Secrecy in Broadcast Channels with Receiver Side Information

Rafael F. Wyrembelski*, Aydin Sezgin†, and Holger Boche*

*Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, Germany
†Chair of Communication Systems, Ruhr-University Bochum, Germany

***Abstract*—We study secret communication for broadcast channels with two legitimate receivers and one eavesdropper. The transmitter sends two independent confidential messages to the legitimate receivers which have to be kept secret from the eavesdropper. Here, each legitimate receiver is interested in one confidential message having the other one already as side information available. This problem arises for example in the broadcast phase in a bidirectional relay network, where a relay node establishes a bidirectional communication between two nodes while keeping the communication secure from an eavesdropper outside the network. We provide achievable rate regions and an outer bound on the secrecy capacity region.**

I. Introduction

In wireless networks a transmitted signal is received by intended users but can also be overheard by non-legitimate receivers. Thus, operators of such networks are interested in keeping the communication secret from eavesdroppers outside the network. Since secrecy techniques on higher layers are usually based on the assumption of insufficient computational capabilities of non-legitimate receivers, the use of physical layer secrecy techniques is becoming more and more attractive.

Physical layer secrecy was initiated by Wyner's seminal work [1], in which he introduced the *wiretap channel* which characterizes the scenario with one transmitter, one receiver, and one eavesdropper. Since then, there has been a growing interest in physical layer secrecy, cf. for example [2, 3]. For instance, the approach of Wyner was extended by Csiszár and Körner to the *broadcast channel with confidential messages* [4]. There are also other extensions to multi-user settings such as the MAC with confidential messages [5], the interference channel with confidential messages [6], the MIMO Gaussian broadcast channel with common and confidential messages [7, 8], or the two-way wiretap channel [9].

In this work we consider the broadcast channel with two legitimate receivers and one eavesdropper as shown in Figure 1. The transmitter sends two independent confidential messages while keeping them secret from the non-legitimate eavesdropper. The setup has its interesting twist in the fact that each legitimate receiver is interested in merely one message while having the other confidential message already as side information available for decoding. The eavesdropper wants to intercept the communication having no side information about the confidential messages available.

The work of R. F. Wyrembelski was supported by the German Research Foundation (DFG) under Grant BO 1734/25-1 and the TUM Graduate School / Faculty Graduate Center FGC-EI at Technische Universität München, Germany. The work of A. Sezgin was supported by the German Research Foundation (DFG) under Grant SE 1697/7. The work of H. Boche was supported by the German Ministry of Education and Research (BMBF) under Grant 01BU920.

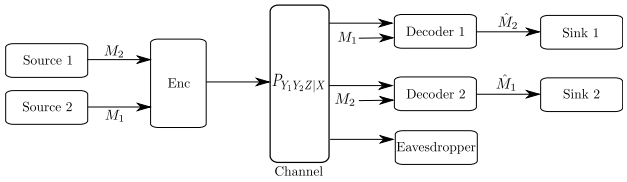

Fig. 1. Broadcast channel with legitimate receivers and one eavesdropper. The two legitimate receivers have complementary side information.

The problem at hand 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 [10, 11]. In the initial MAC phase both nodes transmit their messages to the relay node which decodes them. Assuming that in the first phase the eavesdropper was absent or not able to intercept information about the messages, the succeeding broadcast phase corresponds to the above described broadcast channel with receiver side information. In this context, it is also known as the *bidirectional broadcast wiretap channel (BBWC)*. Transmit strategies for the BBWC are also studied in [12, 13]. Privacy within the bidirectional relay network is studied in [14, 15].

II. Broadcast Channel with Receiver Side Information

Let $\mathcal{X}$ be the input set and $\mathcal{Y}_1$, $\mathcal{Y}_2$, and $\mathcal{Z}$ be the output sets of the legitimate receivers and the eavesdropper. Then for input and output sequences $x^n \in \mathcal{X}^n$ and $y_1^n \in \mathcal{Y}_1^n$, $y_2^n \in \mathcal{Y}_2^n$, $z^n \in \mathcal{Z}^n$ of length n, the discrete memoryless *broadcast channel* is given by $P_{\mathrm{Y}_1^n\mathrm{Y}_2^n\mathrm{Z}^n|\mathrm{X}^n}(y_1^n, y_2^n, z^n|x^n) := \prod_{k=1}^n P_{\mathrm{Y}_1\mathrm{Y}_2\mathrm{Z}|\mathrm{X}}(y_{1,k}, y_{2,k}, z_k|x_k)$. Since we do not allow any cooperation between the receiving nodes, it is sufficient to consider the marginal transition probabilities $P_{\mathrm{Y}_i^n|\mathrm{X}^n}(y_i^n|x^n) := \prod_{k=1}^n P_{\mathrm{Y}_i|\mathrm{X}}(y_{i,k}|x_k)$, $P_{\mathrm{Z}^n|\mathrm{X}^n}(z^n|x^n) := \prod_{k=1}^n P_{\mathrm{Z}|\mathrm{X}}(z_k|x_k)$.

