MIMO Gaussian Broadcast Channels with Private and Confidential Messages and with Receiver Side Information

Rafael F. Schaefer*, H. Vincent Poor†, and Holger Boche*

*Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

†Department of Electrical Engineering
Princeton University, Princeton, NJ 08544 USA

***Abstract*—In this paper the two-receiver MIMO Gaussian broadcast channel with private and confidential messages and receiver side information is studied. In this communication scenario, each receiver is interested in one private and one confidential message having the other private message as side information for decoding available. Each confidential message is exclusively intended for one receiver and must therefore be kept secret from the other receiver. A complete characterization of the secrecy capacity region is established using channel enhancement arguments and an extremal entropy inequality.**

I. Introduction

Securing sensitive information in wireless networks from unauthorized access is gaining in importance so that operators of cellular systems are becoming increasingly interested in providing secure services in coexistence with other non-secure private services. Thus, the efficient physical layer implementation of multiple services such as simultaneous transmission of private and confidential messages has attracted considerable recent interest.

Secrecy techniques typically use cryptographic techniques to keep information secret. Such techniques rely on the assumption of insufficient computational capabilities of non-legitimate receivers. Due to increasing computational power and improved algorithms, these techniques are becoming less and less secure.

In this context, the concept of physical layer security is becoming attractive, since it uses only the properties of the wireless channel in order to establish security. So, regardless of the applied post-processing of non-legitimate receivers, the confidential information cannot be reproduced. Physical layer security was initiated by Wyner, who introduced the wiretap channel [1]. Later this scenario was generalized by Csiszár and Körner to the *broadcast channel with confidential messages* [2]. Recently, there has been growing interest in physical layer security; for instance see [3–5].

Since multiple-input multiple-output (MIMO) techniques can improve wireless performance significantly [6], they have been identified as a key technology for future wireless systems. Accordingly, physical layer security for MIMO systems is of growing interest. The secrecy capacity of the MIMO Gaussian wiretap channel has been established in [7–10] where the latter applied channel enhancement arguments [11, 12] to derive the secrecy capacity. Subsequently, by appropriately extending the concept of *channel enhancement*, the secrecy capacities of several MIMO multi-user scenarios have been found. This includes the broadcast channel (BC) with common and confidential messages [13], the BC with two confidential messages [14], or the BC with common and two confidential messages [15, 16].

In this paper we study the two-receiver *MIMO Gaussian BC with private and confidential messages and receiver side information*. Here, each receiver is interested in one private and one confidential message having the other private message as side information for decoding. Each confidential message is solely intended for one receiver and must therefore be kept secret from the other one. The corresponding communication scenario is depicted in Figure 1. A similar work is [17], which studies the BC with private messages and receiver side information but for discrete memoryless channels and without any secrecy constraints.

The problem at hand can be motivated by the concept of *bidirectional relaying* in a three-node network, in which a relay node establishes bidirectional communication between two other nodes using a decode-and-forward protocol. The capacity region of the bidirectional broadcast phase has been established in [18] and [19] for discrete memoryless channels and in [20] for MIMO Gaussian channels. Based on this result, the optimal transmit strategies have been characterized in [21] and [22]. In particular, if the relay transmits additional confidential information to both receivers in the broadcast phase, which has to be kept secret from the non-legitimate receiver, this corresponds exactly to the communication scenario under

This research was supported in part by the German Ministry of Education and Research (BMBF) under Grant 01BQ1050, in part by the U. S. National Science Foundation under Grant CCF-1016671, in part by the U. S. Office of Naval Research under Grant N00014-12-1-0767, and in part by the Marie Curie International Outgoing Fellowship Program under Award No. FP7-PEOPLE-IOF-2011-298532.

978-1-4673-5577-3/13/$31.00 ©2013 IEEE

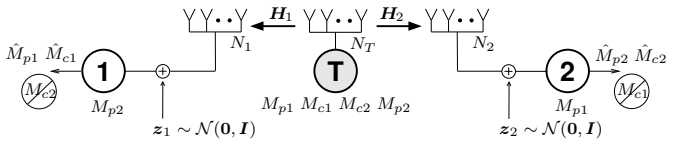

Fig. 1. MIMO Gaussian broadcast channel with private and confidential messages. Each receiver has one private message as side information available for decoding.

investigation. The efficient integration of additional services in bidirectional relay networks is further studied in [23–25].[1]

II. MIMO Gaussian Broadcast Channel

In this paper we consider a MIMO Gaussian BC with two receivers. We assume N_T antennas at the transmitter and N_i antennas at receiver i, $i = 1, 2$. Then the input-output relation between the transmitter and receiver i is given by

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

where $\boldsymbol{y}_i \in \mathbb{R}^{N_i \times 1}$ is the output at receiver i, $\boldsymbol{H}_i \in \mathbb{R}^{N_i \times N_T}$ is the multiplicative channel matrix, $\boldsymbol{x} \in \mathbb{R}^{N_T \times 1}$ is the input of the transmitter, and $\boldsymbol{z}_i \in \mathbb{R}^{N_i \times 1}$ is independent additive Gaussian noise having zero mean and identity covariance matrix. As in [13, 15, 16] and [25] we consider the matrix power constraint

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

where $\boldsymbol{S} \succeq \boldsymbol{0}$ is a positive semidefinite matrix. Note that this is a general power constraint which subsumes the average power constraint $\frac{1}{n} \sum_{k=1}^{n} \boldsymbol{x}_k^T \boldsymbol{x}_k \leq P$ as a special case.

