Optimal Full-Rank Signaling Over MIMO Wiretap Channels Under Interference Constraint

Sergey Loyka and Limeng Dong

***Abstract*—A closed-form full-rank solution for an optimal transmit covariance matrix over a strictly degraded MIMO wiretap channel and its secrecy capacity are obtained under an interference constraint, in addition to the transmit power constraint. A number of its properties are pointed out. The regimes when one of the constraints is inactive are studied. The interference constraint affects significantly the optimal covariance and induces its new properties, which cannot be found under the total transmit power constraint only.**

***Index Terms*—MIMO, wiretap channel, secrecy capacity, interference.**

I. Introduction

BROADCAST nature of wireless channels makes them susceptible to eavesdropping and other security threats, especially in multi-user environments, where multiple systems/users share the same spectrum. In this context, physical-layer security is a valuable addition to cryptographic techniques, which exploits the properties of wireless channels to ensure secrecy of communications [1]. The secrecy capacity of the Gaussian MIMO wiretap channel (WTC) has been established in [2] and [3] as an optimization problem over the input covariance, and the respective optimal transmit (Tx) covariance matrix has been found in many cases [4], [5], while the general case remains an open problem. On the contrary, little is known about the secrecy capacity of MIMO WTC in interference-limited settings (e.g., cognitive radio [6]), beyond the MISO case [7]. Aggressive frequency re-use and non-orthogonal multiple access (NOMA) schemes, envisioned in 5G systems as a key technology [8], call for a detailed study of interference-constrained settings.

In this letter, we obtain a closed-form full-rank solution for the optimal transmit covariance matrix and the respective secrecy capacity under the total transmit as well as interference power constraints (TPC and IPC) for a strictly-degraded channel. We also obtain sufficient conditions for this solution to hold as well as sufficient conditions for either constraint to be inactive. In stark contrast to the regular MIMO WTC, this channel in the interference-constrained setting induces a number of unusual properties of the optimal covariance matrix. In particular, an optimal covariance may be not unique and of full-rank even when the channel is not strictly degraded, and the TPC may be inactive (but at least one constraint is always active unless the secrecy capacity is zero). These unusual properties are due to the interplay between the TPC and IPC and disappear when the latter is removed or relaxed. This demonstrates that neither constraint can be "absorbed" into another in general, as was sometimes suggested in [6].

Notations: bold capitals denote matrice while bold lower-case letters denote column vectors; $\boldsymbol{R}^+$ is the Hermitian conjugation of $\boldsymbol{R}$; $\boldsymbol{R} \geq 0$ means that $\boldsymbol{R}$ is positive semi-definite, $|\boldsymbol{R}|$ and $\mathrm{tr}(\boldsymbol{R})$ denote determinant and trace respectively, while $\lambda_i(\boldsymbol{R})$ is i-th eigenvalue of $\boldsymbol{R}$; unless indicated otherwise, eigenvalues are in decreasing order, $\lambda_1 \geq \lambda_2 \geq \cdots$; $\boldsymbol{I}$ is an identity matrix of appropriate size.

II. Channel Model and Secrecy Capacity

Let us consider the standard AWGN wiretap channel model where a transmitter (Tx) sends confidential information to a legitimate receiver (Rx) while an eavesdropper (Ev) intercepts the transmission. The objective is to ensure reliable communications between the Tx and Rx (the reliability criterion) while keeping the Ev ignorant about transmitted data (the secrecy criterion). The secrecy capacity is the largest transmission rate subject to the reliability and secrecy criteria [1], to which power constraint can also be added.

