Gaussian MIMO Wiretap Channel Under Receiver Side Power Constraints

Karim Banawan Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland College Park, MD 20742
kbanawan@umd.edu *ulukus@umd.edu*

Abstract—**We consider the multiple-input multiple-output (MIMO) wiretap channel under a minimum receiver-side power constraint in addition to the usual maximum transmitter-side power constraint. This problem is motivated by energy harvesting communications with wireless energy transfer, where an added goal is to deliver a minimum amount of energy to a receiver in addition to delivering secure data to another receiver. In this paper, we characterize the exact secrecy capacity of the MIMO wiretap channel under transmitter and receiver-side power constraints. We first show that solving this problem is equivalent to solving the secrecy capacity of a wiretap channel with a double-sided correlation matrix constraint on the channel input. We show the converse by extending the channel enhancement technique to our case. We present two achievable schemes that achieve the secrecy capacity: the first achievable scheme uses a Gaussian codebook with a fixed mean, and the second achievable scheme uses artificial noise (or cooperative jamming) together with a Gaussian codebook. The role of the mean or the artificial noise is to enable energy transfer without sacrificing from the secure rate. This is the first instance of a channel model where either the use of a mean signal or use of channel prefixing via artificial noise is strictly necessary in the MIMO wiretap channel.**

I. Introduction

Most existing literature on Gaussian channels is based on a transmitter-side average power constraint. This constraint models the *maximum* allowable power at the transmitter-side. Gastpar [1] was the first to consider a receiver-side power constraint. In [1], he considered a *maximum* receiver-side power constraint motivated by the desire to limit the received interference in a band in a cognitive radio application. He observed that, while the solution does not change with respect to a classical transmitter-side power constraint for a single-input single-output (SISO) channel, it changes significantly for a multiple-input multiple-output (MIMO) channel. Subsequently, Varshney [2] considered a *minimum* receiver-side power constraint motivated by the desire to transport both information and energy simultaneously over a wireless channel. This *minimum* receiver-side power constraint signified the power (in addition to data) transferred to the receiver by the same physical signal. Varshney as well observed that while the solution does not change with respect to a classical transmitter-side power constrained SISO channel, it changes significantly with respect to a classical transmitter-side amplitude constrained SISO channel [3].

In this paper, we consider a multi-user and multi-objective version of the problem considered by Gastpar and Varshney. In particular, we consider a MIMO wiretap channel where the transmitter wishes to have secure communication with a legitimate receiver in the presence of an eavesdropper. In this model, messages need to be sent at the highest reliable rate to the legitimate receiver with perfect secrecy from the eavesdropper. We impose the usual transmitter-side power constraint in addition to a receiver-side power constraint. While we can impose two receiver-side power constraints, one at the legitimate receiver, and one at the eavesdropper, in this paper, we limit our presentation to imposing a receiver-side power constraint only at one of the receivers, which we choose as the eavesdropper. Therefore, our model generalizes the receiver-side power constraint of Gastpar and Varshney from a single-user setting to a multi-user scenario of a wiretap channel with three nodes, and also to a multi-objective setting where we have both reliability and security constraints.

The wiretap channel was first considered by Wyner in [4], where he determined the rate-equivocation region of a degraded wiretap channel. This model was generalized to arbitrary, not necessarily degraded, channels by Csiszar and Korner in [5], where they determined the rate-equivocation region of the most general wiretap channel. The SISO Gaussian wiretap channel, which is degraded, was considered under a transmitter-side power constraint in [6], which showed that Gaussian signalling is optimal. The MIMO Gaussian wiretap channel was considered for the 2-2-1 case in [7], for the general case in [8], [9], under a transmitter-side power constraint. These references showed that channel prefixing is not needed, even though the MIMO wiretap channel is not degraded, and Gaussian signalling is optimal. An interesting alternative proof is given in [10] based on the *channel enhancement* technique developed in [11]. Reference [10] considers the MIMO wiretap channel under a transmitter-side *covariance constraint* which is more general than a transmitter-side power constraint.

In this paper, we characterize the secrecy capacity of the general MIMO wiretap channel under a receiver-side power constraint at the eavesdropper. The extensions to receiver-side power constraint at the legitimate receiver, and dual receiver-side power constraints at both receivers are not presented in this paper due to space constraints. In this paper, we first show that, solving the secrecy capacity of the MIMO wiretap channel under a transmitter-side *maximum* power constraint

This work was supported by NSF Grants CNS 13-14733, CCF 14-22111 and CCF 14-22129.

and a receiver-side *minimum* power constraint is equivalent to solving the secrecy capacity of a MIMO wiretap channel under a *double-sided* correlation matrix constraint on the channel input at the transmitter. This is a generalization of the approach of [10], [11], which states that solving the capacity under a transmitter-side *maximum* power constraint is equivalent to solving the capacity under a transmitter-side maximum covariance constraint. We then generalize the channel enhancement technique of [10], [11] to the case of *double-sided* correlation matrix constraint. This gives us the converse. We next show that the rates given in the converse can be achieved by two different achievable schemes: a *mean* based scheme where the transmitter uses a Gaussian codebook with a fixed mean, and an *artificial noise* (or cooperative jamming [12]) based scheme, which uses Gaussian channel prefixing with a Gaussian codebook. The role of the mean or the artificial noise is to enable energy transfer without sacrificing from the secure rate; this helps achieving the receiver-side power constraint by sending non-message carrying signals. This is the first instance of a channel model where either the use of a mean signal or the use of channel prefixing via artificial noise is strictly necessary in the canonical MIMO wiretap channel. Note that while [13, Section III] shows an alternative way of achieving MIMO secrecy capacity using artificial noise, this is valid in the case of a covariance constraint, and the use of artificial noise in the MIMO wiretap channel under a transmitter-side power constraint is sub-optimal. Finally, we note that, in related work, references [14], [15] consider simultaneous information and energy transfer in a MISO wiretap channel, and focus on optimizing the performance of a specific artificial noise based achievable scheme with no claim of optimality.

II. System Model and Preliminaries

The MIMO wiretap channel with N_t antennas at the transmitter, N_r antennas at the legitimate receiver and N_e antennas at the eavesdropper is given by,

$$\mathbf{Y} = \mathbf{H}\mathbf{X} + \mathbf{W}_1 \tag{1}$$

$$\mathbf{Z} = \mathbf{G}\mathbf{X} + \mathbf{W}_2 \tag{2}$$

where $\mathbf{X} \in \mathbb{R}^{N_t}$ is the channel input, $\mathbf{Y} \in \mathbb{R}^{N_r}$ is the legitimate receiver's channel output, and $\mathbf{Z} \in \mathbb{R}^{N_e}$ is the eavesdropper's channel output; $\mathbf{W}_1$ and $\mathbf{W}_2$ are independent Gaussian random vectors with zero-mean and identity covariance matrix. The channel matrices of legitimate receiver $\mathbf{H}$ and the eavesdropper $\mathbf{G}$ are real-valued matrices of dimensions $N_r \times N_t$ and $N_e \times N_t$, respectively. The channel matrices are fixed and known to all entities. The channel input is constrained by the usual *maximum* average power constraint

$$\text{tr}(\mathbb{E}[\mathbf{X}\mathbf{X}^T]) \leq P \tag{3}$$

where P is the average power constraint. In this paper, we additionally impose a receiver-side *minimum* average power constraint

$$\text{tr}(\mathbb{E}[\mathbf{Z}\mathbf{Z}^T]) \geq E \tag{4}$$

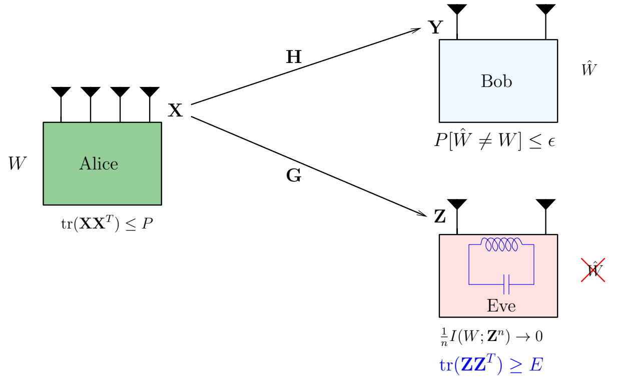
Y
H
Bob
$\hat{W}$
$P[\hat{W} \neq W] \leq \epsilon$
X
W
Alice
$\text{tr}(\mathbf{X}\mathbf{X}^T) \leq P$
G
Z
Eve
$\cancel{\hat{W}}$
$\frac{1}{n}I(W;\mathbf{Z}^n) \to 0$
$\text{tr}(\mathbf{Z}\mathbf{Z}^T) \geq E$

