Bidirectional Broadcast Channels with Common and Confidential Messages

Rafael F. Wyrembelski and Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

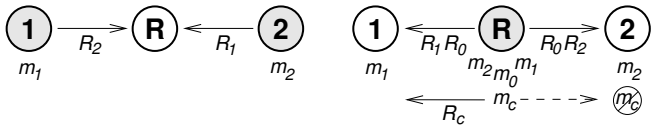
***Abstract*—In this work, we study the *bidirectional broadcast channel with common and confidential messages* and establish the capacity-equivocation and secrecy capacity regions. This problem is motivated by the concept of bidirectional relaying in a three-node network, where a relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol and thereby efficiently integrates additional common and confidential services.**

I. Introduction

Recent research developments show that the concept of *bidirectional relaying* has the potential to significantly improve the overall performance and coverage in wireless networks. This is mainly based on the fact that the property of bidirectional communication can efficiently be exploited to reduce the inherent loss in spectral efficiency induced by half-duplex relays [1, 2]. 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 [3–5]. This is also known as two-way relaying.

Furthermore, already current cellular system operators offer not only traditional services such as (bidirectional) voice communication, but also additional multicast services or confidential services that are subject to certain secrecy constraints. Nowadays, this is realized by allocating different services on different logical channels and further applying secrecy techniques on higher levels. But there is a trend to merge coexisting services efficiently from an information theoretic point of view such that they work on the same wireless resources. This is referred to as *physical layer service integration*.

Secrecy techniques on higher layers are usually based on the assumption of insufficient computational capabilities of non-legitimated receivers. Thus, physical-layer secrecy techniques are becoming more and more attractive since they do not rely on such assumptions and therefore provide so-called unconditional security. In the seminal work [6] Wyner introduced the *wiretap channel* which characterizes the secure communication problem for a point-to-point link with an eavesdropper. Csiszár and Körner generalized this to the *broadcast channel with confidential messages* in [7]. Recently, there has been growing interest in physical-layer secrecy, cf. for example [8]. Besides the (wireless) point-to-point link [6, 9, 10], there are extensions to multi-user settings as the multiple access channel with confidential messages [11], the interference channel with confidential messages [12], the MIMO Gaussian broadcast channel with common and confidential messages [13], or the two-way wiretap channel [14, 15].



(a) MAC phase (b) BBC phase

Fig. 1. Decode-and-forward bidirectional relaying. 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 and a confidential message m_c for node 1 with rate R_c to the communication which should be kept as secret as possible from node 2.

In this work, we consider bidirectional relaying where the relay node integrates additional common and confidential services within such a network. We concentrate on the broadcast phase where the relay has successfully decoded the two individual messages the nodes have sent in the previous multiple access (MAC) phase. In addition to the transmission of both individual messages the relay node 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 as secret as possible from the other, non-legitimated node. Since the receiving nodes can use their own messages from the previous phase for decoding, this channel differs from the classical broadcast channel scenario and is therefore called *bidirectional broadcast channel (BBC) with common and confidential messages*. Note that this differs from the wiretap scenario where the bidirectional communication itself should be secure from eavesdroppers outside the wireless network as for example studied in [16, 17].[1]

The authors gratefully acknowledge the support of the TUM Graduate School / Faculty Graduate Center FGC-EI at Technische Universität München, Germany. The work was supported by the German Research Foundation (DFG) under Grant BO 1734/25-1 and by the German Ministry of Education and Research (BMBF) under Grant 01BU920.

[1] *Notation:* Discrete random variables are denoted by non-italic capital letters and their realizations and ranges by lower case letters and script letters, respectively; $H(\cdot)$ and $I(\cdot;\cdot)$ are the traditional entropy and mutual information; $\mathcal{P}(\cdot)$ denotes the set of all probability distributions.

II. Bidirectional Broadcast Channel with Common and Confidential Messages

Let $\mathcal{X}$ and $\mathcal{Y}_i$, $i = 1, 2$, be finite input and output sets. Then for input and output sequences $x^n \in \mathcal{X}^n$ and $y_i^n \in \mathcal{Y}_i^n$, $i = 1, 2$, of length n, the discrete memoryless broadcast channel is given by $W^{\otimes n}(y_1^n, y_2^n|x^n) \coloneqq \prod_{k=1}^n W(y_{1,k}, y_{2,k}|x_k)$. We do not allow any cooperation between the receiving nodes so that it is sufficient to consider the marginal transition probabilities $W_i^{\otimes n} \coloneqq \prod_{k=1}^n W_i(y_{i,k}|x_k)$, $i = 1, 2$ only.

