SECRECY IN MIMO GAUSSIAN BIDIRECTIONAL BROADCAST CHANNELS

Rafael F. Wyrembelski and Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

ABSTRACT

Recent research developments show that the concept of bidirectional relaying significantly improves the performance in wireless networks. This applies to three-node networks, where a half-duplex relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol. In this work we assume multiple transmit and receive antennas and consider the scenario when in the broadcast phase the relay transmits additional confidential information to one node, which should be kept completely secret from the other, non-intended node. This is the *MIMO Gaussian bidirectional broadcast channel with confidential messages* for which we establish the secrecy capacity region.

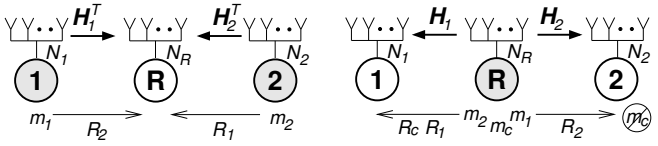
1. INTRODUCTION

The use of relays seems to be attractive since they can improve the performance of wireless networks. Unfortunately, current hardware cannot enable transmission and reception at the same time and frequency. But the inherent loss in spectral efficiency can be reduced if bidirectional communication is considered. Further, since spatial MIMO techniques improve the performance, we assume multiple antennas at all nodes.

Further, current cellular system operators offer for several users different services simultaneously subject to certain secrecy constraints. Due to the broadcast nature of the wireless medium, a transmitted signal is received by the intended user but can also be overheard by non-intended users. Consequently, the design of systems that enable secure communication to certain receivers becomes an important issue especially for the transmission of confidential information, where non-legitimated receivers should be kept ignorant of it.

In his seminal work [1] Wyner characterized the secure communication problem for a single source-destination link with an eavesdropper, the so called *wiretap channel*. In [2] Csiszár and Körner generalized this model and studied the *broadcast channel with confidential messages*. Recently, this was extended to the MIMO case by Ly *et.al.* [3].

The authors gratefully acknowledge the support of the TUM Graduate School / Faculty Graduate Center FGC-EI at Technische Universität München, Germany. The work of Holger Boche was partly supported by the German Research Foundation (DFG) under Grant BO 1734/20-1.



(a) MIMO MAC phase (b) MIMO BBC phase

Fig. 1. MIMO bidirectional relaying where the relay transmits an additional confidential message in the BBC phase.

We consider *bidirectional relaying* in a three-node network, where a relay establishes a bidirectional communication between two other nodes using a two-phase decode-and-forward protocol and thereby adds an own confidential message to the communication as shown in Fig. 1. In this work, we concentrate on the broadcast phase, where the relay has successfully decoded the two messages that it received in the previous multiple access (MAC) phase. The task of the relay is then to transmit both messages and an additional confidential message to one node, which should be kept secret from the other, non-intended node. For decoding the receiving nodes can exploit the messages they have sent in the previous phase as side information so that this channel differs from the classical broadcast channel with confidential messages and is therefore called *MIMO Gaussian bidirectional broadcast channel (BBC) with confidential messages*. Note that this differs from the wiretap scenario where the bidirectional communication itself should be secure from possible eavesdroppers outside of the network as for example studied in [4, 5].

For the MIMO Gaussian BBC without confidential messages [6], the capacity-achieving strategy combines both individual messages based on the network coding idea. Here, we have an additional confidential communication so that the optimal processing is by no means self-evident. Interestingly it shows that a superposition strategy that superimposes two signals, one for the bidirectional and one for the confidential communication, achieves the desired secrecy. The analysis of the secrecy capacity is the indispensable basis for the design of further signal processing applications and algorithms.[1]

[1] *Notation:* Mutual information and differential entropy are denoted by $I(\cdot;\cdot)$ and $h(\cdot)$; $(\cdot)^{-1}$ and $(\cdot)^T$ denote inverse and transpose; $\mathrm{tr}(\cdot)$ is the trace of a matrix; $\boldsymbol{Q} \succeq \mathbf{0}$ means the matrix $\boldsymbol{Q}$ is positive semidefinite.

