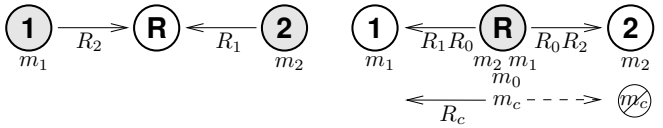
Service Integration in Multiantenna Bidirectional Relay Networks: Public and Confidential Messages

Rafael F. Wyrembelski and Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

***Abstract*—To increase the spectral efficiency of next generation wireless networks, it is important to wisely integrate multiple services at the physical layer. Here, we consider *physical layer service integration* in multiantenna bidirectional relay networks, where a relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol. In the broadcast phase the relay efficiently integrates additional common and confidential services at the physical layer, which requires the study of the *MIMO Gaussian bidirectional broadcast channel (BBC) with common and confidential messages*. We establish the secrecy capacity region which unifies previous (partial) results, where the relay provides only some of the services.**



(a) MAC phase (b) BBC phase

Fig. 1. Physical layer service integration in bidirectional relay networks. In the initial MAC phase, nodes 1 and 2 transmit their messages m_1 and m_2 with rates R_2 and R_1 to the relay node. Then, in the BBC phase, the relay forwards the messages m_1 and m_2 and adds a common message m_0 with rate R_0 to the communication and further a confidential message m_c for node 1 with rate R_c which should be kept secret from node 2.

I. Introduction

Recently, significant progress has been made in improving the performance of next generation cellular networks. One research area that is gaining importance is the efficient implementation of multiple services at the physical layer. For example, in current cellular systems, operators already offer not only traditional services such as (bidirectional) voice communication, but also further multicast services or confidential services that are subject to certain secrecy constraints. Nowadays, this is realized by policies that allocate different services on different logical channels and further by applying secrecy techniques on higher levels. In general this is quite inefficient and thus there is a trend to merge multiple coexisting services efficiently so that they work on the same wireless resources. This is referred to as *physical layer service integration* and has the potential to significantly increase the spectral efficiency for next generation wireless networks.

Since bidirectional and multicast services do not require that they are kept secret from non-legitimated receivers, they are classified as *public services*. Accordingly, services that have this additional secrecy requirement are classified as *confidential services*. Physical layer secrecy techniques are becoming more and more attractive since they do not rely on assumptions such as insufficient capabilities of non-legitimated receivers and therefore provide so-called unconditional security, cf. for example [1] for a recent survey. The *wiretap channel* [2–5] characterizes the secure communication problem for a point-to-point link with an additional eavesdropper. The *broadcast channel with confidential messages* [6, 7] generalizes this model and characterizes the optimal integration of common and confidential services at the physical layer. There are further extensions such as the MIMO Gaussian broadcast channel with common and confidential messages [8, 9], the multiple access channel with confidential messages [10], the interference channel with confidential messages [11], or the two-way wiretap channel [12].

The concept of *bidirectional relaying* has the potential to significantly improve the overall performance in wireless networks such as ad-hoc, sensor, and even cellular systems. This is mainly based on the fact that it advantageously exploits the property of bidirectional communication to reduce the inherent loss in spectral efficiency induced by half-duplex relays [13, 14]. It 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 the initial multiple access (MAC) phase two nodes transmit their messages to the relay node which decodes them. Then, in the bidirectional broadcast (BBC) phase the relay re-encodes and transmits both messages in such a way that both receiving nodes can decode their intended message using their own message from the previous phase as side information [15, 16].

In this work, we consider physical layer service integration in multiantenna bidirectional relay networks. Here, the relay integrates additional common and confidential services in the BBC phase. More precisely, in addition to the transmission of both individual messages the relay has the following tasks as shown in Figure 1: the transmission of a common message to both nodes and further, the transmission of a confidential message to one node, which should be kept secret from the other, non-legitimated node. Since the receiving nodes can use

The work was partly supported by the German Research Foundation (DFG) under Grant BO 1734/12-1 and by the German Ministry of Education and Research (BMBF) under Grant 01BU920.