In the discrete-time AWGN MIMO channel model, the signals received by the Rx and the Ev can be expressed as

$$\boldsymbol{y}_1 = \boldsymbol{H}_1\boldsymbol{x} + \boldsymbol{\xi}_1, \quad \boldsymbol{y}_2 = \boldsymbol{H}_2\boldsymbol{x} + \boldsymbol{\xi}_2 \tag{1}$$

where $\boldsymbol{y}_1, \boldsymbol{y}_2$ are the respective received signals, $\boldsymbol{x}$ is the transmitted signal, $\boldsymbol{\xi}_1, \boldsymbol{\xi}_2$ represent zero-mean unit-variance i.i.d. noise at the Rx and Ev end respectively; $\boldsymbol{H}_1, \boldsymbol{H}_2$ are the channel matrices collecting channel gains from the Tx to the Rx and Ev respectively. The Tx has m antennas, while the Rx and Ev have n_1 and n_2 antennas. In addition to this and following the interference-constrained model, there is a primary receiver (PR, or another user in a NOMA system) whose received signal is

$$\boldsymbol{y}_3 = \boldsymbol{H}_3\boldsymbol{x} + \boldsymbol{\xi}_3 \tag{2}$$

where $\boldsymbol{H}_3$ and $\boldsymbol{\xi}_3$ are the channel matrix and noise of the PR. For further use, let $\boldsymbol{W}_k = \boldsymbol{H}_k^+\boldsymbol{H}_k$, $k = 1 \cdots 3$. Following [1]–[3], we assume that full CSI is available to the Tx, Rx and Ev.

Manuscript received December 7, 2017; revised January 6, 2018; accepted January 9, 2018. Date of publication January 15, 2018; date of current version August 21, 2018. The associate editor coordinating the review of this paper and approving it for publication was J. Xu. *(Corresponding author: Sergey Loyka.)*

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

L. Dong is with the School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China (e-mail: dlm_nwpu@hotmail.com).

Digital Object Identifier 10.1109/LWC.2018.2793264

In the interference-constrained setting, the transmission is subject to power and interference constraints, so that any Tx covariance matrix $\boldsymbol{R} = E\{\boldsymbol{x}\boldsymbol{x}^+\}$ must satisfy the total power (TPC) and interference (IPC) constraints:

$$\mathrm{tr}(\boldsymbol{R}) \le P_T,\ \ \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}) \le P_I \tag{3}$$

where $P_T,\ P_I$ are the maximum allowed Tx and interference powers respectively. The interference power constraint $\mathrm{tr}\,\boldsymbol{H}_3\boldsymbol{R}\boldsymbol{H}_3^+ = \mathrm{tr}\,\boldsymbol{W}_3\boldsymbol{R} \le P_I$ ensures that the total interference power $\mathrm{tr}\,\boldsymbol{H}_3\boldsymbol{R}\boldsymbol{H}_3^+$ at the PR does not exceed the threshold P_I so that its performance is not distorted. The secrecy capacity of the interference-limited WTC is defined operationally as the largest achievable rate subject to the power, reliability, secrecy and interference constraints simultaneously (see [1] for more details in the context of the regular WTC and [7] in the interference-constrained setting).

The secrecy capacity of the Gaussian MIMO WTC in the interference-constrained setting above can be characterized, following the approach in [2], as follows [9]:

$$C_s = \max_{\boldsymbol{R}\in S_{\boldsymbol{R}}} R_-(\boldsymbol{R}) \tag{4}$$

where

$$R_-(\boldsymbol{R}) = \ln|\boldsymbol{I} + \boldsymbol{W}_1\boldsymbol{R}| - \ln|\boldsymbol{I} + \boldsymbol{W}_2\boldsymbol{R}|,$$
$$S_{\boldsymbol{R}} = \{\boldsymbol{R} : \boldsymbol{R} \ge \boldsymbol{0},\ \mathrm{tr}(\boldsymbol{R}) \le P_T,\ \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}) \le P_I\} \tag{5}$$

Unfortunately, no closed-form solution is known to this optimization problem in the general case. Even in the MISO case, where the optimal covariance is known to be rank-one [7], no closed-form solution is known either. A challenging nature of this problem is in part due to its non-convex nature (unless the channel is degraded, for which case no general closed-form solution is known either, even without the IPC). In the following, we establish a closed-form full-rank solution to this problem for a strictly-degraded WTC and explore a number of its properties.

III. Full-Rank Optimal Signalling Under Interference Constraint

The following Theorem gives a closed-form full-rank solution for an optimal Tx covariance matrix in (4) under the TPC and the IPC in (3).