Fig. 1. Gaussian MIMO wiretap channel with receiver-side power constraint.

where E is the minimum power level that should be maintained at the eavesdropper's receiver. In addition, we have the following reliability constraint at the legitimate receiver

$$\mathbb{P}[\hat{W} \neq W] \leq \epsilon \tag{5}$$

where $\hat{W}$ is the estimate of the legitimate receiver of the transmitted message W based on its observation $\mathbf{Y}^n$, and the secrecy constraint on the confidential message W as

$$\lim_{n\to\infty} \frac{1}{n} I(W;\mathbf{Z}^n) = 0 \tag{6}$$

Although, we will determine the secrecy capacity under a maximum transmitter-side power constraint in (3) and a minimum receiver-side power constraint in (4), we will initially characterize the secrecy capacity under a general double-sided correlation matrix constraint as

$$\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2 \tag{7}$$

for $\mathbf{S}_1 \prec \mathbf{S}_2$, where $\preceq$ denotes the partial ordering of positive semi-definite matrices, and $\mathbf{Q} = \mathbb{E}[\mathbf{X}\mathbf{X}^T]$ is the channel input correlation matrix. We will show in a similar way to [11, Section II.B] that the secrecy capacity with a maximum transmitter-side power constraint in (3) and a minimum receiver-side power constraint in (4) can be obtained from the secrecy capacity with a more general double-sided correlation constraint in (7) by maximizing this secrecy capacity over all correlation matrices $\mathbf{S}_1 \prec \mathbf{S}_2$ that lie in the compact set $\mathcal{S}_{PE}$

$$\mathcal{S}_{PE} = \{\mathbf{S} : \text{tr}(\mathbf{S}) \leq P, \quad \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \geq \tilde{E}\} \tag{8}$$

where $\tilde{E} = E - N_e$.

We evaluate the secrecy capacity based on Csiszar-Korner secrecy capacity expression [5]

$$C_s = \max_{V,\mathbf{X}} I(V;\mathbf{Y}) - I(V;\mathbf{Z}) \tag{9}$$

where V carries the message signal and $\mathbf{X}$ is the channel input. The maximization is over all jointly distributed $(V, \mathbf{X})$ that satisfy the Markov chain $V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z}$.

III. Main Result

The main result of this paper is the exact characterization of the secrecy capacity of the MIMO wiretap channel under the transmitter-side power constraint in (3) and receiver-side power constraint in (4).

Theorem 1 *The secrecy capacity of a MIMO wiretap channel with a transmitter-side power constraint P and a receiver-side power constraint E, $C(E,P,\mathbf{H},\mathbf{G})$, is given as*

$$\begin{aligned} C(E,P,\mathbf{H},\mathbf{G}) = \max_{\mathbf{Q},\boldsymbol{\mu}} \quad & \frac{1}{2}\log|\mathbf{I}+\mathbf{H}\mathbf{Q}\mathbf{H}^T| \\ & -\frac{1}{2}\log|\mathbf{I}+\mathbf{G}\mathbf{Q}\mathbf{G}^T| \\ \text{s.t.} \quad & \operatorname{tr}(\mathbf{Q}+\boldsymbol{\mu}\boldsymbol{\mu}^T) \leq P \\ & \operatorname{tr}(\mathbf{G}(\mathbf{Q}+\boldsymbol{\mu}\boldsymbol{\mu}^T)\mathbf{G}^T) \geq \tilde{E} \quad (10) \end{aligned}$$

where $\tilde{E} = E - N_e$. This secrecy capacity is achieved by $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu},\mathbf{Q})$, i.e., with a mean but no channel prefixing.

Alternatively, the secrecy capacity, $C(E,P,\mathbf{H},\mathbf{G})$, is also given as

$$\begin{aligned} C(E,P,\mathbf{H},\mathbf{G}) = \max_{\mathbf{Q}_1,\mathbf{Q}_2} \quad & \frac{1}{2}\log\frac{|\mathbf{I}+\mathbf{H}(\mathbf{Q}_1+\mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I}+\mathbf{H}\mathbf{Q}_2\mathbf{H}^T|} \\ & -\frac{1}{2}\log\frac{|\mathbf{I}+\mathbf{G}(\mathbf{Q}_1+\mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I}+\mathbf{G}\mathbf{Q}_2\mathbf{G}^T|} \\ \text{s.t.} \quad & \operatorname{tr}(\mathbf{Q}_1+\mathbf{Q}_2) \leq P \\ & \operatorname{tr}(\mathbf{G}(\mathbf{Q}_1+\mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E} \quad (11) \end{aligned}$$

where $\mathbf{X} = \mathbf{V}+\mathbf{U}$, with jointly Gaussian $\mathbf{V} \sim \mathcal{N}(\mathbf{0},\mathbf{Q}_1)$ and $\mathbf{U} \sim \mathcal{N}(\mathbf{0},\mathbf{Q}_2)$, i.e., with Gaussian channel prefixing.

IV. Achievability Schemes

In this section, we provide two coding schemes that achieve the secrecy capacity of the MIMO wiretap with transmitter and receiver-side power constraints.

A. Gaussian Coding with Fixed Mean

The first achievable scheme is Gaussian coding with fixed mean, i.e., $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu},\mathbf{Q}_1)$. In this case, the fixed mean will not play a role in evaluating the secrecy capacity except for consuming part of the overall correlation matrix and only provides the required power level at the receiver side. Then, we choose $V = \mathbf{X}$, i.e., no channel prefixing. Hence, we have

$$\begin{aligned} & C(\mathbf{S}_1,\mathbf{S}_2,\mathbf{H},\mathbf{G}) \\ & \quad \geq \max_{\mathbf{Q}_1,\boldsymbol{\mu}} \quad I(\mathbf{X};\mathbf{Y}) - I(\mathbf{X};\mathbf{Z}) \\ & \quad = \max_{\mathbf{Q}_1,\boldsymbol{\mu}} \quad \frac{1}{2}\log|\mathbf{I}+\mathbf{H}\mathbf{Q}_1\mathbf{H}^T| - \frac{1}{2}\log|\mathbf{I}+\mathbf{G}\mathbf{Q}_1\mathbf{G}^T| \\ & \quad\quad \text{s.t.} \quad \mathbf{S}_1 \preceq \mathbf{Q}_1+\boldsymbol{\mu}\boldsymbol{\mu}^T \preceq \mathbf{S}_2 \quad (12) \end{aligned}$$

In the converse proof, we call $\mathbf{Q}_2 = \boldsymbol{\mu}\boldsymbol{\mu}^T$. In order to have a feasible coding scheme, $\mathbf{Q}_2$ must be constrained to unit-rank correlation matrices. In the converse proof, we ignore this unit-rank constraint. Although, the solution of $\mathbf{Q}_2$ is generally not unit-rank for arbitrary correlation matrices $\mathbf{S}_1,\mathbf{S}_2$, we show in the following lemma that for the special case of maximum transmitter-side power constraint P, and minimum receiver-side power constraint E, the solution is guaranteed to be of unit-rank, and hence the coding scheme is feasible.