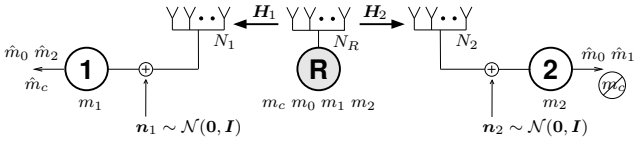


Fig. 2. General MIMO Gaussian BBC with common and confidential messages.

their own messages from the previous phase for decoding, this channel differs from the classical broadcast scenario and is therefore called *MIMO Gaussian bidirectional broadcast channel (BBC) with common and confidential messages*. For this scenario we completely characterize the integration of bidirectional, common, and confidential services at the physical layer. Further, this solves not only the optimal processing for bidirectional relay networks, but also gives us first insights for larger and more complex networks so that our results are not only relevant for itself.[1]

II. Bidirectional Broadcast Channel with Common and Confidential Messages

We assume N_R antennas at the relay node and N_i antennas at node i, $i = 1, 2$, as shown in Figure 2. The input-output relation between the relay and node i, $i = 1, 2$, 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.

We follow [7, 17] and consider two different power constraints: an average power constraint and a general matrix power constraint. An input sequence $\boldsymbol{x}^n = (\boldsymbol{x}_1, \boldsymbol{x}_2, ..., \boldsymbol{x}_n)$ of length n satisfies an average power constraint P if

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

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 $\boldsymbol{S} \succeq \boldsymbol{0}$ is a positive semidefinite matrix.

For the BBC phase we assume that the relay has successfully decoded the individual messages m_1 and m_2 which nodes 1 and 2 have been transmitted in the previous MAC phase. Besides the transmission of both individual messages, the relay has the tasks to transmit an additional common message m_0 to both nodes and a confidential message m_c to node 1 which has to be kept completely secret from the non-legitimated node 2. This is measured by the information theoretic concept of secrecy [2, 6], i.e., we require

$$\frac{1}{n} I(\mathrm{M}_c; \mathbf{Y}_2^n | \mathrm{M}_2) \underset{n \to \infty}{\longrightarrow} 0$$

which is also known as *perfect secrecy*. Here, M_c and M_2 are random variables that are uniformly distributed over the set of confidential and individual messages of node 2, respectively, and $\mathbf{Y}_2^n = (\mathbf{Y}_{2,1}, \mathbf{Y}_{2,2}, ..., \mathbf{Y}_{2,n})$ denotes the received sequence at node 2.

For discrete memoryless channels the corresponding scenario is analyzed in [18]. The resulting secrecy capacity region is restated in the following theorem.

Theorem 1 ([18]): The secrecy capacity region of the discrete memoryless BBC with common and confidential messages is the set of all rate tuples $\boldsymbol{R} = (R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ that satisfy

$$\begin{aligned} R_c &\leq I(\mathrm{V}; \mathrm{Y}_1 | \mathrm{U}) - I(\mathrm{V}; \mathrm{Y}_2 | \mathrm{U}) \\ R_0 + R_i &\leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \end{aligned}$$

for some $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$, where U and V are auxiliary random variables, cf. [18] for further details. ■

In this work, we establish a similar result for MIMO Gaussian channels under a matrix and average power constraint.

Theorem 2: The secrecy capacity region $\mathcal{C}_{\text{BBC}}(\boldsymbol{S})$ of the MIMO Gaussian BBC with common and confidential messages under the matrix power constraint $\boldsymbol{S}$ is given by the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$R_c \leq \frac{1}{2} \log \left| \boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}^{(c)} \boldsymbol{H}_1^T \right| - \frac{1}{2} \log \left| \boldsymbol{I}_{N_2} + \boldsymbol{H}_2 \boldsymbol{Q}^{(c)} \boldsymbol{H}_2^T \right| \tag{4a}$$

$$R_0 + R_i \leq \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{S} \boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{Q}^{(c)} \boldsymbol{H}_i^T} \right|, \quad i = 1, 2 \tag{4b}$$

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

With [17, Lemma 1] we can immediately deduce the secrecy capacity region for an average power constraint (2) from the corresponding result for a matrix power constraint (3).