We consider the standard model with a block code of arbitrary but fixed length n. The set of individual messages of node i, $i = 1, 2$, is denoted by $\mathcal{M}_i \coloneqq \{1, ..., M_i^{(n)}\}$, which is also known at the relay node. Further, the sets of common and confidential messages of the relay node are denoted by $\mathcal{M}_0 \coloneqq \{1, ..., M_0^{(n)}\}$ and $\mathcal{M}_c \coloneqq \{1, ..., M_c^{(n)}\}$, respectively. We make use of the abbreviation $\mathcal{M} \coloneqq \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$.

In the bidirectional broadcast (BBC) phase, we assume that the relay has successfully decoded both individual messages $m_1 \in \mathcal{M}_1$ and $m_2 \in \mathcal{M}_2$ that nodes 1 and 2 transmitted in the previous multiple access (MAC) phase. Besides both individual messages the relay additionally transmits a common message $m_0 \in \mathcal{M}_0$ to both nodes and a confidential message $m_c \in \mathcal{M}_c$ to node 1, which should be kept as secret as possible from the non-legitimated node 2.

Definition 1: An $(n, M_c^{(n)}, M_0^{(n)}, M_1^{(n)}, M_2^{(n)})$*-code* for the BBC with common and confidential messages consists of one (stochastic) encoder at the relay node

$$f : \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \to \mathcal{X}^n$$

and decoders at nodes 1 and 2

$$g_1 : \mathcal{Y}_1^n \times \mathcal{M}_1 \to \mathcal{M}_c \times \mathcal{M}_0 \times \mathcal{M}_2 \cup \{0\}$$
$$g_2 : \mathcal{Y}_2^n \times \mathcal{M}_2 \to \mathcal{M}_0 \times \mathcal{M}_1 \cup \{0\}$$

where the element 0 in the definition of the decoders plays the role of an erasure symbol and is included for convenience.

Secure communication may benefit from randomized encoding [7, 8] so that we allow the encoder f to be stochastic. More precisely, the codeword $x^n \in \mathcal{X}^n$ used to transmit message $m = (m_c, m_0, m_1, m_2) \in \mathcal{M}$ is specified by conditional probabilities $f(x^n|m)$ with $\sum_{x^n \in \mathcal{X}^n} f(x^n|m) = 1$.

When the relay has sent the message $m = (m_c, m_0, m_1, m_2)$, and nodes 1 and 2 have received y_1^n and y_2^n, the decoder at node 1 is in error if $g_1(y_1^n, m_1) \neq (m_c, m_0, m_2)$. Accordingly, the decoder at node 2 is in error if $g_2(y_2^n, m_2) \neq (m_0, m_1)$. Then, the average probability of error at node i, $i = 1, 2$ is given by

$$\mu_i^{(n)} \coloneqq \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \lambda_i(m)$$

with $\lambda_1(m) = \mathbb{P}\{g_1(y_1^n, m_1) \neq (m_c, m_0, m_2)|m \text{ sent}\}$ and $\lambda_2(m) = \mathbb{P}\{g_2(y_2^n, m_2) \neq (m_0, m_1)|m \text{ sent}\}$.

The ignorance of the non-legitimated node 2 about the confidential message $m_c \in \mathcal{M}_c$ is measured by the concept of equivocation rate. Here, the equivocation rate $\frac{1}{n} H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2)$ characterizes the secrecy level of the confidential message. The higher the equivocation rate, the more ignorant is node 2 about the confidential message.