Lemma 1 *The coding scheme $\mathbf{X} \sim \mathcal{N}(\mathbb{V}(\mathbf{Q}_2^*),\mathbf{Q}_1^*)$ is achievable for the wiretap channel under transmitter-side power constraint P and receiver-side power constraint E given that the matrix $\mathbf{G}^T\mathbf{G}$ has unique maximum eigenvalue. The secrecy rate is characterized by the following optimization problem:*

$$\begin{aligned} \max_{\mathbf{Q}_1,\mathbf{Q}_2} \quad & \frac{1}{2}\log|\mathbf{I}+\mathbf{H}\mathbf{Q}_1\mathbf{H}^T| - \frac{1}{2}\log|\mathbf{I}+\mathbf{G}\mathbf{Q}_1\mathbf{G}^T| \\ \text{s.t.} \quad & \mathbf{Q}_1 \succeq \mathbf{0} \\ & \mathbf{Q}_2 \succeq \mathbf{0} \\ & \operatorname{tr}(\mathbf{Q}_1+\mathbf{Q}_2) \leq P \\ & \operatorname{tr}(\mathbf{G}(\mathbf{Q}_1+\mathbf{Q}_2)\mathbf{G}^T) \geq \tilde{E} \quad (13) \end{aligned}$$

where $\mathbb{V}(\mathbf{Q}_2^*)$ denotes the eigenvector of matrix $\mathbf{Q}_2^*$.

Proof: We note that $\mathbf{Q}_2$ does not appear in the objective function; it only appears in the constraint set. Therefore, its only role is to enlarge the feasible set for $\mathbf{Q}_1$ as much as possible. Thus, $\mathbf{Q}_2$ must be chosen such that, when the third line of the feasible set of (13) is fixed, it maximizes the feasible set for $\mathbf{Q}_1$ in the fourth line, i.e., $\mathbf{Q}_2$ must be the solution of

$$\begin{aligned} \max_{\mathbf{Q}_2} \quad & \operatorname{tr}(\mathbf{G}\mathbf{Q}_2\mathbf{G}^T) \\ \text{s.t.} \quad & \operatorname{tr}(\mathbf{Q}_2) = \tilde{P} \quad (14) \end{aligned}$$

Eigenvector decomposition for $\mathbf{Q}_2$, which is symmetric, is

$$\mathbf{Q}_2 = \sum_{i=1}^{r} \lambda_i \mathbf{q}_i \mathbf{q}_i^T \quad (15)$$

where r, λ_i, $\mathbf{q}_i$ are the rank, ith eigenvalue and the corresponding orthonormal eigenvector of $\mathbf{Q}_2$, respectively. Thus, we can write the constraint as $\operatorname{tr}(\mathbf{Q}_2) = \sum_{i=1}^{r}\lambda_i = \tilde{P}$. Moreover, the objective function can be written as

$$\begin{aligned} \operatorname{tr}(\mathbf{G}\mathbf{Q}_2\mathbf{G}^T) &= \operatorname{tr}\left(\mathbf{G}\left(\sum_{i=1}^{r}\lambda_i\mathbf{q}_i\mathbf{q}_i^T\right)\mathbf{G}^T\right) \quad (16) \\ &= \sum_{i=1}^{r}\lambda_i\|\mathbf{G}\mathbf{q}_i\|^2 \quad (17) \end{aligned}$$

Hence, the optimization problem in (14) can be written as

$$\begin{aligned} \max_{\lambda_i,\mathbf{q}_i} \quad & \sum_{i=1}^{r}\lambda_i\|\mathbf{G}\mathbf{q}_i\|^2 \\ \text{s.t.} \quad & \sum_{i=1}^{r}\lambda_i = \tilde{P} \quad (18) \end{aligned}$$

which is a linear program in λ_i. The optimum solution is $\lambda_m = \tilde{P}$, and $\lambda_i = 0$ for $i \neq m$, where

$$m = \arg\max_i \|\mathbf{G}\mathbf{q}_i\|^2 \quad (19)$$

Hence, the optimal solution for this problem is to beamform all the available power $\tilde{P}$ to the direction of the largest $\|\mathbf{G}\mathbf{q}_i\|^2$. In this case, $\mathbf{Q}_2 = \tilde{P}\mathbf{q}_m\mathbf{q}_m^T$, i.e., it is unit-rank with eigenvector $\boldsymbol{\mu} = \sqrt{\tilde{P}}\mathbf{q}_m$, and the problem is feasible. ■

B. Gaussian Coding with Gaussian Artificial Noise

The second achievable scheme is Gaussian coding with Gaussian artificial noise. In this case, we choose $\mathbf{X} = \mathbf{V} + \mathbf{U}$, where $\mathbf{V}$, $\mathbf{U}$ are independent and $\mathbf{V} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_1)$ and $\mathbf{U} \sim \mathcal{N}(\mathbf{0}, \mathbf{Q}_2)$. Here, $\mathbf{V}$ carries the message, $\mathbf{X}$ is the channel input, and $\mathbf{U}$ is the artificial noise (or cooperative jamming [12]) signal. In this case, we use channel prefixing, hence $\mathbf{V} \neq \mathbf{X}$. The extra randomness $\mathbf{U}$ is sent by the transmitter to provide extra noise floor at both receivers, and confuses the eavesdropper. The added significance of this artificial noise in our problem is to provide a suitable level of received power at the receiver, i.e., we utilize the artificial noise as a source of power. In this case, the secrecy capacity is

$$\begin{aligned} C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \geq \max_{\mathbf{Q}_1, \mathbf{Q}_2} \quad & I(\mathbf{V}; \mathbf{Y}) - I(\mathbf{V}; \mathbf{Z}) \\ = \max_{\mathbf{Q}_1, \mathbf{Q}_2} \quad & \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{H}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{H}^T|}{|\mathbf{I} + \mathbf{H}\mathbf{Q}_2\mathbf{H}^T|} \\ & - \frac{1}{2} \log \frac{|\mathbf{I} + \mathbf{G}(\mathbf{Q}_1 + \mathbf{Q}_2)\mathbf{G}^T|}{|\mathbf{I} + \mathbf{G}\mathbf{Q}_2\mathbf{G}^T|} \\ \text{s.t.} \quad & \mathbf{S}_1 \preceq \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2 \end{aligned} \tag{20}$$

V. Converse Proof

In this section, we prove the reverse implication using the channel enhancement technique [10], [11]. We will consider the case of having $\mathbf{S}_2 \succ \mathbf{S}_1 \succ \mathbf{0}$ and aligned MIMO case which implies that the channel matrices are square and invertible. The general MIMO case follows directly from the limiting arguments in [10], as the additional receiver-side power constraint is irrelevant in the limit. Therefore, we focus on the aligned case here. The aligned MIMO model is obtained by multiplying by the inverse of the channel matrices as

$$\tilde{\mathbf{Y}} = \mathbf{X} + \mathbf{H}^{-1}\mathbf{W}_1 = \mathbf{X} + \tilde{\mathbf{W}}_1 \tag{21}$$

$$\tilde{\mathbf{Z}} = \mathbf{X} + \mathbf{G}^{-1}\mathbf{W}_2 = \mathbf{X} + \tilde{\mathbf{W}}_2 \tag{22}$$

where $\tilde{\mathbf{W}}_1$ and $\tilde{\mathbf{W}}_2$ are the equivalent zero-mean Gaussian random vectors with covariance matrices $\mathbf{N}_1 = \mathbf{H}^{-1}\mathbf{H}^{-T}$ and $\mathbf{N}_2 = \mathbf{G}^{-1}\mathbf{G}^{-T}$, respectively.

