ISIT'2013 1569712541

Further Results on Optimal Signaling over Secure MIMO Channels

Sergey Loyka, Charalambos D. Charalambous

***Abstract*—Optimal signalling over the wire-tap MIMO Gaussian channel is studied under the total transmit power constraint. The recent results are extended in several directions, including a rank-deficient solution for the optimal covariance, lower and upper capacity bounds for the general case, and characterization of optimality of the isotropic signaling.**

An isotropic eavesdropper model is studied, which provides (tight) upper and lower capacity bounds for the non-isotropic case and also serves as the worst-case scenario. The optimal signaling for this model is obtained in an explicit form and its properties are studied, including the high and low-SNR behavior, the conditions for the eavesdropper to be negligible and the capacity saturation effect.

I. Introduction

Information-theoretic perspective on secure communications has recently attracted a significant attention [1]-[7]. In particular, the secure Gaussian MIMO channel has been a subject of intensive studies using Wyner's wire-tap model [3]-[10]. A number of results have been obtained, including the proof of optimality of Gaussian signaling (far from trivial). The optimal transmit covariance has been obtained for some special cases (low/high SNR, MISO channel, rank-one case) but the general case remains an open problem.

It was conjectured in [7] and proved in [6] using an indirect approach (via the degraded channel) that the optimal signaling is on the positive directions of the difference channel. A direct proof (based on the necessary KKT conditions) has been obtained in [9]. A weaker result (non-negative instead of positive directions) has been obtained in [10].

Recently, an exact full-rank solution for the optimal covariance has been obtained in [9] and its properties have been characterized. In particular, unlike the regular channel (no eavesdropper), the optimal power allocation does not converge to uniform one at high SNR and the latter remains sub-optimal at any finite SNR. In the case of weak eavesdropper, the optimal signaling mimics the conventional one (water-filling over the channel eigenmodes) with an adjustment for the eavesdropper channel.

In the present paper, we extend the recent results in several directions:

* The full-rank solution in [9] is extended to a rank-deficient case where the null space of the legitimate channel belongs to the null space of the eavesdropper channel.

S. Loyka is with the School of Electrical Engineering and Computer Science, University of Ottawa, Ontario, Canada, K1N 6N5, e-mail: sergey.loyka@ieee.org.

C.D. Charalambous is with the ECE Department, University of Cyprus, 75 Kallipoleos Avenue, P.O. Box 20537, Nicosia, 1678, Cyprus, e-mail: chadcha@ucy.ac.cy

* Lower and upper (tight) capacity bounds are obtained for the general case, which are achievable by an isotropic eavesdropper.

* The case of isotropic eavesdropper is studied in details, including the optimal signaling in an explicit closed form and its properties. This case is shown to be the worst-case MIMO wire-tap channel.

* The set of channels for which isotropic signaling is optimal is fully characterized. It turns out to be much richer than that of the conventional (no eavesdropper) MIMO channel.

It is hardly possible to expect that the eavesdropper will share its channel with the transmitter to make eavesdropping harder. Therefore, only limited eavesdropper channel state information can be expected by the transmitter. To address this issue, we use an isotropic eavesdropper model with only one parameter, the channel power gain, which is known to the transmitter, and study it in details in Section V. Not only this model provides (tight) upper and lower bounds for the non-isotropic eavesdropper case (Proposition 2), but it also serves as the worst-case eavesdropper. From the physical viewpoint, this model emerges when there is a minimum (protection) distance to the transmitter beyond which the eavesdropper cannot approach the transmitter, so that its channel power gain is upper-bounded due to the propagation path loss but otherwise is not constrained. We obtain the optimal Tx covariance in an explicit form (Proposition 2). This includes transmission on the legitimate channel eigenmodes (akin to the regular MIMO channel) and an optimal power allocation among the eigenmodes which somewhat resembles the standard water-filling but is not identical to it. Properties of this optimal power allocation are studied (Proposition 3): all sufficiently strong eigenmodes are active at high SNR, but there is a capacity saturation effect (increasing the SNR beyond a threshold does not increase the capacity), while only the strongest eigenmode is active at low SNR. The impact of the eavesdropper at high SNR is multiplicative (i.e. very significant and never negligible) SNR loss (resulting in the saturation effect) and an additive (mild) SNR loss at low SNR. The conditions for the eavesdropper to be negligible are given. Overall, the low-SNR regime (e.g. as in CDMA) is more friendly for secure communications in the sense that the impact of eavesdropper is not that high or even negligible.

