

## Relay Channel With Private Messages

Ramy Tannious, *Student Member, IEEE*, and  
Aria Nosratinia, *Senior Member, IEEE*

**Abstract**—The relay channel with private messages (RCPM) is a generalized relay channel model where in addition to the traditional communication from source to destination (assisted by relay), the source has a private message for the relay, and the relay has a private message for the destination. This paper develops coding strategies for this channel based on decode-and-forward and compress-and-forward schemes. Achievable rate regions as well as outer bounds on the capacity region are obtained for the discrete memoryless relay channel with private messages. Then, the Gaussian versions of this channel are studied and achievable rate regions are characterized. Numerical results are provided that give insights into the trade-offs between private messaging and relayed messaging in this hybrid three-node network.

**Index Terms**—Channel capacity, channel coding, relay channels, wireless networks.

### I. INTRODUCTION

The three-terminal relay channel was proposed by van der Meulen [1] and studied by Cover and El Gamal [2]. The relay node in this model has no role aside from relaying, in particular, it is neither a source nor a sink of information.

When dedicated relays are unavailable, relaying must be done by network nodes that are also a source/sink of data. Thus, one is interested in the network performance limits when a relay must handle both relayed messages, as well as their own (private) messages. A representative channel model is shown in Fig. 1, which we call *relay channel with private messages* (RCPM). This is a network with both point-to-point as well as relayed links, a generalization of the traditional relay channel.

In the following, we mention some of the literature that is most directly related to the present discussion. Liang and Veeravalli [3] studied a cooperative relay broadcast channel. The bounds in this work are further improved by Liang and Kramer [4]. Reznik *et al.* [5] address a similar problem with multiple relays. Dabora and Servetto [6] study a broadcast channel with a secure cooperative link between the receivers. Lai *et al.* [7] study a half-duplex, fading, three-way channel.

In our analysis of RCPM we use new combinations of coding strategies inspired by the MAC channel with generalized feedback, and Marton’s approach to the broadcast channel. We derive achievable rates for the discrete memoryless and Gaussian RCPM, and outer bounds for the DMC case. The discrete memoryless and Gaussian RCPM generalize their counterparts in the original relay channel and relay-broadcast channels.

Throughout the paper, we use regular encoding and backward decoding [8]. Backward decoding has been used previously for degraded relay channel in [9] and more recently for the general relay channel with

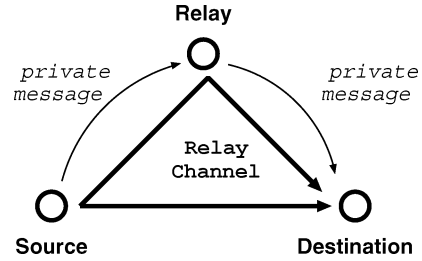


Fig. 1. Relay channel with private messaging.

partial decode-and-forward in [10]. As a by-product of our work, we demonstrate that backward decoding does not improve the achievable rate of a non-degraded relay channel employing compress-and-forward scheme.

### II. DEFINITIONS AND SYSTEM MODEL

In this work,  $X$ ,  $\mathcal{X}$ , and  $\|\mathcal{X}\|$  denote a random variable, its range, and cardinality.  $A_\epsilon^{(n)}(X)$  denotes the  $\epsilon$ -typical set according to  $X$ , in the strong or weak sense. Deterministic scalars and vectors are shown by lower case and lower-case bold-face letters. We further define  $X_t^i \triangleq (X_{t,1}, X_{t,2}, \dots, X_{t,i})$ , the capacity function  $\mathcal{C}(x) = \frac{1}{2} \log_2(1+x)$ , and for usage in convex combinations, we define  $\bar{x} = 1-x$ .

**Definition 1:** A relay channel with private messages consists of a channel input alphabet  $\mathcal{X}_1$ , a relay input alphabet  $\mathcal{X}_2$ , two channel output alphabets  $\mathcal{Y}_2$  and  $\mathcal{Y}_3$ , and a probability transition function  $p(y_2, y_3 | x_1, x_2)$ , where  $x_1, x_2$  denote source and relay inputs, respectively, while  $y_2$  and  $y_3$  denote the outputs at the relay and destination nodes, respectively.

The channel is similar to the one defined in [2], however, we also consider private messages in addition to relayed message.