A. Equivalance of a Double-Sided Correlation Constraint

For the MIMO broadcast and wiretap channels under a transmitter-side maximum power constraint, references [10], [11] showed that it is sufficient to prove the converse under a maximum covariance constraint on the channel input. We first note here that in our case with maximum transmitter-side and minimum receiver-side power constraints, a single correlation constraint on the channel input, i.e., $\mathbf{Q} \preceq \mathbf{S}$, is not sufficient. Next, we show the equivalence of solving our problem with a *double-sided* correlation matrix constraint on the channel input, i.e., $\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2$. Then, our problem can be solved in two stages: the inner problem finds the capacity under fixed correlation matrices $\mathbf{S}_1$ and $\mathbf{S}_2$ constraints, and the outer problem finds the optimal $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}$ in (8). Finally, we modify the original channel enhancement technique [10], [11] to prove the optimality of the achievable schemes presented in the previous section.

We first note that solving the problem for $\mathbf{Q} \preceq \mathbf{S}$, where $\mathbf{S} \in \mathcal{S}_{PE}$ is insufficient. Consider solving the secrecy capacity under maximum transmitter-side and minimum receiver-side power constraints in two stages, first, solving the problem under a fixed correlation matrix $\mathbf{S}$, and then choosing the optimal $\mathbf{S} \in \mathcal{S}_{PE}$, i.e.,

$$\max_{\mathbf{S} \in \mathcal{S}_{PE}} \quad \max_{\mathbf{Q} \preceq \mathbf{S}} \quad R_s \tag{23}$$

Since $\mathbf{Q} \preceq \mathbf{S}$, we have $\mathbf{G}\mathbf{Q}\mathbf{G}^T \preceq \mathbf{G}\mathbf{S}\mathbf{G}^T$ and hence $\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \leq \text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T)$. Then, although any $\mathbf{S} \in \mathcal{S}_{PE}$ satisfies the minimum receiver-side power constraint, i.e., $\text{tr}(\mathbf{G}\mathbf{S}\mathbf{G}^T) \geq \tilde{E}$, the input correlation matrix $\mathbf{Q}$ is not guaranteed to satisfy $\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^T) \geq \tilde{E}$. Hence, the single correlation constraint is not sufficient for solving problems involving minimum receiver-side power constraints.

Lemma 2 *Since $\mathcal{S}_{PE}$ is a compact set of positive semi-definite matrices, and $C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ is continuous with respect to $\mathbf{S}_2$, we have*

$$C(E, P, \mathbf{H}, \mathbf{G}) = \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \prec \mathbf{S}_2} \quad C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \tag{24}$$

Proof: To see

$$C(E, P, \mathbf{H}, \mathbf{G}) \geq \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \prec \mathbf{S}_2} \quad C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \tag{25}$$

we note that for any $\mathbf{S}_1 \preceq \mathbf{Q} \preceq \mathbf{S}_2$ where $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}$, we have $\mathbf{Q} \in \mathcal{S}_{PE}$.

To see

$$C(E, P, \mathbf{H}, \mathbf{G}) \leq \max_{\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}, \mathbf{S}_1 \prec \mathbf{S}_2} \quad C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) \tag{26}$$

we should prove that $C(E, P, \mathbf{H}, \mathbf{G}) = C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})$ for some $\mathbf{S}_1, \mathbf{S}_2 \in \mathcal{S}_{PE}$ [11]. If $R = C(E, P, \mathbf{H}, \mathbf{G})$ is achievable, then there exists an infinite sequence of codebooks $\mathcal{C}(n_i, \mathbf{S}_{0_i}, R, \epsilon_i), i = 1, \dots$ with rate R and decreasing probability of error $\epsilon_i \to 0$ as $i \to \infty$. Choose $\mathbf{S}_1 \preceq \mathbf{S}_{0_i} \forall i$, $\mathbf{S}_1 \in \mathcal{S}_{PE}$. As $\mathcal{S}_{PE}$ is compact [16], [17], for any infinite sequence of points in $\mathcal{S}_{PE}$, there must be sub-sequence that converges to a point $\mathbf{S}_0 \in \mathcal{S}_{PE}$. Hence, for any arbitrary $\delta > 0$, we can find an increasing subsequence $i(k)$ such that $\mathbf{S}_1 \preceq \mathbf{S}_{0_{i(k)}} \preceq \mathbf{S}_0 + \delta\mathbf{I}$.

This implies that we can find a sequence of codebooks $\mathcal{C}(n_k, \mathbf{S}_0 + \delta\mathbf{I}, R, \epsilon_k)$ with $\mathbf{S}_0 \in \mathcal{S}_{PE}, \mathbf{S}_0 \succeq \mathbf{S}_1$ achieving small probability of error. Therefore, for every $\delta > 0$, we have $R = C(\mathbf{S}_1, \mathbf{S}_0 + \delta\mathbf{I}, \mathbf{H}, \mathbf{G})$. Since $C(\mathbf{S}_1, \mathbf{S}_0 + \delta\mathbf{I}, \mathbf{H}, \mathbf{G})$ is continuous [11], with respect to its second argument, then we have that every ϵ-ball around R contains $C(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G})$ and therefore R is a limit point of $\mathcal{C}(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G})$ and hence $C(E, P, \mathbf{H}, \mathbf{G}) = C(\mathbf{S}_1, \mathbf{S}_0, \mathbf{H}, \mathbf{G})$. ■

B. Converse Proof for Gaussian Coding with Fixed Mean

First, we begin with writing the equivalent optimization problem corresponding to the achievability scheme in the aligned MIMO case with Gaussian coding $\mathbf{X} \sim$

$\mathcal{N}(\mathbb{V}(\mathbf{Q}_2^*),\mathbf{Q}_1^*)$:

$$\begin{aligned}\max_{\mathbf{Q}_1,\mathbf{Q}_2}\quad & \frac{1}{2}\log\frac{|\mathbf{Q}_1+\mathbf{N}_1|}{|\mathbf{N}_1|}-\frac{1}{2}\log\frac{|\mathbf{Q}_1+\mathbf{N}_2|}{|\mathbf{N}_2|}\\ \text{s.t.}\quad & \mathbf{Q}_1\succeq\mathbf{0}\\ & \mathbf{Q}_2\succeq\mathbf{0}\\ & \mathbf{Q}_1+\mathbf{Q}_2\succeq\mathbf{S}_1\\ & \mathbf{Q}_1+\mathbf{Q}_2\preceq\mathbf{S}_2 \end{aligned}\tag{27}$$

