Strong Secrecy in Bidirectional Relay Networks

Rafael F. Wyrembelski, Moritz Wiese, and Holger Boche

Lehrstuhl für Theoretische Informationstechnik
Technische Universität München, Germany

***Abstract*—To increase the spectral efficiency of future wireless networks, it is important to wisely integrate multiple services at the physical layer. Here we study the efficient integration of confidential services in 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 transmits an additional confidential message to one node while keeping the other node completely ignorant of it. We use the concept of *strong information theoretic security* to ensure that the non-legitimate node cannot decode the confidential message no matter what its computational resources are. This results in the study of the *bidirectional broadcast channel with confidential messages* for which we establish the strong secrecy capacity region.**

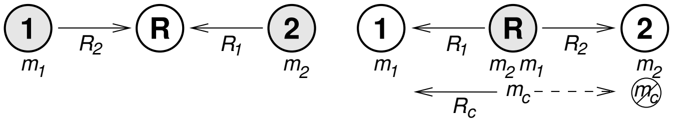
I. Introduction

Operators of wireless networks are confronted with an inherent problem: due to the open nature of the wireless channel a transmitted signal is received by its intended users but can also easily be eavesdropped by non-legitimate receivers. To keep information secret, current systems usually apply cryptographic techniques which are based on the assumption of insufficient computational capabilities of non-legitimate receivers. It is clear that with increasing computational power these techniques become more and more insecure.

Information theoretic, or physical layer, security uses the physical properties of the wireless channel in order to establish a higher level of security. This security only depends on the channel; so whatever transformation is applied to the signals that are received by non-legitimate receivers, the original message cannot be reproduced with high probability.

Information theoretic security was initiated by Wyner, who introduced the *wiretap channel* [1], and later generalized by Csiszár and Körner to the *broadcast channel with confidential messages* [2]. Recently, there is growing interest in information theoretic security, for example we refer to [3, 4]. There is also work on multi-user settings such as the multiple access channel with confidential messages [5], the MIMO Gaussian broadcast channel with common and confidential messages [6, 7], the interference channel with confidential messages [8], or the two-way wiretap channel [9, 10].

However, most of these works use the criterion of *weak secrecy* which is heuristic in nature, in that no operational meaning has been given to it yet. This means that even if this criterion holds, one still does not know what a non-legitimate receiver can or cannot do to decode the confidential message. A criterion that can be given an operational meaning is the criterion of *strong secrecy* introduced by Maurer and Wolf in [11]: it was established in [12, 13] for the wiretap channel that under the strong secrecy criterion, the average decoding error at a non-legitimate receiver tends to one for any decoder it may use. This criterion is stronger than the one used so far.



(a) MAC phase (b) BBC phase

Fig. 1. Decode-and-forward bidirectional relaying. In the initial multiple access (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. In the succeeding bidirectional broadcast (BBC) phase, the relay forwards the messages m_1 and m_2 with rates R_2 and R_1 and adds a confidential message m_c for node 1 with rate R_c to the communication which has to be kept secret from node 2.

The observation of [12, 13] constitutes the main motivation to consider strong secrecy in *bidirectional relay networks* as depicted in Figure 1. Here a relay node establishes a bidirectional communication between two other nodes using a decode-and-forward protocol [14–17] and at the same time transmits an additional confidential message to one node while keeping the other non-legitimate node completely ignorant of it. In the initial multiple access (MAC) phase both nodes transmit their messages to the relay node which decodes them. This is the classical MAC. In the succeeding broadcast phase the relay re-encodes both individual messages and the additional confidential message in such a way that the receiving nodes can conclude on their intended messages using their own message from the previous phase as side information. Due to the side information at the receivers this differs from the classical broadcast scenario und is therefore known as *bidirectional broadcast channel (BBC) with confidential messages*. In the following we establish the corresponding secrecy capacity region for the strong secrecy criterion. Strong security has further been investigated in [12, 13, 18–20].[1]

The authors gratefully acknowledge the support of the TUM Graduate School / Faculty Graduate Center FGC-EI at Technische Universität München, Germany. The work of R. F. Wyrembelski was supported by the German Ministry of Education and Research (BMBF) under Grant 01BU920. The work of M. Wiese and H. Boche was supported by the German Research Foundation (DFG) under Grants BO 1734/25-1 and BO 1734/12-1.