II. Wire-Tap Gaussian MIMO Channel Model

Let us consider the standard wire-tap Gaussian MIMO channel model,

$$\mathbf{y}_1 = \mathbf{H}_1\mathbf{x} + \xi_1, \quad \mathbf{y}_2 = \mathbf{H}_2\mathbf{x} + \xi_2 \tag{1}$$

where $\mathbf{x} = [x_1, x_2, ...x_m]^T \in C^{m,1}$ is the transmitted complex-valued signal vector of dimension $m \times 1$, "T" denotes transposition, $\mathbf{y}_{1(2)} \in C^{n,1}$ are the received vectors at the receiver (eavesdropper), $\xi_{1(2)}$ is the circularly-symmetric additive white Gaussian noise at the receiver (eavesdropper) (normalized to unit variance in each dimension), $\mathbf{H}_{1(2)} \in C^{n_{1(2)},m}$ is the $n_{1(2)} \times m$ matrix of the complex channel gains between each Tx and each receive (eavesdropper) antenna, $n_{1(2)}$ and m are the numbers of Rx (eavesdropper) and Tx antennas respectively. The channels $\mathbf{H}_{1(2)}$ are assumed to be quasistatic (i.e., constant for a sufficiently long period of time so that the infinite horizon information theory assumption holds) and frequency-flat, with full channel state information (CSI) at the Rx and Tx ends.

For a given transmit covariance matrix $\mathbf{R} = E\{\mathbf{x}\mathbf{x}^+\}$, where $E\{\cdot\}$ is statistical expectation, the maximum achievable secure rate between the Tx and Rx (so that the rate between the Tx and eavesdropper is zero) is [3]-[7]

$$C(\mathbf{R}) = \ln \frac{|\mathbf{I} + \mathbf{W}_1\mathbf{R}|}{|\mathbf{I} + \mathbf{W}_2\mathbf{R}|} = C_1(\mathbf{R}) - C_2(\mathbf{R}) \tag{2}$$

where negative $C(\mathbf{R})$ is interpreted as zero rate, $\mathbf{W}_i = \mathbf{H}_i^+\mathbf{H}_i$, $()^+$ means Hermitian conjugation, and the secrecy capacity subject to the total Tx power constraint is

$$C_s = \max_{\mathbf{R}\geq 0} C(\mathbf{R}) \text{ s.t. } tr\mathbf{R} \leq P_T \tag{3}$$

where P_T is the total transmit power (also the SNR since the noise is normalized). It is well-known that the problem in (3) is not convex in general and explicit solutions for the optimal Tx covariance is not known for the general case, but only for some special cases (e.g. low/high SNR, MISO channels, or for the full-rank case [5][6][8][9]).

III. Optimal Signaling: Prior Results

Below, we summarize the relevant prior results in [9] for reference purposes.

Theorem 1: Let $\mathbf{R}^*$ be an optimal covariance in (3),

$$\mathbf{R}^* = \arg\max_{\mathbf{R}\geq 0} C(\mathbf{R}) \text{ s.t. } tr\mathbf{R} \leq P_T$$

and let $\mathbf{u}_{i+}$ be its active eigenvector (i.e. corresponding to a positive eigenvalue). Then,[1]

$$\mathbf{U}_{r+}^+(\mathbf{W}_1 - \mathbf{W}_2)\mathbf{U}_{r+} > \mathbf{0} \tag{4}$$

where the columns of $\mathbf{U}_{r+}$ are the active eigenvectors $\{\mathbf{u}_{i+}\}$, so that $\mathbf{x}^+(\mathbf{W}_1 - \mathbf{W}_2)\mathbf{x} > \mathbf{0} \quad \forall \mathbf{x} \in span\{\mathbf{u}_{i+}\}$, i.e. a necessary condition for an optimal signaling strategy in (3) is to transit over the positive directions of $\mathbf{W}_1 - \mathbf{W}_2$ (where the legitimate channel is stronger than the eavesdropper).

The full-rank solution of the optimization problem in (3) is given in the following Theorem.