2. MIMO BIDIRECTIONAL BROADCAST CHANNEL WITH CONFIDENTIAL MESSAGES

We assume N_R antennas at the relay node and N_i antennas at node i, $i = 1, 2$, as shown in Fig. 1. In the bidirectional broadcast (BBC) phase, the input-output relation between the relay node and node i is given by

$$\boldsymbol{y}_i = \boldsymbol{H}_i \boldsymbol{x} + \boldsymbol{n}_i, \tag{1}$$

where $\boldsymbol{y}_i \in \mathbb{R}^{N_i \times 1}$ denotes the output at node i, $\boldsymbol{H}_i \in \mathbb{R}^{N_i \times N_R}$ the multiplicative channel matrix, $\boldsymbol{x} \in \mathbb{R}^{N_R \times 1}$ the input of the relay node, and $\boldsymbol{n}_i \in \mathbb{R}^{N_i \times 1}$ the independent additive noise according to a Gaussian distribution $\mathcal{N}(\boldsymbol{0}, \boldsymbol{I}_{N_i})$ with zero mean and identity covariance matrix. We assume perfect channel state information at all nodes.

As in [3, 7] we consider two different kinds of power constraints: an average power constraint and a more general matrix power constraint. An input sequence $\boldsymbol{x}^n = (\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_n)$ satisfies an average power constraint P if

$$\frac{1}{n} \sum_{k=1}^{n} \boldsymbol{x}_k^T \boldsymbol{x}_k \leq P \tag{2}$$

holds. Similarly, $\boldsymbol{x}^n$ satisfies a matrix power constraint $\boldsymbol{S}$ if

$$\frac{1}{n} \sum_{k=1}^{n} \boldsymbol{x}_k \boldsymbol{x}_k^T \preceq \boldsymbol{S} \tag{3}$$

where $\boldsymbol{S}$ is a positive semidefinite matrix.

For the BBC phase we assume that the relay has successfully decoded the individual messages m_1 from node 1 and m_2 from node 2 that it received in the previous MAC phase. Then the relay transmits both individual messages to the corresponding nodes and an additional confidential message m_c to node 1 which has to be kept secret from node 2. The ignorance of node 2 about the confidential message m_c is measured by the concept of secrecy [1, 2], i.e., we require

$$\frac{1}{n} I(\mathrm{M}_c; \mathbf{Y}_2^n) \to 0 \tag{4}$$

as $n \to \infty$ where M_c denotes the random variable that is uniformly distributed over the set of confidential messages and $\mathbf{Y}_2^n = (\mathbf{Y}_{2,1}, \mathbf{Y}_{2,2}, ..., \mathbf{Y}_{2,n})$.

In our previous work [8] we analyzed the discrete memoryless case with finite input and output alphabets. There, we established the corresponding secrecy capacity region.

Theorem 1 ([8])**.** *The secrecy capacity region of the discrete memoryless BBC with confidential messages is the set of all rate triples* $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ *satisfying*

$$\begin{aligned} R_c &\leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V}; \mathrm{Y}_2|\mathrm{U}), \\ R_i &\leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \end{aligned} \tag{5}$$

for some $\mathrm{U} \to \mathrm{V} \to \mathrm{X} \to (\mathrm{Y}_1, \mathrm{Y}_2)$*, where* U *and* V *are auxiliary random variables, cf. [8] for details.*

Here, we extend this to MIMO Gaussian channels and establish the corresponding secrecy capacity region under matrix and average power constraints.