We consider the communication scenario as depicted in Figure 1. The transmitter has two private messages M_{p1} and M_{p2} and two independent confidential messages M_{c1} and M_{c2}. The private message M_{p1} and the confidential message M_{c1} are intended for receiver 1, which has the private message M_{p2} as side information available for decoding. Accordingly, M_{p2} and M_{c2} are intended for receiver 2, which has M_{p1} available. The confidential message M_{c1} (intended for receiver 1) has to be kept secret from receiver 2. Similarly, M_{c2} (for receiver 2) has to be kept secret from receiver 1. The secrecy is measured using the information theoretic criteria [2]

$$\frac{1}{n} I(M_{c1}; \boldsymbol{Y}_2^n | M_{p1}) \to 0 \quad \text{and} \quad \frac{1}{n} I(M_{c2}; \boldsymbol{Y}_1^n | M_{p2}) \to 0$$

as $n \to \infty$ where $\boldsymbol{Y}_i^n = (\boldsymbol{Y}_{i,1}, \boldsymbol{Y}_{i,2}, ..., \boldsymbol{Y}_{i,n})$ is the output at receiver i, $i = 1, 2$. Recall that the conditioning on the private messages comes from the fact that the receivers have side information.

[1] *Notation:* Mutual information and differential entropy are denoted by $I(\cdot;\cdot)$ and $h(\cdot)$; $(\cdot)^{-1}$ and $(\cdot)^T$ are the inverse and transpose; $|\cdot|$ denotes the determinant; $\boldsymbol{A} \succeq \boldsymbol{B}$ means the matrix $\boldsymbol{A} - \boldsymbol{B}$ is positive semidefinite.

III. Secrecy Capacity

The following theorem states the main result of this paper, which is a complete characterization of the secrecy capacity region of the MIMO Gaussian BC with private and confidential messages under receiver side information.

Theorem 1: The secrecy capacity region $\mathcal{C}(\boldsymbol{S})$ of the MIMO Gaussian BC with private and confidential messages and receiver side information under the matrix power constraint $\boldsymbol{S}$ is given by the set of all rate tuples $(R_{p1}, R_{p2}, R_{c1}, R_{c2}) \in \mathbb{R}_+^4$ that satisfy

$$R_{pi} \leq \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{S} \boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i (\boldsymbol{S} - \boldsymbol{Q}_p) \boldsymbol{H}_i^T} \right|, \quad i = 1, 2$$

$$R_{c1} \leq \frac{1}{2} \log \left| \boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}_c \boldsymbol{H}_1^T \right| - \frac{1}{2} \log \left| \boldsymbol{I}_{N_2} + \boldsymbol{H}_2 \boldsymbol{Q}_c \boldsymbol{H}_2^T \right|$$

$$R_{c2} \leq \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_2} + \boldsymbol{H}_2 (\boldsymbol{S} - \boldsymbol{Q}_p) \boldsymbol{H}_2^T}{\boldsymbol{I}_{N_2} + \boldsymbol{H}_2 \boldsymbol{Q}_c \boldsymbol{H}_2^T} \right| - \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_1} + \boldsymbol{H}_1 (\boldsymbol{S} - \boldsymbol{Q}_p) \boldsymbol{H}_1^T}{\boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}_c \boldsymbol{H}_1^T} \right|$$

for some $\boldsymbol{Q}_p \succeq \boldsymbol{0}$, $\boldsymbol{Q}_c \succeq \boldsymbol{0}$, and $\boldsymbol{Q}_p + \boldsymbol{Q}_c \preceq \boldsymbol{S}$.

Having [11, Lemma 1] in mind, the secrecy capacity under the corresponding average power constraint follows immediately.

Corollary 1: The secrecy capacity region $\mathcal{C}(P)$ of the MIMO Gaussian BC with private and confidential messages and receiver side information under the average power constraint P is given by

$$\mathcal{C}(P) = \bigcup_{\boldsymbol{S} \succeq \boldsymbol{0},\, \mathrm{tr}(\boldsymbol{S}) \leq P} \mathcal{C}(\boldsymbol{S}).$$

IV. Proof of Theorem 1

To prove the desired result, it is desirable to follow previous works such as [13, 15, 16] and [25] and to consider first the *aligned* case, in which the channel matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ are square and invertible. Then, the channel model (1) can equivalently be expressed as

$$\boldsymbol{y}_i = \boldsymbol{x} + \boldsymbol{z}_i \tag{2}$$

where the additive Gaussian noise $\boldsymbol{z}_i$ has now covariance matrix $\boldsymbol{N}_i = \boldsymbol{H}_i^{-1} \boldsymbol{H}_i^{-T} \in \mathbb{R}^{N_T \times N_T}$. The corresponding secrecy capacity region of the aligned case is then specified as follows.