Definition 2: A rate-equivocation tuple $(R_c, R_e, R_0, R_1, R_2) \in \mathbb{R}_+^5$ is said to be *achievable* for the BBC with common and confidential messages if for any $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_c^{(n)}, M_0^{(n)}, M_1^{(n)}, M_2^{(n)})$-codes such that for all $n \geq n(\delta)$ we have $\frac{1}{n} \log M_c^{(n)} \geq R_c - \delta$, $\frac{1}{n} \log M_0^{(n)} \geq R_0 - \delta$, $\frac{1}{n} \log M_2^{(n)} \geq R_1 - \delta$, $\frac{1}{n} \log M_1^{(n)} \geq R_2 - \delta$, and

$$\tfrac{1}{n} H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2) \geq R_e - \delta \tag{1}$$

while $\mu_1^{(n)}, \mu_2^{(n)} \to 0$ as $n \to \infty$. The set of all achievable rate-equivocation tuples defines the *capacity-equivocation region of the BBC with common and confidential messages* and is denoted by $\mathcal{C}_{\mathrm{BBC}}$.

Remark 1: The secrecy condition (1) is also referred to as *weak secrecy* which is based on the fact that the information the non-legitimated node receive is small in terms of the rate. This does not imply that the absolute amount of information is also small. Therefore, this concept includes the case where the non-legitimated node might have partial knowledge about the confidential message. There exist a stronger version where (1) is strengthened by dropping the division by n. For details we refer for example to [9, 10, 18].

Now we are in the position to present the capacity-equivocation region of the BBC with common and confidential messages which is the main result of this work.

Theorem 1: The capacity-equivocation region $\mathcal{C}_{\mathrm{BBC}}$ of the BBC with common and confidential messages is the set of rate-equivocation tuples $(R_c, R_e, R_0, R_1, R_2) \in \mathbb{R}_+^5$ that satisfy

$$\begin{aligned} 0 \leq R_e &\leq R_c \\ R_e &\leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V}; \mathrm{Y}_2|\mathrm{U}) \\ R_c + R_0 + R_i &\leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \\ R_0 + R_i &\leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1, 2 \end{aligned}$$

for random variables $(\mathrm{U}, \mathrm{V}, \mathrm{X}, \mathrm{Y}_1, \mathrm{Y}_2) \in \mathcal{U} \times \mathcal{V} \times \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2$ and joint probability distribution $P_{\mathrm{U}}(u) P_{\mathrm{V}|\mathrm{U}}(v|u) P_{\mathrm{X}|\mathrm{V}}(x|v) W(y_1, y_2|x)$. The cardinalities of the ranges of U and V can be bounded by

$$|\mathcal{U}| \leq |\mathcal{X}| + 3, \qquad |\mathcal{V}| \leq |\mathcal{X}|^2 + 4|\mathcal{X}| + 3.$$

Theorem 1 immediately establishes the *secrecy capacity region $\mathcal{C}_{BBC}^S$ of the BBC with common and confidential messages* that is given by the set of all rate tuples $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ for which $(R_c, R_c, R_0, R_1, R_2) \in \mathcal{C}_{\mathrm{BBC}}$ holds.

Corollary 1: The secrecy capacity region $\mathcal{C}_{\mathrm{BBC}}^S$ of the BBC with common and confidential messages is the set of all rate tuples $(R_c, R_0, R_1, R_2) \in \mathbb{R}_+^4$ 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 random variables $(\mathrm{U}, \mathrm{V}, \mathrm{X}, \mathrm{Y}_1, \mathrm{Y}_2) \in \mathcal{U} \times \mathcal{V} \times \mathcal{X} \times \mathcal{Y}_1 \times \mathcal{Y}_2$ and joint probability distribution $P_{\mathrm{U}}(u) P_{\mathrm{V}|\mathrm{U}}(v|u) P_{\mathrm{X}|\mathrm{V}}(x|v) W(y_1, y_2|x)$. ∎

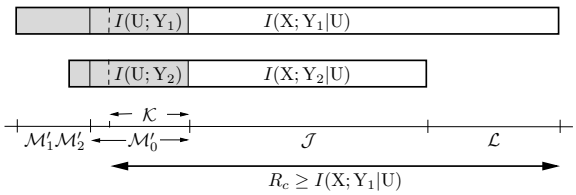


Fig. 2. The available resources of each link are split up into two parts: one designated for the common and bidirectional communication (gray) and one for the confidential message (white). Since $R_c \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, the confidential message need some resources of the common communication.