[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; $\mathbb{E}[\cdot]$ and $\mathbb{P}\{\cdot\}$ are the expectation and the probability.

II. Bidirectional Broadcast Channel with 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 $W^{\otimes n}(y_1^n, y_2^n|x^n) := \prod_{k=1}^n W(y_{1,k}, y_{2,k}|x_k)$. Since we do not allow any cooperation between the receiving nodes, it is sufficient to consider the marginal channels $W_i^{\otimes n}(y_i^n|x^n) = \prod_{k=1}^n W_i(y_{i,k}|x_k)$, $i=1,2$, only.

In this work 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 $\mathcal{M}_i := \{1, ..., M_i^{(n)}\}$, which is also known at the relay node. Further, the set of confidential messages of the relay node is denoted by $\mathcal{M}_c := \{1, ..., M_c^{(n)}\}$. We will frequently use the abbreviations $\mathcal{M} := \mathcal{M}_1 \times \mathcal{M}_2$ and $m := (m_1, m_2)$.

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 have sent in the previous multiple access (MAC) phase. Besides both individual messages the relay additionally integrates and transmits a confidential message $m_c \in \mathcal{M}_c$ intended for node 1, which has to be kept secret from the non-legitimate node 2.

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

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

and decoders at nodes 1 and 2

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

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

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

$$\mu_i^{(n)} := \frac{1}{|\mathcal{M}_c||\mathcal{M}_1||\mathcal{M}_2|} \sum_{m_c, m} \lambda_i(m_c, m)$$

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

To ensure that the confidential message is kept secret from the non-legitimate node 2, we require $I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_2) \leq \epsilon$ for some (small) $\epsilon > 0$ with M_c and M_2 the random variables uniformly distributed over the sets $\mathcal{M}_c$ and $\mathcal{M}_2$ and $\mathrm{Y}_2^n = (\mathrm{Y}_{2,1}, \mathrm{Y}_{2,2}, ..., \mathrm{Y}_{2,n})$ the corresponding output at node 2. This criterion is known as *strong secrecy* [11].

Remark 1: It is shown in [12, 13] for the wiretap channel that the strong secrecy criterion has the following operational meaning: no matter how the non-legitimate node 2 tries to decode the confidential message, the average probability of error tends to one. More precisely, assume that for any given code of Definition 1 the non-legitimate node has a decoder

$$g_2' : \mathcal{Y}_2^n \times \mathcal{M}_2 \to \mathcal{M}_c.$$

Then

$$\mathbb{P}\{g_2'(\mathrm{Y}_2^n, \mathrm{M}_2) \neq \mathrm{M}_c\} \geq 1 - \epsilon'(\epsilon)$$

with $\lim_{\epsilon \to 0} \epsilon'(\epsilon) \to 0$.

Definition 2: A rate triple $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ is said to be *achievable* for the BBC with confidential messages if for any $\delta > 0$ there is an $n(\delta) \in \mathbb{N}$ and a sequence of $(n, M_c^{(n)}, M_1^{(n)}, M_2^{(n)})$-codes such that for all $n \geq n(\delta)$ we have $\frac{1}{n}\log M_c^{(n)} \geq R_c - \delta$, $\frac{1}{n}\log M_2^{(n)} \geq R_1 - \delta$, and $\frac{1}{n}\log M_1^{(n)} \geq R_2 - \delta$, and

$$I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_2) \leq \epsilon^{(n)} \tag{1}$$

while $\mu_1^{(n)}, \mu_2^{(n)}, \epsilon^{(n)} \to 0$ as $n \to \infty$. The set of all achievable rate triples is the *strong secrecy capacity region* of the BBC with confidential messages and is denoted by $\mathcal{C}_{\text{BBC}}^S$.