The Lagrangian of this optimization problem can be written as:

$$\begin{aligned}\mathcal{L}=&\log\frac{|\mathbf{Q}_1+\mathbf{N}_2|}{|\mathbf{N}_2|}-\log\frac{|\mathbf{Q}_1+\mathbf{N}_1|}{|\mathbf{N}_1|}\\ &-\operatorname{tr}(\mathbf{Q}_1\mathbf{M}_1)-\operatorname{tr}(\mathbf{Q}_2\mathbf{M}_2)-\operatorname{tr}((\mathbf{Q}_1+\mathbf{Q}_2-\mathbf{S}_1)\mathbf{M}_3)\\ &+\operatorname{tr}((\mathbf{Q}_1+\mathbf{Q}_2-\mathbf{S}_2)\mathbf{M}_4)\end{aligned}\tag{28}$$

where $\mathbf{M}_1\succeq\mathbf{0},\mathbf{M}_2\succeq\mathbf{0},\mathbf{M}_3\succeq\mathbf{0}$ and $\mathbf{M}_4\succeq\mathbf{0}$ are the Lagrange multipliers for each constraint. The corresponding KKT optimality conditions can be written as complementary slackness conditions

$$\mathbf{Q}_1^*\mathbf{M}_1=\mathbf{0}\tag{29}$$

$$\mathbf{Q}_2^*\mathbf{M}_2=\mathbf{0}\tag{30}$$

$$(\mathbf{Q}_1^*+\mathbf{Q}_2^*-\mathbf{S}_1)\mathbf{M}_3=\mathbf{0}\tag{31}$$

$$(\mathbf{S}_2-\mathbf{Q}_1^*-\mathbf{Q}_2^*)\mathbf{M}_4=\mathbf{0}\tag{32}$$

the stationarity condition of $\mathbf{Q}_1^*$

$$(\mathbf{Q}_1^*+\mathbf{N}_2)^{-1}-(\mathbf{Q}_1^*+\mathbf{N}_1)^{-1}-\mathbf{M}_1-\mathbf{M}_3+\mathbf{M}_4=\mathbf{0}\tag{33}$$

and the stationary conditions for $\mathbf{Q}_2^*$

$$\begin{aligned}-\mathbf{M}_2-\mathbf{M}_3+\mathbf{M}_4&=\mathbf{0}\\ \mathbf{M}_2=\mathbf{M}_4-\mathbf{M}_3&\succeq\mathbf{0}\end{aligned}\tag{34}$$

Now, using the optimality condition (33) and (34), we can construct an enhanced channel that can serve as an upper bound for the original legitimate receiver's channel and at the same time, the eavesdropper's channel is degraded with respect to it. The covariance of the enhanced channel is chosen as $\tilde{\mathbf{N}}$ such that

$$(\mathbf{Q}_1^*+\mathbf{N}_2)^{-1}+\mathbf{M}_2=(\mathbf{Q}_1^*+\mathbf{N}_1)^{-1}+\mathbf{M}_1=(\mathbf{Q}_1^*+\tilde{\mathbf{N}})^{-1}\tag{35}$$

Using this definition of the enhanced channel, we explore various characteristics of $\tilde{\mathbf{N}}$.

First, to prove the validity of the covariance matrix $\tilde{\mathbf{N}}$, we note that

$$\begin{aligned}\tilde{\mathbf{N}}&=[(\mathbf{Q}_1^*+\mathbf{N}_1)^{-1}+\mathbf{M}_1]^{-1}-\mathbf{Q}_1^* &(36)\\ &=(\mathbf{I}+\mathbf{N}_1\mathbf{M}_1)^{-1}(\mathbf{Q}_1^*+\mathbf{N}_1)-\mathbf{Q}_1^* &(37)\\ &=(\mathbf{I}+\mathbf{N}_1\mathbf{M}_1)^{-1}[(\mathbf{Q}_1^*+\mathbf{N}_1)-(\mathbf{I}+\mathbf{N}_1\mathbf{M}_1)\mathbf{Q}_1^*] &(38)\\ &=(\mathbf{I}+\mathbf{N}_1\mathbf{M}_1)^{-1}\mathbf{N}_1 &(39)\\ &=(\mathbf{N}_1^{-1}+\mathbf{M}_1)^{-1}\succeq\mathbf{0} &(40)\end{aligned}$$

and hence the covariance matrix of the constructed enhanced channel is positive semi-definite, and hence it is a feasible covariance matrix.

Next, we want to show that the constructed channel is enhanced with respect to $\mathbf{N}_1$, i.e., $\mathbf{N}_1\succeq\tilde{\mathbf{N}}$. To show that we note from (40) that $\tilde{\mathbf{N}}=(\mathbf{N}_1^{-1}+\mathbf{M}_1)^{-1}$ and hence, $\mathbf{N}_1\succeq\tilde{\mathbf{N}}$. Similarly by considering $(\mathbf{Q}_1^*+\mathbf{N}_2)^{-1}+\mathbf{M}_2=(\mathbf{Q}_1^*+\tilde{\mathbf{N}})^{-1}$ we note that $\mathbf{N}_2\succeq\tilde{\mathbf{N}}$. Hence, we conclude that the enhanced channel has better channel conditions than the original legitimate user's channel, therefore the constructed channel is an upper bound for the legitimate receiver. Moreover, the eavesdropper's channel is degraded with respect to the constructed channel. Consequently the secrecy capacity of the enhanced channel is known. In other words, we have $\tilde{\mathbf{Y}}=\mathbf{X}+\tilde{\mathbf{W}}$ such that $\tilde{\mathbf{W}}\sim\mathcal{N}(\mathbf{0},\tilde{\mathbf{N}})$ and $\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Y}$ and $\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Z}$.

In order to have a meaningful upper bound, we need to show that the rate is preserved between the original problem and the constructed channel. To show that, we have

$$\begin{aligned}(\mathbf{Q}_1^*+\tilde{\mathbf{N}})^{-1}\tilde{\mathbf{N}}&=(\mathbf{Q}_1^*+\tilde{\mathbf{N}})^{-1}(\tilde{\mathbf{N}}+\mathbf{Q}_1^*-\mathbf{Q}_1^*) &(41)\\ &=\mathbf{I}-(\mathbf{Q}_1^*+\tilde{\mathbf{N}})^{-1}\mathbf{Q}_1^* &(42)\\ &=\mathbf{I}-[(\mathbf{Q}_1^*+\mathbf{N}_1)^{-1}+\mathbf{M}_1]\mathbf{Q}_1^* &(43)\\ &=\mathbf{I}-(\mathbf{Q}_1^*+\mathbf{N}_1)^{-1}\mathbf{Q}_1^* &(44)\\ &=(\mathbf{Q}_1^*+\mathbf{N}_1)^{-1}\mathbf{N}_1 &(45)\end{aligned}$$

where (43) follows from the definition of the enhanced channel and (44) follows from the complementary slackness condition (29). Therefore, we have

$$\frac{|\tilde{\mathbf{N}}+\mathbf{Q}_1^*|}{|\tilde{\mathbf{N}}|}=\frac{|\mathbf{N}_1+\mathbf{Q}_1^*|}{|\mathbf{N}_1|}\tag{46}$$

To show a similar rate preservation argument for the degraded channel $\mathbf{N}_2$, we will need the following lemma.

Lemma 3 *The optimal covariance matrix for the achievable scheme with Gaussian signaling with a fixed mean* $\mathbf{Q}_1^*$ *satisfies* $(\mathbf{S}_2-\mathbf{Q}_1^*)\mathbf{M}_2=\mathbf{0}$.

Proof: We return to the KKT conditions. Considering the correlation constraint, three cases can possibly occur.

The first case: the correlation constraint is satisfied with equality, consequently $\mathbf{S}_2-\mathbf{Q}_1^*=\mathbf{Q}_2^*$. In this case, $(\mathbf{S}_2-\mathbf{Q}_1^*)\mathbf{M}_2=\mathbf{Q}_2^*\mathbf{M}_2=\mathbf{0}$ from (30).

The second case: the correlation constraint is strictly loose, i.e, $\mathbf{Q}_1+\mathbf{Q}_2\prec\mathbf{S}_2$. In this case, we can define a matrix $\Delta=\mathbf{S}_2-\mathbf{Q}_1^*-\mathbf{Q}_2^*\succ\mathbf{0}$, and therefore Δ is full rank matrix. Thus, $\mathbf{M}_4=\mathbf{0}$ and from (34), we have $\mathbf{M}_2=-\mathbf{M}_3$. The matrices $\mathbf{M}_2$, $\mathbf{M}_3$ are both positive semi-definite matrices. Therefore, we must have $\mathbf{M}_2=\mathbf{M}_3=\mathbf{0}$.