Theorem 2: Consider the case of $\mathbf{W}_1 > \mathbf{W}_2 \geq \mathbf{0}$ (a degraded full-rank channel) and $P_T > P_{T0}$, where P_{T0} is a certain threshold power (i.e. sufficiently high but finite SNR). Then, $\mathbf{R}^*$ is of full rank and is given by:

$$\mathbf{R}^* = \mathbf{U}\mathbf{\Lambda}_1\mathbf{U}^+ - \mathbf{W}_1^{-1} \tag{5}$$

where the columns of the unitary matrix $\mathbf{U}$ are the eigenvectors of $\mathbf{Z} = \mathbf{W}_2 + \mathbf{W}_2(\mathbf{W}_1 - \mathbf{W}_2)^{-1}\mathbf{W}_2$, $\mathbf{\Lambda}_1 = diag\{\lambda_{1i}\} > \mathbf{0}$ is a diagonal positive-definite matrix, where

$$\lambda_{1i} = \frac{\mu_i}{2}\left(\sqrt{1 + \frac{4}{\lambda\mu_i}} - 1\right) \tag{6}$$

and $\mu_i > 0$ are the eigenvalues of $\mathbf{Z}^{-1}$; $\lambda > 0$ is found from the total power constraint $tr\mathbf{R}^* = P_T$ as a unique solution of the following equation:

$$\sum_i \frac{\mu_i}{2}\left(\sqrt{1 + \frac{4}{\lambda\mu_i}} - 1\right) = P_T - tr(\mathbf{W}_1^{-1}) \tag{7}$$

P_{T0} can be found as a unique solution of the following equation:

$$\lambda_{1min}(P_{T0})\lambda_{min}(\mathbf{W}_1) = 1$$

where $\lambda_{1min} = \min_i\{\lambda_{1i}\}$ and $\lambda_{min}(\mathbf{W}_1)$ is the minimum eigenvalue of $\mathbf{W}_1$.

It should be pointed out that Theorem 2 gives an exact (not approximate) optimal covariance at finite SNR (no $P_T \to \infty$) since P_{T0} is a finite constant that depends only on $\mathbf{W}_1$ and $\mathbf{W}_2$ and can be found numerically.

IV. Optimal Signaling: A Rank-Deficient Solution

Let us now extend this full-rank solution to the scenario where the optimal covariance is rank-deficient.

Proposition 1. *Consider the problem in* (3) *when* $\mathcal{N}(\mathbf{W}_1) \in \mathcal{N}(\mathbf{W}_2)$, *where* $\mathcal{N}(\mathbf{W}) = \{\mathbf{x} : \mathbf{W}\mathbf{x} = \mathbf{0}\}$ *is the null space of matrix* $\mathbf{W}$ *[13], and assume that*

$$\mathbf{x}^+(\mathbf{W}_1 - \mathbf{W}_2)\mathbf{x} > 0 \ \forall \mathbf{x} \in \mathcal{N}_\perp \tag{8}$$

where $\mathcal{N}_\perp$ *is orthogonal complement of* $\mathcal{N}(\mathbf{W}_1)$, *i.e.* $\mathbf{W}_1 - \mathbf{W}_2$ *is positive definite on* $\mathcal{N}_\perp$. *At sufficiently high SNR (as in Theorem 2), the optimal covariance in* (3) *is*

$$\mathbf{R}^* = \mathbf{U}_\perp\tilde{\mathbf{R}}^*\mathbf{U}_\perp^+ \tag{9}$$

where $\tilde{\mathbf{R}}^*$ *is the optimal covariance of Theorem 2 with the substitution* $\mathbf{W}_i \to \mathbf{U}_\perp^+\mathbf{W}_i\mathbf{U}_\perp$ *and the columns of semi-unitary matrix* $\mathbf{U}_\perp$ *form an orthonormal basis of* $\mathcal{N}_\perp$. *Furthermore,* $rank(\mathbf{R}^*) = dim(\mathcal{N}_\perp)$.

Proof: Observe that $\mathbf{W}_i\mathbf{x} = \mathbf{W}_i\mathbf{x}_\perp$, where $\mathbf{x}_\perp = \mathbf{U}_\perp\mathbf{U}_\perp^+\mathbf{x}$ is the orthogonal projection of $\mathbf{x}$ on $\mathcal{N}_\perp$, so that

$$\begin{aligned} |\mathbf{I} + \mathbf{W}_i\mathbf{R}| &= |\mathbf{I} + \mathbf{W}_i\mathbf{U}_\perp\mathbf{U}_\perp^+\mathbf{R}\mathbf{U}_\perp\mathbf{U}_\perp^+| \\ &= |\mathbf{I} + \mathbf{U}_\perp^+\mathbf{W}_i\mathbf{U}_\perp\mathbf{U}_\perp^+\mathbf{R}\mathbf{U}_\perp| \end{aligned} \tag{10}$$