Theorem 2: The secrecy capacity region $\mathcal{C}_{\text{aligned}}(\boldsymbol{S})$ of the aligned MIMO Gaussian BC with private and confidential messages and receiver side information under the matrix power constraint $\boldsymbol{S}$ is given by

$$R_{pi} \leq \frac{1}{2} \log \left| \frac{\boldsymbol{S} + \boldsymbol{N}_i}{(\boldsymbol{S} - \boldsymbol{Q}_p) + \boldsymbol{N}_i} \right|, \quad i = 1, 2 \tag{3a}$$

$$R_{c1} \leq \frac{1}{2} \log \left| \frac{\boldsymbol{Q}_c + \boldsymbol{N}_1}{\boldsymbol{N}_1} \right| - \frac{1}{2} \log \left| \frac{\boldsymbol{Q}_c + \boldsymbol{N}_2}{\boldsymbol{N}_2} \right| \tag{3b}$$

$$R_{c2} \leq \frac{1}{2} \log \left| \frac{(\boldsymbol{S} - \boldsymbol{Q}_p) + \boldsymbol{N}_2}{\boldsymbol{Q}_c + \boldsymbol{N}_2} \right| - \frac{1}{2} \log \left| \frac{(\boldsymbol{S} - \boldsymbol{Q}_p) + \boldsymbol{N}_1}{\boldsymbol{Q}_c + \boldsymbol{N}_1} \right| \tag{3c}$$

for some $\boldsymbol{Q}_p \succeq \mathbf{0}$, $\boldsymbol{Q}_c \succeq \mathbf{0}$, and $\boldsymbol{Q}_p + \boldsymbol{Q}_c \preceq \boldsymbol{S}$.

Having established the secrecy capacity region of the aligned MIMO Gaussian BC, the secrecy capacity region of the general MIMO Gaussian BC follows from standard approximation and limiting arguments as in [11] and [13].

A. Proof of Achievability

Similarly to the analysis in [15] and [16], to prove the achievability of the rate region given in Theorems 1 and 2, we make use of an auxiliary result for the discrete memoryless counterpart.

Lemma 1: An achievable rate region for the discrete memoryless BC with private and confidential messages and receiver side information is given by all rate tuples $(R_{p1}, R_{p2}, R_{c1}, R_{c2}) \in \mathbb{R}_+^4$ that satisfy

$$\begin{aligned} R_{pi} &\leq I(\boldsymbol{U}; \boldsymbol{Y}_i), \quad i = 1, 2 \\ R_{c1} &\leq I(\boldsymbol{V}_1; \boldsymbol{Y}_1 | \boldsymbol{U}) - I(\boldsymbol{V}_1; \boldsymbol{V}_2, \boldsymbol{Y}_2 | \boldsymbol{U}) \\ R_{c2} &\leq I(\boldsymbol{V}_2; \boldsymbol{Y}_2 | \boldsymbol{U}) - I(\boldsymbol{V}_2; \boldsymbol{V}_1, \boldsymbol{Y}_1 | \boldsymbol{U}) \end{aligned}$$

for random variables satisfying the Markov chain relationship $(\boldsymbol{U}, \boldsymbol{V}_1, \boldsymbol{V}_2) - \boldsymbol{X} - (\boldsymbol{Y}_1, \boldsymbol{Y}_2)$.

Sketch of Proof: To achieve the desired rates we use a coding scheme that combines superposition coding and double binning similarly to the approach taken in [26]. Here, the auxiliary random variable $\boldsymbol{U}$ will carry the two private messages, cf. for example [25], while $\boldsymbol{V}_1$ and $\boldsymbol{V}_2$ are designated for the two confidential messages using a double binning technique. ■

Now, similarly to [15] and [16], the achievability for MIMO Gaussian channels follows from Lemma 1 with the choices

$$\boldsymbol{U} = \boldsymbol{U}_0 \tag{4a}$$

$$\boldsymbol{V}_1 = \boldsymbol{U}_1 + \boldsymbol{F}\boldsymbol{U}_2, \quad \boldsymbol{V}_2 = \boldsymbol{U}_2 \tag{4b}$$

$$\boldsymbol{X} = \boldsymbol{U}_0 + \boldsymbol{U}_1 + \boldsymbol{U}_2 \tag{4c}$$

with independent $\boldsymbol{U}_0 \sim \mathcal{N}(\mathbf{0}, \boldsymbol{Q}_p)$ for private messages M_{p1} and M_{p2}, $\boldsymbol{U}_1 \sim \mathcal{N}(\mathbf{0}, \boldsymbol{Q}_c)$ for confidential message M_{c1}, and $\boldsymbol{U}_2 \sim \mathcal{N}(\mathbf{0}, \boldsymbol{S} - \boldsymbol{Q}_p - \boldsymbol{Q}_c)$ for M_{c2}, and further

$$\boldsymbol{F} = \boldsymbol{Q}_c \boldsymbol{H}_1^T \big(\boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}_c \boldsymbol{H}_1^T\big)^{-1} \boldsymbol{H}_1.$$

As the following converse shows, it turns out that such a combination of superposition coding and secret dirty-paper coding, cf. (4b), suffices to achieve the entire secrecy capacity region.

B. Proof of Converse

The converse is shown by contradiction using channel enhancement arguments as used in [13, 15] and [16]. To do so, we construct a rate tuple $(R_{p1}^o, R_{p2}^o, R_{c1}^o, R_{c2}^o) \in \mathbb{R}_+^4$ that lies outside the desired region $\mathcal{C}_{\text{aligned}}(\boldsymbol{S})$ and assume that this rate tuple is achievable.