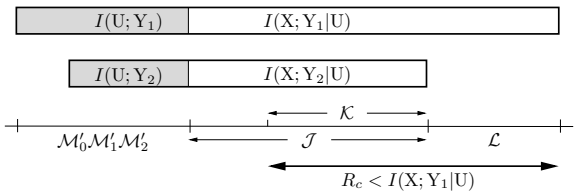


Fig. 3. Since $R_c < I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, there are more resources for the confidential message available than needed. This allows the relay to enable a stochastic encoding strategy which exploits all the available resources by introducing a mapping from $\mathcal{J}$ to $\mathcal{K}$.

Theorem 1 is proved in the following two sections which present the proof of achievability and the weak converse.

III. Achievability

Here, we present a coding strategy that achieves the desired rates with the required secrecy level. Fortunately, we are able to use the codebook design that was presented in [19] for the BBC with confidential messages (and no common message).

Lemma 1 ([19]): For any $\delta > 0$ let $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ be a Markov chain of random variables and $I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$.

i) There exists a set of codewords $u^n_{m'} \in \mathcal{U}^n$, $m' = (m_0', m_1', m_2') \in \mathcal{M}_0' \times \mathcal{M}_1' \times \mathcal{M}_2' =: \mathcal{M}'$, with

$$\tfrac{1}{n}\big(\log|\mathcal{M}_0'| + \log|\mathcal{M}_2'|\big) \geq I(\mathrm{U};\mathrm{Y}_1) - \delta$$
$$\tfrac{1}{n}\big(\log|\mathcal{M}_0'| + \log|\mathcal{M}_1'|\big) \geq I(\mathrm{U};\mathrm{Y}_2) - \delta$$

such that

$$\frac{1}{|\mathcal{M}'|}\sum_{m'\in\mathcal{M}'} \lambda_1(m_0', m_2'|m_1') \leq \epsilon^{(n)}$$
$$\frac{1}{|\mathcal{M}'|}\sum_{m'\in\mathcal{M}'} \lambda_2(m_0', m_1'|m_2') \leq \epsilon^{(n)}$$

and $\epsilon^{(n)} \to 0$ as $n \to \infty$. Thereby, $\lambda_1(m_0', m_2'|m_1')$ denotes the probability that node 1 decodes $(m_0', m_2') \in \mathcal{M}_0' \times \mathcal{M}_2'$ incorrectly if $m_1' \in \mathcal{M}_1'$ is given. The probability of error $\lambda_2(m_0', m_1'|m_2')$ for node 2 is defined accordingly.

ii) For each $u^n_{m'} \in \mathcal{U}^n$ there exists a set of codewords $x^n_{jlm'} \in \mathcal{X}^n$, $j \in \mathcal{J}$, $l \in \mathcal{L}$, $m' \in \mathcal{M}'$, with

$$\tfrac{1}{n}\log|\mathcal{J}| \geq I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta$$
$$\tfrac{1}{n}\log|\mathcal{L}| \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta$$

such that

$$\frac{1}{|\mathcal{J}||\mathcal{L}||\mathcal{M}'|}\sum_{j\in\mathcal{J}}\sum_{l\in\mathcal{L}}\sum_{m'\in\mathcal{M}'} \lambda_1(j,l|m') \leq \epsilon^{(n)}$$
$$\frac{1}{|\mathcal{J}||\mathcal{L}||\mathcal{M}'|}\sum_{j\in\mathcal{J}}\sum_{l\in\mathcal{L}}\sum_{m'\in\mathcal{M}'} \lambda_2(j|l,m') \leq \epsilon^{(n)}$$

and $\epsilon^{(n)} \to 0$ as $n \to \infty$. Here, $\lambda_1(j,l|m')$ is the probability that node 1 decodes $j \in \mathcal{J}$ or $l \in \mathcal{L}$ incorrectly if $m' \in \mathcal{M}'$ is known. Similarly, $\lambda_2(j|l,m')$ is the probability that node 2 decodes $j \in \mathcal{J}$ incorrectly if $(l,m') \in \mathcal{L} \times \mathcal{M}'$ are given. ■

This codebook reveals a specific structure with two layers. The first layer corresponds to a codebook that already enables the relay to transmit (bidirectional) individual messages and a common message, while the second layer is used for the transmission of the confidential message.

Next, we define suitable encoder and decoders for the BBC with common and confidential messages which map the confidential, common, and individual messages in an appropriate way into the codebook of Lemma 1.