In this work we consider the standard model with a block code of arbitrary but fixed length n. Let $\mathcal{M}_i := \{1, ..., M_i^{(n)}\}$ be the set of messages of node i, $i = 1, 2$, which is also known

at the transmitter. Further, we use $\mathcal{M} \coloneqq \mathcal{M}_1 \times \mathcal{M}_2$.

Definition 1: An $(n, M_1^{(n)}, M_2^{(n)})$-*code* for the broadcast channel with receiver side information consists of one encoder at the transmitter

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

and decoders at the legitimate receivers 1 and 2

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

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

When the transmitter has sent the message $m = (m_1, m_2)$, and the legitimate receivers have received y_1^n and y_2^n, the decoder at receiver 1 is in error if $g_1(y_1^n, m_1) \neq m_2$. Accordingly, the decoder at receiver 2 is in error if $g_2(y_2^n, m_2) \neq m_1$. We denote the average probability of error at receiver i by $\mu_i^{(n)}$, $i = 1, 2$.

The ignorance of the eavesdropper about the confidential messages $m_1 \in \mathcal{M}_1$ and $m_2 \in \mathcal{M}_2$ is measured by the concept of equivocation. Here, the equivocation rate $\frac{1}{n} H(\mathrm{M}_1, \mathrm{M}_2 | \mathrm{Z}^n)$ characterizes the secrecy level of the confidential messages. The higher the equivocation rate is, the more ignorant the eavesdropper about the confidential messages is.

Definition 2: A rate pair $(R_1, R_2) \in \mathbb{R}_+^2$ is said to be *achievable* for the broadcast channel with receiver side information if for any $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_1^{(n)}, M_2^{(n)})$-codes such that for all $n \geq n(\delta)$ we have $\frac{\log M_2^{(n)}}{n} \geq R_1 - \delta$, $\frac{\log M_1^{(n)}}{n} \geq R_2 - \delta$, and further

$$\tfrac{1}{n} H(\mathrm{M}_1, \mathrm{M}_2 | \mathrm{Z}^n) \geq R_1 + R_2 - \delta \tag{1}$$

while $\mu_1^{(n)}, \mu_2^{(n)} \to 0$ as $n \to \infty$. The set of all achievable rate pairs is the *secrecy capacity region* of the broadcast channel with receiver side information.

Remark 1: Note that condition (1) on the joint equivocation rate immediately implies for the single equivocation rates that

$$\tfrac{1}{n} H(\mathrm{M}_1 | \mathrm{Z}^n) \geq R_2 - \delta \quad \text{and} \quad \tfrac{1}{n} H(\mathrm{M}_2 | \mathrm{Z}^n) \geq R_1 - \delta$$

are also satisfied, cf. [16, Lemma 15] for details.

In the following sections we present two achievable secrecy rate regions and an outer bound on the secrecy capacity region of the broadcast channel with receiver side information.

III. Secret Key Approach

To keep the confidential messages secret from the eavesdropper, we make explicitly use of the available side information at the legitimate receivers in this approach.

Theorem 1: An achievable secrecy rate region for the broadcast channel with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy

$$R_i \leq \max_{P_{\mathrm{X}}} \min \big\{ I(\mathrm{X}; \mathrm{Y}_1), I(\mathrm{X}; \mathrm{Y}_2) \big\}, \quad i = 1, 2. \tag{2}$$

Proof: Recall the broadcast situation considered here. The relay wants to transmit messages m_1 and m_2 while at each receiver one of them is already as side information available. The key idea is to interpret each message as a secret key for the other message and use them as an one-time pad [17]. In more detail, the relay encodes a combined *XOR*-message

$$\widetilde{m} = m_1 \otimes m_2$$

and transmits it to both receivers. Then, this corresponds to a multicast problem and, therefore, the transmission will only be successful if the rates R_1 and R_2 satisfy (2).

If the receivers have decoded the combined message $\widetilde{m}$, they use their own message as side information to conclude on the other one, i.e., $\widetilde{m} \otimes m_1 = m_1 \otimes m_2 \otimes m_1 = m_2$ at receiver 1 and similarly $\widetilde{m} \otimes m_2 = m_1 \otimes m_2 \otimes m_2 = m_1$ at receiver 2.