**Definition 2:** A  $\left( \left( 2^{nR_{12}}, 2^{nR_{23}}, 2^{nR_{13}} \right), n \right)$  code for the relay channel with private messages consists of the following:

- three sets of integers,  $\mathcal{W}_{12} = \{1, 2, \dots, 2^{nR_{12}}\}$ ,  $\mathcal{W}_{23} = \{1, 2, \dots, 2^{nR_{23}}\}$ , and  $\mathcal{W}_{13} = \{1, 2, \dots, 2^{nR_{13}}\}$ ;
- an encoder,

$$X_1 : \mathcal{W}_{12} \times \mathcal{W}_{13} \rightarrow \mathcal{X}_1^n;$$

- a set of relay functions  $\{f_i\}_{i=1}^n$ ,

$$x_{2,i} = f_i(y_{2,1}, \dots, y_{2,i-1}, w_{23}), \quad 1 \leq i \leq n;$$

- two decoding functions,

$$d_1 : \mathcal{Y}_2^n \rightarrow \mathcal{W}_{12}$$

$$d_2 : \mathcal{Y}_3^n \rightarrow \mathcal{W}_{13} \times \mathcal{W}_{23}.$$

Fig. 2 illustrates the encoding and decoding structure of different messages. The channels considered in this paper are memoryless. Thus, the current outputs depend on the past only through present input symbols. The relay node is assumed to operate in full duplex mode and to be causal, i.e., its input is allowed to depend only on its past observations.

**Definition 3:** A relay channel with private messages is said to be degraded if its transition probability satisfies

$$p(y_2, y_3 | x_1, x_2) = p(y_2 | x_1, x_2) p(y_3 | y_2, x_2) \quad (1)$$

i.e.,  $Y_3$  is independent of  $X_1$  conditioned on knowing  $Y_2$  and  $X_2$ .

Manuscript received September 1, 2006; revised January 15, 2007. This work was supported in part by the National Science Foundation under Grant CNS-0435429. The material in this correspondence was presented in part at the IEEE Global Telecommunications Conference (GLOBECOM), San Francisco, CA, November 2006.

The authors are with Department of Electrical Engineering, The University of Texas at Dallas, Richardson, TX 75083 USA (e-mail: ramy@student.utdallas.edu; aria@utdallas.edu).

Communicated by M. Gastpar, Guest Editor for the Special Issue on Relaying and Cooperation.

Color version of Figure 5 in this correspondence is available online at <http://ieeexplore.ieee.org>.

Digital Object Identifier 10.1109/TIT.2007.904787

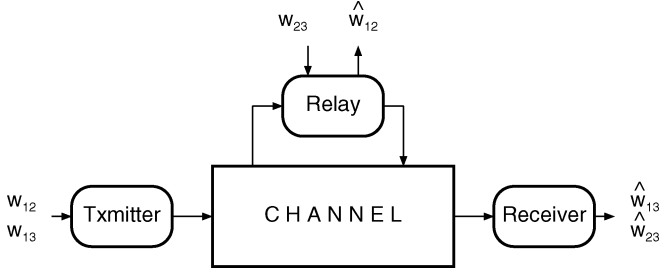


Fig. 2. The encoding and decoding structure for relay with private messages.

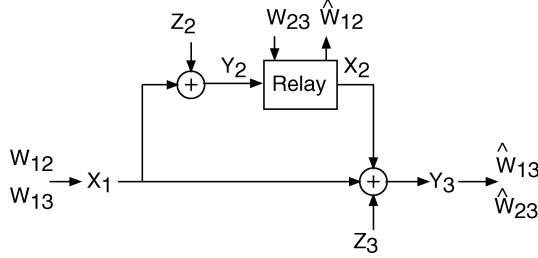


Fig. 3. Gaussian relay channel with private messages.

*Definition 4:* An AWGN relay channel with private messages is a RCPM with a continuous input and output alphabets and independent, additive white Gaussian noise. The channel outputs of the relay and destination are given by:

$$Y_2 = X_1 + Z_2 \quad (2)$$

$$Y_3 = X_1 + X_2 + Z_3 \quad (3)$$

where  $Z_2 \sim \mathcal{N}(0, N_2)$  and  $Z_3 \sim \mathcal{N}(0, N_3)$  are independent Gaussian noise.

Fig. 3 illustrates this channel and the flow of information between the three nodes. The input sequences are subject to the power constraints  $\mathcal{E}[x_1^2] < P_1$  and  $\mathcal{E}[x_2^2] < P_2$ .