Theorem 2. *The secrecy capacity region* $\mathcal{C}_{BBC}(\boldsymbol{S})$ *of the MIMO Gaussian BBC with confidential messages under the matrix power constraint* $\boldsymbol{S}$ *is given by the set of all rate triples* $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ *that satisfy*

$$\begin{aligned} R_c &\leq \frac{1}{2} \log \left| \boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}^{(c)} \boldsymbol{H}_1^T \right| - \frac{1}{2} \log \left| \boldsymbol{I}_{N_2} + \boldsymbol{H}_2 \boldsymbol{Q}^{(c)} \boldsymbol{H}_2^T \right| \\ R_i &\leq \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{S} \boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{Q}^{(c)} \boldsymbol{H}_i^T} \right|, \quad i = 1, 2 \end{aligned}$$

for some $\boldsymbol{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}$*.*

Having [7, Lemma 1] in mind, we immediately obtain from Theorem 2 with a matrix power constraint (3) the corresponding result for an average power constraint (2) which, of course, characterizes the practically more relevant case.

Corollary 1. *The secrecy capacity region* $\mathcal{C}_{BBC}(P)$ *of the MIMO Gaussian BBC with confidential messages under the average power constraint* P *is given by the set of all rate triples* $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ *that satisfy*

$$\begin{aligned} R_c &\leq \frac{1}{2} \log \left| \boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}^{(c)} \boldsymbol{H}_1^T \right| - \frac{1}{2} \log \left| \boldsymbol{I}_{N_2} + \boldsymbol{H}_2 \boldsymbol{Q}^{(c)} \boldsymbol{H}_2^T \right| \\ R_i &\leq \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i (\boldsymbol{Q}^{(c)} + \boldsymbol{Q}^{(12)}) \boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{Q}^{(c)} \boldsymbol{H}_i^T} \right|, \quad i = 1, 2 \end{aligned}$$

for some $\boldsymbol{Q}^{(c)} \succeq \boldsymbol{0}$ *and* $\boldsymbol{Q}^{(12)} \succeq \boldsymbol{0}$ *with* $tr(\boldsymbol{Q}^{(c)} + \boldsymbol{Q}^{(12)}) \leq P$*.*

3. SECRECY-ACHIEVING STRATEGY

To prove Theorem 2 we present a secrecy-achieving strategy and, more important, prove its optimality. The main idea is to restrict the channel matrices to be square and invertible and prove the corresponding result by contradiction using channel-enhancement arguments. Then, the extension to arbitrary channel matrices follows from approximation arguments similarly as in [3, 7] for the classical MIMO Gaussian broadcast channel (with and without confidential messages).

3.1. Aligned MIMO Bidirectional Broadcast Channel

First, we consider the case where the channel matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ are square and invertible. Then, the channel model (1) can equivalently be expressed as

$$\boldsymbol{y}_i = \boldsymbol{x} + \boldsymbol{n}_i \tag{6}$$

where $\boldsymbol{y}_i, \boldsymbol{x}, \boldsymbol{n}_i \in \mathbb{R}^{N_R \times 1}$ but the additive noise $\boldsymbol{n}_i$ is now Gaussian distributed with zero mean and covariance matrix

$$\boldsymbol{\Sigma}_i = \boldsymbol{H}_i^{-1} \boldsymbol{H}_i^{-T} \in \mathbb{R}^{N_R \times N_R},$$

i.e., $\boldsymbol{n}_i \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_i)$. We follow the notation as used in [3, 7] and call the scenario (6) the *aligned* MIMO Gaussian BBC and (1) the *general* MIMO Gaussian BBC.

Theorem 3. *The secrecy capacity region $\mathcal{C}_{BBC}^{aligned}(\boldsymbol{S})$ of the aligned MIMO Gaussian BBC with confidential messages under the matrix power constraint $\boldsymbol{S}$ is given by the set of all rate triples $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ that satisfy*

$$R_c \leq \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \tag{7a}$$

$$R_i \leq \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_i}\right|, \quad i=1,2 \tag{7b}$$

for some $\mathbf{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}$.