Since all messages are independent, the eavesdropper is not able to conclude on the confidential messages m_1 or m_2 even if it is able to decode the combined message $\widetilde{m}$. Thus, the secrecy condition (1) is obviously satisfied. ∎

This approach exploits the structure of the network and makes use of the available side information at the receivers to guarantee the confidentiality of the transmitted messages. A drawback of this approach is that both rates are limited by the worst channel.

IV. Channel Coding Approach

In this approach we exploit the nature of the wireless channel to establish the secret communication.

Theorem 2: An achievable secrecy rate region for the broadcast channel with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ that satisfy

$$R_i \leq I(\mathrm{V}; \mathrm{Y}_i) - I(\mathrm{V}; \mathrm{Z}), \quad i = 1, 2 \tag{3}$$

for random variables $\mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Z})$.

Proof: It is sufficient to show that the rate region given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}_+^2$ satisfying

$$R_i \leq I(\mathrm{X}; \mathrm{Y}_i) - I(\mathrm{X}; \mathrm{Z}), \quad i = 1, 2,$$

with $I(\mathrm{X}; \mathrm{Y}_i) > I(\mathrm{X}; \mathrm{Z})$, $i = 1, 2$, is achievable with perfect secrecy, cf. (1). Then, the region (3) with the prefixed random variable V follows immediately from standard arguments as in [4, Lemma 4].

A. Random Codebook Generation and Coding

The most important part is the construction of a codebook with a product structure similarly as in [4]. Thereby, one part is designated for the messages to transmit and the other one is spent for additional randomization. This is done in such a way that the eavesdropper is forced to decode the randomization index at the maximum rate its channel provides so that it cannot decode the remaining information.

To achieve this, we define message sets $\mathcal{M}_1$ and $\mathcal{M}_2$ with $|\mathcal{M}_2| = \lfloor 2^{n(I(\mathrm{X};\mathrm{Y}_1) - I(\mathrm{X};\mathrm{Z}) - \delta/4)} \rfloor$ and $|\mathcal{M}_1| = \lfloor 2^{n(I(\mathrm{X};\mathrm{Y}_2) - I(\mathrm{X};\mathrm{Z}) - \delta/4)} \rfloor$ and further a randomization set $\mathcal{J}$ with $|\mathcal{J}| = \lfloor 2^{n(I(\mathrm{X};\mathrm{Z}) - \delta/4)} \rfloor$. We only consider the case where these sets are non-empty and set $\epsilon \coloneqq \delta/16$. We generate $|\mathcal{J}||\mathcal{M}_1||\mathcal{M}_2|$ independent codewords $x_{jm_1m_2}^n \in \mathcal{X}^n$ according to $P_{\mathrm{X}^n}(x^n) = \prod_{k=1}^n P_{\mathrm{X}}(x_k)$.

To sent the messages $(m_1, m_2) \in \mathcal{M}_1 \times \mathcal{M}_2$, the relay chooses uniformly at random a randomization index $j \in \mathcal{J}$ and transmits the codeword $x^n_{jm_1m_2} \in \mathcal{X}^n$.

The receivers use typical set decoding where the legitimate receivers exploit their side information to create the decoding sets. In more detail, if $x^n_{jm_1m_2} \in \mathcal{X}^n$ has been sent, receiver 1 uses the received $y^n_1 \in \mathcal{Y}^n_1$ and its own $m_1 \in \mathcal{M}_1$ to create

$$\mathcal{D}_1(m_1, y^n_1) \coloneqq \big\{(j, m_2) : (x^n_{jm_1m_2}, y^n_1) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Y}_1)\big\}.$$

If there is a unique $(j, m_2) \in \mathcal{D}_1(m_1, y^n_1)$, it declares that (j, m_1, m_2) has been sent. The decoding set $\mathcal{D}_2(m_2, y^n_2)$ and the decoding rules for receiver 2 are defined accordingly.

For given $(m_1, m_2) \in \mathcal{M}_1 \times \mathcal{M}_2$ the eavesdropper define

$$\mathcal{D}_e(m_1, m_2, z^n) \coloneqq \big\{j : (x^n_{jm_1m_2}, z^n) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Z})\big\}.$$

It declares that (j, m_1, m_2) has been sent if there is a unique $j \in \mathcal{D}_e(m_1, m_2, z^n)$.