*Definition 5:* A degraded AWGN relay channel with private messages is a AWGN RCPM where the source and destination signals are independent given the relay input and output, which is equivalent to saying that the relay knows everything that the destination knows. The channel outputs at the relay and destination are given by

$$Y_2 = X_1 + Z_2 \quad (4)$$

$$Y_3 = X_1 + X_2 + Z_2 + Z' \quad (5)$$

where  $Z_2$  and  $Z'$  are independent zero mean Gaussian random variables with variances  $N_2$  and  $N_3 - N_2$ , respectively, where  $N_2 < N_3$ .

*Definition 6:* The average probability of error is defined as the probability that the decoded messages are different from the transmitted ones

$$P_e^{(n)} = P\left(\hat{W}_{12} \neq W_{12} \text{ or } (\hat{W}_{13}, \hat{W}_{23}) \neq (W_{13}, W_{23})\right) \quad (6)$$

where,  $\hat{W}$  denotes an estimate of  $W$ . We assume that the source and relay nodes select their messages  $(W_{12}, W_{23}, W_{13})$  independently and uniformly over  $\mathcal{W}_{12} \times \mathcal{W}_{23} \times \mathcal{W}_{13}$ . The probability of error at the relay and destination, respectively, is defined as

$$P_{e,R}^{(n)} = P(\hat{W}_{12} \neq W_{12}) \quad (7)$$

$$P_{e,D}^{(n)} = P\left((\hat{W}_{13}, \hat{W}_{23}) \neq (W_{13}, W_{23})\right) \quad (8)$$

where each codeword contains  $n$  symbols. Note that by the union bound, we have

$$\max\{P_{e,R}^{(n)}, P_{e,D}^{(n)}\} \leq P_e^{(n)} \leq P_{e,R}^{(n)} + P_{e,D}^{(n)}. \quad (9)$$

Hence, if  $P_e^{(n)} \rightarrow 0$  then both  $P_{e,R}^{(n)}$  and  $P_{e,D}^{(n)}$  go to zero.

*Definition 7:* A rate triple  $(R_{12}, R_{23}, R_{13})$  is said to be achievable for the relay channel with private messages if there exist a sequence of codes  $\left(\left(2^{nR_{12}}, 2^{nR_{23}}, 2^{nR_{13}}\right), n\right)$  with average probability of error  $P_e^{(n)} \rightarrow 0$  as  $n \rightarrow \infty$ .

### III. ACHIEVABLE RATE REGIONS

In this section, we obtain achievable rate regions for RCPM when the relay node use the well known decode-and-forward and compress-and-forward schemes [2, Theorem 1, Theorem 6].

#### A. Relaying Via Decode-and-forward

Here, we assume the relay is able to fully decode both his private message and the message intended for the destination. The relay node then re-encodes the source node message  $W_{13}$  along with its message for the destination  $W_{23}$ .

*Theorem 1:* The rates  $(R_{12}, R_{23}, R_{13})$  are achievable for the discrete memoryless relay channel with private messages if

$$R_{13} < \min\{I(U, V; Y_3), I(V; Y_2|U, X_2)\} \quad (10)$$

$$R_{23} < I(X_2; Y_3|U, V), \quad (11)$$

$$R_{12} < I(X_1; Y_2|U, V, X_2) \quad (12)$$

for some joint distribution

$$p(u)p(v|u)p(x_1|u, v)p(x_2|u)p(y_2, y_3|x_1, x_2).$$

*Proof:* The coding arguments use ideas from relay channels, broadcast channels and MAC channel with generalized feedback [2], [11], [12]. The source uses a three-level superposition block Markov encoding, while the relay uses superposition coding. Furthermore, we use the regular encoding/backward decoding techniques.

Consider a transmission period of  $B$  blocks, each of  $n$  symbols. We assume that  $n$  is sufficiently large to allow reliable decoding. The source and relay send sequences of  $B - 1$  messages  $(W_{13}(b), W_{12}(b))$  and  $W_{23}(b)$ , respectively, over the channel in  $nB$  transmissions, where  $b$  denotes the block index,  $b = 1, 2, \dots, B - 1$ . The rate tuple  $(R_{13}^{\frac{B-1}{B}}, R_{12}^{\frac{B-1}{B}}, R_{23}^{\frac{B-1}{B}})$  approaches  $(R_{13}, R_{12}, R_{23})$  as  $B \rightarrow \infty$ . In the following, we use random variables chosen according to an arbitrary probability distribution  $p(u, v, x_1, x_2) = p(u)p(v|u)p(x_1|u, v)p(x_2|u)$ .