First, we observe that the achievable private rates R_{p1}^o and R_{p2}^o are bounded from above by $R_{pi}^o \leq \frac{1}{2} \log \big| \frac{\boldsymbol{S}+\boldsymbol{N}_i}{\boldsymbol{N}_i} \big|$, $i = 1, 2$. Note that for $R_{c1}^o = R_{c2}^o = 0$ with $\boldsymbol{Q}_p = \boldsymbol{S}$ and $\boldsymbol{Q}_c = \mathbf{0}$ in (3), these rates are actually achievable.

For given achievable private rates R_{p1}^o and R_{p2}^o, the maximal achievable weighted secrecy sum-rate $\lambda_1 R_{c1}^* + \lambda_2 R_{c2}^*$ for some $\lambda_1, \lambda_2 \geq 0$, can be characterized by the following optimization problem:

$$\begin{aligned} \max_{\boldsymbol{Q}_p, \boldsymbol{Q}_c} \quad & \lambda_1 f_{c1}(\boldsymbol{Q}_c) + \lambda_2 f_{c2}(\boldsymbol{Q}_p, \boldsymbol{Q}_c) \\ \text{subject to} \quad & f_{pi}(\boldsymbol{Q}_p) \geq R_{pi}^o, \quad i = 1, 2, \\ & \boldsymbol{Q}_p \succeq \mathbf{0}, \quad \boldsymbol{Q}_c \succeq \mathbf{0}, \\ & \boldsymbol{Q}_p + \boldsymbol{Q}_c \preceq \boldsymbol{S} \end{aligned} \tag{5}$$

where

$$\begin{aligned} f_{pi}(\boldsymbol{Q}_p) &\coloneqq \frac{1}{2} \log \left| \frac{\boldsymbol{S} + \boldsymbol{N}_i}{(\boldsymbol{S} - \boldsymbol{Q}_p) + \boldsymbol{N}_i} \right|, \quad i = 1, 2 \\ f_{c1}(\boldsymbol{Q}_c) &\coloneqq \frac{1}{2} \log \left| \frac{\boldsymbol{Q}_c + \boldsymbol{N}_1}{\boldsymbol{N}_1} \right| - \frac{1}{2} \log \left| \frac{\boldsymbol{Q}_c + \boldsymbol{N}_2}{\boldsymbol{N}_2} \right| \\ f_{c2}(\boldsymbol{Q}_p, \boldsymbol{Q}_c) &\coloneqq \frac{1}{2} \log \left| \frac{(\boldsymbol{S} - \boldsymbol{Q}_p) + \boldsymbol{N}_2}{\boldsymbol{Q}_c + \boldsymbol{N}_2} \right| \\ &\quad - \frac{1}{2} \log \left| \frac{(\boldsymbol{S} - \boldsymbol{Q}_p) + \boldsymbol{N}_1}{\boldsymbol{Q}_c + \boldsymbol{N}_1} \right|. \end{aligned}$$

Finally, we set R_{c1}^o and R_{c2}^o such that

$$\lambda_1 R_{c1}^o + \lambda_2 R_{c2}^o = \lambda_1 R_{c1}^* + \lambda_2 R_{c2}^* + \delta \tag{6}$$

where $\delta > 0$ ensures that $(R_{p1}^o, R_{p2}^o, R_{c1}^o, R_{c2}^o)$ actually lies outside the region $\mathcal{C}_{\text{aligned}}(\boldsymbol{S})$.

Then, the Lagrangian for the corresponding minimization problem of (5) is

$$\begin{aligned} &\mathcal{L}(\boldsymbol{Q}_p, \boldsymbol{Q}_c, \boldsymbol{\mu}, \boldsymbol{M}_p, \boldsymbol{M}_{c1}, \boldsymbol{M}_{c2}) \\ &\quad = -\lambda_1 f_{c1}(\boldsymbol{Q}_c) - \lambda_2 f_{c2}(\boldsymbol{Q}_p, \boldsymbol{Q}_c) \\ &\qquad + \sum_{i=1}^{2} \mu_i \big(R_{pi}^o - f_{pi}(\boldsymbol{Q}_p)\big) - \operatorname{tr}(\boldsymbol{M}_p \boldsymbol{Q}_p) \\ &\qquad - \operatorname{tr}(\boldsymbol{M}_{c1} \boldsymbol{Q}_c) + \operatorname{tr}((\boldsymbol{Q}_p + \boldsymbol{Q}_c - \boldsymbol{S}) \boldsymbol{M}_{c2}) \end{aligned}$$

with Lagrange multipliers $\boldsymbol{\mu} = (\mu_1, \mu_2) \in \mathbb{R}_+^2$ and $\boldsymbol{M}_p, \boldsymbol{M}_{c1}, \boldsymbol{M}_{c2} \succeq \mathbf{0}$. We know from the Karush-Kuhn-Tucker (KKT) conditions that the derivatives of the Lagrangian must vanish at an optimal $(\boldsymbol{Q}_p^*, \boldsymbol{Q}_c^*)$ which yields