and $tr(\mathbf{U}_\perp^+\mathbf{R}\mathbf{U}_\perp) \leq tr(\mathbf{R})$ so that one can use the projected matrices $\tilde{\mathbf{R}} = \mathbf{U}_\perp^+\mathbf{R}\mathbf{U}_\perp, \tilde{\mathbf{W}}_i = \mathbf{U}_\perp^+\mathbf{W}_i\mathbf{U}_\perp$ in Theorem 2 to obtain the desired solution. (8) insures that $\tilde{\mathbf{W}}_1 - \tilde{\mathbf{W}}_2 > 0$ so that Theorem 2 applies. ■

[1] $\mathbf{A} > \mathbf{B}$ means that $\mathbf{A} - \mathbf{B}$ is positive definite.

V. Isotropic Eavesdropper and Capacity Bounds

While it is a challenging analytical task to evaluate the secure capacity in the general case, lower and upper bounds can be obtained for the general case using the standard matrix inequalities $\epsilon_m \mathbf{I} \le \mathbf{W}_2 \le \epsilon_1 \mathbf{I}$, where $\epsilon_i = \lambda_i(\mathbf{W}_2)$ denotes i-th largest eigenvalue of $\mathbf{W}_2$, and the equalities are achieved when $\epsilon_1 = \epsilon_m$, i.e. $\mathbf{W}_2$ has identical eigenvalues.

Proposition 2. *The MIMO secrecy capacity in* (3) *is bounded as follows:*

$$C^*(\epsilon_1) \le C_s \le C^*(\epsilon_m) \tag{11}$$

where $C^*(\epsilon)$ is the secrecy capacity C_s when $\mathbf{W}_2 = \epsilon \mathbf{I}$, i.e. for the isotropically-strong eavesdropper,

$$C^*(\epsilon) = \max_{\substack{\mathbf{R}\ge 0 \\ tr\mathbf{R}\le P_T}} \ln \frac{|\mathbf{I}+\mathbf{W}_1\mathbf{R}|}{|\mathbf{I}+\epsilon\mathbf{R}|} = \sum_i \ln \frac{1+g_i\lambda_i^*}{1+\epsilon\lambda_i^*} \tag{12}$$

$g_i = \lambda_i(\mathbf{W}_1)$, and $\lambda_i^* = \lambda_i(\mathbf{R}^*)$ are the eigenvalues of the optimal transmit covariance $\mathbf{R}^* = \mathbf{U}_1 \mathbf{\Lambda}^* \mathbf{U}_1^+$,

$$\lambda_i^* = \frac{\epsilon + g_i}{2\epsilon g_i}\left(\sqrt{1+\frac{4\epsilon g_i}{(\epsilon+g_i)^2}\left(\frac{g_i-\epsilon}{\lambda}-1\right)_+}-1\right) \tag{13}$$

and $\lambda > 0$ is found from the total power constraint $\sum_i \lambda_i^* = P_T$, the columns of $\mathbf{U}_1$ are the eigenvectors of $\mathbf{W}_1$.

Proof: See Appendix. ∎

Thus, the optimal signalling is on the eigenvectors of $\mathbf{W}_1$ (or right singular vectors of $\mathbf{H}_1$), identically to the regular MIMO channel, with the optimal power allocation somewhat similar (but not identical) to the conventional water filling. The latter is further elaborated for the high and low SNR regimes below. Unlike the general case (of non-isotropic eavesdropper), the secure capacity of the isotropic eavesdropper case does not depend on the eigenvectors of $\mathbf{W}_1$ (but the optimal signalling does) but only on its eigenvalues, so that the optimal signaling problem here separates into 2 independent parts: (i) optimal signalling directions are selected as the eigenvectors of $\mathbf{W}_1$, and (ii) optimal power allocation is done based on the eigenvalues of $\mathbf{W}_1$ and the eavesdropper channel gain ϵ. It is the lack of this separation that makes the optimal signaling problem so difficult in the general case.

The bounds in (11) coincide when $\epsilon_1 = \epsilon_m$ thus giving the secrecy capacity of the isotropic eavesdropper. Furthermore, they are reasonably close to each other when the condition number ϵ_1/ϵ_m of $\mathbf{W}_2$ is not too large, thus providing a reasonable estimate of the capacity, see Fig. 1.

We note that the power allocation in (13) has properties similar to those of the conventional water-filling, as established next.