Theorem 1: Let the wiretap channel be strictly degraded, $\boldsymbol{W}_1 > \boldsymbol{W}_2$. When the optimal Tx covariance matrix in (4) is of full-rank, it can be expressed as

$$\boldsymbol{R}^* = \boldsymbol{W}_\mu^{-\frac{1}{2}}\boldsymbol{U}\boldsymbol{\Lambda}_1\boldsymbol{U}^+\boldsymbol{W}_\mu^{-\frac{1}{2}} - \boldsymbol{W}_1^{-1} \tag{6}$$

where $\boldsymbol{W}_\mu = \mu\boldsymbol{I} + \mu_3\boldsymbol{W}_3$; $\mu,\ \mu_3 \ge 0$ are dual variables (Lagrange multipliers) responsible for the TPC and IPC respectively; the columns of unitary matrix $\boldsymbol{U}$ are the eigenvectors of

$$\widetilde{\boldsymbol{Z}} = \widetilde{\boldsymbol{W}}_2 + \widetilde{\boldsymbol{W}}_2(\widetilde{\boldsymbol{W}}_1 - \widetilde{\boldsymbol{W}}_2)^{-1}\widetilde{\boldsymbol{W}}_2 \tag{7}$$

where $\widetilde{\boldsymbol{W}}_k = \boldsymbol{W}_\mu^{-\frac{1}{2}}\boldsymbol{W}_k\boldsymbol{W}_\mu^{-\frac{1}{2}}$, $k = 1, 2$; $\widetilde{\boldsymbol{R}} = \boldsymbol{W}_\mu^{\frac{1}{2}}\boldsymbol{R}\boldsymbol{W}_\mu^{\frac{1}{2}}$, and $\boldsymbol{\Lambda}_1 = \mathrm{diag}\{\lambda_{1i}\} > 0$ is a diagonal positive-definite matrix, where

$$\lambda_{1i} = 2\left(\sqrt{1 + 4\lambda_{zi}} + 1\right)^{-1} \tag{8}$$

and $\lambda_{zi} \ge 0$ are the eigenvalues of $\widetilde{\boldsymbol{Z}}$. The dual variables $\mu,\ \mu_3 \ge 0$ are found as solutions of the following equations:

$$\mu(\mathrm{tr}(\boldsymbol{R}^*) - P_T) = 0,\ \ \mu_3(\mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}^*) - P_I) = 0 \tag{9}$$

The corresponding secrecy capacity is

$$C_s = \ln\frac{|\widetilde{\boldsymbol{W}}_1||\boldsymbol{\Lambda}_1|}{|\boldsymbol{I} - \widetilde{\boldsymbol{W}}_2(\widetilde{\boldsymbol{W}}_1^{-1} - \boldsymbol{U}\boldsymbol{\Lambda}_1\boldsymbol{U}^+)|} = \ln\frac{|\boldsymbol{W}_1|}{|\boldsymbol{W}_2|} + \ln\frac{|\boldsymbol{\Lambda}_1|}{|\boldsymbol{\Lambda}_2|} \tag{10}$$

where $\boldsymbol{\Lambda}_2 = \boldsymbol{\Lambda}_1 + \mathrm{diag}\{\lambda_{zi}^{-1}\}$ and the 2nd equality holds when $\boldsymbol{W}_2 > 0$.

Proof: Based on the KKT conditions (see [10] for a background on these conditions), which are sufficient for optimality in this case. When the optimal covariance is of full-rank, the KKT conditions can be expressed as:

$$(\boldsymbol{I} + \boldsymbol{W}_1\boldsymbol{R})^{-1}\boldsymbol{W}_1 - \boldsymbol{W}_2(\boldsymbol{I} + \boldsymbol{R}\boldsymbol{W}_2)^{-1} = \boldsymbol{W}_\mu \tag{11}$$
$$\mu(\mathrm{tr}(\boldsymbol{R}) - P_T) = 0,\ \ \mu_3(\mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}) - P_I) = 0 \tag{12}$$
$$\mu,\ \ \mu_3 \ge 0,\ \ \boldsymbol{R} > 0 \tag{13}$$
$$\mathrm{tr}(\boldsymbol{R}) \le P_T,\ \ \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}) \le P_I \tag{14}$$