Corollary 1: The secrecy capacity region $\mathcal{C}_{\text{BBC}}(P)$ of the MIMO Gaussian BBC with common and confidential messages under the average power constraint P is given by the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$R_c \leq \frac{1}{2} \log \left| \boldsymbol{I}_{N_1} + \boldsymbol{H}_1 \boldsymbol{Q}^{(c)} \boldsymbol{H}_1^T \right| - \frac{1}{2} \log \left| \boldsymbol{I}_{N_2} + \boldsymbol{H}_2 \boldsymbol{Q}^{(c)} \boldsymbol{H}_2^T \right|$$

$$R_0 + R_i \leq \frac{1}{2} \log \left| \frac{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i (\boldsymbol{Q}^{(c)} + \boldsymbol{Q}^{(p)}) \boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i} + \boldsymbol{H}_i \boldsymbol{Q}^{(c)} \boldsymbol{H}_i^T} \right|, \quad i = 1, 2$$

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

III. Optimal Service Integration

In this section we prove Theorem 2 and therewith establish the optimal processing for service integration at the physical layer. Similarly as for the classical broadcast channel with common and confidential messages [7] it will be convenient to first consider the special case of square and invertible channel matrices and prove the corresponding result for this case.

[1] *Notation:* Vectors and matrices are denoted by bold lower case letters and bold capital letters; $I(\cdot;\cdot)$ is the mutual information; $(\cdot)^{-1}$ and $(\cdot)^T$ denote the inverse and transpose; $\mathrm{tr}(\cdot)$ and $|\cdot|$ are the trace and determinant of a matrix; $\boldsymbol{Q} \succeq \boldsymbol{0}$ means the matrix $\boldsymbol{Q}$ is positive semidefinite.

Then, this result can easily be extended to arbitrary (possibly non-square and non-invertible) channel matrices using standard approximation arguments as in [7, 17].

A. Aligned MIMO Bidirectional Broadcast Channel

We first consider the case of square and invertible channel matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ so that multiplying both sides of (1) by $\boldsymbol{H}_i^{-1}$ yields an equivalent channel model

$$\boldsymbol{y}_i = \boldsymbol{x} + \boldsymbol{n}_i \tag{5}$$

where $\boldsymbol{y}_i, \boldsymbol{x}, \boldsymbol{n}_i \in \mathbb{R}^{N_R \times 1}$ but $\boldsymbol{n}_i$ 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., $\boldsymbol{n}_i \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_i)$, $i = 1, 2$. According to [7] we call (1) the *general* MIMO Gaussian BBC and (5) the *aligned* MIMO Gaussian BBC. For the aligned case the secrecy capacity region becomes the following.

Theorem 3: The secrecy capacity region $\mathcal{C}_{\text{BBC}}^{\text{aligned}}(\boldsymbol{S})$ of the aligned MIMO Gaussian BBC with common and confidential messages under the matrix power constraint $\boldsymbol{S}$ is the set of all rate tuples $\boldsymbol{R} \in \mathbb{R}_+^4$ that satisfy

$$R_c \le \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| \tag{6a}$$

$$R_0 + R_i \le \frac{1}{2}\log\left|\frac{\boldsymbol{S} + \boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_i}\right|, \quad i = 1, 2 \tag{6b}$$

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

1) Proof of Achievability: To prove the achievability of all rate tuples specified by (6), we follow the proof of its discrete counterpart, cf. Theorem 1 and [18], with a proper choice of auxiliary and input random variables. More precisely, we choose $\mathrm{G} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{Q}^{(c)})$ for the confidential message and $\mathrm{U} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{S} - \boldsymbol{Q}^{(c)})$ for the public messages with G and U are independent, and further $\mathrm{V} = \mathbf{X} = \mathrm{U} + \mathrm{G}$. Then, similarly as in [7] we obtain the desired region (6) immediately. ∎

2) Proof of Converse: Since the proof of converse is quite similar to the one for the MIMO Gaussian BBC with confidential messages (and no common messages) [19], we only sketch the main ideas in the following.