Lemma 2: Let $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ and $I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) > I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$. Using the codebook from Lemma 1 all rate-equivocation tuples $(R_c, R_e, R_0, R_1, R_2) \in \mathbb{R}_+^5$ that satisfy

$$0 \leq R_e = I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) \leq R_c \quad (2a)$$
$$R_c + R_0 + R_i \leq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_i), \quad i = 1,2 \quad (2b)$$
$$R_0 + R_i \leq I(\mathrm{U};\mathrm{Y}_i), \quad i = 1,2 \quad (2c)$$

are achievable for the BBC with common and confidential messages.

Proof: For given rate-equivocation tuple $(R_c, R_e, R_0, R_1, R_2) \in \mathbb{R}_+^5$ that satisfy (2a)-(2c) we have to construct message sets, encoder, and decoders with

$$\tfrac{1}{n}\log|\mathcal{M}_c| \geq R_c - \delta, \quad (3a)$$
$$\tfrac{1}{n}\log|\mathcal{M}_0| \geq R_0 - \delta, \quad (3b)$$
$$\tfrac{1}{n}\log|\mathcal{M}_1| \geq R_2 - \delta, \quad \tfrac{1}{n}\log|\mathcal{M}_2| \geq R_1 - \delta \quad (3c)$$

and further, cf. also (1),

$$\tfrac{1}{n}H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2) \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U}) - \delta. \quad (4)$$

The construction is an extension of [19] by further integrating the common message and is mainly based on an idea of [7]. In the following we have to distinguish between two cases as shown in Figures 2 and 3.

If $R_c \geq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, cf. Figure 2, the set of confidential messages is given by

$$\mathcal{M}_c := \mathcal{J} \times \mathcal{L} \times \mathcal{K}$$

where $\mathcal{J}$ and $\mathcal{L}$ are chosen according to Lemma 1 and $\mathcal{K}$ is an arbitrary set such that (3a) holds. The sets $\mathcal{M}_1' = \mathcal{M}_1$, $\mathcal{M}_2' = \mathcal{M}_2$, and $\mathcal{M}_0' = \mathcal{M}_0 \times \mathcal{K}$ are chosen such that (3b)-(3c) are satisfied. The deterministic encoder f maps the confidential message $(j,l,k) \in \mathcal{M}_c$, and the common and individual messages $m_i \in \mathcal{M}_i$, $i = 0,1,2$, into the codeword $x^n_{jlm'} \in \mathcal{X}^n$ with $m' = (m_0', m_1', m_2')$ with $m_0' = (m_0, k)$ and $m_i' = m_i$, $i = 1,2$.

If $R_c < I(\mathrm{X};\mathrm{Y}_1|\mathrm{U})$, cf. Figure 3, the set of confidential messages is given by $\mathcal{M}_c := \mathcal{K} \times \mathcal{L}$ where $\mathcal{K}$ is arbitrary

chosen such that (3a) is satisfied. In addition, we define a mapping $h : \mathcal{J} \to \mathcal{K}$ which partitions the set $\mathcal{J}$ into subsets of "nearly equal size" [7], i.e.,

$$|h^{-1}(k)| \leq 2|h^{-1}(k')|, \qquad \text{for all } k, k' \in \mathcal{K}.$$

The sets $\mathcal{M}_i' = \mathcal{M}_i$, $i = 0, 1, 2$, are arbitrary such that (3b)-(3c) are satisfied. The stochastic encoder f maps the confidential message $(k, l) \in \mathcal{M}_c$ and the common and individual messages $m_i \in \mathcal{M}_i$, $i = 0, 1, 2$, into the codeword $x_{jlm'}^n \in \mathcal{X}^n$ with $m' = (m_0', m_1', m_2')$ and $m_i' = m_i$, $i = 0, 1, 2$. The index j is uniformly drawn from the set $h^{-1}(k) \subset \mathcal{J}$.