*Random Codebook Construction:*

- 1) Generate  $2^{nR_{13}}$  i.i.d.  $\mathbf{u} = (u_1, u_2, \dots, u_n)$  sequences, each with distribution  $p(\mathbf{u}) = \prod_{i=1}^n p(u_i)$ . Label them  $\mathbf{u}(w'_{13})$ .
- 2) For each  $\mathbf{u}(w'_{13})$  generate  $2^{nR_{13}}$  i.i.d.  $\mathbf{v}$  sequences, each with distribution  $p(\mathbf{v}) = \prod_{i=1}^n p(v_i|u_i)$ . Label them  $\mathbf{v}(w'_{13}, w_{13})$ .
- 3) For every pair  $(\mathbf{u}(w'_{13}), \mathbf{v}(w'_{13}, w_{13}))$  generate  $2^{nR_{12}}$  i.i.d.  $\mathbf{x}_1$  sequences, each with distribution

$$p(\mathbf{x}_1) = \prod_{i=1}^n p(x_{1,i}|u_i(w'_{13}), v_i(w'_{13}, w_{13})).$$

Label them  $\mathbf{x}_1(w'_{13}, w_{13}, w_{12})$ .

- 4) For each  $\mathbf{u}(w'_{13})$  generate  $2^{nR_{23}}$  i.i.d.  $\mathbf{x}_2$  sequences, each with distribution  $p(\mathbf{x}_2) = \prod_{i=1}^n p(x_{2,i}|u_i(w'_{13}))$ . Label them  $\mathbf{x}_2(w'_{13}, w_{23})$ .

*Encoding: At Block  $b$ :*

- 1) The source sends  $\mathbf{x}_1(w_{13,b-1}, w_{13,b}, w_{12,b})$ , where  $w_{13,b-1}$  was denoted above as  $w'_{13}$ .
- 2) Assuming the relay has estimated  $w_{13,b-1}$  correctly from the previous block, it then sends  $\mathbf{x}_2(w_{13,b-1}, w_{23,b})$ .

So, the transmitted codeword pair is

$$\mathbf{x}_1(1, w_{13,1}, w_{12,1}), \mathbf{x}_2(1, w_{23,1}) \quad b = 1$$

$$\mathbf{x}_1(w_{13,b-1}, w_{13,b}, w_{12,b}), \mathbf{x}_2(w_{13,b-1}, w_{23,b}) \quad b = 2, \dots, B-1$$

$$\mathbf{x}_1(w_{13,B-1}, 1, 1), \mathbf{x}_2(w_{13,B-1}, 1) \quad b = B.$$

*Decoding:*

- 1) Assuming the relay has decoded  $w_{13,b-1}$ , it can decode  $w_{13,b}$  by looking for a unique  $\hat{w}_{13,b}$  such that  $\mathbf{u}(w_{13,b-1}), \mathbf{v}(w_{13,b-1}, \hat{w}_{13,b}), \mathbf{x}_2(w_{13,b-1}, w_{23,b})$  and  $\mathbf{y}_2(b)$  are jointly typical. This step can be made reliable if:

$$R_{13} < I(V; \hat{Y}_2 | U, X_2). \quad (13)$$

- 2) The relay decodes  $w_{12,b}$  by looking for  $\hat{w}_{12,b}$  such that  $\mathbf{u}(w_{13,b-1}), \mathbf{v}(w_{13,b-1}, w_{13,b}), \mathbf{x}_1(w_{13,b-1}, w_{13,b}, \hat{w}_{12,b}), \mathbf{x}_2(w_{13,b-1}, \hat{w}_{23,b})$ , and  $\mathbf{y}_2(b)$  are jointly typical. The decoding is reliable if:

$$R_{12} < I(X_1; \hat{Y}_2 | U, V, X_2). \quad (14)$$

- 3) The destination waits until all blocks are received before it starts to decode. Suppose it has decoded  $w_{13,b}$  in block  $(b+1)$ , then in block  $b$ , it looks for a unique  $\hat{w}_{13,b-1}$  such that  $\mathbf{u}(\hat{w}_{13,b-1}), \mathbf{v}(\hat{w}_{13,b-1}, w_{13,b}),$  and  $\mathbf{y}_3(b)$  are jointly typical. Upon successful decoding of  $w_{13,b-1}$ , the destination decodes  $w_{23,b}$  by looking for a unique  $\hat{w}_{23,b}$  such that  $\mathbf{u}(w_{13,b-1}), \mathbf{v}(w_{13,b-1}, w_{13,b}), \mathbf{x}_2(w_{13,b-1}, \hat{w}_{23,b})$ , and  $\mathbf{y}_3(b)$  are jointly typical. This sequential decoding at the destination node clearly achieves the following rates:

$$R_{13} < I(U, V; Y_3) \quad (15)$$

$$R_{23} < I(X_2; Y_3 | U, V). \quad (16)$$

The achievable rate region then follows directly from combining the previous set of equations.  $\square$