Proposition 3. *Properties of the optimum power allocation:*

1. λ_i^* is an increasing function of g_i (strictly increasing unless $\lambda_i^* = 0$ or P_T) , i.e. stronger eigenmodes get more power (as in the standard WF).

2. λ_i^* is an increasing function of P_T (strictly increasing unless $\lambda_i^* = 0$). $\lambda_i^* = 0$ for $i > 1$ and $\lambda_1^* = P_T$ as $P_T \to 0$ if $g_1 > g_2$, i.e. only the strongest eigenmode is active at low SNR, and $\lambda_i^* > 0$ if $g_i > \epsilon$ as $P_T \to \infty$, i.e. all sufficiently strong eigenmodes are active at high SNR.

3. $\lambda_i^* > 0$ only if $g_i > \epsilon$, i.e. only the legitimate eigenmodes stronger than the eavesdropper ones can be active.

4. λ is a strictly decreasing function of P_T and $0 < \lambda < g_1 - \epsilon$; $\lambda \to 0$ as $P_T \to \infty$ and $\lambda \to g_1 - \epsilon$ as $P_T \to 0$.

5. There are m_+ active eigenmodes if the following inequalities hold:

$$P_{m_+} < P_T \le P_{m_++1} \tag{14}$$

where P_{m_+} is a threshold power (to have at least m_+ active eigenmodes):

$$P_{m_+} = \sum_{i=1}^{m_+-1} \frac{\epsilon+g_i}{2\epsilon g_i}\left(\sqrt{1+\frac{4\epsilon g_i}{(\epsilon+g_i)^2}\frac{g_i-g_{m_+}}{(g_{m_+}-\epsilon)_+}}-1\right), \tag{15}$$

for $m_+ = 2...m$ and $P_1 = 0$, so that m_+ is an increasing function of P_T.

Proof: Follows from Proposition 2 (details are ommited due to the page limit). ∎

It follows from Proposition 3 that there is only one active eigenmode, i.e. beamforming is optimal, if $g_2 > \epsilon$ and

$$P_T \le P_2 \tag{16}$$

e.g. in the low SNR regime (note however that the single-mode regime extends well beyond low SNR if $\epsilon \to g_2$ and $g_1 > g_2$), or at any SNR if $g_1 > \epsilon$ and $g_2 \le \epsilon$.

A further importance of the isotropic eavesdropper model is coming from the fact that it is hardly possible to expect that the eavesdropper will communicate its channel to the transmitter to make eavesdropping harder. Therefore, the transmitter has to assume a worst-case scenario due to the lack of its precise knowledge, which is the isotropic eavesdropper from the lower bound in (11). In our view, this isotropic eavesdropper model is more practical than the full Tx CSI model.

A. High SNR regime

Let us now consider the isotropic eavesdropper model when the SNR grows large, so that $g_i\lambda_i^* \gg 1, \epsilon\lambda_i^* \gg 1$. In this case, (12) simplifies to

$$C_\infty^* = \sum_{i_+} \ln \frac{g_i}{\epsilon} \tag{17}$$

where the summation is over active eigenmodes only, $i_+ = \{i : g_i > \epsilon\}$, so that the capacity is independent of the SNR (saturation effect) and the impact of the eavesdropper is the multiplicative SNR loss, which is never negligible. To obtain a threshold value of P_T at which the saturation takes place, observe that $\lambda \to 0$ as $P_T \to \infty$ so that (13) becomes

$$\lambda_i^* = \frac{P_T\alpha_i}{\sum_{i_+}\alpha_i}(1+o(1)),\ \alpha_i = \sqrt{\epsilon^{-1}-g_i^{-1}}. \tag{18}$$

Using (18), the capacity becomes

$$C^*(\epsilon) = \sum_{i_+} \ln \frac{g_i}{\epsilon} - \frac{1}{P_T} \left(\sum_{i_+} \alpha_i \right)^2 + o\left(\frac{1}{P_T}\right) \qquad (19)$$

which is a refinement of (17). The saturation takes place when the second term is much smaller than the first one, so that

$$P_T \gg \left(\sum_{i_+} \alpha_i \right)^2 / \sum_{i_+} \ln \frac{g_i}{\epsilon} \qquad (20)$$

and $C^*(\epsilon) \approx C^*_\infty$ under this condition. Another way to interpret (20) is to say that its right-hand side gives the SNR threshold beyond which further increase does not increase the capacity significantly and thus is not justified. This effect in illustrated in Fig. 1.