Theorem 1: The strong secrecy capacity region $\mathcal{C}_{\text{BBC}}^S$ of the BBC with confidential messages is the set of all rate triples $(R_c, R_1, R_2) \in \mathbb{R}_+^3$ that satisfy

$$R_c \leq I(\mathrm{V}; \mathrm{Y}_1|\mathrm{U}) - I(\mathrm{V}; \mathrm{Y}_2|\mathrm{U}) \tag{2a}$$
$$R_i \leq I(\mathrm{U}; \mathrm{Y}_i), \quad i = 1,2 \tag{2b}$$

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

Proof: In [21] we established the *weak secrecy capacity region* of the BBC with confidential messages where the condition (1) is replaced by the weaker condition $\frac{1}{n}I(\mathrm{M}_c; \mathrm{Y}_2^n|\mathrm{M}_2) \leq \epsilon^{(n)}$. Thus, it is clear that the strong secrecy capacity region $\mathcal{C}_{\text{BBC}}^S$ is contained in the weak secrecy capacity region $\mathcal{C}_{\text{BBC}}^W$, i.e., $\mathcal{C}_{\text{BBC}}^S \subseteq \mathcal{C}_{\text{BBC}}^W$. Since interestingly, $\mathcal{C}_{\text{BBC}}^W$ is given by exactly the same rate triples (2), the weak secrecy capacity region $\mathcal{C}_{\text{BBC}}^W$ establishes immediately the converse for $\mathcal{C}_{\text{BBC}}^S$. Therefore, it remains to show the achievability of (2) for the strong secrecy criterion.

III. Key Idea for Strong Secrecy

In this work we use Devetak's approach [19] to establish strong secrecy in bidirectional relay networks. Therefore we start with a basic observation concerning the relationship of total variation distance[2] and mutual information.

Lemma 1: Let $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{C}$ be finite sets and A, B, and C be corresponding random variables. If

$$\|P_{\mathrm{A}|\mathrm{C}=c} \otimes P_{\mathrm{B}|\mathrm{C}=c} - P_{\mathrm{AB}|\mathrm{C}=c}\| \leq \epsilon \leq \frac{1}{2} \quad \forall\, c \in \mathcal{C}$$

then

$$I(\mathrm{A}; \mathrm{B}|\mathrm{C}) \leq -\epsilon \log \frac{\epsilon}{|\mathcal{A}||\mathcal{B}|}$$

with $P_\mathrm{A} \otimes P_\mathrm{B}(a, b) = P_\mathrm{A}(a)P_\mathrm{B}(b)$.

[2] The total variation distance of measures μ, ν on $\mathcal{A}$ is defined as

$$\|\mu - \nu\| := \sum_{a \in \mathcal{A}} |\mu(a) - \nu(a)|.$$

Proof: The proof is quite similar to [22, Lemma 1.2.7] and omitted for brevity. ■

Thus, for $I(\mathrm{M}_c;\mathrm{Y}_2^n|\mathrm{M}_2)$ to be small, it suffices to find for every $\epsilon > 0$ a code that satisfies for all $m_2 \in \mathcal{M}_2$

$$\|P_{\mathrm{Y}_2^n|\mathrm{M}_2=m_2} \otimes P_{\mathrm{M}_c|\mathrm{M}_2=m_2} - P_{\mathrm{Y}_2^n\mathrm{M}_c|\mathrm{M}_2=m_2}\| \leq \epsilon.$$

Writing $P_{\mathrm{Y}_2^n|m_c,m_1,m_2} := P_{\mathrm{Y}_2^n|\mathrm{M}_c=m_c,\mathrm{M}_1=m_1,\mathrm{M}_2=m_2}$ for brevity, we have

$$P_{\mathrm{Y}_2^n|M_2=m_2} = \frac{1}{|\mathcal{M}_c||\mathcal{M}_1|}\sum_{m_c,m_1} P_{\mathrm{Y}_2^n|m_c,m_1,m_2}$$

and it suffices to find for every $(m_c, m) \in \mathcal{M}_c \times \mathcal{M}$ a measure θ_m on $\mathcal{Y}_2^n$ such that

$$\|P_{\mathrm{Y}_2^n|m_c,m} - \theta_m\| \leq \epsilon. \tag{3}$$

IV. Codebook Design for Strong Secrecy

In this section we prove the achievability of Theorem 1. Therefore, we construct a codebook that enables reliable communication of the individual messages $m = (m_1, m_2)$ and the confidential message m_c to their respective receivers and further ensures the confidentiality of m_c. We show by random coding arguments that the codewords constructed in this way will have both these properties with high probability.

In order to prove (3), we use the following lemma which is due to Hoeffding [23].