The converse is shown by contradiction. Therefore, we construct a rate tuple $\boldsymbol{R}^o = (R_c^o, R_0^o, R_1^o, R_2^o) \in \mathbb{R}_+^4$ that lies outside the desired region, i.e., $\boldsymbol{R}^o \notin \mathcal{C}_{\text{BBC}}^{\text{aligned}}(\boldsymbol{S})$, and assume that this rate tuple is achievable. Following [19] we obtain that for some $\mu_1, \mu_2 > 0$ the weighted secrecy sum-capacity of this constructed (outside) rate tuple $\boldsymbol{R}^o$ is given by

$$R_c^o + \mu_1(R_0^o + R_1^o) + \mu_2(R_0^o + R_2^o) = \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S} + \boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)} + \boldsymbol{\Sigma}_i}\right| + \delta \tag{7}$$

with $\delta > 0$.

To establish a contradiction to (7) it is beneficial to reinterpret the transmission scenario by splitting the legitimate node 1 into two virtual receivers: one designated for the public and one for the confidential messages. Then (5) can equivalently be written as

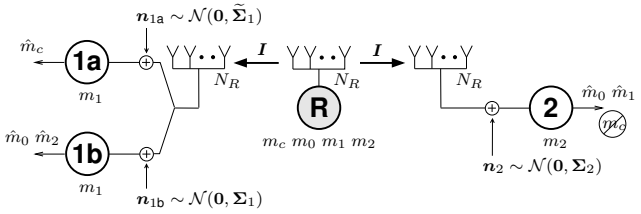


Fig. 3. Enhanced MIMO Gaussian BBC with common and confidential messages. Node 1 is split up into two virtual receivers, one enhanced for the confidential message and one for the public messages. For receiver 1a the noise covariance matrix $\boldsymbol{\Sigma}_1$ is replaced by $\widetilde{\boldsymbol{\Sigma}}_1$ to enhance the channel for the confidential message.

$$\boldsymbol{y}_{1a} = \boldsymbol{x} + \boldsymbol{n}_{1a} \tag{8a}$$

$$\boldsymbol{y}_{1b} = \boldsymbol{x} + \boldsymbol{n}_{1b} \tag{8b}$$

$$\boldsymbol{y}_2 = \boldsymbol{x} + \boldsymbol{n}_2 \tag{8c}$$

with $\boldsymbol{n}_{1a}, \boldsymbol{n}_{1b} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_1)$ and $\boldsymbol{n}_2 \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{\Sigma}_2)$. Here, each (virtual) receiver is only interested in either the public or the confidential messages. In more detail, receiver 1a is interested in the confidential message m_c, receiver 1b in the public messages m_0 and m_2, and receiver 2 in the public messages m_0 and m_1. Clearly, m_c has to be kept secret only from receiver 2 but need not be kept secret from receiver 1b.

The next step is to enhance the channel designated for the confidential message, i.e., (virtual) receiver 1a. Similarly as in [19] the idea is to construct a noise covariance matrix $\widetilde{\boldsymbol{\Sigma}}_1$ that shows the following the degradedness property

$$\widetilde{\boldsymbol{\Sigma}}_1 \preceq \boldsymbol{\Sigma}_i, \quad i = 1, 2. \tag{9}$$

Then, replacing $\boldsymbol{\Sigma}_1$ of the confidential receiver 1a by the enhanced version $\widetilde{\boldsymbol{\Sigma}}_1$, yields for (8a) the relation

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

with $\tilde{\boldsymbol{n}}_{1a} \sim \mathcal{N}(\boldsymbol{0}, \widetilde{\boldsymbol{\Sigma}}_1)$, while the channels for receiver 1b and 2 remain the same as depicted in Figure 3. Because of (9), the received signals $\boldsymbol{y}_{1b}$ and $\boldsymbol{y}_2$ at the public receivers 1b and 2 are (stochastically) degraded with respect to the received signal $\tilde{\boldsymbol{y}}_{1a}$ at the confidential receiver 1a. We call this the *enhanced* MIMO Gaussian BBC. Clearly, its secrecy capacity region is at least as large as of the original aligned BBC.

