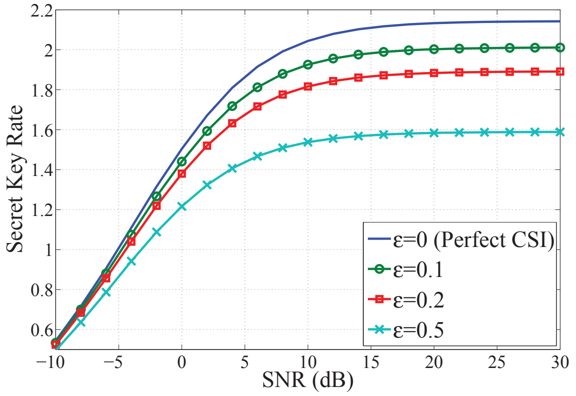

Fig. 3. Performance analysis of the robust solution obtained from (5). $N_A = N_B = N_E = 4$.

secret key rate for high SNR) to zero. In other words, the saturation effect in the secret key rates indicates that there exists a point in which increasing the transmission power is useless, and instead of that, Alice and Bob should focus on improving their estimates of the eavesdropper channel. In any case, we can see that positive practical secret key rates can be achieved even without perfect CSI.

In the second example, we consider a toy problem with $N_A = N_B = N_E = 2$, $\epsilon = 0.1$, $\mathbf{H}_{AB} = \mathbf{H}_{BA} = \mathrm{diag}(10, 1)$, $\mathbf{H}_{AE} = 5\mathbf{I}_2$ and $\mathbf{H}_{BE} = \mathrm{diag}(10, 0)$. Fig. 4 shows the rates obtained when only one node (Alice or Bob) transmits, and also certificates the optimality of the time sharing solutions provided by Algorithm 1.

Finally, we consider the case with very limited CSI ($\hat{\mathbf{H}}_{AE} = \mathbf{0}$) for different uncertainty radius ϵ. Fig. 5 shows the averaged results of 300 independent simulations with $N_A = 4$ and $N_B = N_E = 2$, for the waterfilling (Lemma 3) and matched-filtering (Lemma 4) algorithms. As expected, for sufficiently large radius, both techniques provide identical results.

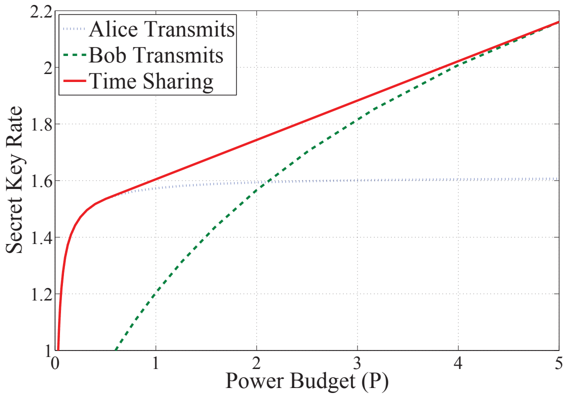

Fig. 4. Optimality of the time-sharing solutions. $N_A = N_B = N_E = 2$, $\epsilon = 0.1$.

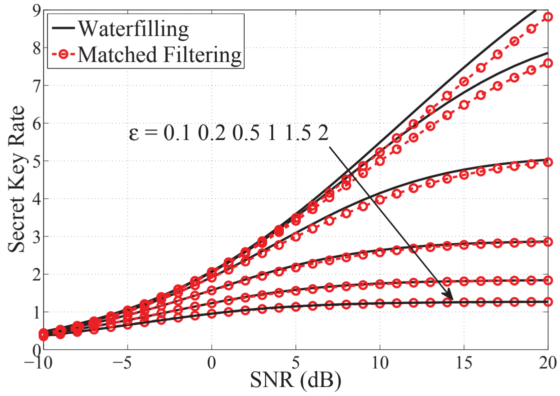

Fig. 5. Comparison of the waterfilling and matched-filtering algorithms. $\hat{\mathbf{H}}_{AE} = \mathbf{0}$, $N_A = 4$, $N_B = N_E = 2$.

5. CONCLUSIONS

We have presented a robust approach to the design of covariance matrices for maximizing the secret key capacity (SKC) in a Gaussian MIMO induced source model. In the cases of unavailable or highly inaccurate estimates of the eavesdropper channel, the optimal transmit covariance matrix can be obtained by means of waterfilling like or matched filtering like algorithms. Moreover, we have illustrated the benefits of allowing time sharing between transmissions of the two legitimate nodes, providing an efficient algorithm for this general scenario.

6. REFERENCES

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[2] L. Sankar, W. Trappe, H. Poor, and M. Debbah, "Signal processing for cybersecurity and privacy [from the guest editors]," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 14–15, 2013.

[3] A. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[4] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, 2009.

[5] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part I: The MISOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[6] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part ii: The MIMOME wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[7] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S.W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[9] Q. Li and W. K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semidefinite programming," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3799–3812, 2011.

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

[11] S.A.A. Fakoorian and A.L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2620–2631, 2013.

[12] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless Security*, New York, NY, USA, 2006, pp. 33–42, ACM.

[13] L. Xiao, L.J. Greenstein, Narayan B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, 2008.

[14] P.L. Yu, J.S. Baras, and B.M. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, 2008.

[15] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564–2573, 2012.

[16] T-H Chang, W-C Chiang, Y.P. Hong, and C-Y Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Transactions on Signal Processing*, vol. 58, no. 12, pp. 6223–6237, 2010.

[17] C-W Huang, T-H Chang, X. Zhou, and Y.-W.P. Hong, "Two-way training for discriminatory channel estimation in wireless MIMO systems," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2724–2738, 2013.

[18] F. Renna, M.R. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," *IEEE Transactions on Communications*, vol. 61, no. 2, pp. 620–627, 2013.

[19] A. Khisti, "Interference alignment for the multiantenna compound wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2976–2993, 2011.

[20] G. H. Golub and C. F. van Loan, *Matrix Computations*, Johns Hopkins University Press, Baltimore, 2nd edition, 1989.

[21] Z.-Q. Luo, J. F. Sturm, and S. Zhang, "Multivariate nonnegative quadratic mappings," *SIAM J. on Optimization*, vol. 14, no. 4, pp. 1140–1162, Apr. 2004.

[22] J. Kiefer, "Sequential minimax search for a maximum," *Proceedings of the American Mathematical Society*, vol. 4, no. 3, pp. pp. 502–506, 1953.

[23] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, March 2004.