Lemma 2: Let $b > 0$ and let $\mathrm{Z}_1, \ldots, \mathrm{Z}_L$ be i.i.d. random variables with values in $[0, b]$. Let $\mu = \mathbb{E}[\mathrm{Z}_1]$ be the expectation of Z_1. Then

$$\mathbb{P}\left\{\frac{1}{L}\sum_{l=1}^{L}\mathrm{Z}_l \notin [(1\pm\epsilon)\mu]\right\} \leq 2\exp\left(-L\cdot\frac{\epsilon^2\mu}{2b\ln 2}\right).$$

We will exploit this concentration of sums of i.i.d. random variables around their expectation for the marginal channel W_2. Before, we need to define the random coding scheme. Let $\mathcal{U}$ be a finite alphabet and let $P_\mathrm{U} \in \mathcal{P}(\mathcal{U})$ be a probability distribution on $\mathcal{U}$. Further let $P_{\mathrm{X}|\mathrm{U}} : \mathcal{U} \to \mathcal{P}(\mathcal{X})$ be a stochastic matrix with inputs from $\mathcal{U}$ and outputs in $\mathcal{X}$. Let U be a random variable distributed according to P_U and let X be a random variable whose distribution conditional on U is $P_{\mathrm{X}|\mathrm{U}}$. In order to extend these distributions to sequences of length n, we recall the concept of δ-typical sequences.

Let $\delta > 0$. Then $\mathcal{T}_{\mathrm{U},\delta}^n$ denotes the set of those sequences $u^n \in \mathcal{U}^n$ for which $|N(u|u^n) - nP_\mathrm{U}(u)| \leq n\delta$ for every $u \in \mathcal{U}$, where $N(u|u^n)$ is the number of indices $1, \ldots, n$ for which $u_i = u$. Further, for every $u^n \in \mathcal{U}$, the set $\mathcal{T}_{\mathrm{X}|\mathrm{U},\delta}^n(u^n)$ contains those $x^n \in \mathcal{X}^n$ which satisfy $|N(x, u|x^n, u^n) - P_{\mathrm{X}|\mathrm{U}}N(u|u^n)| \leq n\delta$ for all $(u, x) \in \mathcal{U}\times\mathcal{X}$, where $N(x, u|x^n, u^n)$ is the number of indices $1, \ldots, n$ for which $(x_i, u_i) = (x, u)$.

We can now define a probability measure $P'_{\mathrm{U}^n} \in \mathcal{P}(\mathcal{U}^n)$ such that

$$P'_{\mathrm{U}^n}(u^n) := \frac{P_\mathrm{U}^{\otimes n}(u^n)}{P_\mathrm{U}^{\otimes n}(\mathcal{T}_{\mathrm{U},\delta}^n)}$$

if $u^n \in \mathcal{T}_{\mathrm{U},\delta}^n$ and $P'_{\mathrm{U}^n}(u^n) = 0$ else, where $P_\mathrm{U}^{\otimes n}(u^n) = \prod_{k=1}^n P_\mathrm{U}(u_k)$. Also we extend $P_{\mathrm{X}|\mathrm{U}}$ to a stochastic matrix $P'_{\mathrm{X}^n|\mathrm{U}^n}$ with in- and outputs of length n by

$$P'_{\mathrm{X}^n|\mathrm{U}^n}(x^n|u^n) := \frac{P_{\mathrm{X}|\mathrm{U}}^{\otimes n}(x^n|u^n)}{P_{\mathrm{X}|\mathrm{U}}^{\otimes n}(\mathcal{T}_{\mathrm{X}|\mathrm{U},\delta}(u^n))}$$

if $x^n \in \mathcal{T}_{\mathrm{X}|\mathrm{U},\delta}^n(u^n)$ and $P'_{\mathrm{X}^n|\mathrm{U}^n}(x^n|u^n) = 0$ else, where $P_{\mathrm{X}|\mathrm{U}}^{\otimes n}(x^n|u^n) := \prod_{k=1}^n P_{\mathrm{X}|\mathrm{U}}(x_k|u_k)$.