Proof. Similarly as for the classical aligned MIMO Gaussian broadcast channel [3] the proof of achievability is a straightforward extension of its discrete counterpart. To obtain the desired region (7) for the aligned MIMO Gaussian BBC we follow the proof of the discrete case restated in Theorem 1, cf. also [8], with a proper choice of auxiliary and input random variables. More precisely, with $\mathrm{G} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{Q}^{(c)})$ and $\mathrm{U} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{S}-\boldsymbol{Q}^{(c)})$ with G and U are independent, and further $\mathrm{V}=\mathbf{X}=\mathrm{U}+\mathrm{G}$, the region (7) follows immediately from (5). Therefore we omit the details for brevity.

Remark 1. *Interestingly, a simple superposition strategy that superimposes two signals, one for the bidirectional and one for the confidential communication, suffices to achieve capacity. Moreover, an additional randomization as in the discrete case, realized by the auxiliary random variable* V *in Theorem 1, is no longer needed for MIMO Gaussian channels.*

It remains to show that this strategy is already optimal. In the following we show this by contradiction. Therefore, we construct a rate triple $(R_c^o, R_1^o, R_2^o) \in \mathbb{R}_+^3$ that lies outside the desired region (7) and assume that this rate triple is achievable by an arbitrary strategy (not necessarily the one presented above) for the aligned MIMO Gaussian BBC with confidential messages. Without loss of generality, we can assume that the matrix power constraint fulfills $\boldsymbol{S} \succ \mathbf{0}$, cf. [7, Lemma 2] for a detailed discussion.

First, we observe that achievable (individual) rates R_1^o and R_2^o are bounded from above by $R_i^o \leq \frac{1}{2}\log|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{\Sigma}_i}|$, $i=1,2$. We note that for $R_c^o = 0$ setting $\boldsymbol{Q}^{(c)} = \mathbf{0}$ in (7) actually achieves the upper bound. Further, for given achievable rates R_1^o and R_2^o the maximal achievable confidential rate R_c^* can be characterized by the following optimization problem

$$\begin{aligned} \max_{\boldsymbol{Q}^{(c)}} \quad & \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ \text{s.t.} \quad & \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_i}\right| \geq R_i^o, \quad i=1,2 \\ & \mathbf{0} \preceq \boldsymbol{Q}^{(c)} \preceq \boldsymbol{S}. \end{aligned} \tag{8}$$

Finally, we set $R_c^o = R_c^* + \delta$ for some $\delta > 0$ to ensure that the rate triple (R_c^o, R_1^o, R_2^o) lies outside the region (7) as required.

Then the Lagrangian for the corresponding minimization problem of (8) is given by

$$\begin{aligned} \mathcal{L}(\boldsymbol{Q}^{(c)}, \boldsymbol{\mu}, \boldsymbol{\Psi}_1, \boldsymbol{\Psi}_2) = {} & \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| \\ & + \sum_{i=1}^{2}\mu_i\Big(R_i^o - \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_i}\right|\Big) \\ & - \mathrm{tr}(\boldsymbol{Q}^{(c)}\boldsymbol{\Psi}_1) + \mathrm{tr}\big((\boldsymbol{Q}^{(c)}-\boldsymbol{S})\boldsymbol{\Psi}_2\big) \end{aligned}$$

with Lagrange multipliers $\boldsymbol{\mu} = (\mu_1, \mu_2) \in \mathbb{R}^2$, and $\boldsymbol{\Psi}_i \succeq \mathbf{0}$, $i=1,2$. Then, we know from the Karush-Kuhn-Tucker (KKT) conditions that the derivative of the Lagrangian must vanish at an optimal $\boldsymbol{Q}_{\text{opt}}^{(c)}$, i.e., $\nabla_{\boldsymbol{Q}^{(c)}}\mathcal{L}(\boldsymbol{Q}^{(c)}, \boldsymbol{\mu}, \boldsymbol{\Psi}_1, \boldsymbol{\Psi}_2) = \mathbf{0}$, which yields[2]

$$\begin{aligned} \frac{\mu_1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1} + \frac{\mu_2+1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1} + \boldsymbol{\Psi}_2 \\ = \frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1} + \boldsymbol{\Psi}_1 \end{aligned} \tag{9}$$