B. Analysis of Probability of Error

For the analysis we introduce for any $(j, m_1, m_2) \in \mathcal{J} \times \mathcal{M}_1 \times \mathcal{M}_2$ the random error events at receiver 1:

$$\begin{aligned} E_{11}(j, m_2|m_1) &\coloneqq \{(x^n_{jm_1m_2}, y^n_1) \notin A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Y}_1)\} \\ E_{12}(j, m_2|m_1) &\coloneqq \{\exists(\hat{j}, \hat{m}_2) \neq (j, m_2) : \\ &\qquad (x^n_{\hat{j}m_1\hat{m}_2}, y^n_1) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Y}_1)\}. \end{aligned}$$

Obviously, from the union bound we have for the probability of error at receiver 1

$$\lambda_1(j, m_2|m_1) \leq \mathbb{P}\{E_{11}(j, m_2|m_1)\} + \mathbb{P}\{E_{12}(j, m_2|m_1)\} \quad (4)$$

where we bound each event separately in the following using standard arguments, cf. for example [18].

For the first event we know from the definition of the decoding sets, cf. also [18], that for increasing n we have

$$\mathbb{P}\big\{(x^n_{jm_1m_2}, y^n_1) \notin A^{(n)}_\epsilon(\mathrm{X}; \mathrm{Y}_1)\big\} \underset{n\to\infty}{\longrightarrow} 0. \quad (5)$$

For the second event we get

$$\begin{aligned} \mathbb{P}\big\{E_{12}\big\} &\leq |\mathcal{J}||\mathcal{M}_2|\mathbb{P}\big\{(x^n_{\hat{j}m_1\hat{m}_2}, y^n_1) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Y}_1)\big\} \\ &= |\mathcal{J}||\mathcal{M}_2| \sum_{(x^n_{\hat{j}m_1\hat{m}_2}, y^n_1) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Y}_1)} P_{\mathrm{Y}^n_1}(y^n_1) P_{\mathrm{X}^n}(x_{\hat{j}m_1\hat{m}_2}) \\ &\leq 2^{n(I(\mathrm{X};\mathrm{Z})-\delta/4)} 2^{n(I(\mathrm{X};\mathrm{Y}_1)-I(\mathrm{X};\mathrm{Z})-\delta/4)} \\ &\qquad \times 2^{n(H(\mathrm{X},\mathrm{Y}_1)+\epsilon)} 2^{-n(H(\mathrm{Y}_1)-\epsilon)} 2^{-n(H(\mathrm{X})-\epsilon)} \\ &= 2^{-n5\epsilon} \underset{n\to\infty}{\longrightarrow} 0 \end{aligned} \quad (6)$$

where the first inequality follows from the union bound, the second one from the definition of the sets $\mathcal{J}$, $\mathcal{M}_2$ and $|A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Y}_1)| \leq 2^{n(H(\mathrm{X},\mathrm{Y}_1)+\epsilon)}$, cf. [18], and the last equality from $\delta = 16\epsilon$.

Substituting (5) and (6) into (4) we conclude that $\lambda_1(j, m_2|m_1) \to 0$ as $n \to \infty$. Similarly, we also obtain $\lambda_2(j, m_1|m_2) \to 0$ as $n \to \infty$ for receiver 2.

The analysis of probability of error at the eavesdropper follows accordingly with the random error events $E_{e1}(j|m_1, m_2) \coloneqq \{(x^n_{jm_1m_2}, z^n) \notin A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Z})\}$ and $E_{e2} \coloneqq \{\exists \hat{j} \neq j : (x^n_{\hat{j}m_1m_2}, z^n) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Z})\}$. Using the same arguments it is straightforward to show that

$$\begin{aligned} \lambda_e(j|m_1, m_2) &\leq \mathbb{P}\{E_{e1}(j|m_1, m_2)\} \\ &\quad + \mathbb{P}\{E_{e2}(j|m_1, m_2)\} \underset{n\to\infty}{\longrightarrow} 0. \end{aligned} \quad (7)$$

From (4)-(7) we conclude that the probabilities of error, averaged over all codewords and codebooks, get arbitrarily small. From the random coding argument it follows that for n large enough there exists a codebook with the desired rates.

C. Equivocation Computation

It remains to verify that this codebook construction achieves the required secrecy condition (1) at the eavesdropper. Therefore, we have to show that $\frac{1}{n}H(\mathrm{M}_1, \mathrm{M}_2|\mathrm{Z}^n) \geq I(\mathrm{X}; \mathrm{Y}_1) + I(\mathrm{X}; \mathrm{Y}_2) - 2I(\mathrm{X}; \mathrm{Z}) - \delta$ is satisfied.