These definitions allow us to define the random coding scheme with block length n as follows. Let $L^{(n)}, M_c^{(n)}, M_1^{(n)}, M_2^{(n)}$ be integers which we will fix later and let $\mathcal{L} := \{1, \ldots, L^{(n)}\}$. Then let $\{\mathrm{U}_m^n : m \in \mathcal{M}\}$ be i.i.d. random variables with values in $\mathcal{U}^n$ and distribution P'_{U^n}. For each m, we define random variables $\{\mathrm{X}_{lm_cm}^n : (l, m_c) \in \mathcal{L}\times\mathcal{M}_c\}$ taking values in $\mathcal{X}^n$, which are i.i.d. conditional on U_m^n and whose distribution equals $P'_{\mathrm{X}^n|\mathrm{U}^n}$.

We come now to the application of Lemma 2. Note that W_2 can also be regarded as a stochastic matrix with inputs from $\mathcal{U}\times\mathcal{X}$ where the $\mathcal{U}$-inputs do not make any difference. For this interpretation of W_2 one can define $\mathcal{T}_{\mathrm{Y}_2|\mathrm{XU},\delta}^n(x^n, u^n)$ analogous to $\mathcal{T}_{\mathrm{X}|\mathrm{U},\delta}^n(u^n)$. For every (l, m_c, m) and $y_2^n \in \mathcal{Y}_2^n$, we now consider the random variable

$$\begin{aligned}&\widetilde{W}_2^n(y_2^n|\mathrm{X}_{lm_cm}^n, \mathrm{U}_m) \\ &\qquad := W_2^{\otimes n}(y_2^n|\mathrm{X}_{lm_cm}^n)1_{\mathcal{T}_{\mathrm{Y}_2|\mathrm{XU},\delta}^n(\mathrm{X}_{lm_cm}^n,\mathrm{U}_m)}(y_2^n),\end{aligned} \tag{4}$$

where for any set $\mathcal{A} \subset \mathcal{Y}_2^n$, we let $1_\mathcal{A}(y_2^n) = 1$ if $y_2^n \in \mathcal{A}$ and $1_\mathcal{A}(y_2^n) = 0$ else. Conditional on U_m^n, these random variables are i.i.d. Moreover, as the input pair $(\mathrm{X}_{lm_cm}^n, \mathrm{U}_m^n)$ is jointly δ-typical with respect to P_{XU}, the joint distribution of X and U, and the outputs of $\widetilde{W}_2^n$ are δ-typical conditional on the inputs, it is well-known that (4) is upper-bounded by

$$\widetilde{W}_2^n(y_2^n|\mathrm{X}_{lm_cm}^n, \mathrm{U}_m) \leq 2^{-n(H(\mathrm{Y}_2|\mathrm{X},\mathrm{U})-\delta_1)},$$

(see e.g. [22]), where Y_2 is a random variable on $\mathcal{Y}_2$ whose distribution conditional on X and U is W_2. Let $\theta'_m(y_2^n) = \mathbb{E}[\widetilde{W}_2^n(y_2^n|\mathrm{X}_{lm_cm}^n, \mathrm{U}_m^n)|\mathrm{U}_m^n]$ be the expectation of (4) conditional on U_m^n, and set for any $\epsilon > 0$

$$\begin{aligned}\mathcal{F}_m := \{&y_2^n \in \mathcal{T}_{\mathrm{Y}_2|\mathrm{U},2|\mathcal{X}|\delta}^n(\mathrm{U}_m^n) : \\ &\theta'_m(y_2^n) \geq \epsilon|\mathcal{T}_{\mathrm{Y}_2|\mathrm{U},2|\mathcal{X}|\delta}^n(\mathrm{U}_m^n)|^{-1}\}.\end{aligned}$$

Finally, we set $\theta_m(y_2^n) := \theta'_m(y_2^n)1_{\mathcal{F}_m}(y_2^n)$. Then we define $\mathcal{A}_m(y_2^n)$ to be the event that

$$\frac{1}{L^{(n)}}\sum_{l=1}^{L^{(n)}}\widetilde{W}_2^n(y_2^n|\mathrm{X}_{lm_cm}^n, \mathrm{U}_m^n) \in [(1\pm\epsilon)\theta_m(y_2^n)]. \tag{5}$$