Similarly as in [7] or [19] one can show that for the enhanced MIMO Gaussian BBC with common and confidential messages the rates are bounded from above by the following mutual information terms

$$\begin{aligned} R_c &\le I(\mathbf{X}; \widetilde{\mathbf{Y}}_{1a}|\mathrm{U}) - I(\mathbf{X}; \mathbf{Y}_2|\mathrm{U}) \\ R_0 + R_1 &\le I(\mathrm{U}; \mathbf{Y}_{1b}) \\ R_0 + R_2 &\le I(\mathrm{U}; \mathbf{Y}_2) \end{aligned}$$

for some $\mathrm{U} - \mathbf{X} - \widetilde{\mathbf{Y}}_{1a} - (\mathbf{Y}_{1b}, \mathbf{Y}_2)$.

Remark 1: Because of (9) and the resulting inherent Markov chain property we need only one auxiliary random

variable U instead of both U and V as in the non-degraded case, cf. Theorem 1. This makes the evaluation of the secrecy capacity region for the enhanced MIMO Gaussian BBC tractable.

The Markov chain relation and the resulting absence of V makes it possible to apply an extremal inequality [20, Corollary 4] as in [19]. This allows us to bound for any rate tuple $\boldsymbol{R} \in \mathbb{R}_+^4$ the weighted secrecy sum-capacity in such a way that we finally end up with

$$R_c + \mu_1(R_0+R_1) + \mu_2(R_0+R_2) \leq \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_1}{\boldsymbol{\Sigma}_1}\right| - \frac{1}{2}\log\left|\frac{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_2}{\boldsymbol{\Sigma}_2}\right| + \sum_{i=1}^{2}\frac{\mu_i}{2}\log\left|\frac{\boldsymbol{S}+\boldsymbol{\Sigma}_i}{\boldsymbol{Q}^{(c)}+\boldsymbol{\Sigma}_i}\right|. \quad (10)$$

Since the secrecy capacity region of the aligned BBC is contained in the corresponding region of the enhanced BBC, it is clear that for any rate tuple $\boldsymbol{R} \in \mathbb{R}_+^4$ the upper bound on the weighted secrecy sum-capacity (10) - established above for the enhanced BBC - holds, of course, also the non-enhanced aligned BBC. But since $\delta > 0$, this contradicts (7) and completes the proof of converse. ∎

B. General MIMO Bidirectional Broadcast Channel

With the result for the aligned MIMO Gaussian BBC it is straightforward to obtain the desired corresponding result for the general MIMO Gaussian BBC.

As in the aligned case the achievability follows immediately from Theorem 1 with the same choice of auxiliary and input random variables. The converse part is established by standard approximation arguments. We follow [7, 17] and approximate any general MIMO Gaussian BBC (with possibly non-square and non-invertible) channel matrices by an appropriate aligned MIMO Gaussian BBC so that Theorem 3 is applicable. ∎

IV. Discussion

In previous section we established the secrecy capacity region of the BBC with common and confidential messages. This unifies previous results such as the BBC with confidential messages [19], the BBC with common messages [21], or the classical broadcast channel with common and confidential messages [7]. For the case of no common messages we get the following.