where (11) is the stationarity condition, (12) are the complementary slackness conditions, (13) and (14) are primal and dual feasibility conditions. Note that these conditions are sufficient for optimality under $\boldsymbol{W}_1 - \boldsymbol{W}_2 > 0$ (since the problem is convex and Slater's condition holds). (11) can be transformed to

$$(\boldsymbol{I} + \boldsymbol{W}_1\boldsymbol{R})\boldsymbol{W}_\mu(\boldsymbol{I} + \boldsymbol{R}\boldsymbol{W}_2) = \boldsymbol{W}_1 - \boldsymbol{W}_2 \tag{15}$$

from which it follows that $\boldsymbol{W}_\mu > 0$, i.e., either the TPC is active ($\mu > 0$) or/and the IPC is active ($\mu_3 > 0$) and $\boldsymbol{W}_3 > 0$, so that singular $\boldsymbol{W}_3$ ensures that the TPC is always active. Consider now the case of $\boldsymbol{W}_2 > 0$ (the singular case will follow from the continuity argument). (11) can be expressed as

$$(\boldsymbol{W}_1^{-1} + \boldsymbol{R})^{-1} - (\boldsymbol{W}_2^{-1} + \boldsymbol{R})^{-1} = \boldsymbol{W}_\mu$$

so that

$$\widetilde{\boldsymbol{R}}_1^{-1} - \widetilde{\boldsymbol{R}}_2^{-1} = \boldsymbol{I} \tag{16}$$

where $\widetilde{\boldsymbol{R}}_k = \widetilde{\boldsymbol{W}}_k^{-1} + \widetilde{\boldsymbol{R}}$, from which it follows that $\widetilde{\boldsymbol{R}}_1,\ \widetilde{\boldsymbol{R}}_2$ have the same eigenvectors and hence $\widetilde{\boldsymbol{R}}_k = \boldsymbol{U}\boldsymbol{\Lambda}_k\boldsymbol{U}^+$, where $\boldsymbol{U}$ is the unitary matrix of eigenvectors and $\boldsymbol{\Lambda}_k$ is a diagonal matrix of eigenvalues. Since

$$\widetilde{\boldsymbol{R}}_1 - \widetilde{\boldsymbol{R}}_2 = \widetilde{\boldsymbol{W}}_1^{-1} - \widetilde{\boldsymbol{W}}_2^{-1} \tag{17}$$

$\boldsymbol{U}$ is also the matrix of eigenvectors of $\widetilde{\boldsymbol{W}}_1^{-1} - \widetilde{\boldsymbol{W}}_2^{-1}$, which are also the eigenvectors of $\widetilde{\boldsymbol{Z}} = (\widetilde{\boldsymbol{W}}_2^{-1} - \widetilde{\boldsymbol{W}}_1^{-1})^{-1}$. It follows from (16), (17) that

$$\boldsymbol{\Lambda}_1^{-1} - \boldsymbol{\Lambda}_2^{-1} = \boldsymbol{I},\ \ \boldsymbol{\Lambda}_1 - \boldsymbol{\Lambda}_2 = -\mathrm{diag}\{\lambda_i^{-1}(\widetilde{\boldsymbol{Z}})\} \tag{18}$$

from which (8) follows. Since $\widetilde{\boldsymbol{R}}_1 = \boldsymbol{U}\boldsymbol{\Lambda}_1\boldsymbol{U}^+ = \widetilde{\boldsymbol{W}}_1^{-1} + \widetilde{\boldsymbol{R}}$, (6) follows. (10) follows by using (6) in (4). ∎

Note that (9) is a system of two nonlinear equations in the dual variables $\mu,\ \mu_3$, which are hardly possible to solve analytically in the general case. However, they can be solved

numerically. An alternative approach is to consider $\mu,\ \mu_3$ as independent variables parameterizing $P_T,\ P_I$. Further note that when the IPC and the secrecy constraint are relaxed, i.e., $\boldsymbol{W}_2 = \boldsymbol{W}_3 = 0$, the solution in (6) reduces to the standard water-filling solution for the regular MIMO channel: $\boldsymbol{R}^* = \mu^{-1}\boldsymbol{I} - \boldsymbol{W}_1^{-1}$, as it should be.