As in [4] we let X^n be the input random variable whose realizations are the codewords $x^n_{jm_1m_2} \in \mathcal{X}^n$. Further, let M_1 and M_2 be random variables associated with the second and third coordinate of the realization of X^n. Then, using the chain rule for entropy we get for the equivocation

$$\begin{aligned} H(\mathrm{M}_1, \mathrm{M}_2|\mathrm{Z}^n) &= H(\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n) - H(\mathrm{Z}^n) \\ &= H(\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n, \mathrm{X}^n) - H(\mathrm{X}^n|\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n) - H(\mathrm{Z}^n) \\ &= H(\mathrm{M}_1, \mathrm{M}_2, \mathrm{X}^n) + H(\mathrm{Z}^n|\mathrm{M}_1, \mathrm{M}_1, \mathrm{X}^n) \\ &\qquad - H(\mathrm{X}^n|\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n) - H(\mathrm{Z}^n) \\ &\geq H(\mathrm{X}^n) + H(\mathrm{Z}^n|\mathrm{X}^n) - H(\mathrm{X}^n|\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n) - H(\mathrm{Z}^n) \end{aligned} \quad (8)$$

where the last step follows from the fact that $(\mathrm{M}_1, \mathrm{M}_2) - \mathrm{X}^n$ forms a Markov chain. In the following we analyze all terms in (8) separately.

Since X^n has $|\mathcal{J}||\mathcal{M}_1||\mathcal{M}_2|$ possible values and we assume X^n to be independently and uniformly distributed, we have $H(\mathrm{X}^n) = \log|\mathcal{J}| + \log|\mathcal{M}_1| + \log|\mathcal{M}_2|$. From the construction of these sets, cf. Section IV-A, we obtain $\frac{1}{n}H(\mathrm{X}^n) \underset{n\to\infty}{\longrightarrow} I(\mathrm{X}; \mathrm{Y}_1) + I(\mathrm{X}; \mathrm{Y}_2) - I(\mathrm{X}; \mathrm{Z}) - \frac{3}{4}\delta$.

For second term in (8) we get from the weak law of large numbers $\frac{1}{n}H(\mathrm{Z}^n|\mathrm{X}^n) \to H(\mathrm{Z}|\mathrm{X})$ as $n \to \infty$.

For the third term we define $\varphi(m_1, m_2, z^n) = x^n_{jm_1m_2}$ if $(x^n_{jm_1m_2}, z^n) \in A^{(n)}_\epsilon(\mathrm{X}, \mathrm{Z})$ for some unique $j \in \mathcal{J}$ and arbitrary otherwise. Then we have $\mathbb{P}\{\mathrm{X}^n \neq \varphi(\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n)\} \leq \epsilon^{(n)}$ with $\epsilon^{(n)} \to 0$ as $n \to \infty$ and therefore, by Fano's lemma, cf. [2, 4], $\frac{1}{n}H(\mathrm{X}^n|\mathrm{M}_1, \mathrm{M}_2, \mathrm{Z}^n) \to 0$ as $n \to \infty$.

For the last term we obtain $\frac{1}{n}H(\mathrm{Z}^n) \to H(\mathrm{Z})$ as $n \to \infty$. Finally, substituting into (8) shows that the desired secrecy condition is fulfilled. ∎

V. Outer Bound on Secrecy Capacity

Theorem 3: An outer bound on the secrecy capacity region of the broadcast channel with receiver side information is given by the set of all rate pairs $(R_1, R_2) \in \mathbb{R}^2_+$ that satisfy

$$\begin{aligned} R_i &\leq I(\mathrm{V}; \mathrm{Y}_i), \quad i = 1, 2 \\ R_1 + R_2 &\leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) + I(\mathrm{V}; \mathrm{Y}_2|\mathrm{U}) - I(\mathrm{V}; \mathrm{Z}|\mathrm{U}) \end{aligned}$$

for random variables $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2, \mathrm{Z})$.

Proof: To show the desired outer bound we need a version of Fano's lemma suitable for the broadcast channel with receiver side information given by $H(\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) \leq n\epsilon_1^{(n)}$ and $H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \leq n\epsilon_2^{(n)}$ with $\epsilon_1^{(n)},\epsilon_2^{(n)} \to 0$ as $n \to \infty$, cf. for example [10].