Finally, the third case: the correlation constraint is partially loose, that is we have $\Delta=\mathbf{S}_2-\mathbf{Q}_1-\mathbf{Q}_2\succeq\mathbf{0}$, hence Δ is not a full-rank matrix. We define $\mathbf{\Sigma}=\mathbf{S}_2-\mathbf{S}_1\succ\mathbf{0}$, i.e., $\mathbf{S}_1=\mathbf{S}_2-\mathbf{\Sigma}$. In this case, we sum the KKT conditions (31) and (32) to obtain the following implications:

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^*)(\mathbf{M}_3 - \mathbf{M}_4) - \mathbf{S}_1\mathbf{M}_3 + \mathbf{S}_2\mathbf{M}_4 = \mathbf{0} \tag{47}$$

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^*)(\mathbf{M}_3 - \mathbf{M}_4) - \mathbf{S}_2\mathbf{M}_3 + \boldsymbol{\Sigma}\mathbf{M}_3 + \mathbf{S}_2\mathbf{M}_4 = \mathbf{0} \tag{48}$$

$$(\mathbf{S}_2 - \mathbf{Q}_1^* - \mathbf{Q}_2^*)(\mathbf{M}_4 - \mathbf{M}_3) = -\boldsymbol{\Sigma}\mathbf{M}_3 \tag{49}$$

$$(\mathbf{S}_2 - \mathbf{Q}_1^* - \mathbf{Q}_2^*)\mathbf{M}_2 = -\boldsymbol{\Sigma}\mathbf{M}_3 \tag{50}$$

$$(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2 = -\boldsymbol{\Sigma}\mathbf{M}_3 \tag{51}$$

where (50) follows from (34) and (51) follows from (30). Since $(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2 \succeq \mathbf{0}$ and $\boldsymbol{\Sigma}\mathbf{M}_3 \succeq \mathbf{0}$, or at least $(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2$ and $\boldsymbol{\Sigma}\mathbf{M}_3$ have the same number of non-negative eigenvalues of $\mathbf{M}_2$ and $\mathbf{M}_3$, respectively [18], the only way to satisfy (51) is to have all the eigenvalues of both matrices equal zero, i.e, $(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2 = -\boldsymbol{\Sigma}\mathbf{M}_3 = \mathbf{0}$. Hence, we conclude that for all three cases we have

$$(\mathbf{S}_2 - \mathbf{Q}_1^*)\mathbf{M}_2 = \mathbf{0} \tag{52}$$

completing the proof of Lemma 3. ■

Hence, using Lemma 3, we write:

$$\begin{aligned}
&(\tilde{\mathbf{N}} + \mathbf{S}_2)(\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1} \\
&\quad = (\mathbf{S}_2 - \mathbf{Q}_1^*)(\mathbf{Q}_1^* + \tilde{\mathbf{N}})^{-1} + \mathbf{I} \qquad (53)\\
&\quad = (\mathbf{S}_2 - \mathbf{Q}_1^*)[(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2] + \mathbf{I} \qquad (54)\\
&\quad = (\mathbf{S}_2 - \mathbf{Q}_1^*)(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{I} \qquad (55)\\
&\quad = [(\mathbf{N}_2 + \mathbf{S}_2) - (\mathbf{Q}_1^* + \mathbf{N}_2)](\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} + \mathbf{I} \qquad (56)\\
&\quad = (\mathbf{N}_2 + \mathbf{S}_2)(\mathbf{Q}_1^* + \mathbf{N}_2)^{-1} \qquad (57)
\end{aligned}$$

where (54) follows from the definition of the enhanced channel (35), and (55) follows from Lemma 3. Hence, we have

$$\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|} = \frac{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}|}{|\mathbf{Q}_1^* + \mathbf{N}_2|} \tag{58}$$

Now, we upper bound the secrecy capacity of the MIMO wiretap channel with receiver-side power constraint by the secrecy capacity of the enhanced channel. Since $\mathbf{S}_2 \in \mathcal{S}_{PE}$, $\mathbf{S}_2$ satisfies the receiver power constraint for the enhanced channel. Therefore, the receiver constraint is valid with the upper bounding argument. The secrecy capacity of the enhanced channel $\tilde{C_s}$ is given by

$$\begin{aligned}
\tilde{C_s} &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\tilde{\mathbf{N}}|} - \frac{1}{2}\log\frac{|\mathbf{S}_2 + \mathbf{N}_2|}{|\mathbf{N}_2|} \qquad (59)\\
&= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|}\cdot\frac{|\mathbf{N}_2|}{|\tilde{\mathbf{N}}|} \qquad (60)\\
&= \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}|}{|\mathbf{Q}_1^* + \mathbf{N}_2|}\cdot\frac{|\mathbf{N}_2|}{|\tilde{\mathbf{N}}|} \qquad (61)\\
&= \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \tilde{\mathbf{N}}|}{|\tilde{\mathbf{N}}|} - \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \mathbf{N}_2|}{|\mathbf{N}_2|} \qquad (62)\\
&= \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \mathbf{N}_1|}{|\mathbf{N}_1|} - \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \mathbf{N}_2|}{|\mathbf{N}_2|} \qquad (63)\\
&= C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G})
\end{aligned}$$

where (61) follows from (58) and (63) follows from (46), completing the converse proof for the case of Gaussian signalling with fixed mean.

C. Converse Proof for Gaussian Coding with Gaussian Artificial Noise

In this section, we follow a similar channel enhancement technique as in Section V-B. The optimization problem corresponding to the Gaussian coding scheme with artificial noise in the aligned model is

$$\begin{aligned}
\max_{\mathbf{Q}_1,\mathbf{Q}_2}\quad & \frac{1}{2}\log\frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2 + \mathbf{N}_1|} - \frac{1}{2}\log\frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_2|}{|\mathbf{Q}_2 + \mathbf{N}_2|}\\
\text{s.t.}\quad & \mathbf{Q}_1 \succeq \mathbf{0}\\
& \mathbf{Q}_2 \succeq \mathbf{0}\\
& \mathbf{Q}_1 + \mathbf{Q}_2 \succeq \mathbf{S}_1\\
& \mathbf{Q}_1 + \mathbf{Q}_2 \preceq \mathbf{S}_2 \qquad (64)
\end{aligned}$$

The Lagrangian for this optimization problem is given by:

$$\begin{aligned}
\mathcal{L} = \log&\frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_2|}{|\mathbf{Q}_2 + \mathbf{N}_2|} - \log\frac{|\mathbf{Q}_1 + \mathbf{Q}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2 + \mathbf{N}_1|}\\
&- \operatorname{tr}(\mathbf{Q}_1\mathbf{M}_1) - \operatorname{tr}(\mathbf{Q}_2\mathbf{M}_2) - \operatorname{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_1)\mathbf{M}_3)\\
&+ \operatorname{tr}((\mathbf{Q}_1 + \mathbf{Q}_2 - \mathbf{S}_2)\mathbf{M}_4) \qquad (65)
\end{aligned}$$

The complementary slackness conditions (29)-(32) are still the same due to the same set of constraints for both problems (64) and (27). The stationarity condition for $\mathbf{Q_1^*}$ is

$$\begin{aligned}
(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} &- (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1}\\
&- \mathbf{M}_1 - \mathbf{M}_3 + \mathbf{M}_4 = \mathbf{0} \qquad (66)
\end{aligned}$$

which is equivalent to:

$$\mathbf{M}_1 = (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \mathbf{M}_3 + \mathbf{M}_4 \tag{67}$$