It follows from the KKT conditions that at least one constraint is always active (unless the capacity is zero) so that both constraints cannot be inactive simultaneously and that, for $\boldsymbol{W}_1 - \boldsymbol{W}_2 > 0$, the TPC is inactive only if $\boldsymbol{W}_3 > 0$, i.e., singular $\boldsymbol{W}_3$ ensures that the TPC is always active in a strictly-degraded channel.

While Theorem 1 gives a closed-form full-rank solution (up to the dual variables), it does not specify conditions for this solution to hold (beyond $\boldsymbol{W}_1 - \boldsymbol{W}_2 > 0$). The following propositions give sufficient conditions for this full-rank solution as well as conditions for either constraint to be inactive.

Proposition 1: Let $\boldsymbol{W}_1 > \boldsymbol{W}_2$,

$$P_T > P_{T0} \triangleq 2\alpha \sum_i \left(\sqrt{1 + 4\alpha\lambda_i(\boldsymbol{Z})} + 1\right)^{-1} - \mathrm{tr}(\boldsymbol{W}_1^{-1}) \quad (19)$$

where $\alpha = (\lambda_1(\boldsymbol{Z}) + \lambda_m(\boldsymbol{W}_1))\lambda_m^{-2}(\boldsymbol{W}_1)$,

$$\boldsymbol{Z} = \boldsymbol{W}_2 + \boldsymbol{W}_2(\boldsymbol{W}_1 - \boldsymbol{W}_2)^{-1}\boldsymbol{W}_2 \quad (20)$$

and, in addition,

$$P_I \geq P_{I0} \triangleq \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}^*(\mu, 0)) \quad (21)$$

where $\boldsymbol{R}^*(\mu, \mu_3)$ is the optimal covariance in (6) as a function of the dual variables $\mu,\ \mu_3$, and $\mu > 0$ is the unique solution of the following equation

$$\frac{2}{\mu}\sum_i \left(\sqrt{1 + \frac{4\lambda_i(\boldsymbol{Z})}{\mu}} + 1\right)^{-1} = P_T + \mathrm{tr}(\mathbf{W}_1^{-1}) \quad (22)$$

Then, the optimal covariance in (4) is $\boldsymbol{R}^*(\mu, 0)$ and of full-rank, the TPC is active ($\mu > 0$) and the IPC is inactive ($\mu_3 = 0$). If, under (19) and (22), $P_I < P_{I0}$, then the IPC is also active, i.e., the bound in (21) is sharp.

Proof: The secrecy capacity under the IPC can be upper-bounded by that without the IPC:

$$C_s \leq \max_{\boldsymbol{R} \in S'_{\boldsymbol{R}}} R_-(\boldsymbol{R}) \quad (23)$$

where the feasible set $S'_{\boldsymbol{R}}$ includes the TPC only:

$$S'_{\boldsymbol{R}} = \{\boldsymbol{R} : \boldsymbol{R} \geq \boldsymbol{0},\ \mathrm{tr}(\boldsymbol{R}) \leq P_T\} \quad (24)$$

Reference [5, Th. 5.2] gives a full-rank solution to the latter problem under the conditions in (22) and (19), which corresponds to $\boldsymbol{R}^*(\mu, 0)$ in (6). The condition in (21) ensures that the IPC is also satisfied by $\boldsymbol{R}^*(\mu, 0)$ and hence the upper bound in (23) is achieved with equality, so that $\boldsymbol{R}^*(\mu, 0)$ is also optimal under the TPC and IPC.

Since the left-hand side of (22) is a monotonically-decreasing function of $\mu \geq 0$, which varies from 0 to ∞, a positive solution always exists and is unique. The bisection method [10] can be used to efficiently solve (22). ■

Note that the condition in (21) defines a large-IPC regime $P_I \geq P_{I0}$, when the IPC is not active and hence does not affect the optimal signaling strategy. Since the conditions in (19) and (21) are rather involved, we give below simpler (albeit not sharp) conditions, which do not depend on dual variables.