$$\begin{aligned} &(\mu_1 + \lambda_2) \big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_1\big]^{-1} + \mu_2 \big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_2\big]^{-1} + \boldsymbol{M}_p \\ &\qquad = \lambda_2 \big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_2\big]^{-1} + \boldsymbol{M}_{c2} \end{aligned} \tag{7}$$

$$\begin{aligned} &(\lambda_1 + \lambda_2)(\boldsymbol{Q}_c^* + \boldsymbol{N}_1)^{-1} + \boldsymbol{M}_{c1} \\ &\qquad = (\lambda_1 + \lambda_2)(\boldsymbol{Q}_c^* + \boldsymbol{N}_2)^{-1} + \boldsymbol{M}_{c2} \end{aligned} \tag{8}$$

while the optimal $(\boldsymbol{Q}_p^*, \boldsymbol{Q}_c^*)$ further have to satisfy the complementary slackness conditions

$$\mu_i \big(R_{pi}^o - f_{pi}(\boldsymbol{Q}_p^*)\big) = 0, \quad i = 1, 2 \tag{9}$$

$$\boldsymbol{Q}_p^* \boldsymbol{M}_p = \mathbf{0}, \ \boldsymbol{Q}_c^* \boldsymbol{M}_{c1} = \mathbf{0}, \ (\boldsymbol{S} - \boldsymbol{Q}_p^* - \boldsymbol{Q}_c^*) \boldsymbol{M}_{c2} = \mathbf{0}. \tag{10}$$

Then, from (5), (6), and (9) it follows that the weighted secrecy sum-rate for the rate tuple $(R_{p1}^o, R_{p2}^o, R_{c1}^o . R_{c2}^o)$ is given by

$$\begin{aligned} &\mu_1 R_{p1}^o + \mu_2 R_{p2}^o + \lambda_1 R_{c1}^o + \lambda_2 R_{c2}^o \\ &\quad = \frac{\mu_1}{2} f_{p1}(\boldsymbol{Q}_p^*) + \frac{\mu_1}{2} f_{p1}(\boldsymbol{Q}_p^*) \\ &\qquad + \lambda_1 f_{c1}(\boldsymbol{Q}_c^*) + \lambda_2 f_{c2}(\boldsymbol{Q}_p^*, \boldsymbol{Q}_c^*) + \delta. \end{aligned} \tag{11}$$

In the following, we will find a contradiction to (11).

1) Splitting up the receivers: Next, we reinterpret the original communication scenario by splitting each receiver into two virtual receivers: one for the private message and one for the confidential message. Then the aligned MIMO Gaussian BC (2) can be equivalently represented by

$$\boldsymbol{y}_{1a} = \boldsymbol{x} + \boldsymbol{z}_{1a} \qquad \boldsymbol{y}_{1b} = \boldsymbol{x} + \boldsymbol{z}_{1b} \tag{12a}$$
$$\boldsymbol{y}_{2a} = \boldsymbol{x} + \boldsymbol{z}_{2a} \qquad \boldsymbol{y}_{2b} = \boldsymbol{x} + \boldsymbol{z}_{2b} \tag{12b}$$

with $\boldsymbol{z}_{1a}, \boldsymbol{z}_{1b} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{N}_1)$ and $\boldsymbol{z}_{2a}, \boldsymbol{z}_{2b} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{N}_2)$. Now, each (virtual) receiver is interested in only one message. The private messages M_{p1} and M_{p2} are intended for receivers 1b and 2b respectively. The confidential message M_{c1} is intended for receiver 1a and needs to be kept secret from receiver 2b, and M_{c2} is intended for receiver 2a and needs to be kept secret from receiver 1b, i.e., $\frac{1}{n} I(M_{c1}; \boldsymbol{Y}_{2b}^n | M_{p1}) \to 0$ and $\frac{1}{n} I(M_{c2}; \boldsymbol{Y}_{1b}^n | M_{p2}) \to 0$ as $n \to \infty$.

We observe that receivers 1a and 1b in (12a) are statistically identical to receiver 1 in (2), and similarly, receivers 2a and 2b in (12b) are statistically identical to receiver 2 in (2). Therefore, any strategy that achieves a certain rate tuple for (2) will do likewise for (12), and vice versa, so that we conclude that both scenarios have the same secrecy capacity region.

2) Channel enhancement: Based on this conclusion, we construct an enhanced MIMO Gaussian BC to introduce some degradedness. Therefore we define the real symmetric matrix

$$\widetilde{\boldsymbol{N}} \coloneqq \Big(\boldsymbol{N}_1^{-1} + \frac{1}{\lambda_1 + \lambda_2} \boldsymbol{M}_{c1} \Big)^{-1}$$

so that $\boldsymbol{0} \prec \widetilde{\boldsymbol{N}} \preceq \boldsymbol{N}_1$. Since $\boldsymbol{M}_{c1} \boldsymbol{Q}_c^* = \boldsymbol{0}$, we know from [11, Lemma 11] that

$$(\lambda_1 + \lambda_2)(\boldsymbol{Q}_c^* + \widetilde{\boldsymbol{N}})^{-1} = (\lambda_1 + \lambda_2)(\boldsymbol{Q}_c^* + \boldsymbol{N}_1)^{-1} + \boldsymbol{M}_{c1}$$

and

$$\left| \frac{\boldsymbol{Q}_c + \widetilde{\boldsymbol{N}}}{\widetilde{\boldsymbol{N}}} \right| = \left| \frac{\boldsymbol{Q}_c + \boldsymbol{N}_1}{\boldsymbol{N}_1} \right|. \tag{13}$$