In both cases the decoders are immediately determined by the codebook design from Lemma 1. It remains to show that the equivocation rate fulfills (4). Since the confidential message is encoded in the same way as in [19] for the BBC with confidential messages (and no common message), we omit the details for brevity. ∎

Once we have established the achievable rate-equivocation region in Lemma 2, it is straightforward to show that this region equals the capacity-equivocation region stated in Theorem 1. Since the argumentation follows exactly the one presented in [19] or [7] we omit the details for brevity. ∎

IV. Weak Converse

We have to show that for any given sequence of $(n, M_c^{(n)}, M_0^{(n)}, M_1^{(n)}, M_2^{(n)})$-codes with $\mu_1^{(n)}, \mu_2^{(n)} \to 0$ there exist random variables $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$ such that

$$\begin{aligned}
\tfrac{1}{n} H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2) &\leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V};\mathrm{Y}_2|\mathrm{U}) + o(n^0) \\
\tfrac{1}{n}\big(H(\mathrm{M}_c) + H(\mathrm{M}_0) + H(\mathrm{M}_2)\big) &\leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_1) + o(n^0) \\
\tfrac{1}{n}\big(H(\mathrm{M}_c) + H(\mathrm{M}_0) + H(\mathrm{M}_1)\big) &\leq I(\mathrm{V};\mathrm{Y}_1|\mathrm{U}) + I(\mathrm{U};\mathrm{Y}_2) + o(n^0) \\
\tfrac{1}{n}\big(H(\mathrm{M}_0) + H(\mathrm{M}_2)\big) &\leq I(\mathrm{U};\mathrm{Y}_1) + o(n^0) \\
\tfrac{1}{n}\big(H(\mathrm{M}_0) + H(\mathrm{M}_1)\big) &\leq I(\mathrm{U};\mathrm{Y}_2) + o(n^0)
\end{aligned}$$

are satisfied. For this purpose we need a version of Fano's lemma suitable for the BBC with common and confidential messages.

Lemma 3 (Fano's inequality): For the BBC with common and confidential messages we have the following versions of Fano's inequality

$$\begin{aligned}
&H(\mathrm{M}_c, \mathrm{M}_0, \mathrm{M}_2|\mathrm{Y}_1^n, \mathrm{M}_1) \\
&\qquad \leq \mu_1^{(n)} \log(M_c^{(n)} M_0^{(n)} M_2^{(n)}) + 1 = n\epsilon_1^{(n)}, \\
&H(\mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) \\
&\qquad \leq \mu_2^{(n)} \log(M_0^{(n)} M_1^{(n)}) + 1 = n\epsilon_2^{(n)},
\end{aligned}$$

with $\epsilon_1^{(n)} = \frac{1}{n}\log(M_c^{(n)} M_0^{(n)} M_2^{(n)})\mu_1^{(n)} + \frac{1}{n} \to 0$ and $\epsilon_2^{(n)} = \frac{1}{n}\log(M_0^{(n)} M_1^{(n)})\mu_2^{(n)} + \frac{1}{n} \to 0$ for $n \to \infty$ as $\mu_1^{(n)}, \mu_2^{(n)} \to 0$.

Proof: The lemma can be shown analogously as in [3, 20], where similar versions of Fano's inequality for the BBC (without confidential messages) are presented. Therefore, we omit the details for brevity. ∎

For notational convenience we introduce the following abbreviation $\mathrm{M}_{012} = (\mathrm{M}_0, \mathrm{M}_1, \mathrm{M}_2)$. From the independence of M_c, M_0, M_1, M_2, the chain rule for entropy, the definition of mutual information, Fano's inequality, cf. Lemma 3, and the chain rule for mutual information we get for the entropies of the individual and common messages

$$\begin{aligned}
H(\mathrm{M}_0) + H(\mathrm{M}_2) &= H(\mathrm{M}_0, \mathrm{M}_2|\mathrm{M}_1) \\
&= I(\mathrm{M}_0, \mathrm{M}_2; \mathrm{Y}_1^n|\mathrm{M}_1) + H(\mathrm{M}_0, \mathrm{M}_2|\mathrm{Y}_1^n, \mathrm{M}_1) \\
&\leq I(\mathrm{M}_0, \mathrm{M}_2; \mathrm{Y}_1^n|\mathrm{M}_1) + n\epsilon_1^{(n)} \\
&\leq I(\mathrm{M}_{012}; \mathrm{Y}_1^n) + n\epsilon_1^{(n)} \qquad (5)
\end{aligned}$$

and similarly

$$H(\mathrm{M}_0) + H(\mathrm{M}_1) \leq I(\mathrm{M}_{012}; \mathrm{Y}_2^n) + n\epsilon_2^{(n)}. \qquad (6)$$