Note that, from (18), the optimal power allocation behaves almost like water-filling in this case, due to the α_i term.

Using (17), the gap $\Delta C^*_\infty = C^*_\infty(\epsilon_m) - C^*_\infty(\epsilon_1)$ between the lower and upper bounds in (11) becomes

$$\Delta C^*_\infty = m_1 \ln \frac{\epsilon_1}{\epsilon_m} + \sum_{i=m_1+1}^{m_2} \ln \frac{g_i}{\epsilon_m} \qquad (21)$$

where $m_{1(2)}$ is the number of active eigenmodes when $\epsilon = \epsilon_{1(m)}$. Note that this gap is SNR-independent and if $m_1 = m_2 = m_+$, which is the case if $g_{m+} > \epsilon_1$, then

$$\Delta C^*_\infty = m_+ \ln \frac{\epsilon_1}{\epsilon_m} \qquad (22)$$

i.e. also independent of the eigenmode gains of the legitimate user and is determined solely by the condition number of the eavesdropper channel and the number of active eigenmodes.

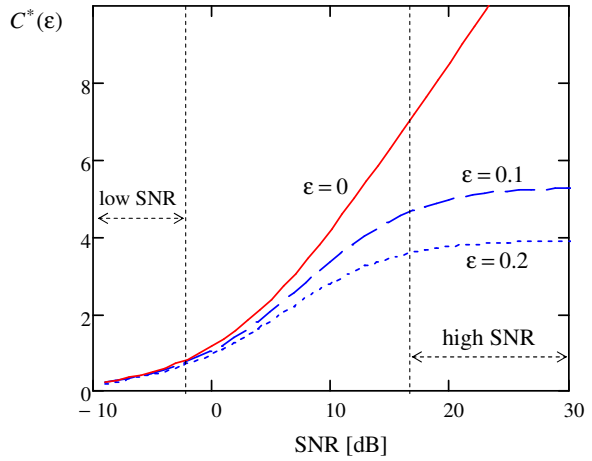

Fig. 1. Secrecy capacity for the isotropic eavesdropper and the capacity of the regular MIMO channel (no eavesdropper, $\epsilon = 0$) vs. the SNR ($= P_T$ since the noise variance is unity); $g_1 = 2$, $g_2 = 1$. Note the saturation effect at high SNR , where the capacity strongly depends on ϵ but not the SNR, and the negligible impact of the eavesdropper at low SNR.

B. When is the eavesdropper negligible?

It is clear from (12) that under fixed $\{g_i\}$ and P_T, the secure capacity converges to the conventional one $C^*(0)$ as $\epsilon \to 0$. However, no any small but fixed ϵ can insure by itself that the eavesdropper is negligible since one can always select sufficiently high P_T to make the saturation effect important (see Fig. 1). To answer the question, we use (12) to obtain:

$$\begin{aligned} C^*(\epsilon) &= \max_{\substack{\lambda_i \geq 0 \\ \sum_i \lambda_i = P_T}} \sum_i \ln \left(1 + \frac{1 + (g_i - \epsilon)\lambda_i}{1 + \epsilon \lambda_i} \right) \\ &\overset{(a)}{\approx} \max_{\{\lambda_i\}} \sum_i \ln(1 + (g_i - \epsilon)\lambda_i) \\ &\overset{(b)}{\approx} \max_{\{\lambda_i\}} \sum_i \ln(1 + g_i \lambda_i) = C^*(0) \end{aligned} \qquad (23)$$

where (a) holds if

$$P_T \ll 1/\epsilon \qquad (24)$$

(since $\lambda_i \leq P_T$), i.e. if the SNR is not too large, and (b) holds if

$$\epsilon \ll g_{i+} \qquad (25)$$

where i_+ is the set of active eigenmodes, i.e. if the eavesdropper is much weaker than the legitimate active eigenmodes. It is the combination of (24) and (25) that insures that the eavesdropper is negligible. Neither condition alone is able to do so. Fig. 1 illustrates this point. Eq. (23) also indicates that the impact of the eavesdropper is the per-eigenmode gain loss of ϵ. Unlike the high-SNR regime in (17) where the loss is multiplicative (i.e. very significant and never negligible), here it is additive (mild or negligible in many cases).