Let us define the following auxiliary random variables

$$\mathrm{U}_i \coloneqq (\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n), \qquad \mathrm{V}_i \coloneqq (\mathrm{M}_1,\mathrm{M}_2,\mathrm{U}_i) \tag{9}$$

which satisfy the following Markov chain conditions $\mathrm{U}_i - \mathrm{V}_i - \mathrm{X}_i - (\mathrm{Y}_{1i},\mathrm{Y}_{2i},\mathrm{Z}_i)$. We follow [2, 4] and get

$$\begin{aligned}
nR_1 &\leq H(\mathrm{M}_2|\mathrm{Z}^n) + n\delta \leq H(\mathrm{M}_2) + n\delta = H(\mathrm{M}_2|\mathrm{M}_1) + n\delta \\
&= I(\mathrm{M}_2;\mathrm{Y}_1^n|\mathrm{M}_1) + H(\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) + n\delta \\
&\leq I(\mathrm{M}_2;\mathrm{Y}_1^n|\mathrm{M}_1) + n(\epsilon_1^{(n)}+\delta) \leq I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_1^n) + n(\epsilon_1^{(n)}+\delta) \\
&= \sum_{i=1}^n I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) + n(\epsilon_1^{(n)}+\delta) \\
&\leq \sum_{i=1}^n I(\mathrm{M}_1,\mathrm{M}_2,\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-1},\mathrm{Z}_{i-1}^n;\mathrm{Y}_{1i}) + n(\epsilon_1^{(n)}+\delta) \\
&= \sum_{i=1}^n I(\mathrm{V}_i;\mathrm{Y}_{1i}) + n(\epsilon_1^{(n)}+\delta)
\end{aligned} \tag{10}$$

where the first inequality follows from the perfect secrecy condition (1) and [16, Lemma 15], cf. also Remark 1, for some $\delta > 0$ and the last equality from the definition of the auxiliary random variables (9). Accordingly, we get also get

$$nR_2 \leq \sum_{i=1}^n I(\mathrm{V}_i;\mathrm{Y}_{2i}) + n(\epsilon_2^{(n)} + \delta). \tag{11}$$

Again, from the perfect secrecy condition (1) we also get

$$\begin{aligned}
n(R_1+R_2) &\leq H(\mathrm{M}_1,\mathrm{M}_2|\mathrm{Z}^n) + n\delta \\
&= H(\mathrm{M}_1,\mathrm{M}_2|\mathrm{Z}^n) - H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) + H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\
&\quad - H(\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) + H(\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) + n\delta \\
&\leq H(\mathrm{M}_1,\mathrm{M}_2|\mathrm{Z}^n) - H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) \\
&\quad - H(\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) + n(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta) \\
&= H(\mathrm{M}_1|\mathrm{M}_2) + H(\mathrm{M}_2|\mathrm{M}_1) - H(\mathrm{M}_1,\mathrm{M}_2) + H(\mathrm{M}_1,\mathrm{M}_2|\mathrm{Z}^n) \\
&\quad - H(\mathrm{M}_1|\mathrm{Y}_2^n,\mathrm{M}_2) - H(\mathrm{M}_2|\mathrm{Y}_1^n,\mathrm{M}_1) + n(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta) \\
&= I(\mathrm{M}_1;\mathrm{Y}_2^n|\mathrm{M}_2) + I(\mathrm{M}_2;\mathrm{Y}_1^n|\mathrm{M}_1) \\
&\quad - I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Z}^n) + n(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta) \\
&\leq I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_1^n) + I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_2^n) \\
&\quad - I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Z}^n) + n(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta).
\end{aligned} \tag{12}$$

As in [4] we analyze the mutual information terms in (12) separately. For the first term $I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_1^n) = \sum_{i=1}^n I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1})$ we get with identity

$$\begin{aligned}
I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) &= I(\mathrm{M}_1,\mathrm{M}_2,\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) \\
&\quad - I(\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1},\mathrm{M}_1,\mathrm{M}_2) \\
&= I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \\
&\quad + I(\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) \\
&\quad - I(\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1},\mathrm{M}_1,\mathrm{M}_2)
\end{aligned}$$

the following expression

$$\begin{aligned}
I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_1^n) &= \sum_{i=1}^n I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \\
&\quad + \Sigma_1 - \Sigma_{1m}
\end{aligned} \tag{13}$$

with

$$\Sigma_1 = \sum_{i=1}^n I(\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) \tag{14a}$$

$$\Sigma_{1m} = \sum_{i=1}^n I(\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1},\mathrm{M}_1,\mathrm{M}_2). \tag{14b}$$

Similarly, we get for the second term

$$\begin{aligned}
I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_2^n) &= \sum_{i=1}^n I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{2i}|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \\
&\quad + \Sigma_2 - \Sigma_{2m}
\end{aligned} \tag{15}$$

with Σ_2 and Σ_{2m} the analogous versions of (14a) and (14b) where the indices of the legitimate receivers Y_1 and Y_2 are swapped. For the third term $I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Z}^n)$ of the eavesdropper we get

$$\begin{aligned}
I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Z}^n) &= \sum_{i=1}^n I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Z}_i|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \\
&\quad + \Sigma_e - \Sigma_{em}
\end{aligned} \tag{16}$$

with slightly different $\Sigma_e = \sum_{i=1}^n I(\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-1};\mathrm{Z}_i|\mathrm{Z}_{i+1}^n)$ and $\Sigma_{em} = \sum_{i=1}^n I(\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-1};\mathrm{Z}_i|\mathrm{Z}_{i+1}^n,\mathrm{M}_1,\mathrm{M}_2)$.