Corollary 1: Let $\boldsymbol{W}_1 > \boldsymbol{W}_2$, and

$$P_T > \frac{m\lambda_1(\boldsymbol{Z})}{\lambda_m^2(\boldsymbol{W}_1)} + \frac{m-1}{\lambda_m(\boldsymbol{W}_1)} \quad (25)$$

$$P_I \geq \lambda_1(\boldsymbol{W}_3)P_T \quad (26)$$

Then, the optimal covariance in (4) is $\boldsymbol{R}^*(\mu, 0)$ and of full-rank, the TPC is active, $\mu > 0$ is found from (22) and the IPC is inactive ($\mu_3 = 0$).

Proof: P_{T0} in (19) can be upper-bounded as follows:

$$P_{T0} \leq \alpha \cdot m - \mathrm{tr}(\boldsymbol{W}_1^{-1}) \leq \frac{m\lambda_1(\boldsymbol{Z})}{\lambda_m^2(\boldsymbol{W}_1)} + \frac{m-1}{\lambda_m(\boldsymbol{W}_1)} \quad (27)$$

so that (25) implies (19). Likewise, $P_{I0} \leq \lambda_1(\boldsymbol{W}_3)P_T$, so that (26) implies (21). ■

The next proposition characterises a large-TPC regime, via (30), when the total power constraint is not active and the IPC alone determines the optimal signaling strategy.

Proposition 2: Let $\boldsymbol{W}_1 - \boldsymbol{W}_2 > 0,\ \boldsymbol{W}_3 > 0$, and

$$P_I > P_{I1} \triangleq 2\alpha' \sum_i \left(\sqrt{1 + 4\alpha'\lambda_i(\boldsymbol{Z}')} + 1\right)^{-1} - \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{W}_1^{-1}) \quad (28)$$

where $\alpha' = (\lambda_1(\boldsymbol{Z}') + \lambda_m(\boldsymbol{W}_1'))\lambda_m^{-2}(\boldsymbol{W}_1')$, $\boldsymbol{Z}' = \boldsymbol{W}_3^{-\frac{1}{2}}\boldsymbol{Z}\boldsymbol{W}_3^{-\frac{1}{2}}$, $\boldsymbol{W}_k' = \boldsymbol{W}_3^{-\frac{1}{2}}\boldsymbol{W}_k\boldsymbol{W}_3^{-\frac{1}{2}}$, $k = 1, 2$, and let $\mu_3 > 0$ be a unique solution of the following equation

$$\frac{2}{\mu_3}\sum_i \left(\sqrt{1 + \frac{4\lambda_i(\boldsymbol{Z}')}{\mu_3}} + 1\right)^{-1} = P_I + \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{W}_1^{-1}) \quad (29)$$

and

$$P_T \geq P_{T1} \triangleq \mathrm{tr}(\boldsymbol{R}^*(0, \mu_3)) \quad (30)$$

Then, the optimal covariance in (4) is $\boldsymbol{R}^*(0, \mu_3)$ and of full-rank, the IPC is active ($\mu_3 > 0$) and the TPC is inactive ($\mu = 0$). If, under (28) and (29), $P_T < P_{T1}$, then the TPC is also active, i.e., the bound in (30) is sharp.

Proof: The secrecy capacity under the TPC and IPC can be upper-bounded by that without the TPC:

$$C_s \leq \max_{\boldsymbol{R} \in S'_{\boldsymbol{R}}} R_-(\boldsymbol{R}) \quad (31)$$

where the feasible set $S'_{\boldsymbol{R}}$ includes the IPC only:

$$S'_{\boldsymbol{R}} = \{\boldsymbol{R} : \boldsymbol{R} \geq \boldsymbol{0},\ \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}) \leq P_I\}$$