Now let $y_2^n \in \mathcal{F}_m$. For the probability of the complement $\mathcal{A}_m(y_2^n)^c$, we have

$$\begin{aligned}\mathbb{P}\{\mathcal{A}_m(y_2^n)^c\} &= \sum_{u^n\in\mathcal{U}^n}\mathbb{P}\{\mathrm{U}_m^n = u^n\}\mathbb{P}\{\mathcal{A}_m(y_2^n)^c|\mathrm{U}_m^n = u^n\} \\ &\leq 2\exp\left(-L^{(n)}\cdot\frac{\epsilon^2 2^{n(H(\mathrm{Y}_2|\mathrm{X},\mathrm{U})-\delta_1)}\theta_m(y_2^n)}{2\ln 2}\right) \\ &\leq 2\exp\left(-L^{(n)}\cdot\frac{\epsilon^3 2^{-n(I(\mathrm{Y}_2;\mathrm{X}|\mathrm{U})+\delta_2)}}{2\ln 2}\right),\end{aligned} \tag{6}$$

where the equality is the law of total probability, the first inequality is due to Lemma 2, and second inequality follows from the well-known fact (see e.g. [22]) that

$$|\mathcal{T}^n_{\mathrm{Y}_2|\mathrm{U},2|\mathcal{X}|\delta}(\mathrm{U}^n_m)| \leq 2^{n(H(\mathrm{Y}_2|\mathrm{U})+\tilde{\delta}_2)}$$

which applies here because U^n_m is δ-typical. Note that if $\epsilon = 2^{-n\beta}$ for some $\beta \leq \delta/4$, this bound tends to zero doubly-exponentially for

$$L^{(n)} \geq 2^{n(I(\mathrm{Y}_2;\mathrm{X}|\mathrm{U})+2\delta_2)}. \tag{7}$$

This provides the basis for the proof of (3).

The bounds on $M_c^{(n)}, M_1^{(n)}, M_2^{(n)}$ come from the constraint (7) together with the communication constraints from the following result. It treats achievable rates for the bidirectional broadcast channel with messages m_1 and m_2 as above and another individual message intended for node 1. Similarly as the confidential message in Theorem 1 this messages originates from the relay node, but it does not have to be kept secret from node 2.

Theorem 2: An achievable rate region for the BBC with an additional message from the relay to node 1 is given by set of all rate triples $(R_1', R_1, R_2) \in \mathbb{R}^3_+$ that satisfy

$$R_1' \leq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U});$$
$$R_i \leq I(\mathrm{U};\mathrm{Y}_i), \quad i = 1,2$$

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

Proof: The proof is straightforward and can be done using a standard random coding arguments. ■

Now we put the confidentiality and the communication aspects together. Without loss of generality, we may assume that $I(\mathrm{Y}_2;\mathrm{X}|\mathrm{U}) < I(\mathrm{Y}_1;\mathrm{X}|\mathrm{U})$. Then we can choose δ small enough such that (7) is satisfied and that at the same time

$$\frac{1}{n}\log L^{(n)} \leq I(\mathrm{Y}_2;\mathrm{X}|\mathrm{U}) + 3\delta_2 \leq I(\mathrm{Y}_1;\mathrm{X}|\mathrm{U}).$$

For a rate triple (R_1', R_1, R_2) contained in the achievable set from Theorem 2, choose numbers $M_1^{'(n)}, M_1^{(n)}, M_2^{(n)}$ satisfying $M_1^{'(n)} \geq L^{(n)}$ and

$$R_i - \delta \leq \frac{1}{n}\log M_i^{(n)} \leq R_i - \frac{\delta}{2}, \quad i = 1,2$$

and further

$$R_1' - \delta \leq \frac{1}{n}\log M_1^{'(n)} \leq R_1' - \frac{\delta}{2}.$$

Then we can write $\mathcal{M}_1' = \mathcal{L} \times \mathcal{M}_c$. With these numbers given, we perform the above construction of the random variables $\mathrm{U}^n_{m_1m_2}, \mathrm{X}^n_{lm_cm_1m_2}$. Obviously, this construction yields rates that satisfy the corresponding conditions given in (2), i.e., $R_c \leq I(\mathrm{X};\mathrm{Y}_1|\mathrm{U}) - I(\mathrm{X};\mathrm{Y}_2|\mathrm{U})$ and $R_i \leq I(\mathrm{U};\mathrm{Y}_i)$, $i = 1,2$.