Corollary 2 ([19]): The secrecy capacity region of the MIMO Gaussian BBC with confidential messages under the average power constraint P is the set of all rate triples $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ that satisfy

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

for some $\boldsymbol{Q}^{(c)} \succeq \boldsymbol{0}$, $\boldsymbol{Q}^{(p)} \succeq \boldsymbol{0}$ with $\mathrm{tr}(\boldsymbol{Q}^{(c)}+\boldsymbol{Q}^{(p)}) \leq P$. ∎

If there are no confidential services for the relay to integrate, it solely transmits public services and the scenario reduces to the BBC with common messages.

Corollary 3 ([21]): The capacity region of the MIMO Gaussian BBC with common messages under the average power constraint P is the set of all rate triples $(R_0, R_1, R_2) \in \mathbb{R}_+^3$ that satisfy

$$R_0 + R_i \leq \frac{1}{2}\log\left|\boldsymbol{I}_{N_i}+\boldsymbol{H}_i\boldsymbol{Q}^{(p)}\boldsymbol{H}_i^T\right|, \quad i=1,2$$

for some $\boldsymbol{Q}^{(p)} \succeq \boldsymbol{0}$ with $\mathrm{tr}(\boldsymbol{Q}^{(p)}) \leq P$. ∎

For the case of no bidirectional messages we end up with the classical broadcast channel with common and confidential messages.

Corollary 4 ([7]): The secrecy capacity region of the MIMO Gaussian broadcast channel with common and confidential messages under the average power constraint P is the set of all rate pairs $(R_c, R_0) \in \mathbb{R}_+^2$ that satisfy

$$R_c \leq \frac{1}{2}\log\left|\boldsymbol{I}_{N_1}+\boldsymbol{H}_1\boldsymbol{Q}^{(c)}\boldsymbol{H}_1^T\right| - \frac{1}{2}\log\left|\boldsymbol{I}_{N_2}+\boldsymbol{H}_2\boldsymbol{Q}^{(c)}\boldsymbol{H}_2^T\right|$$
$$R_0 \leq \min_{i\in\{1,2\}}\left\{\frac{1}{2}\log\left|\frac{\boldsymbol{I}_{N_i}+\boldsymbol{H}_i(\boldsymbol{Q}^{(c)}+\boldsymbol{Q}^{(p)})\boldsymbol{H}_i^T}{\boldsymbol{I}_{N_i}+\boldsymbol{H}_i\boldsymbol{Q}^{(c)}\boldsymbol{H}_i^T}\right|\right\},$$

for some $\boldsymbol{Q}^{(c)} \succeq \boldsymbol{0}$, $\boldsymbol{Q}^{(p)} \succeq \boldsymbol{0}$ with $\mathrm{tr}(\boldsymbol{Q}^{(c)}+\boldsymbol{Q}^{(p)}) \leq P$. ∎

Remark 2: Clearly, the whole discussion and Corollaries 2-4 also holds for the general matrix power constraint (3).

V. Optimization Problem

The optimal transmit covariance matrices are determined by non-convex optimization problems and so the weighted rate sum optimal rate tuples as well. Hence, obtaining the boundary of the secrecy capacity region is in general non-trivial.

For the MISO scenario we can reformulate the optimization problem in such a way that it becomes convex and therewith tractable. Since the relay has multiple transmit antennas but nodes 1 and 2 have only single receive antennas, the channel matrices $\boldsymbol{H}_i$ reduce to vectors $\boldsymbol{h}_i$, $i=1,2$, and the region (4) of Theorem 2 can be written as

$$R_c \leq \frac{1}{2}\log\left(1+\frac{\boldsymbol{h}_1\boldsymbol{Q}^{(c)}\boldsymbol{h}_1^T-\boldsymbol{h}_2\boldsymbol{Q}^{(c)}\boldsymbol{h}_2^T}{1+\boldsymbol{h}_2\boldsymbol{Q}^{(c)}\boldsymbol{h}_2^T}\right) \quad (11a)$$

$$R_0+R_i \leq \frac{1}{2}\log\left(1+\frac{\boldsymbol{h}_i(\boldsymbol{S}-\boldsymbol{Q}^{(c)})\boldsymbol{h}_i^T}{1+\boldsymbol{h}_i\boldsymbol{Q}^{(c)}\boldsymbol{h}_i^T}\right),\ i=1,2. \quad (11b)$$