For the entropy of the confidential message we obtain

$$\begin{aligned}
H(\mathrm{M}_c) &= H(\mathrm{M}_c|\mathrm{M}_{012}) \\
&= I(\mathrm{M}_c; \mathrm{Y}_1^n|\mathrm{M}_{012}) + H(\mathrm{M}_c|\mathrm{Y}_1^n, \mathrm{M}_{012}) \\
&\leq I(\mathrm{M}_c; \mathrm{Y}_1^n|\mathrm{M}_{012}) + H(\mathrm{M}_c, \mathrm{M}_0, \mathrm{M}_2|\mathrm{Y}_1^n, \mathrm{M}_1) \\
&\leq I(\mathrm{M}_c; \mathrm{Y}_1^n|\mathrm{M}_{012}) + n\epsilon_1^{(n)} \qquad (7)
\end{aligned}$$

and further for the equivocation at the non-legitimated node

$$\begin{aligned}
H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_2) &= H(\mathrm{M}_c|\mathrm{Y}_2^n, \mathrm{M}_{012}) + I(\mathrm{M}_c; \mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) \\
&= H(\mathrm{M}_c|\mathrm{M}_{012}) - I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_{012}) \\
&\qquad + I(\mathrm{M}_c; \mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) \\
&= I(\mathrm{M}_c; \mathrm{Y}_1^n|\mathrm{M}_{012}) - I(\mathrm{M}_c; \mathrm{Y}_2|\mathrm{M}_{012}) \\
&\qquad + H(\mathrm{M}_c|\mathrm{Y}_1^n, \mathrm{M}_{012}) + I(\mathrm{M}_c; \mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) \\
&\leq I(\mathrm{M}_c; \mathrm{Y}_1^n|\mathrm{M}_{012}) - I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_{012}) \\
&\qquad + n\epsilon_1^{(n)} + n\epsilon_2^{(n)} \qquad (8)
\end{aligned}$$

where the last inequality follows from $H(\mathrm{M}_c|\mathrm{Y}_1^n, \mathrm{M}_{012}) \leq H(\mathrm{M}_c, \mathrm{M}_0, \mathrm{M}_2|\mathrm{Y}_1^n, \mathrm{M}_1) \leq n\epsilon_1^{(n)}$, $I(\mathrm{M}_c; \mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) = H(\mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) - H(\mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_c, \mathrm{M}_2) \leq H(\mathrm{M}_0, \mathrm{M}_1|\mathrm{Y}_2^n, \mathrm{M}_2) \leq n\epsilon_2^{(n)}$, and Fano's inequality, cf. Lemma 3.

Next, we expand the mutual information terms in (5)-(8) by making extensively use of the chain rule for mutual information. For notational convenience we define $\mathrm{Y}_1^k = (\mathrm{Y}_{1,1}, ..., \mathrm{Y}_{1,k})$ and $\widetilde{\mathrm{Y}}_2^k = (\mathrm{Y}_{2,k}, ..., \mathrm{Y}_{2,n})$ as suggested in [7, Sec. V] for the classical broadcast channel with confidential messages. By replacing the common message in [7, Sec. V] with our (bidirectional) individual and common messages, it is straightforward to show that, similarly as in [7, Eqs. (38)-(41)], the mutual information terms appearing in (5)-(8) can be expressed as

$$\begin{aligned}
I(\mathrm{M}_c; \mathrm{Y}_1^n|\mathrm{M}_{012}) &= \sum_{k=1}^{n} I(\mathrm{M}_c; \mathrm{Y}_{1,k}|\mathrm{Y}_1^{k-1}, \widetilde{\mathrm{Y}}_2^{k+1}, \mathrm{M}_{012}) \\
&\qquad + \Sigma_1 - \Sigma_2 \qquad (9a) \\
I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_{012}) &= \sum_{k=1}^{n} I(\mathrm{M}_c; \mathrm{Y}_{2,k}|\mathrm{Y}_1^{k-1}, \widetilde{\mathrm{Y}}_2^{k+1}, \mathrm{M}_{012}) \\
&\qquad + \Sigma_1^* - \Sigma_2^* \qquad (9b)
\end{aligned}$$

and

$$I(\mathrm{M}_{012};\mathrm{Y}_1^n) \leq \sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012};\mathrm{Y}_{1,k}) - \Sigma_1 \quad (10a)$$