For the latter optimization problem, the KKT conditions can be expressed, using (11)-(14) with $\mu = 0$, as

$$(\boldsymbol{I} + \boldsymbol{W}_1'\boldsymbol{R}')^{-1}\boldsymbol{W}_1' - (\boldsymbol{I} + \boldsymbol{W}_2'\boldsymbol{R}')^{-1}\boldsymbol{W}_2' = \mu_3\boldsymbol{I} \quad (32)$$

$$\mu_3(\mathrm{tr}\,\boldsymbol{R}' - P_I) = 0 \quad (33)$$

$$\mu_3 \geq 0,\ \boldsymbol{R}' \geq 0,\ tr\boldsymbol{R}' \leq P_I \quad (34)$$

where $\boldsymbol{R}' = \boldsymbol{W}_3^{\frac{1}{2}}\boldsymbol{R}\boldsymbol{W}_3^{\frac{1}{2}}$. Using the same steps as in the proof of Theorem 1, one concludes that the optimal covariance for this problem is $\boldsymbol{R}^*(0, \mu_3)$. The condition in (28) ensures that

$\boldsymbol{R}^*(0,\mu_3) > 0$; (29) ensures that $\mathrm{tr}\,\boldsymbol{W}_3\boldsymbol{R} = P_I$ so that (33) and (34) also hold. Under (30), the upper bound in (31) is attained with equality and hence is the secrecy capacity and $\boldsymbol{R}^*(0,\mu_3)$ is the optimal covariance. ■

The next corollary gives more explicit (albeit less general) conditions than those in Proposition 2, which do not depend on dual variables.

Corollary 2: Let $\boldsymbol{W}_1 - \boldsymbol{W}_2 > 0$, $\boldsymbol{W}_3 > 0$, and

$$P_I > \frac{m\lambda_1(\boldsymbol{Z}')}{\lambda_m^2(\boldsymbol{W}_1')} + \frac{m-1}{\lambda_m(\boldsymbol{W}_1')} \tag{35}$$

$$P_T \geq P_I/\lambda_m(\boldsymbol{W}_3) \tag{36}$$

Then, the optimal covariance in (4) is $\boldsymbol{R}^*(0,\mu_3)$ and of full-rank, the IPC is active, $\mu_3 > 0$ is found from (29) and the TPC is inactive ($\mu = 0$).

Proof: P_{I1} can be upper-bounded as follows:

$$P_{I1} \leq \frac{m\lambda_1(\boldsymbol{Z}')}{\lambda_m^2(\boldsymbol{W}_1')} + \frac{m-1}{\lambda_m(\boldsymbol{W}_1')} \tag{37}$$

so that (35) implies (28). Likewise, $P_I \geq \mathrm{tr}(\boldsymbol{W}_3\boldsymbol{R}^*) \geq \lambda_m(\boldsymbol{W}_3)\,\mathrm{tr}(\boldsymbol{R}^*)$, so that (36) implies (30). ■

IV. Examples

Example 1: Fig. 1 illustrates the dependence of the secrecy capacity on the total transmit and interference powers for the following channels:

$$\boldsymbol{W}_1 = \begin{bmatrix} 1.5 & 0.5 \\ 0.5 & 1.5 \end{bmatrix}, \boldsymbol{W}_2 = \begin{bmatrix} 0.35 & 0.15 \\ 0.15 & 0.35 \end{bmatrix}, \boldsymbol{W}_3 = \begin{bmatrix} 0.3 & 0.1 \\ 0.1 & 0.3 \end{bmatrix}$$

Note that the full-rank solution becomes valid already at SNR $= -5$ dB, i.e., not high at all, and that P_I affects significantly the capacity at the high-SNR (saturation) regime, which corresponds to inactive TPC, as in Proposition and Corollary 2. While there is also saturation in the secrecy capacity without the IPC as SNR $\to \infty$ (see [2], [5]), the IPC makes 2 key differences: (i) it lowers the saturation level (as obvious from Fig. 1), and (ii) it makes the saturation effect hard rather than soft, i.e., the saturation takes place at finite SNR (about 6 and 12 dB respectively, after which the capacity does not increase at all) and not only asymptotically, slowly approaching the limit as SNR $\to \infty$, without the IPC.