The bound (6) ensures that (5) is satisfied for every m_c, m_1, m_2 and every $y_2^n \in \mathcal{F}_{m_1m_2}$ with probability close to 1. From the random coding proof of Theorem 2, we know that the random codewords we have chosen are the codewords of a deterministic code achieving average errors $\mu_1^{(n)}, \mu_2^{(n)} \leq 2^{-n\zeta}$ for some $\zeta > 0$ with probability close to 1. Thus there must be a realization of $\mathrm{U}^n_{m_1m_2}, \mathrm{X}^n_{lm_cm_1m_2}$ which also has these properties. We denote this realization by $u^n_{m_1m_2}, x^n_{lm_cm_1m_2}$.

Now we construct the code with stochastic encoder which will do what we want. We take the sets $\mathcal{M}_c, \mathcal{M}_1, \mathcal{M}_2$ as message sets. The message triple (m_c, m_1, m_2) is mapped to the codeword $x^n_{lm_cm_1m_2}$ with probability $1/L$. This defines a stochastic encoder. The decoder at node 1 stays the same, i.e., it decodes the complete quadruple (l, m_c, m_1, m_2). Decoder 2 also stays the same. As we already know that the code is good for reliably transmitting all the messages to their respective destinations, it remains to prove (3).

Using the triangle inequality and again writing $m = (m_1, m_2)$, we obtain for every $(m_c, m) \in \mathcal{M}_c \times \mathcal{M}$

$$\begin{aligned}
&\|P_{\mathrm{Y}_2^n|m_c,m} - \theta_m\| \\
&\quad \leq \|P_{\mathrm{Y}_2^n|m_c,m} - \frac{1}{L^{(n)}}\sum_{l=1}^{L^{(n)}} \widetilde{W}_2^n(\cdot|x_{lm_cm})\| \\
&\qquad + \|\frac{1}{L^{(n)}}\sum_{l=1}^{L^{(n)}} \widetilde{W}_2^n(\cdot|x_{lm_cm})(1 - 1_{\mathcal{F}_m})\| \\
&\qquad + \|\frac{1}{L^{(n)}}\sum_{l=1}^{L^{(n)}} \widetilde{W}_2^n(\cdot|x_{lm_cm})1_{\mathcal{F}_m} - \theta_m\|.
\end{aligned}$$

We denote the three parts of the above sum by I, II, III in that order. As the codewords satisfy (5), we have $III \leq \epsilon$.

Term I equals

$$\frac{1}{L^{(n)}}\sum_{l=1}^{L^{(n)}} W_2^{\otimes n}(\mathcal{Y}_2^n \setminus \mathcal{T}^n_{\mathrm{Y}_2|\mathrm{XU},\delta}(x^n_{lm_cm}, u^n_m)|x^n_{lm_cm})$$
$$\leq 2^{-nc\delta^2}$$

for some constant $c > 0$, where we again interpret W_2 as a channel from $\mathcal{U} \times \mathcal{X}$ to $\mathcal{Y}_2$ and use the fact that the probability that the output of a channel is not δ-typical conditional on the inputs is exponentially small.

Finally, II can be written as

$$1 - \frac{1}{L^{(n)}}\sum_{l=1}^{L^{(n)}} \widetilde{W}_2^n(\mathcal{F}_m|x^n_{lm_cm}),$$

which by the validity of (5) is at most $1 - (1-\epsilon)\theta'_m(\mathcal{F}_m)$. Now note that if y_2^n is δ-typical conditional on $(x^n_{lm_cm}, u^n_m)$, then it is $2|\mathcal{X}|\delta$-typical conditional on u^n_m, so $\theta'_m(y_2^n) \neq 0$ only for $y_2^n \in \mathcal{T}^n_{\mathrm{Y}_2|\mathrm{U},2|\mathcal{X}|\delta}(u^n_m)$. With the definition of $\mathcal{F}_m$, this implies

$$\begin{aligned}
\theta'_m(\mathcal{F}_m) &\geq \theta'_m(\mathcal{Y}_2^n) - \epsilon \\
&= \mathbb{E}[W_2^{\otimes n}(\mathcal{T}^n_{\mathrm{Y}_2|\mathrm{XU},\delta}(\mathrm{X}^n_{11m}, \mathrm{U}^n_m)|\mathrm{X}_{11m})|\mathrm{U}_m] - \epsilon,
\end{aligned}$$

and this can also be bounded from below by $1 - 2^{-nc\delta^2} - \epsilon$ by the same argument as in the estimation of I. In total, this gives an upper bound of

$$2\epsilon + 2^{-nc\delta}$$

on II.