while the optimal $\boldsymbol{Q}_{\text{opt}}^{(c)}$ further has to satisfy the complementary slackness conditions

$$\mu_i\Big(R_i^o - \frac{1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right|\Big) = 0, \quad i=1,2 \tag{10}$$

$$\boldsymbol{Q}_{\text{opt}}^{(c)}\boldsymbol{\Psi}_1 = \mathbf{0}, \qquad (\boldsymbol{S}-\boldsymbol{Q}_{\text{opt}}^{(c)})\boldsymbol{\Psi}_2 = \mathbf{0} \tag{11}$$

with $\mu_i \geq 0$, $i=1,2$.

From (8) and (10) we get that the weighted secrecy sum-capacity for the rate triple (R_c^o, R_1^o, R_2^o) is given by

$$\begin{aligned} R_c^o + \mu_1 R_1^o + \mu_2 R_2^o = {} & \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ & + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right| + \delta. \end{aligned} \tag{12}$$

But in the following we show that for any achievable rate triple (R_c, R_1, R_2) the weighted secrecy sum-capacity is bounded from above by

$$\begin{aligned} R_c + \mu_1 R_1 + \mu_2 R_2 \leq {} & \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ & + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right| \end{aligned} \tag{13}$$

which establishes the desired contradiction to (12).

[2] Similarly as in [7, Appendix IV] or [3] one can easily show that a set of constraint qualifications hold for the optimization problem (8). This implies that the KKT conditions hold and are necessary for characterizing the optimal transmit covariance matrix.

3.2. Reinterpretation of Legitimate Receiver

It is beneficial to reinterpret this scenario by splitting the legitimate node 1 into two virtual receivers: one for the individual and one for the confidential message. Then, the aligned MIMO Gaussian BBC can be equivalently represented by

$$\boldsymbol{y}_{1\mathrm{a}} = \boldsymbol{x} + \boldsymbol{n}_{1\mathrm{a}} \tag{14a}$$

$$\boldsymbol{y}_{1\mathrm{b}} = \boldsymbol{x} + \boldsymbol{n}_{1\mathrm{b}} \tag{14b}$$

$$\boldsymbol{y}_{2} = \boldsymbol{x} + \boldsymbol{n}_{2} \tag{14c}$$

with $\boldsymbol{n}_{1\mathrm{a}}, \boldsymbol{n}_{1\mathrm{b}} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_1)$ and $\boldsymbol{n}_2 \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_2)$. Now, each (virtual) receiver is only interested in one message. Receiver 1a wants to know the confidential message m_c, receiver 1b the individual message m_2, and receiver 2 the individual message m_1. Again, m_c has to be kept secret from receiver 2, but, of course, need not be kept secret from the (virtual) receiver 1b.

Note that the noise of the (virtual) receivers 1a and 1b has the same covariance matrix $\boldsymbol{\Sigma}_1$ as the noise of the legitimate node 1 in (6). Similarly, the noise of receiver 2 has the same covariance matrix $\boldsymbol{\Sigma}_2$ as the one of the non-legitimated node 2 in (6). Therefore, any strategy that achieves a certain rate triple for (6) will do likewise for (14), and vice versa, so that both scenarios have the same secrecy capacity region.

3.3. Channel Enhancement

Next, we use this to construct an enhanced MIMO Gaussian BBC that reveals some kind of degradedness. For this purpose let $\widetilde{\boldsymbol{\Sigma}}_1$ be a real symmetric matrix that satisfies

$$\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)} + \widetilde{\boldsymbol{\Sigma}}_1)^{-1} = \frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1)^{-1} + \boldsymbol{\Psi}_1. \tag{15}$$