C. Low SNR regime

Let us now consider the low-SNR regime, which is characteristic for CDMA-type systems. Traditionally, this regime is defined via $P_T \to 0$. We, however, use a more relaxed definition requiring that $m_+ = 1$, which holds under (16). In this regime, assuming $g_1 > \epsilon$,

$$C^*(\epsilon) = \ln \left(1 + \frac{(g_1 - \epsilon)P_T}{1 + \epsilon P_T} \right) \overset{(a)}{\approx} \ln(1 + (g_1 - \epsilon)P_T) \qquad (26)$$

where (a) holds when $P_T \ll 1/\epsilon$. It is clear from the last expression that the impact of the eavesdropper is an additive SNR loss of ϵP_T, which is negligible when $\epsilon \ll g_1$. Note a significant difference to the high SNR regime in (17), where this impact is never negligible.

Note further from (26) that the difference between the lower and upper bounds in (11) is the SNR gap of $(\epsilon_1 - \epsilon_m)P_T$ so that the bounds in (11) estimate the capacity accurately if $g_1 \gg \epsilon_1 - \epsilon_m$. This may be the case even if the condition number ϵ_1/ϵ_m is large. Therefore, we conclude that the impact of the eavesdropper is more pronounced in the high-SNR regime and is negligible in the low-SNR one if its channel is weaker than the strongest eigenmode of the legitimate user.

VI. When Is the Isotropic Signaling Optimal?

In the regular MIMO channel ($\mathbf{W_2} = \mathbf{0}$), isotropic signaling is optimal ($\mathbf{R}^* = a\mathbf{I}$) iff $\mathbf{W}_1 = b\mathbf{I}$, i.e. $\mathbf{W}_1$ has identical eigenvalues. Since this transmission strategy is appealing due to its low complexity (all antennas send independent data streams, no precoding, no Tx CSI and thus no feedback is required), we consider the isotropic signaling over the wire-tap MIMO channel and characterize the set of channels on which it is optimal. It turns out to be much richer than that of the regular MIMO channel.

Proposition 4. *Consider the MIMO wire-tap channel in* (1)*. The isotropic signaling is optimal, i.e.* $\mathbf{R}^* = a\mathbf{I}$ *in* (3)*, for the set of channels* $\{\mathbf{W}_1, \mathbf{W}_2\}$ *that can be characterized as follows:*

* $\mathbf{W}_1$ *and* $\mathbf{W}_2$ *have the same (otherwise arbitrary) eigenvectors,* $\mathbf{U}_1 = \mathbf{U}_2$.

* $\mathbf{W}_1 > \mathbf{W}_2$ *so that* $\lambda_i(\mathbf{W}_1) = a_i^{-1} > \lambda_i(\mathbf{W}_2) = b_i^{-1}$*, where* $\lambda_i(\mathbf{W})$ *are ordered eigenvalues of* $\mathbf{W}$.

* *Take any* $b_1 > 0$ *and* $a_1 < b_1$ *and set*

$$\lambda = (a_1 + a)^{-1} - (b_1 + a)^{-1} > 0, \tag{27}$$

* *For* $i = 2...m$*, take any* b_i *such that*

$$b_i > \lambda a^2 (1 - \lambda a)^{-1} > 0, \tag{28}$$

and set

$$a_i = -a + (\lambda + (b_i + a)^{-1})^{-1} > 0 \tag{29}$$

This gives the complete characterization of the set of channels for which isotropic signaling is optimal.

Proof: It is straightforward to see that any channel in the given set satisfies the conditions of Theorem 2 and the corresponding optimal covariance is isotropic. The converse follows from Theorem 1, which requires $\mathbf{W}_1 > \mathbf{W}_2$, so that the optimization problem is strictly convex and thus has a unique solution. For isotropic signaling to be optimal, the corresponding KKT conditions (see the proofs of Theorems 1 and 2 in [9]) imply the conditions stated above. ■

Note that the special case of this Proposition is when $\mathbf{W}_1$ and $\mathbf{W}_2$ have identical eigenvalues, as in the case of the regular MIMO channel, but, unlike the regular channel, there is also a large set of channels with distinct eigenvalues which dictate the isotropic signaling as well. It is the interplay between the legitimate user and the eavesdropper that is responsible for this phenomenon, i.e. a non-isotropic nature of the 1st channel is compensated for by a carefully-adjusted non-isotropy of the 2nd one.