Similarly as in [15], we also obtain with (8)

$$(\lambda_1 + \lambda_2)(\boldsymbol{Q}_c^* + \widetilde{\boldsymbol{N}})^{-1} = (\lambda_1 + \lambda_2)(\boldsymbol{Q}_c^* + \boldsymbol{N}_1)^{-1} + \boldsymbol{M}_{c2} \tag{14}$$

so that $\boldsymbol{0} \prec \widetilde{\boldsymbol{N}} \preceq \boldsymbol{N}_2$ and similarly

$$\big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \widetilde{\boldsymbol{N}}\big](\boldsymbol{Q}_c^* + \widetilde{\boldsymbol{N}})^{-1} = \big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_2\big](\boldsymbol{Q}_c^* + \boldsymbol{N}_2)^{-1}$$

as well as

$$\left| \frac{(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \widetilde{\boldsymbol{N}}}{\boldsymbol{Q}_c^* + \widetilde{\boldsymbol{N}}} \right| = \left| \frac{(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_2}{\boldsymbol{Q}_c^* + \boldsymbol{N}_2} \right|. \tag{15}$$

In addition, (7) and (14) imply

$$\begin{aligned}(\lambda_1 + \lambda_2) &\big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \widetilde{\boldsymbol{N}}\big]^{-1} \\ &= (\lambda_2 + \mu_1)\big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_1\big]^{-1} \\ &\quad + (\lambda_1 + \mu_2)\big[(\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_2\big]^{-1} + \boldsymbol{M}_p. \end{aligned} \tag{16}$$

This allows us to construct an enhanced MIMO Gaussian BC by replacing the noise covariance matrices $\boldsymbol{N}_1$ and $\boldsymbol{N}_2$ of the (virtual) receivers 1a and 2a by the enhanced version $\widetilde{\boldsymbol{N}}$. Then, (2) becomes

$$\tilde{\boldsymbol{y}}_{1a} = \boldsymbol{x} + \tilde{\boldsymbol{z}}_{1a} \qquad \boldsymbol{y}_{1b} = \boldsymbol{x} + \boldsymbol{z}_{1b} \tag{17a}$$
$$\tilde{\boldsymbol{y}}_{2a} = \boldsymbol{x} + \tilde{\boldsymbol{z}}_{2a} \qquad \boldsymbol{y}_{2b} = \boldsymbol{x} + \boldsymbol{z}_{2b} \tag{17b}$$

with $\tilde{\boldsymbol{z}}_{1a}, \tilde{\boldsymbol{z}}_{2a} \sim \mathcal{N}(\boldsymbol{0}, \widetilde{\boldsymbol{N}})$, $\boldsymbol{z}_{1b} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{N}_1)$, and $\boldsymbol{z}_{2b} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{N}_2)$. Since $\widetilde{\boldsymbol{N}} \preceq \boldsymbol{N}_i$, $i = 1, 2$, the secrecy capacity region of the enhanced channel (17) is at least as large as of the aligned channel (12).

The induced degradedness can be expressed in terms of the Markov relationships $\boldsymbol{X} - \widetilde{\boldsymbol{Y}}_{1a} - (\boldsymbol{Y}_{1b}, \boldsymbol{Y}_{2b})$ and $\boldsymbol{X} - \widetilde{\boldsymbol{Y}}_{2a} - (\boldsymbol{Y}_{1b}, \boldsymbol{Y}_{2b})$ and we obtain for the corresponding discrete memoryless counterpart the following single-letter outer bound.

Lemma 2: An outer bound on the secrecy capacity region of the discrete memoryless degraded BC with private and confidential messages and receiver side information with Markov chains $\boldsymbol{X} - \widetilde{\boldsymbol{Y}}_{1a} - (\boldsymbol{Y}_{1b}, \boldsymbol{Y}_{2b})$ and $\boldsymbol{X} - \widetilde{\boldsymbol{Y}}_{2a} - (\boldsymbol{Y}_{1b}, \boldsymbol{Y}_{2b})$ is given by

$$\begin{aligned} R_{pi} &\le I(\boldsymbol{U}; \boldsymbol{Y}_{ib}), \quad i = 1, 2 \\ R_{c1} &\le I(\boldsymbol{X}; \widetilde{\boldsymbol{Y}}_{1a} | \boldsymbol{U}) - I(\boldsymbol{X}; \boldsymbol{Y}_{2b} | \boldsymbol{U}) \\ R_{c2} &\le I(\boldsymbol{X}; \widetilde{\boldsymbol{Y}}_{2a} | \boldsymbol{U}) - I(\boldsymbol{X}; \boldsymbol{Y}_{1b} | \boldsymbol{U}). \end{aligned}$$

Sketch of proof: Following [15, Lemma 4] or [16, Lemma 4], the proof is straightforward and omitted due to space constraints. ∎