Then we know from [7, Lemma 11] that

$$\boldsymbol{0} \prec \widetilde{\boldsymbol{\Sigma}}_1 \preceq \boldsymbol{\Sigma}_1 \tag{16}$$

and

$$\left| \frac{\boldsymbol{Q}_{\text{opt}}^{(c)} + \widetilde{\boldsymbol{\Sigma}}_1}{\widetilde{\boldsymbol{\Sigma}}_1} \right| = \left| \frac{\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1} \right| \tag{17}$$

hold. With (15) Equation (9) becomes

$$\frac{\mu_1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)^{-1} + \frac{\mu_2+1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1} + \boldsymbol{\Psi}_2 = \frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)^{-1}. \tag{18}$$

Since the matrices $(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_1)^{-1}$, $(\boldsymbol{Q}_{\text{opt}}^{(c)} + \boldsymbol{\Sigma}_2)^{-1}$, and $\boldsymbol{\Psi}_2$ on the left hand side of (18) are all positive semidefinite, it follows immediately that $\frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)^{-1} \succeq \frac{1}{2}(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)^{-1}$ and consequently

$$\widetilde{\boldsymbol{\Sigma}}_1 \preceq \boldsymbol{\Sigma}_2. \tag{19}$$

This allows us to construct an enhanced MIMO Gaussian BBC by replacing the noise covariance matrix $\boldsymbol{\Sigma}_1$ of the (virtual) receiver 1a with its enhanced version $\widetilde{\boldsymbol{\Sigma}}_1$, cf. (16). Then, (14a) becomes

$$\tilde{\boldsymbol{y}}_{1\mathrm{a}} = \boldsymbol{x} + \tilde{\boldsymbol{n}}_{1\mathrm{a}} \tag{20}$$

with $\tilde{\boldsymbol{n}}_{1\mathrm{a}} \sim \mathcal{N}(\boldsymbol{0}, \widetilde{\boldsymbol{\Sigma}}_1)$, while the channels for receiver 1b and 2 remain the same. Since $\widetilde{\boldsymbol{\Sigma}}_1 \preceq \boldsymbol{\Sigma}_1$, cf. (16), the covariance matrix of the noise for receiving m_c for the enhanced BBC (20) is "*smaller*" than for the aligned BBC (14). Hence, its secrecy capacity region is at least as large as of the aligned MIMO Gaussian BBC. Moreover, (16) and (19) yield

$$\boldsymbol{0} \preceq \widetilde{\boldsymbol{\Sigma}}_1 \preceq \boldsymbol{\Sigma}_i, \quad i = 1, 2 \tag{21}$$

which means that not only the received signal $\boldsymbol{y}_{1\mathrm{b}}$ at the (virtual) receiver 1b but also $\boldsymbol{y}_2$ at the receiver 2 are (stochastically) degraded with respect to the received signal $\tilde{\boldsymbol{y}}_{1\mathrm{a}}$ at the (virtual) receiver 1a.

Similarly as in [3] for the classical MIMO Gaussian broadcast channel with confidential messages one can show that for the enhanced BBC it holds

$$R_c \leq I(\mathbf{X}; \widetilde{\mathbf{Y}}_{1\mathrm{a}}|\mathrm{U}) - I(\mathbf{X}; \mathbf{Y}_2|\mathrm{U}) \tag{22a}$$

$$R_1 \leq I(\mathrm{U}; \mathbf{Y}_{1\mathrm{b}}), \quad R_2 \leq I(\mathrm{U}; \mathbf{Y}_2) \tag{22b}$$

for some $\mathrm{U} \to \mathbf{X} \to (\widetilde{\mathbf{Y}}_{1\mathrm{a}}, \mathbf{Y}_{1\mathrm{b}}, \mathbf{Y}_2)$. Similarly as in [3, Proposition 1] the proof uses the same ideas and techniques as used for the non-degraded case [8] taking the characteristic of the bidirectional communication into account. Therefore, only slight adaptations are needed.