The stationarity condition for $\mathbf{Q_2^*}$ is:

$$\begin{aligned}
(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1}&\\
+ (\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \mathbf{M}_2 - \mathbf{M}_3 + \mathbf{M}_4 = \mathbf{0}& \qquad (68)
\end{aligned}$$

Using (67), we can write (68) as:

$$\mathbf{M}_1 - (\mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + (\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \mathbf{M}_2 = \mathbf{0} \tag{69}$$

In this case, we again construct an enhanced channel with similar steps as in Section V-B. The enhanced channel is constructed as:

$$(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 = (\mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + \mathbf{M}_2 = (\mathbf{Q}_2^* + \tilde{\mathbf{N}})^{-1} \tag{70}$$

which is the same as in the previous section. Therefore, it follows that $\tilde{\mathbf{N}} \succeq \mathbf{0}, \tilde{\mathbf{N}} \preceq \mathbf{N}_1, \tilde{\mathbf{N}} \preceq \mathbf{N}_2$. Similarly, we can prove that the rate is preserved for the eavesdropper (as in the set of equations (41)-(46) with $\mathbf{Q}_2^*$ instead of $\mathbf{Q}_1^*$, i.e.,

$$\frac{|\tilde{\mathbf{N}} + \mathbf{Q}_2^*|}{|\tilde{\mathbf{N}}|} = \frac{|\mathbf{N}_2 + \mathbf{Q}_2^*|}{|\mathbf{N}_2|} \tag{71}$$

To prove the rate preservation for the legitimate receiver, we will need the following lemma.

Lemma 4 *To achieve positive secrecy rate using Gaussian coding with artificial noise,* $\mathbf{S}_2$ *must be fully used, i.e.,* $\mathbf{S}_2 = \mathbf{Q}_1^* + \mathbf{Q}_2^*$*, and the optimal covariance matrix used for the artificial noise component,* $\mathbf{Q}_2^*$*, satisfies* $(\mathbf{S}_2 - \mathbf{Q}_2^*)\mathbf{M}_1 = \mathbf{0}$.

Proof: We start by proving the first part of the lemma by contradiction. Assume that a positive secrecy rate can be achieved using artificial noise coding scheme, and $\mathbf{S}_2$ is partially used. Then, we have two cases.

The first case: $\Delta = \mathbf{S}_2 - \mathbf{Q}_1^* - \mathbf{Q}_2^* \succ \mathbf{0}$. Hence, Δ is a full-rank matrix, then $\mathbf{M}_4 = \mathbf{0}$. From (66), we can write

$$(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1 + \mathbf{M}_3 = (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} \tag{72}$$

and hence, $(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} \preceq (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1}$, which results in $\mathbf{N}_2 \preceq \mathbf{N}_1$. This means that the legitimate channel is degraded with respect to the eavesdropper channel and hence no positive secrecy rate can be achieved. This contradicts our assumption.

The second case: Δ is not full-rank. Due to the similarity of the complementary slackness conditions for the artificial noise setting and the Gaussian coding with fixed mean, we will have also equation (49), and from (66), we have

$$\begin{aligned}\mathbf{M}_4 - \mathbf{M}_3 \\ &= (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} + \mathbf{M}_1\end{aligned} \tag{73}$$

substituting this in (49), we have the following implications:

$$\begin{aligned}&\Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} \\ &\quad + \Delta\mathbf{M}_1 = -\mathbf{\Sigma}\mathbf{M}_3 && (74)\\ &\Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)^{-1} - \Delta(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} \\ &\quad = -\Delta\mathbf{M}_1 - \mathbf{\Sigma}\mathbf{M}_3 && (75)\\ &\Delta[(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)]^{-1}] \succeq \mathbf{0} && (76)\end{aligned}$$

Then, $(\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2)^{-1} - (\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1)]^{-1} \succeq \mathbf{0}$ to have the product (76) hold true [19], and then we have $\mathbf{N}_2 \preceq \mathbf{N}_1$ as the previous case, which also contradicts the assumption of having positive secrecy rate. Hence,

$$\mathbf{Q}_1^* + \mathbf{Q}_2^* = \mathbf{S}_2 \tag{77}$$

For the second part of the lemma, we now have $\mathbf{S}_2 - \mathbf{Q}_2^* = \mathbf{Q}_1^*$, and from the complementary slackness condition $\mathbf{Q}_1^*\mathbf{M}_1 = \mathbf{0}$. Then, we conclude that $(\mathbf{S}_2 - \mathbf{Q}_2^*)\mathbf{M}_1 = \mathbf{0}$, completing the proof of Lemma 4. ■

Using the results of Lemma 4, we can prove the rate preservation for the legitimate receiver as follows:

$$\begin{aligned}&(\tilde{\mathbf{N}} + \mathbf{S}_2)(\mathbf{Q}_2^* + \tilde{\mathbf{N}})^{-1} \\ &\quad = (\mathbf{S}_2 - \mathbf{Q}_2^*)(\mathbf{Q}_2^* + \tilde{\mathbf{N}})^{-1} + \mathbf{I} && (78)\\ &\quad = (\mathbf{S}_2 - \mathbf{Q}_2^*)[(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{M}_1] + \mathbf{I} && (79)\\ &\quad = (\mathbf{S}_2 - \mathbf{Q}_2^*)(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{I} && (80)\\ &\quad = [(\mathbf{N}_1 + \mathbf{S}_2) - (\mathbf{Q}_2^* + \mathbf{N}_1)](\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} + \mathbf{I} && (81)\\ &\quad = (\mathbf{N}_1 + \mathbf{S}_2)(\mathbf{Q}_2^* + \mathbf{N}_1)^{-1} && (82)\end{aligned}$$

where (79) follows from the definition of the enhanced channel (70), and (80) follows from Lemma 4. Therefore, we have

$$\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{Q}_2^* + \tilde{\mathbf{N}}|} = \frac{|\mathbf{S}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} \tag{83}$$

Hence, the enhanced channel secrecy capacity is given by

$$\begin{aligned}\tilde{C_s} &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\tilde{\mathbf{N}}|} - \frac{1}{2}\log\frac{|\mathbf{S}_2 + \mathbf{N}_2|}{|\mathbf{N}_2|} && (84)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|}\cdot\frac{|\mathbf{N}_2|}{|\tilde{\mathbf{N}}|} && (85)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{S}_2 + \mathbf{N}_2|}\cdot\frac{|\mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{Q}_2^* + \tilde{\mathbf{N}}|} && (86)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \tilde{\mathbf{N}}|}{|\mathbf{Q}_2^* + \tilde{\mathbf{N}}|}\cdot\frac{|\mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{S}_2 + \mathbf{N}_2|} && (87)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|}\cdot\frac{|\mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{S}_2 + \mathbf{N}_2|} && (88)\\ &= \frac{1}{2}\log\frac{|\mathbf{S}_2 + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} - \frac{1}{2}\log\frac{|\mathbf{S}_2 + \mathbf{N}_2|}{|\mathbf{Q}_2^* + \mathbf{N}_2|} && (89)\\ &= \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_1|}{|\mathbf{Q}_2^* + \mathbf{N}_1|} - \frac{1}{2}\log\frac{|\mathbf{Q}_1^* + \mathbf{Q}_2^* + \mathbf{N}_2|}{|\mathbf{Q}_2^* + \mathbf{N}_2|} && (90)\\ &= C(\mathbf{S}_1, \mathbf{S}_2, \mathbf{H}, \mathbf{G}) && (91)\end{aligned}$$

where (86) follows from (71), (88) follows from (83), and (90) follows from (77), completing the converse proof for the case of Gaussian signalling with Gaussian artificial noise.