3) Outer bound: Finally, it remains to combine the previous results to contradict (11). Therefore, we bound the weighted secrecy sum-rate of the enhanced MIMO Gaussian BC as follows. From Lemma 1 we know

$$\begin{aligned} &\mu_1 R_{p1} + \mu_2 R_{p2} + \lambda_1 R_{c1} + \lambda_2 R_{c2} \\ &\quad = \mu_1 I(\boldsymbol{U}; \boldsymbol{Y}_{1b}) + \mu_2 I(\boldsymbol{U}; \boldsymbol{Y}_{2b}) \\ &\qquad + \lambda_1 \big(I(\boldsymbol{X}; \widetilde{\boldsymbol{Y}}_{1a} | \boldsymbol{U}) - I(\boldsymbol{X}; \boldsymbol{Y}_{2b} | \boldsymbol{U}) \big) \\ &\qquad + \lambda_2 \big(I(\boldsymbol{X}; \widetilde{\boldsymbol{Y}}_{2a} | \boldsymbol{U}) - I(\boldsymbol{X}; \boldsymbol{Y}_{1b} | \boldsymbol{U}) \big) \\ &\quad = \mu_1 h(\boldsymbol{X} + \boldsymbol{Z}_{1b}) + \mu_2 h(\boldsymbol{X} + \boldsymbol{Z}_{2b}) \\ &\qquad + \lambda_1 \big(h(\boldsymbol{Z}_{2b}) - h(\widetilde{\boldsymbol{Z}}_{1a}) \big) \\ &\qquad + \lambda_1 \big(h(\boldsymbol{Z}_{1b}) - h(\widetilde{\boldsymbol{Z}}_{2a}) \big) + \eta \\ &\quad \le \frac{\mu_1}{2} \log |2\pi e(\boldsymbol{S} + \boldsymbol{N}_1)| + \frac{\mu_2}{2} \log |2\pi e(\boldsymbol{S} + \boldsymbol{N}_2)| \\ &\qquad + \frac{\lambda_1}{2} \log \left| \frac{2\pi e \boldsymbol{N}_2}{2\pi e \widetilde{\boldsymbol{N}}} \right| + \frac{\lambda_2}{2} \log \left| \frac{2\pi e \boldsymbol{N}_1}{2\pi e \widetilde{\boldsymbol{N}}} \right| + \eta \end{aligned} \tag{18}$$

with

$$\begin{aligned} \eta \coloneqq{}& \lambda_1 h(\boldsymbol{X}; \widetilde{\boldsymbol{Z}}_{1a} | \boldsymbol{U}) + \lambda_2 h(\boldsymbol{X}; \widetilde{\boldsymbol{Z}}_{2a} | \boldsymbol{U}) \\ &- (\lambda_2 + \mu_1) h(\boldsymbol{X}; \boldsymbol{Z}_{1b} | \boldsymbol{U}) - (\lambda_1 + \mu_2) h(\boldsymbol{X}; \boldsymbol{Z}_{2b} | \boldsymbol{U}). \end{aligned}$$

Since $\boldsymbol{0} \prec \widetilde{\boldsymbol{N}} \preceq \{\boldsymbol{N}_1, \boldsymbol{N}_2\}$, $\boldsymbol{0} \prec \boldsymbol{Q}_p^* \preceq \boldsymbol{S}$, and $\boldsymbol{Q}_p^* \boldsymbol{M}_p = \boldsymbol{0}$, we get from [12, Corollary 4] and (16)

$$\begin{aligned} \eta \le{}& \frac{\lambda_1 + \lambda_2}{2} \log \big| 2\pi e \big((\boldsymbol{S} - \boldsymbol{Q}_p^*) + \widetilde{\boldsymbol{N}} \big) \big| \\ &- \frac{\lambda_2 + \mu_1}{2} \log \big| 2\pi e \big((\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_1 \big) \big| \\ &- \frac{\lambda_1 + \mu_2}{2} \log \big| 2\pi e \big((\boldsymbol{S} - \boldsymbol{Q}_p^*) + \boldsymbol{N}_2 \big) \big|. \end{aligned}$$

Inserting this into (18) yields

$$\begin{aligned}
&\mu_1 R_{p1} + \mu_2 R_{p2} + \lambda_1 R_{c1} + \lambda_2 R_{c2} \\
&\le \frac{\mu_1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{N}_1}{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_1}\right| + \frac{\mu_2}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{N}_2}{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_2}\right| \\
&\quad + \lambda_1\left(\frac{1}{2}\log\left|\frac{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\widetilde{\boldsymbol{N}}}{\widetilde{\boldsymbol{N}}}\right| - \frac{1}{2}\log\left|\frac{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_2}{\boldsymbol{N}_2}\right|\right) \\
&\quad + \lambda_2\left(\frac{1}{2}\log\left|\frac{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\widetilde{\boldsymbol{N}}}{\widetilde{\boldsymbol{N}}}\right| - \frac{1}{2}\log\left|\frac{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_1}{\boldsymbol{N}_1}\right|\right) \\
&= \frac{\mu_1}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{N}_1}{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_1}\right| + \frac{\mu_2}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{N}_2}{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_2}\right| \\
&\quad + \lambda_1\left(\frac{1}{2}\log\left|\frac{\boldsymbol{Q}_c^*+\boldsymbol{N}_1}{\boldsymbol{N}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}_c^*+\boldsymbol{N}_2}{\boldsymbol{N}_2}\right|\right) \\
&\quad + \lambda_2\left(\frac{1}{2}\log\left|\frac{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_2}{\boldsymbol{Q}_c^*+\boldsymbol{N}_2}\right| - \frac{1}{2}\log\left|\frac{(\boldsymbol{S}-\boldsymbol{Q}_p^*)+\boldsymbol{N}_1}{\boldsymbol{Q}_c^*+\boldsymbol{N}_1}\right|\right) \\
&= \frac{\mu_1}{2} f_{p1}(\boldsymbol{Q}_p^*) + \frac{\mu_1}{2} f_{p1}(\boldsymbol{Q}_p^*) \\
&\qquad + \lambda_1 f_{c1}(\boldsymbol{Q}_c^*) + \lambda_2 f_{c2}(\boldsymbol{Q}_p^*, \boldsymbol{Q}_c^*) \qquad (19)
\end{aligned}$$