VII. Appendix

1st equality in (12) follows from (3). For 2nd equality, use

$$|\mathbf{I} + \mathbf{W}_1\mathbf{R}| \leq \prod_i (1 + \lambda_i(\mathbf{W}_1)\lambda_i(\mathbf{R})) \tag{30}$$

which follows from Theorem 3.3.14(c) in [14] with $f(x) = \ln(1 + x)$, where the eigenvalues $\lambda_i(\mathbf{W}_1), \lambda_i(\mathbf{R})$ are ordered likewise and the equality is achieved when $\mathbf{W}_1, \mathbf{R}$ have the same eigenvectors, in addition to $|\mathbf{I} + \epsilon\mathbf{R}| = \prod_i (1 + \epsilon\lambda_i(\mathbf{R}))$, so that the maximum is achieved when the eigenvectors of $\mathbf{W}_1$ and $\mathbf{R}$ are the same, $\mathbf{R}^* = \mathbf{U}_1\mathbf{\Lambda}^*\mathbf{U}_1^+$. The remaining maximization is over the eigenvalues of $\mathbf{R}$ only, i.e. the optimal power allocation in (13), which can be formulated as

$$C^*(\epsilon) = \max_{\{\lambda_i\}} \sum_i \ln \frac{1 + g_i\lambda_i}{1 + \epsilon\lambda_i}, \text{ s.t. } \lambda_i \geq 0, \sum_i \lambda_i = P_T \tag{31}$$

First, we note that this optimization problem is not convex in general (unless $\epsilon < g_m$) so that KKT conditions are not sufficient for optimality [11]. However, when projected on the set of active eigenmodes, the problem becomes convex and KKT conditions provide a unique optimum. Formally, we proceed using the 4-step method of Brinkhuis and Tikhomirov [12]:

1) Establish an existence of a global solution: since the objective is a continuous function of $\{\lambda_i\}$ and the constraint set is compact, the existence of a solution follows from Weierstrass theorem.

2) Find necessary conditions: KKT conditions are necessary for optimality (this follows from e.g. Slater condition [11]), so that a global optimum is a solution of KKT conditions.

3) Find all solutions of KKT conditions.

4) By inspection, find the global maximum.

The rest of the proof is based on the KKT conditions in [9] and follows the same steps as the proof of Theorem 2 there.

References

[1] Y. Liang, H. V. Poor and S. Shamai(Shitz), Information Theoretic Security, Foundations and Trends in Communications and Information Theory, v. 5, No. 45 (2008), pp. 355-580.

[2] P. K. Gopala, L. Lai, H. El Gamal, On the Secrecy Capacity of Fading Channels, IEEE Trans. Info. Theory, v. 54, No. 10, Oct. 2008.

[3] R. Bustin et al, An MMSE Approach to the Secrecy Capacity of the MIMO Gaussian Wiretap Channel, EURASIP Journal on Wireless Communications and Networking, 2009, Article ID 370970.

[4] T. Liu, S. Shamai (Shitz), A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel, IEEE Trans. Info. Theory, v. 55, No. 6, June 2009.

[5] A. Khisti, G.W. Wornell, Secure Transmission With Multiple Antennas—Part I: The MISOME Wiretap Channel, IEEE Trans. Info. Theory, v. 56, No. 7, July 2010.

[6] A. Khisti, G.W. Wornell, Secure Transmission With Multiple Antennas—Part II: The MIMOME Wiretap Channel, IEEE Trans. Info. Theory, v. 56, No. 11, Nov. 2010.

[7] F. Oggier, B. Hassibi, The Secrecy Capacity of the MIMO Wiretap Channel, IEEE Trans. Info. Theory, v. 57, No. 8, Aug. 2011.

[8] Z. Li, W. Trappe, and R. Yates, Secret communication via multi-antenna transmission, Conf. Inform. Sci., Syst. (CISS), Baltimore, MD, Mar. 2007.

[9] S. Loyka, C.D. Charalambous, On Optimal Signaling over Secure MIMO Channels, IEEE ISIT-12, Boston, USA, July 2012.

[10] J. Li, A. Petropulu, Transmitter Optimization for Achieving Secrecy Capacity in Gaussian MIMO Wiretap Channels, arXiv:0909.2622v1, Sep 2009.

[11] S. Boyd, L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.

[12] J. Brinkhuis, V. Tikhomirov, Optimization: Insights and Applications, Princeton University Press, 2005.

[13] F. Zhang, Matrix Theory, Springer, 1999.

[14] R.A. Horn, C.R. Johnson, Topics in Matrix Analysis, Cambridge University Press, 1991.