Substituting (13), (15), and (16) into (12) we get

$$\begin{aligned}
n(R_1+R_2) \leq \sum_{i=1}^n \Big[& I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \\
& + I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Y}_{2i}|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \\
& - I(\mathrm{M}_1,\mathrm{M}_2;\mathrm{Z}_i|\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-2},\mathrm{Z}_{i+1}^n) \Big] \\
& + \Sigma_1 + \Sigma_2 - \Sigma_e - \Sigma_{1m} - \Sigma_{2m} + \Sigma_{em} + n(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta).
\end{aligned} \tag{17}$$

In the following we need a version of Csiszár's sum identity [4, Lemma 7] modified for our broadcast scenario.

Lemma 1: We have the following identities

$$\Sigma_1 + \Sigma_2 = \Sigma_e \tag{18a}$$

$$\Sigma_{1m} + \Sigma_{2m} = \Sigma_{em}. \tag{18b}$$

Proof: To prove the first assertion (18a) we have to show

$$\begin{aligned}
\sum_{i=1}^n I(\mathrm{Y}_2^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) + \sum_{i=1}^n I(\mathrm{Y}_1^{i-1},\mathrm{Z}_{i+1}^n;\mathrm{Y}_{2i}|\mathrm{Y}_2^{i-1}) \\
= \sum_{i=1}^n I(\mathrm{Y}_1^{i-1},\mathrm{Y}_2^{i-1};\mathrm{Z}_i|\mathrm{Z}_{i+1}^n).
\end{aligned} \tag{19}$$

Following [4, Lemma 7], we use the chain rule to express the mutual information terms on the left hand side of (19) as

$$\begin{aligned} I(\mathrm{Y}_2^{i-1}, \mathrm{Z}_{i+1}^n; \mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}) + I(\mathrm{Y}_1^{i-1}, \mathrm{Z}_{i+1}^n; \mathrm{Y}_{2i}|\mathrm{Y}_2^{i-1}) \\ = \sum_{j=i+1}^{n} \Big[I(\mathrm{Z}_j; \mathrm{Y}_{1i}|\mathrm{Y}_1^{i-1}, \mathrm{Y}_2^{i-1}, \mathrm{Z}_{j+1}^n) \\ + I(\mathrm{Z}_j; \mathrm{Y}_{2i}|\mathrm{Y}_1^{i-1}, \mathrm{Y}_2^{i-1}, \mathrm{Z}_{j+1}^n) \Big] \end{aligned} \quad (20)$$

and on the right hand side as

$$\begin{aligned} I(\mathrm{Y}_1^{i-1}, \mathrm{Y}_2^{i-1}; \mathrm{Z}_i|\mathrm{Z}_{i+1}^n) &= \sum_{j=1}^{i-1} I(\mathrm{Y}_{1j}, \mathrm{Y}_{2j}; \mathrm{Z}_i|\mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n) \\ &= \sum_{j=1}^{i-1} \Big[I(\mathrm{Y}_{1j}; \mathrm{Z}_i|\mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n) \\ &\quad + I(\mathrm{Y}_{2j}; \mathrm{Z}_i|\mathrm{Y}_{1j}, \mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n) \Big] \\ &= \sum_{j=1}^{i-1} \Big[I(\mathrm{Y}_{1j}; \mathrm{Z}_i|\mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n) \\ &\quad + I(\mathrm{Y}_{2j}; \mathrm{Z}_i|\mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n) \Big] \end{aligned} \quad (21)$$

where the last step follows from the Markov chain $\mathrm{Y}_{1j} - (\mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n) - (\mathrm{Y}_{2j}, \mathrm{Z}_i)$. Similarly as in [4, Lemma 7] we observe that (20) and (21) split into terms $I(\mathrm{Y}_{1i}; \mathrm{Z}_j|\mathrm{Y}_1^{i-1}, \mathrm{Y}_2^{i-1}, \mathrm{Z}_{j+1}^n) + I(\mathrm{Y}_{2i}; \mathrm{Z}_j|\mathrm{Y}_1^{i-1}, \mathrm{Y}_2^{i-1}, \mathrm{Z}_{j+1}^n)$ with $i < j$ which proves (18a).