Next, we follow [22] or [7, Sec. V] and consider a reparametrization of the rates as

$$R_c = \log(1+\alpha\gamma_c) \quad (12a)$$
$$R_0+R_i = \log(1+\alpha\gamma_i), \quad i=1,2 \quad (12b)$$

where α is an auxiliary parameter and $\gamma_c, \gamma_1, \gamma_2$ can be interpreted as received SNR "weights". Combining (11) and (12) we end up with

$$\boldsymbol{h}_1\boldsymbol{Q}^{(c)}\boldsymbol{h}_1^T-\boldsymbol{h}_2\boldsymbol{Q}^{(c)}\boldsymbol{h}_2^T \geq \alpha\gamma_c(1+\boldsymbol{h}_2\boldsymbol{Q}^{(c)}\boldsymbol{h}_2^T) \quad (13a)$$
$$\boldsymbol{h}_i(\boldsymbol{S}-\boldsymbol{Q}^{(c)})\boldsymbol{h}_i^T \geq \alpha\gamma_i(1+\boldsymbol{h}_i\boldsymbol{Q}^{(c)}\boldsymbol{h}_i^T),\ i=1,2 \quad (13b)$$
$$\boldsymbol{S} \succeq \boldsymbol{Q}^{(c)} \succeq \boldsymbol{0}. \quad (13c)$$

Instead of using (4) to check if a rate tuple is in the capacity region, i.e., $\boldsymbol{R} \in \mathcal{C}_{\mathrm{BBC}}(\boldsymbol{S})$, one can alternatively look for a

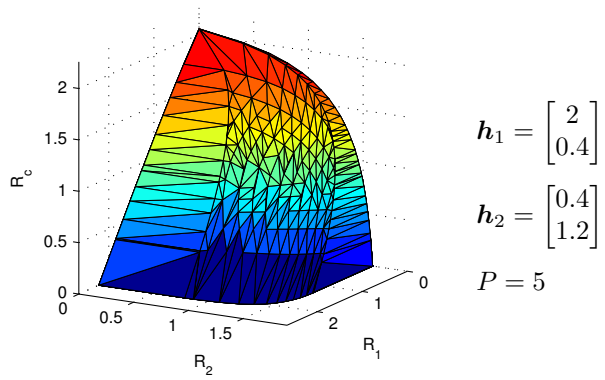


Fig. 4. Secrecy capacity region of the MISO Gaussian BBC with confidential messages with $N_R = 2$ and $N_1 = N_2 = 1$ [19].

positive semidefinite matrix $\boldsymbol{Q}^{(c)}$ that satisfies the conditions (13a)-(13c). Since all these conditions are linear in $\boldsymbol{Q}^{(c)}$, this belongs to the class of convex optimization problems which can be solved efficiently.

Obviously, all rates increase as the auxiliary parameter α increases. Thus we obtain the weighted rate sum optimal rate triple on the boundary of the secrecy capacity region $\mathcal{C}_{\text{BBC}}(\boldsymbol{S})$ for fixed weights $\gamma_c, \gamma_1, \gamma_2$ by finding the maximum α such that (13a)-(13c) provide at least one feasible solution, cf. also [7, 22]. Finally, running through all weight vectors with $\gamma_c + \gamma_1 + \gamma_2 = 1$ yields all weighted rate sum optimal rate tuples and characterizes the boundary of $\mathcal{C}_{\text{BBC}}(\boldsymbol{S})$.