*Remark 1:* The capacity of partially cooperative relay broadcast channel in [3] and also the capacity of the degraded relay channel [2] can be recovered from the above rate region. To see that, set  $U = X_2, V = U$  and the region will reduce to that in [3, Theorem 3], also if we let  $U = X_2, V = X_1$ , we have the result of [2, Theorem 1].

### B. Relaying Via Compress-and-Forward

Even when the relay node cannot fully decode the message it is supposed to relay, it can still render some help to the destination. If the channel between relay and destination had unlimited capacity,  $\hat{Y}_2$  could be transferred to the destination, however, this is often not the case. Therefore relay's received signal is compressed into a new random variable,  $\hat{Y}_2$ , characterized by an index  $z$ —possibly via vector quantization—which is conveyed to the destination via  $X_2$ . Upon decoding  $z$ , the receiver uses  $\hat{Y}_2(z)$  to resolve the uncertainty in  $Y_3$  about the source's message. This strategy which was introduced in [2] has been commonly known as estimate-and-forward or compress-and-forward.

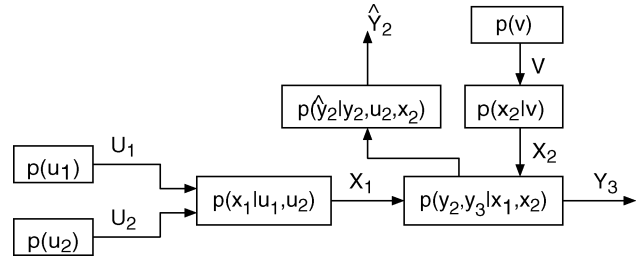


Fig. 4. Relationship of auxiliary variables.

*Theorem 2:* In the discrete memoryless relay channel with private messages, a set of private and relayed rates  $(R_{12}, R_{23}, R_{13})$  is achievable if

$$R_{13} < I(U_1; \hat{Y}_2, Y_3 | V, X_2) \quad (17)$$

$$R_{12} < I(U_2; Y_2 | X_2) \quad (18)$$

$$R_{13} + R_{12} < I(U_1; \hat{Y}_2, Y_3 | V, X_2) + I(U_2; Y_2 | X_2) - I(U_1; U_2) \quad (19)$$

$$R_{23} < I(V; Y_3) \quad (20)$$

subject to

$$I(\hat{Y}_2; Y_2 | U_2, V, X_2) \leq I(X_2; \hat{Y}_2; Y_3 | V) \quad (21)$$

where the random variables are drawn from any joint distribution

$$p(u_1, u_2)p(v)p(x_1|u_1, u_2)p(x_2|v)p(\hat{y}_2|y_2, x_2, v)p(y_2, y_3|x_1, x_2).$$

*Proof:* The proof uses ideas developed for the general nondegraded relay channels, the nondegraded broadcast channels and source coding with side information at the decoder [2], [13], [14]. In particular, the source uses a Slepian–Wolf binning-type coding strategy developed by Marton for the general broadcast channels, while the relay uses superposition coding. We note that the coding used by the source corresponds to Marton's simplified region (in the Remarks of [13, Theorem 2]) where no condition on the independence of different random variables of the source's codeword is imposed and the random variable representing the information decoded by both receivers is set to a constant. Again, the regular encoding/backward decoding technique is adopted. The relationship between the auxiliary random variables, channel inputs and channel outputs are depicted in Fig. 4. We consider a transmission over  $B$  blocks, each of  $n$  symbols. A sequence of  $B-1$  messages  $W_{13}(b), W_{12}(b),$  and  $W_{23}(b)$  will be sent over the channel in  $nB$  transmissions, where  $b$  denotes the block index,  $b = 1, 2, \dots, B-1$ . The rate tuple  $(R_{13} \frac{B-1}{B}, R_{12} \frac{B-1}{B}, R_{23} \frac{B-1}{B})$  approaches  $(R_{13}, R_{12}, R_{23})$  as  $B \rightarrow \infty$ .