Remark 2. *In contrast to the non-degraded case, cf. Theorem 1, we only need one auxiliary random variable instead of two. Since the channels already reveal Markov chain properties, prefix coding realized by* V *in Theorem 1 is no longer needed.*

3.4. Weighted Secrecy Sum-Capacity

Finally, we bound the weighted secrecy sum-capacity of the enhanced MIMO Gaussian BBC to obtain the desired bound (13). This will establish the required contradiction to (12). From (22) we get for any rate triple $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ for the enhanced channel (20)

$$\begin{aligned}
&R_c + \mu_1 R_1 + \mu_2 R_2 \\
&\leq I(\mathbf{X};\widetilde{\mathbf{Y}}_{1\mathrm{a}}|\mathrm{U}) - I(\mathbf{X};\mathbf{Y}_2|\mathrm{U}) + \mu_1 I(\mathrm{U};\mathbf{Y}_{1\mathrm{b}}) + \mu_2 I(\mathrm{U};\mathbf{Y}_2) \\
&= h(\mathbf{N}_2) - h(\widetilde{\mathbf{N}}_{1\mathrm{a}}) + \mu_1 h(\mathbf{X}+\mathbf{N}_{1\mathrm{b}}) + \mu_2 h(\mathbf{X}+\mathbf{N}_2) \\
&\quad + h(\mathbf{X}+\widetilde{\mathbf{N}}_{1\mathrm{a}}|\mathrm{U}) - \mu_1 h(\mathbf{X}+\mathbf{N}_{1\mathrm{b}}|\mathrm{U}) - (\mu_2+1) h(\mathbf{X}+\mathbf{N}_2|\mathrm{U}) \\
&\leq \frac{1}{2}\log|2\pi e \boldsymbol{\Sigma}_2| - \frac{1}{2}\log|2\pi e \widetilde{\boldsymbol{\Sigma}}_1| + \sum_{i=1}^{2} \frac{\mu_i}{2} \log|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_i)| \\
&\quad + h(\mathbf{X}+\widetilde{\mathbf{N}}_{1\mathrm{a}}|\mathrm{U}) - \mu_1 h(\mathbf{X}+\mathbf{N}_{1\mathrm{b}}|\mathrm{U}) - (\mu_2+1) h(\mathbf{X}+\mathbf{N}_2|\mathrm{U})
\end{aligned} \tag{23}$$

where the last inequality follows from $h(\widetilde{\mathbf{N}}_{1\mathrm{a}}) = \frac{1}{2}\log|2\pi e \widetilde{\boldsymbol{\Sigma}}_1|$, $h(\mathbf{N}_2) = \frac{1}{2}\log|2\pi e \boldsymbol{\Sigma}_2|$ and $h(\mathbf{X}+\mathbf{N}_{1\mathrm{b}}) \leq \frac{1}{2}\log|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_1)|$, $h(\mathbf{X}+\mathbf{N}_2) \leq \frac{1}{2}\log|2\pi e(\boldsymbol{S}+\boldsymbol{\Sigma}_2)|$.

As in [3] we can apply an extremal inequality first used in [9, Corollary 4] to analyze the degraded MIMO compound

broadcast channel. With this and $\mu = \mu_1 + \mu_2 + 1$, $\lambda = \frac{\mu_1}{\mu_1+\mu_2+1}$ we get from (18)

$$\begin{aligned} h(\mathbf{X}+\widetilde{\mathbf{N}}_{1a}|\mathrm{U}) - \mu_1 h(\mathbf{X}+\mathbf{N}_{1b}|\mathrm{U}) - (\mu_2+1) h(\mathbf{X}+\mathbf{N}_2|\mathrm{U}) \\ \leq \frac{1}{2}\log|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1)| - \frac{\mu_1}{2}\log|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1)| \\ - \frac{\mu_2+1}{2}\log|2\pi e(\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2)|. \end{aligned}$$

Substituting this into (23) we end up with

$$\begin{aligned} R_c + \sum_{i=1}^{2}\mu_i R_i &\leq \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\widetilde{\boldsymbol{\Sigma}}_1}{\widetilde{\boldsymbol{\Sigma}}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ &\quad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right| \\ &= \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \\ &\quad + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}_{\text{opt}}^{(c)}+\boldsymbol{\Sigma}_i}\right| \end{aligned} \tag{24}$$

where the equality follows from (17), cf. [7, Lemma 11].