where the equality follows from (13) and (15).

This gives us an upper bound on the weighted secrecy sum-rate of the enhanced MIMO Gaussian BC. Since the secrecy capacity region of the original aligned MIMO Gaussian BC (2) is contained the corresponding region of the enhanced MIMO Gaussian BC (17), it is clear that the upper bound (19) for the enhanced MIMO Gaussian BC is also an upper bound for the non-enhanced aligned MIMO Gaussian BC. But since $\delta > 0$, this is a contradiction to (11) which completes the proof of the converse and thereby establishes the secrecy capacity region.

V. Concluding Remarks

In this paper we have studied the two-receiver MIMO Gaussian BC with private and confidential messages and receiver side information. We have established a complete characterization of the secrecy capacity region. Interestingly, a combination of superposition coding and secrecy dirty-paper coding is sufficient to achieve the entire secrecy capacity region. The converse is shown by applying channel enhancement arguments [10, 11] and an extremal entropy inequality [12].

The superposition structure of the optimal coding strategy reveals that the private and confidential messages are encoded each on its on "level". This allows us to further include a common message intended for both receivers similarly as done in [23] and [25]. The common message M_0 with rate R_0 will affect only the two private messages and not the confidential messages. The details are omitted due to space constraints.

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] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information Theoretic Security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, 2009.

[4] E. A. Jorswieck, A. Wolf, and S. Gerbracht, "Secrecy on the Physical Layer in Wireless Networks," *Trends in Telecommunications Technologies*, pp. 413–435, Mar. 2010.

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

[6] E. Biglieri, R. Calderbank, A. Constantinides, A. Goldsmith, A. Paulraj, and H. V. Poor, *MIMO Wireless Communications*. Cambridge University Press, 2007.

[7] A. Khisti and G. W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[8] ——, "Secure Transmission With Multiple Antennas–Part II: The MIMOME Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[9] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[10] T. Liu and S. Shamai (Shitz), "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[11] 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, Sep. 2006.

[12] 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.

[13] 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.

[14] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-Input Multiple-Output Gaussian Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[15] ——, "New Results on Multiple-Input Multiple-Output Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1346–1359, Mar. 2013.

[16] E. Ekrem and S. Ulukus, "Capacity Region of Gaussian MIMO Broadcast Channels With Common and Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 58, no. 9, pp. 5669–5680, Sep. 2012.

[17] G. Kramer and S. Shamai (Shitz), "Capacity for Classes of Broadcast Channels with Receiver Side Information," in *Proc. IEEE Inf. Theory Workshop*, Tahoe City, CA, USA, Sep. 2007, pp. 313–318.

[18] T. J. Oechtering, C. Schnurr, I. Bjelaković, and H. Boche, "Broadcast Capacity Region of Two-Phase Bidirectional Relaying," *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 454–458, Jan. 2008.

[19] S. J. Kim, P. Mitran, and V. Tarokh, "Performance Bounds for Bidirectional Coded Cooperation Protocols," *IEEE Trans. Inf. Theory*, vol. 54, no. 11, pp. 5235–5241, Nov. 2008.

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

[21] T. J. Oechtering, R. F. Wyrembelski, and H. Boche, "Multiantenna Bidirectional Broadcast Channels - Optimal Transmit Strategies," *IEEE Trans. Signal Process.*, vol. 57, no. 5, pp. 1948–1958, May 2009.

[22] T. J. Oechtering, E. A. Jorswieck, R. F. Wyrembelski, and H. Boche, "On the Optimal Transmit Strategy for the MIMO Bidirectional Broadcast Channel," *IEEE Trans. Commun.*, vol. 57, no. 12, pp. 3817–3826, Dec. 2009.

[23] R. F. Wyrembelski, T. J. Oechtering, and H. Boche, "MIMO Gaussian Bidirectional Broadcast Channels with Common Messages," *IEEE Trans. Wireless Commun.*, vol. 10, no. 9, pp. 2950–2959, Sep. 2011.

[24] R. F. Wyrembelski and H. Boche, "Privacy in Bidirectional Relay Networks," *IEEE Trans. Commun.*, vol. 60, no. 6, pp. 1659–1668, Jun. 2012.

[25] ——, "Physical Layer Integration of Private, Common, and Confidential Messages in Bidirectional Relay Networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3170–3179, Sep. 2012.

[26] J. Xu, Y. Cao, and B. Chen, "Capacity Bounds for Broadcast Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529–4542, Oct. 2009.