Then, (18b) follows accordingly using the Markov chain $\mathrm{Y}_{1j} - (\mathrm{Y}_1^{j-1}, \mathrm{Y}_2^{j-1}, \mathrm{Z}_{i+1}^n, \mathrm{M}_1, \mathrm{M}_2) - (\mathrm{Y}_{2j}, \mathrm{Z}_i)$. ■

Due to Lemma 1 most terms in (17) cancel out so that with the definition of the auxiliary random variables (9) we get for the sum rate

$$\begin{aligned} n(R_1 + R_2) \leq \sum_{i=1}^{n} \Big[I(\mathrm{V}_i; \mathrm{Y}_{1i}|\mathrm{U}_i) + I(\mathrm{V}_i; \mathrm{Y}_{2i}|\mathrm{U}_i) \\ - I(\mathrm{V}_i; \mathrm{Z}_i|\mathrm{U}_i) \Big] + n(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta). \end{aligned}$$

Next, we introduce a random variable Q that is independent of all other random variables and uniformly distributed over $\{1, ..., n\}$ and define $\mathrm{U} \coloneqq (\mathrm{U}_\mathrm{Q}, \mathrm{Q})$,$\mathrm{V} \coloneqq (\mathrm{V}_\mathrm{Q}, \mathrm{Q})$, $\mathrm{Y}_1 \coloneqq \mathrm{Y}_{1,\mathrm{Q}}$, $\mathrm{Y}_2 \coloneqq \mathrm{Y}_{2,\mathrm{Q}}$, and $\mathrm{Z} \coloneqq \mathrm{Z}_\mathrm{Q}$.

We obtain for the individual rates (10) and (11)

$$\begin{aligned} R_1 &\leq I(\mathrm{V}_\mathrm{Q}; \mathrm{Y}_{1,\mathrm{Q}}|\mathrm{Q}) + \epsilon_1^{(n)} + \delta \leq I(\mathrm{V}; \mathrm{Y}_1) + \epsilon_1^{(n)} + \delta \\ R_2 &\leq I(\mathrm{V}_\mathrm{Q}; \mathrm{Y}_{2,\mathrm{Q}}|\mathrm{Q}) + \epsilon_2^{(n)} + \delta \leq I(\mathrm{V}; \mathrm{Y}_2) + \epsilon_2^{(n)} + \delta \end{aligned}$$

and further for the sum rate

$$\begin{aligned} R_1 + R_2 &\leq I(\mathrm{V}_\mathrm{Q}; \mathrm{Y}_{1,\mathrm{Q}}|\mathrm{U}_\mathrm{Q}, \mathrm{Q}) + I(\mathrm{V}_\mathrm{Q}; \mathrm{Y}_{2,\mathrm{Q}}|\mathrm{U}_\mathrm{Q}, \mathrm{Q}) \\ &\quad - I(\mathrm{V}_\mathrm{Q}; \mathrm{Z}_\mathrm{Q}|\mathrm{U}_\mathrm{Q}, \mathrm{Q}) + \epsilon^{(n)} + \delta \\ &\leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) + I(\mathrm{V}; \mathrm{Y}_2|\mathrm{U}) - I(\mathrm{V}; \mathrm{Z}|\mathrm{U}) + \epsilon^{(n)} + \delta \end{aligned}$$

which establishes the outer bound and proves Theorem 3. ■

VI. Conclusion

We studied the broadcast channel with receiver side information where the transmitter sends confidential messages to two legitimate receivers with side information while keeping an external eavesdropper ignorant. We provided achievable secrecy rate regions and an outer bound on the secrecy capacity region. We expect that an improved achievable secrecy rate region can be achieved by employing more sophisticated coding techniques which is also indicated in [19] where the transmitter sends a common confidential message to two legitimate receivers in the presence of an external eavesdropper.

References

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

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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, pp. 1891–1895.

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

[16] O. O. Koyluoglu and H. El Gamal, "Cooperative Encoding for Secrecy in Interference Channels," *IEEE Trans. Inf. Theory*, submitted, available at http://arxiv.org/abs/0905.3934v2.

[17] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, p. 656715, Oct. 1949.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Wiley & Sons, 2006.

[19] Y.-K. Chia and A. El Gamal, "3-Receiver Broadcast Channels with Common and Confidential Messages," *IEEE Trans. Inf. Theory*, submitted, available at http://arxiv.org/abs/0910.1407.