Example 2: To see the unusual properties of an optimal covariance in the interference-constrained MIMO WTC, consider the following example:

$$\boldsymbol{W}_1 = \mathrm{diag}\{a,0\},\ \ \boldsymbol{W}_2 = \mathrm{diag}\{b,0\},\ \ \boldsymbol{W}_3 = \mathrm{diag}\{c,0\}$$

where $a > b > 0$, $c > 0$, and let $cP_T > P_I$. It is straightforward to see that the optimal covariance in this setting is of the form $\boldsymbol{R}^* = \mathrm{diag}\{p_1,p_2\}$, where $p_1 = P_I/c$, $0 \leq p_2 \leq P_T - P_I/c$, so that (i) optimal covariance is not unique (but the capacity is), (ii) the TPC can be inactive (if $p_2 < P_T - P_I/c$), and (iii) $\boldsymbol{R}^*$ can be full-rank even though $\boldsymbol{W}_1 - \boldsymbol{W}_2$ in not full-rank. These unusual properties are in stark contrast with those of the regular MIMO WTC (see [5]) and are ultimately due to the interplay between the TPC and the IPC. They disappear if the IPC is removed or relaxed (e.g., if $P_I > cP_T$), in which case $\boldsymbol{R}^* = \mathrm{diag}\{P_T,0\}$. This shows that neither constraint can be absorbed into the other in the general case, as sometimes suggested in the literature.

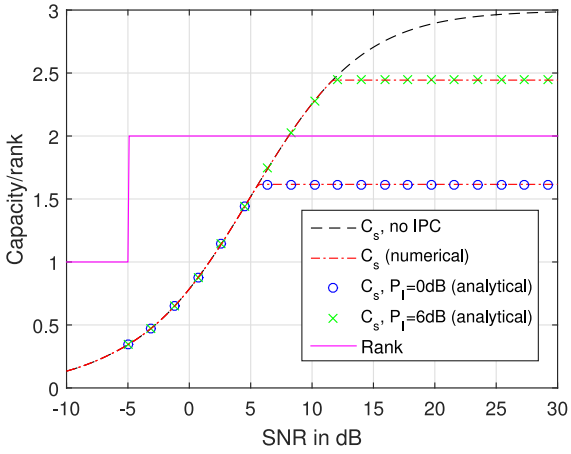

Fig. 1. Secrecy capacity C_s [nat/s/Hz] vs. the SNR (= Tx power) for different values of P_I. Analytical solution in Theorem 1 agrees well with numerical results.

Based on these examples, one concludes that the optimal covariance of the interference-constrained MIMO WTC has a number of very different properties from that of the classical MIMO WTC (see [5] for the latter). In particular,

1. Full-rank solution is not necessarily unique.
2. $\boldsymbol{W}_1 - \boldsymbol{W}_2 > 0$ is not necessary for full-rank optimal covariance.
3. The TPC can be inactive.

The last property also follows from Proposition 2 and Corollary 2. This shows that the interference constraint can affect the optimal signaling strategy in a very significant way and cannot be absorbed into the TPC or vice versa.

References

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

[2] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory.*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[3] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Info. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[4] J. Li and A. Petropulu, "Multiple antennas for physical layer secrecy," in *Trends in Digital Signal Processing*, Y. C. Lim *et al.*, Eds. Singapore: Pan Stanford, 2015.

[5] S. Loyka and C. D. Charalambous, "Secrecy rate maximization in Gaussian MIMO wiretap channels," in *Information Theoretic Security and Privacy of Information Systems*, R. F. Schaefer *et al.*, Eds. New York, NY, USA: Cambridge Univ. Press, 2017.

[6] G. Scutari, D. P. Palomar, and S. Barbarossa, "Cognitive MIMO radio," *IEEE Signal Process. Mag.*, vol. 25, no. 6, pp. 46–59, Nov. 2008.

[7] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[8] M. Shafi *et al.*, "5G: A tutorial overview of standards, trials, challenges, deployment, and practice," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 6, pp. 1201–1221, Jun. 2017.

[9] L. Dong, S. Loyka, and Y. Li, "The operational secrecy capacity of cognitive radio MIMO channel," in *Proc. 15th Can. Workshop Inf. Theory*, Quebec City, QC, Canada, Jun. 2017, pp. 1–5.

[10] S. P. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.