Let  $A^{(n)}(U_1), A^{(n)}(U_2)$ , denote the set of sequences  $\mathbf{u}_1$  and  $\mathbf{u}_2$  that are strongly typical in  $U_1$  and  $U_2$ , respectively, and  $A^{(n)}(U_1, U_2)$  represents the set of strongly jointly typical sequences. Define the set  $A^{(n)}(U_2|\mathbf{u}_1)$  to be [15, Theorem 5.9]

$$A^{(n)}(U_2|\mathbf{u}_1) = \left\{ \mathbf{u}_2 \in A^{(n)}(U_2) : (\mathbf{u}_1, \mathbf{u}_2) \in A^{(n)}(U_1, U_2) \right\}. \quad (22)$$

Let  $S^{(n)}(U_1)$  denotes the set of all sequences  $\mathbf{u}_1 \in A^{(n)}(U_1)$ , such that  $A^{(n)}(U_2|\mathbf{u}_1)$  is nonempty. Similarly, define  $S^{(n)}(U_2)$  for the sequence  $\mathbf{u}_2$ . Consider an arbitrary probability distribution

$$p(u_1, u_2, v, x_1, x_2, \hat{y}_2) \\ = p(u_1, u_2)p(v)p(x_1|u_1, u_2)p(x_2|v)p(\hat{y}_2|y_2, x_2, v).$$

*Random Codebook Construction:*

- 1) Generate  $2^{nR(U_1)}$  sequences  $\mathbf{u}_1$  by drawing i.i.d. according to the probability

$$p(\mathbf{u}_1) = \begin{cases} \frac{1}{\|S^{(n)}(U_1)\|}, & \mathbf{u}_1 \in S^{(n)}(U_1) \\ 0, & \text{otherwise.} \end{cases}$$

- 2) Generate  $2^{nR(U_2)}$  sequences  $\mathbf{u}_2$  by drawing i.i.d. according to the probability

$$p(\mathbf{u}_2) = \begin{cases} \frac{1}{\|S^{(n)}(U_2)\|}, & \mathbf{u}_2 \in S^{(n)}(U_2) \\ 0, & \text{otherwise.} \end{cases}$$

- 3) Randomly assign  $\mathbf{u}_1$ 's into  $2^{nR_{13}}$  bins and the  $\mathbf{u}_2$ 's into  $2^{nR_{12}}$  bins.  
 4) For each product bin find a pair  $(\mathbf{u}_1, \mathbf{u}_2)$  that belong in  $A^{(n)}(U_1, U_2)$ . For a sufficiently large  $n$ , random binning arguments ([16], [17]) guarantee that such a pair exist with high probability if

$$R_{13} + R_{12} < R(U_1) + R(U_2) - I(U_1; U_2) \quad (23)$$

- 5) For each product bin and its designated jointly typical pair  $(\mathbf{u}_1, \mathbf{u}_2)$ , generate  $\mathbf{x}_1(u_1, u_2)$  according to  $\prod_{i=1}^n p(x_{1,i}|u_{1,i}, u_{2,i})$ . Label these  $\mathbf{x}_1(w_{13}, w_{12})$ .  
 6) Generate  $2^{nR_{23}}$  sequences  $\mathbf{v}$  by drawing i.i.d. according to the probability  $p(\mathbf{v}) = \prod_{i=1}^n p(v_i)$ . Label these  $\mathbf{v}(w_{23})$ .  
 7) For each  $\mathbf{v}$  generate  $2^{n\hat{R}}$  sequences  $\mathbf{x}_2$  according to  $\prod_{i=1}^n p(x_{2,i}|v_i)$ . Label these  $\mathbf{x}_2(w_{23}, z')$ .  
 8) For each  $\mathbf{v}(w_{23})$  and  $\mathbf{x}_2(w_{23}, z')$ , generate  $2^{n\hat{R}}$  sequences  $\hat{\mathbf{y}}_2$  according to  $\prod_{i=1}^n p(\hat{y}_{2,i}|x_{2,i}, v_i)$ . Label these  $\hat{\mathbf{y}}_2(w_{23}, z')$ .

Encoding: At block  $b$ :

- 1) The source sends  $\mathbf{x}_1(w_{13,b}, w_{12,b})$ .  
 2) Assuming the relay has determined  $z_{b-1}$ , -denoted above as  $z'$ -, of the compressed signal  $\hat{\mathbf{y}}_2$ , it sends  $\mathbf{x}_2(w_{23,b}, z_{b-1})$ .