Altogether, we can bound the total variation distance between $P_{\mathrm{Y}_2^n|m_c,m_1,m_2}$ and $\theta_{m_1 m_2}$ by $3\epsilon + 2 \cdot 2^{-nc\delta^2}$, so (3) is proved. Note that this distance is exponentially small, as we chose ϵ to have the form $2^{-n\beta}$. Thus the mutual information between M_c and the corresponding output $\mathcal{Y}_2^n$ given M_2 can be made exponentially small as well.

This proves the achievability of rate regions as in (2), but only for random variables $\mathrm{U} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$. However, note that the relay can prefix an artificial channel $P_{\mathrm{X}|\mathrm{V}}$ with a finite alphabet $\mathcal{V}$ to W. Then the above construction can be performed for the channel

$$(P_{\mathrm{X}|\mathrm{V}}W)(y_1, y_2|v) \coloneqq \sum_{x \in \mathcal{X}} W(y_1, y_2|x) P_{\mathrm{X}|\mathrm{V}}(x|v).$$

The effect of the prefix channel can be integrated in the random encoder. Varying $P_{\mathrm{X}|\mathrm{V}}$ yields the achievable rate region claimed in Theorem 1. ■

V. Physical Layer Service Integration

Theorem 1 shows that confidential services with strong secrecy can efficiently be integrated in bidirectional relay networks at the physical layer. But besides such confidential services, operators of current wireless systems usually offer also multicast services where a common message has to be transmitted to a whole group of receivers. The Multimedia Broadcast Multicast Service (MBMS), as specified by the 3GPP organization, is only one example.

In [24, 25] common and confidential messages are integrated in bidirectional relay networks for the weak secrecy criterion. With the results and techniques obtained in the previous sections it is straightforward to efficiently integrate such an additional common message in bidirectional relay networks at the physical layer where strong secrecy is required for the confidential communication.

Corollary 1: The strong secrecy capacity region 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 $\mathrm{U} - \mathrm{V} - \mathrm{X} - (\mathrm{Y}_1, \mathrm{Y}_2)$.

VI. Conclusion

In this work we studied the efficient integration of confidential services in bidirectional relay networks at the physical layer with strong secrecy. This required the analysis of the BBC with confidential messages for which we derived the strong secrecy capacity region. Interestingly, it is shown that the strong secrecy capacity region coincides with the corresponding weak secrecy capacity region. Thus, a requirement of strong security for confidential services in bidirectional relay networks does not lead to a loss in the transmission rates compared to weaker security requirements.

References

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

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

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

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

[5] 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, 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.

[7] 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.

[8] 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.

[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] 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.

[11] 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.

[12] I. Bjelaković, H. Boche, and J. Sommerfeld, "Capacity Results for Compound Wiretap Channels," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 60–64.

[13] ——, "Secrecy Results for Compound Wiretap Channels," submitted 2011, available at http://arxiv.org/abs/1106.2013.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] I. Csiszár, "Almost Independence and Secrecy Capacity," *Probl. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

[19] I. Devetak, "The Private Classical Capacity and Quantum Capacity of a Quantum Channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, Jan. 2005.

[20] M. R. Bloch and J. N. Laneman, "Secrecy from Resolvability," *IEEE Trans. Inf. Theory*, submitted, available at http://arxiv.org/abs/1105.5419.

[21] 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.

[22] I. Csiszár and J. Körner, *Information Theory - Coding Theorems for Discrete Memoryless Systems*, 1st ed. Academic Press, 1981.

[23] W. Hoeffding, "Probability Inequalities for Sums of Bounded Random Variables," *Jour. Amer. Math. Stat. Association*, vol. 58, pp. 13–30, 1963.

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

[25] R. F. Wyrembelski and H. Boche, "Bidirectional Broadcast Channels with Common and Confidential Messages," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 713–717.