Since the secrecy capacity region of the aligned BBC (6) is contained in the corresponding region of the enhanced BBC (20), cf. Sec. 3.3, it is clear that for any rate triple (R_c, R_1, R_2) the upper bound on the weighted secrecy sum-capacity (24) – established above for the enhanced BBC – holds, of course, also for the aligned BBC. Since $\delta > 0$, this contradicts (12) and completes the proof of the optimality. Therewith the secrecy capacity region of the aligned MIMO Gaussian BBC with confidential messages is established. □

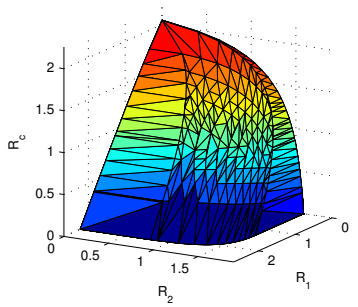
3.5. General MIMO Bidirectional Broadcast Channel

Finally, to prove Theorem 2 it remains to extend the secrecy capacity region of the aligned BBC (6) from the previous section to the general case (1), where the channel matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ need not be necessarily square and invertible. Basically, this is done by approximating the (arbitrary) channel matrices by square and invertible matrices so that Theorem 3 for the aligned case is applicable. The approximation follows [3, Sec. IV], where the corresponding result is proved for the classical broadcast channel with confidential messages.

As an example Fig. 2 depicts the secrecy capacity region of the MISO Gaussian BBC with confidential messages.

4. CONCLUSION

We analyzed secrecy in bidirectional relay networks and characterized the secrecy capacity region where it shows that a strategy that superimposes two signals – one for the bidirectional and one for the confidential communication – is optimal. This is surprising insofar as in contrast to the discrete counterpart [8] no additional randomization is needed.



$$\boldsymbol{h}_1 = \begin{bmatrix} 2 \\ 0.4 \end{bmatrix} \qquad \boldsymbol{h}_2 = \begin{bmatrix} 0.4 \\ 1.2 \end{bmatrix} \qquad P = 5$$

Fig. 2. Secrecy capacity region of the MISO Gaussian BBC with confidential messages with $N_R = 2$ and $N_1 = N_2 = 1$.

5. REFERENCES

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] H. D. Ly, T. Liu, and Y. Liang, "Multiple-Input Multiple-Output Gaussian Broadcast Channels With Common and Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[4] S. Al-Sayed and A. Sezgin, "Secrecy in Gaussian MIMO Bidirectional Broadcast Wiretap Channels: Transmit Strategies," in *Proc. Asilomar Conf. Signals, Systems, Computers*, Pacific Grove, CA, USA, Nov. 2010.

[5] A. Mukherjee and A. L. Swindlehurst, "Securing Multi-Antenna Two-Way Relay Channels With Analog Network Coding Against Eavesdroppers," in *Proc. IEEE Signal Process. Adv. Wireless Commun.*, Marrakech, Morocco, June 2010, pp. 1–5.

[6] R. F. Wyrembelski, T. J. Oechtering, I. Bjelaković, C. Schnurr, and H. Boche, "Capacity of Gaussian MIMO Bidirectional Broadcast Channels," in *IEEE Int. Symp. Inf. Theory*, Toronto, Canada, July 2008, pp. 584–588.

[7] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "The Capacity Region of the Gaussian Multiple-Input Multiple-Output Broadcast Channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sept. 2006.

[8] R. F. Wyrembelski and H. Boche, "Privacy in Bidirectional Relay Networks," *IEEE Trans. Commun.*, submitted, available at www.lti.ei.tum.de/index.php?id=31.

[9] H. Weingarten, T. Liu, S. Shamai (Shitz), Y. Steinberg, and P. Viswanath, "The Capacity Region of the Degraded Multiple-Input Multiple-Output Compound Broadcast Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 11, pp. 5011–5023, Nov. 2009.