So, the transmitted codeword pair is given by:

$$\begin{aligned} \mathbf{x}_1(w_{13,1}, w_{12,1}), \mathbf{x}_2(w_{23,1}, 1), & \quad b = 1 \\ \mathbf{x}_1(w_{13,b}, w_{12,b}), \mathbf{x}_2(w_{23,b}, z_{b-1}), & \quad b = 2, \dots, B-1 \\ \mathbf{x}_1(1, 1), \mathbf{x}_2(1, z_{B-1}), & \quad b = B. \end{aligned}$$

Decoding:

- 1) The relay decodes  $w_{12,b}$  by looking for a unique  $\hat{w}_{12,b}$  such that  $\mathbf{u}_2(\hat{w}_{12,b})$ ,  $\mathbf{x}_2(w_{23,b}, z_{b-1})$ , and  $\mathbf{y}_2(b)$  are jointly typical. This can be made possible with small probability of error if

$$R_{12} < I(U_2; Y_2|X_2). \quad (24)$$

- 2) The relay can determine the index  $z_b$  of the hypothetical output  $\hat{\mathbf{y}}_2(w_{23,b}, z_{b-1}, z_b)$  given it has determined  $z_{b-1}$  correctly, if  $\hat{\mathbf{y}}_2(w_{23,b}, z_{b-1}, \hat{z}_b)$ ,  $\mathbf{y}_2(b)$ ,  $\mathbf{x}_2(w_{23,b}, z_{b-1})$ , and  $\mathbf{v}(w_{23,b})$  are jointly typical. Correct decision of  $z_b$  will occur with high probability if

$$\hat{R} > I(\hat{Y}_2; Y_2|U_2, X_2). \quad (25)$$

- 3) The destination waits until all blocks are received before it starts to decode. At block  $B$ , we let  $(w_{12,B}, w_{13,B}, w_{23,B}) = (0, 0, 0)$  and consequently we let  $z_B = 0$ . Thus, we are left only with  $z_{B-1}$ , which can be decoded if the receiver finds a unique  $\hat{z}_{B-1}$  such that:  $\hat{\mathbf{y}}_2(w_{23,B}, \hat{z}_{B-1}, z_B)$ ,  $\mathbf{y}_3(B)$ ,  $\mathbf{x}_2(w_{23,B}, \hat{z}_{B-1})$ , and  $\mathbf{v}(w_{23,B})$  are jointly typical. This step can be made reliable if

$$\hat{R} < I(X_2, \hat{Y}_2; Y_3|V). \quad (26)$$

- 4) Moving to block  $B-1$  and for a general block  $b$ , the destination finds a unique  $\hat{w}_{23,b}$  such that  $(\mathbf{v}(\hat{w}_{23,b}), \mathbf{y}_3(b))$  are jointly typical. The decoding error can be made small if

$$R_{23} < I(V; Y_3). \quad (27)$$

- 5) Now assuming  $z_b, z_{b-1}$  and  $w_{23,b}$  have been decoded correctly, then  $w_{13,b}$  can be decoded at block  $b$  if the receiver finds a

unique  $\hat{w}_{13,b}$  such that:  $\mathbf{u}_1(\hat{w}_{13,b})$ ,  $\mathbf{v}(\hat{w}_{23,b})$ ,  $\mathbf{x}_2(w_{23,b}, \hat{z}_{b-1})$ ,  $\hat{\mathbf{y}}_2(w_{23,b}, z_{b-1}, z_b)$ , and  $\mathbf{y}_3(b)$  are jointly typical. The decoding error can be made small if

$$R_{13} < I(U_1; \hat{Y}_2, Y_3|V, X_2). \quad (28)$$

Therefore, as long as  $n$  is chosen sufficiently large,  $R(U_1) \geq I(U_1; \hat{Y}_2, Y_3|V, X_2)$  and  $R(U_2) \geq I(U_2; Y_2|X_2)$ , we can decode  $w_{13,b}$  and  $w_{12,b}$ , respectively with an arbitrarily small probability of error.

The achievable rate region of Theorem 2 then follows directly from combining (28), (24), (23) and (27), while the constraint given by (21) follows from combining (25) and (26).  $\square$

*Remark 2:* The symbols  $\mathbf{y}_2$  are here compressed to  $\hat{\mathbf{y}}_2$  after peeling off the component of  $X_1$  intended for the relay node which is represented by  $U_2$ . Hence, we condition on knowing  $U_2$  in (25). A similar situation arises when using compress-and-forward for multiple relays [8].