$$I(\mathrm{M}_{012};\mathrm{Y}_2^n) \leq \sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012};\mathrm{Y}_{2,k}) - \Sigma_1^* \quad (10b)$$

where

$$\Sigma_1 = \sum_{k=1}^{n} I(\widetilde{\mathrm{Y}}_2^{k+1};\mathrm{Y}_{1,k}|\mathrm{Y}_1^{k-1},\mathrm{M}_{012})$$

$$\Sigma_1^* = \sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1};\mathrm{Y}_{2,k}|\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012})$$

and the analogous terms Σ_2 and Σ_2^* with M_{012} replaced by $\mathrm{M}_c,\mathrm{M}_{012}$.

Lemma 4: We have the following identities: $\Sigma_1 = \Sigma_1^*$ and $\Sigma_2 = \Sigma_2^*$.

Proof: In [7, Lemma 7] a similar result for the classical broadcast channel with confidential messages is given. The proof for our result follows immediately by simply replacing the common message in [7, Lemma 7] by our (bidirectional) individual and common messages M_1, M_2, and M_0. ∎

As in [7, Sec. V], the final step is to introduce an auxiliary random variable J that is independent of M_c, M_0, M_1, M_2, X^n, Y_1^n, and Y_2^n and uniformly distributed over $\{1,...,n\}$. Further, let

$$\begin{aligned}\mathrm{U} &\coloneqq (\mathrm{Y}_1^{\mathrm{J}-1},\widetilde{\mathrm{Y}}_2^{\mathrm{J}+1},\mathrm{M}_{012},\mathrm{J}),\\ \mathrm{V} &\coloneqq (\mathrm{U},\mathrm{M}_c),\\ \mathrm{X} &\coloneqq \mathrm{X}_{\mathrm{J}},\\ \mathrm{Y}_i &\coloneqq \mathrm{Y}_{i,\mathrm{J}}, \quad i=1,2\end{aligned}$$

so that

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{M}_c;\mathrm{Y}_{1,k}|\mathrm{Y}_1^{k-1},\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012}) = I(\mathrm{V};\mathrm{Y}_1|\mathrm{U})$$

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{M}_c;\mathrm{Y}_{2,k}|\mathrm{Y}_1^{k-1},\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012}) = I(\mathrm{V};\mathrm{Y}_2|\mathrm{U})$$

and

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012};\mathrm{Y}_{1,k}) = I(\mathrm{U};\mathrm{Y}_1|\mathrm{J}) \leq I(\mathrm{U};\mathrm{Y}_1)$$

$$\frac{1}{n}\sum_{k=1}^{n} I(\mathrm{Y}_1^{k-1},\widetilde{\mathrm{Y}}_2^{k+1},\mathrm{M}_{012};\mathrm{Y}_{2,k}) = I(\mathrm{U};\mathrm{Y}_2|\mathrm{J}) \leq I(\mathrm{U};\mathrm{Y}_2).$$

Now, to complete the proof it remains to substitute this into (9)-(10), apply Lemma 4, so that with (5)-(8) the weak converse is established. ∎

V. Conclusion

We established the capacity-equivocation and secrecy capacity regions of the BBC with common and confidential messages. This work unifies previous partial results such as the BBC with common messages [20] or the BBC with confidential messages [19]. Therefore, it constitutes a general characterization for physical layer service integration in bidirectional relay networks.

This is an important step towards the convergence of wireless services where different services are merged efficiently 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.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

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

[8] 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.

[9] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] A. El Gamal, O. O. Koyluoglu, M. Youssef, and H. El Gamal, "New Achievable Secrecy Rate Regions for the Two Way Wiretap Channel," in *Proc. IEEE Inf. Theory Workshop*, Cairo, Egypt, Jan. 2010, pp. 1–5.

[16] 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, pp. 285–289.

[17] 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, Jun. 2010, pp. 1–5.

[18] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," *Proc. EUROCRYPT 2000 on Advances in Cryptography*, vol. 1807, pp. 351–368, 2000.

[19] R. F. Wyrembelski and H. Boche, "How to Achieve Privacy in Bidirectional Relay Networks," in *Proc. IEEE Int. Symp. Inf. Theory*, Saint Petersburg, Russia, Jul. 2011, accepted.

[20] 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.