Similarly, for an average power constraint P we obtain

$$\begin{aligned} &\boldsymbol{h}_1 \boldsymbol{Q}^{(c)} \boldsymbol{h}_1^T - \boldsymbol{h}_2 \boldsymbol{Q}^{(c)} \boldsymbol{h}_2^T \geq \alpha\gamma_c (1 + \boldsymbol{h}_2 \boldsymbol{Q}^{(c)} \boldsymbol{h}_2^T) \\ &\boldsymbol{h}_i \boldsymbol{Q}^{(p)} \boldsymbol{h}_i^T \geq \alpha\gamma_i (1 + \boldsymbol{h}_i \boldsymbol{Q}^{(c)} \boldsymbol{h}_i^T),\ i = 1, 2 \\ &\text{tr}(\boldsymbol{Q}^{(c)} + \boldsymbol{Q}^{(p)}) \leq P,\ \boldsymbol{Q}^{(c)} \succeq \boldsymbol{0},\ \boldsymbol{Q}^{(p)} \succeq \boldsymbol{0} \end{aligned}$$

which again allows to compute boundary of the secrecy capacity region $\mathcal{C}_{\text{BBC}}(P)$.

For visual feasibility we consider the case with no common messages and depict in Figure 4 the secrecy capacity region of the MISO Gaussian BBC with confidential messages, cf. Corollary 2. For plots of the BBC with common messages and of the classical broadcast channel with common and confidential messages we refer to [21] and [7], respectively.

VI. Conclusion

The BBC with common and confidential messages constitutes a general characterization for efficient physical layer integration of public and confidential services in bidirectional relay networks. Further, this is also a major step towards the efficient service integration in larger networks, since it gives valuable insights how services should be merged from an information-theoretic point of view. This is beneficial since it enables a joint resource allocation policy and it is expected that this will result in a significantly reduced complexity and an improved energy efficiency.

Although the secrecy capacity regions are completely established, it is worth to study the optimal transmit covariance matrices in more detail to obtain further insights as for example done in [21] for the BBC with common messages. This is left for future work.

References

[1] 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, p. 355580, 2009.

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

[3] J. Barros and M. Bloch, "Strong Secrecy for Wireless Channels," in *Int. Conf. on Information-Theoretic Security*, Calgary, Canada, Aug. 2008, pp. 40–53, invited.

[4] 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.

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

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

[7] 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.

[8] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian Broadcast Channels with Confidential and Common Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2578–2582.

[9] E. Ekrem and S. Ulukus, "Gaussian MIMO Broadcast Channels with Common and Confidential Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2583–2587.

[10] Y. Liang and H. V. Poor, "Multiple-Access Channels With Confidential Messages," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, Mar. 2008.

[11] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[12] X. He and A. Yener, "A New Outer Bound for the Secrecy Capacity Region of the Gaussian Two-Way Wiretap Channel," in *Proc. IEEE Int. Conf. Commun.*, Cape Town, South Africa, May 2010, pp. 1–5.

[13] B. Rankov and A. Wittneben, "Spectral Efficient Protocols for Half-Duplex Fading Relay Channels," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 379–389, Feb. 2007.

[14] P. Larsson, N. Johansson, and K.-E. Sunell, "Coded Bi-directional Relaying," in *Proc. 5th Scandinavian Workshop on Ad Hoc Networks*, Stockholm, Sweden, May 2005, pp. 851–855.

[15] 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.

[16] 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.

[17] 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.

[18] R. F. Wyrembelski and H. Boche, "Bidirectional Broadcast Channels with Common and Confidential Messages," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, accepted.

[19] ——, "Secrecy in MIMO Gaussian Bidirectional Broadcast Channels," in *Proc. IEEE Signal Process. Adv. Wireless Commun.*, San Francisco, CA, USA, Jun. 2011, pp. 361–365.

[20] 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.

[21] R. F. Wyrembelski, T. J. Oechtering, and H. Boche, "MIMO Bidirectional Broadcast Channels with Common Message," in *Proc. IEEE Global Commun. Conf.*, Miami, FL, USA, Dec. 2010, pp. 1–5.

[22] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz), "On the Capacity Region of the Multi-Antenna Broadcast Channel with Common Messages," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 2006, pp. 2195–2199.