VI. Numerical Results

In this section, we present simple simulation results for the secrecy capacity of the MIMO wiretap channel with maximum transmitter-side power constraint and minimum receiver-side (eavesdropper-side) power constraint. In these simulations, the average transmit power at the transmitter is taken as $P = 10$ and the noise variances at all antennas at both receivers is taken as $\sigma^2 = 1$.

Fig. 2 shows a secrecy capacity receiver-side power constraint region for a MISO 4-1-1 system, i.e, a system with 4 antennas at the transmitter and single antenna at both the legitimate receiver and the eavesdropper. The figure shows the optimality of the Gaussian signalling with a mean and Gaussian coding with Gaussian artificial noise coding schemes; in particular, the region corresponding to the mean and artificial noise coding schemes are identical. Moreover, the secrecy capacity receiver-side power region of the standard Gaussian coding scheme with no mean or no artificial noise is noticeably smaller than the optimal schemes. Note that this is the optimal scheme without any receiver-side power constraints. That is, the standard Gaussian signaling scheme is strictly sub-optimal for the case of receiver-side power constraints. In addition, we observe that, as the receiver-side power constraint is increased, the secrecy capacity decreases, i.e., there is a trade-off between the power that should be delivered to the eavesdropper's receiver and the confidentiality that can be provided for the

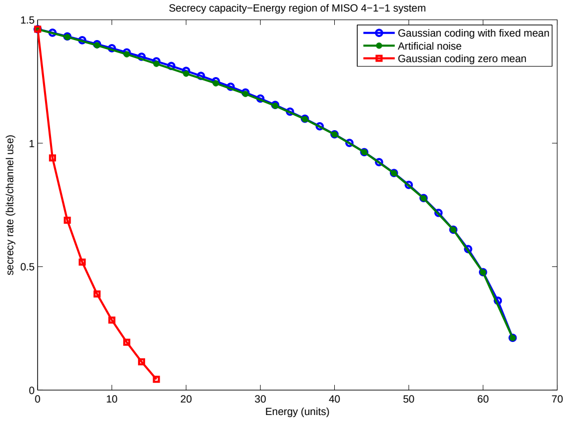

Fig. 2. Secrecy capacity receiver-side power constraint region for a 4-1-1 MISO wiretap channel.

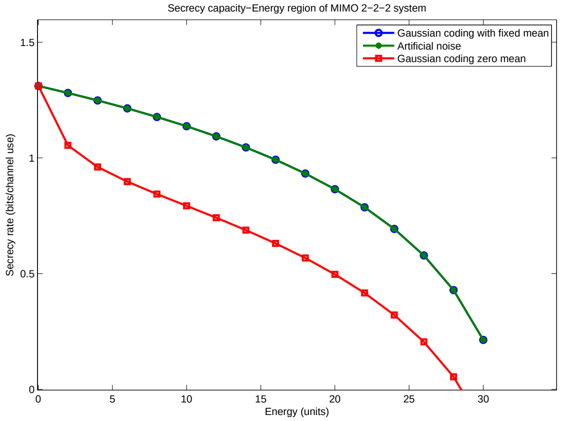

Fig. 3. Secrecy capacity receiver-side power constraint region for a 2-2-2 MIMO wiretap channel.

legitimate receiver. This is because, when the receiver-side power constraint is increased, the problem becomes more confined and more power should be concentrated for the receiver-side power constraint, which decreases the set of signalling choices for the secrecy communications. Fig. 3 shows similar observations for the 2-2-2 MIMO wiretap system.

VII. Conclusions

We considered the MIMO wiretap channel with the usual transmitter-side maximum power constraint and the additional receiver-side minimum power constraint. For the converse, we first proved that the problem is equivalent to solving a secrecy capacity problem with a double-sided correlation matrix constraint on the channel input. We then extended the channel enhancement technique to our setting. For the achievability, we proposed two optimum schemes that achieve the converse rate: Gaussian signalling with a fixed mean and Gaussian signalling with Gaussian channel prefixing (artificial noise). This is the first instance of a problem where transmission with a mean and channel prefixing are strictly necessary for a MIMO wiretap channel under power constraints. The transmission scheme with a mean enables us to deliver the needed power to the receiver without creating interference to the legitimate receiver as it is a deterministic signal. On the other hand, the transmission scheme with Gaussian artificial noise, both jams the eavesdropper contributing to the secrecy as well as delivering the needed power to the receiver. We note that the optimal coding scheme for the MIMO wiretap channel under a transmitter-side power constraint only, which is Gaussian signalling with no channel prefixing or mean, is strictly sub-optimal when we impose a receiver-side power constraint, showing similar to the cases of [1], [2], that receiver-side power constraints may change the solution significantly and may introduce non-trivial trade-offs.

References

[1] M. Gastpar, “On capacity under receive and spatial spectrum-sharing constraints,” *IEEE Trans. on Inform. Theory*, vol. 53, no. 2, pp. 471–487, February 2007.

[2] L. R. Varshney, “Transporting information and energy simultaneously,” in *IEEE ISIT*, July 2008.

[3] J. G. Smith, “The information capacity of amplitude and variance-constrained scalar Gaussian channels,” *Information and Control*, vol. 18, pp. 203–219, April 1971.

[4] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. on Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] S. K. Leung-Yan-Cheung and M. Hellman, “The Gaussian wire-tap channel,” *IEEE Trans. on Inform. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[7] S. Shafiee, N. Liu, and S. Ulukus, “Towards the secrecy capacity of the gaussian mimo wire-tap channel: The 2-2-1 channel,” *IEEE Trans. on Inform. Theory*, vol. 55, no. 9, pp. 4033–4039, September 2009.

[8] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennasPart II: The MIMOME wiretap channel,” *IEEE Trans. on Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, November 2010.

[9] F. Oggier and B. Hassibi, “The secrecy capacity of the MIMO wiretap channel,” *IEEE Trans. on Inform. Theory*, vol. 57, no. 8, pp. 4961–4972, August 2011.

[10] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” *IEEE Trans. on Inform. Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.

[11] H. Weingarten, Y. Steinberg, and S. Shamai, “The capacity region of the gaussian multiple-input multiple-output broadcast channel,” *IEEE Trans. on Inform. Theory*, vol. 52, no. 9, pp. 3936–3964, September 2006.

[12] E. Tekin and A. Yener, “The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming,” *IEEE Trans. on Inform. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.

[13] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “Multiple-input multiple-output Gaussian broadcast channels with confidential messages,” *IEEE Trans. on Inform. theory*, vol. 56, no. 9, pp. 4215–4227, September 2010.

[14] L. Liu, R. Zhang, and K.-C. Chua, “Secrecy wireless information and power transfer with MISO beamforming,” *IEEE Trans. on Signal Proc.*, vol. 62, no. 7, pp. 1850–1863, April 2014.

[15] D. W. K. Ng, E. S. Lo, and R. Schober, “Robust beamforming for secure communication in systems with wireless information and power transfer,” *IEEE Trans. on Wireless Comm.*, vol. 13, no. 8, pp. 4599–4615, August 2014.

[16] V. Bryant, *Metric Spaces: Iteration and Application*. Cambridge University Press, 1985.

[17] H. L. Royden and P. Fitzpatrick, *Real Analysis*. Prentice Hall, 2010.

[18] R. A. Horn and C. R. Johnson, *Matrix analysis*. Cambridge University Press, 2012.

[19] A. R. Meenakshi and C. Rajian, “On a product of positive semidefinite matrices,” *Linear Algebra and its Applications*, vol. 295, no. 1, pp. 3–6, July 1999.