*Remark 3:* The achievability result for the general RCPM given by Theorem 2 generalizes the achievability result of the general relay channel in [2, Theorem 6]. This is can be shown by setting  $U_1 = X_1$ ,  $U_2 = 0$  and  $V = 0$ . The constraint on the relay observation compression rate at the end Theorem 2 also corresponds to the constraint provided in [2, Theorem 6]. To see that, (21) becomes

$$\begin{aligned} I(\hat{Y}_2; Y_2|X_2) & \leq I(X_2, \hat{Y}_2; Y_3) \\ & = I(X_2; Y_3) + I(\hat{Y}_2; Y_3|X_2). \end{aligned} \quad (29)$$

But we have the Markov relation  $Y_3 \rightarrow X_2, Y_2 \rightarrow \hat{Y}_2$ , therefore,

$$I(\hat{Y}_2; Y_2, Y_3|X_2) \leq I(X_2; Y_3) + I(\hat{Y}_2; Y_3|X_2). \quad (30)$$

Further simplification leads to

$$I(\hat{Y}_2; Y_2|X_2, Y_3) \leq I(X_2; Y_3) \quad (31)$$

which is the constraint given in [2, Theorem 6].

Hence, we see that backward decoding does not improve the achievable rate of a relay channel employing compress-and-forward scheme. This is in contrast to the results of [10] when the relay uses the partial decode-forward of [2, Theorem 7].

Recall that in the strategy of Remark 2, the relay makes an observation, removes the part intended for relay, then compresses and transmits  $X_2$  to destination. Alternatively,  $X_2$  may represent the compressed version of  $Y_2$  together with  $W_{23}$ . In this approach, the relay does not peel off any component from its observation.<sup>1</sup> The destination decodes  $X_2$  (and hence  $Z$  and  $W_{23}$ ), reconstructs  $\hat{Y}_2$ , and decodes  $W_{12}$  with the help of both  $\hat{Y}_2$  and  $Y_3$ . It then decodes  $W_{13}$  knowing both  $X_2$  and  $U_2$ . It can be shown, in a manner similar to Theorem 2, that the following rate region is achievable:

$$R_{13} < I(U_1; \hat{Y}_2, Y_3|U_2, V, X_2), \quad (32)$$

$$R_{12} < \min\{I(U_2; Y_2|X_2), I(U_2; \hat{Y}_2, Y_3|X_2)\} \quad (33)$$

$$\begin{aligned} R_{13} + R_{12} & < I(U_1; \hat{Y}_2, Y_3|U_2, V, X_2) - I(U_1; U_2) \\ & + \min\{I(U_2; Y_2|X_2), I(U_2; \hat{Y}_2, Y_3|X_2)\} \end{aligned} \quad (34)$$

$$R_{23} < I(V; Y_3) \quad (35)$$

subject to

$$I(\hat{Y}_2; Y_2|V, X_2) \leq I(X_2, \hat{Y}_2; Y_3|V) \quad (36)$$

<sup>1</sup>We are indebted to one of the anonymous reviewers for pointing out this alternative.

where the random variables are drawn from any joint distribution

$$p(u_1, u_2)p(v)p(x_1|u_1, u_2)p(x_2|v)p(\hat{y}_2|y_2, x_2, v)p(y_2, y_3|x_1, x_2),$$

#### IV. UPPER BOUNDS ON THE CAPACITY REGION

##### A. Upper Bound via Cut-Set Theorem

The following upper rate bounds are obtained using the max-flow-min-cut theorem [16, Theorem 14.10.1] with different choices of subsets.

a) A cut through source-relay and source-destination links gives

$$R_{12} + R_{13} < I(X_1; Y_2, Y_3 | X_2). \quad (37)$$

b) A cut through source-destination and relay-destination links gives

$$R_{13} + R_{23} < I(X_1, X_2; Y_3). \quad (38)$$

c) A cut through source-relay and relay-destination links gives:

$$R_{12} < I(X_1; Y_2 | X_2) \quad (39)$$

$$R_{23} < I(X_2; Y_3 | X_1). \quad (40)$$

##### B. Upper Bounds via Auxiliary Random Variables

We now proceed to improve the above cut-set bounds in several ways. We incorporate the influence of the auxiliary random variables into the bounds, add an explicit individual bound on  $R_{13}$  (which was absent above), and obtain a tighter bound on  $R_{12}$  in the degraded case.

Given any  $\left( \left( 2^{nR_{12}}, 2^{nR_{23}}, 2^{nR_{13}} \right), n \right)$  code for RCPM, the probability mass function on the joint ensemble space  $W_{13} \times W_{13} \times W_{23} \times \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Y}_2^n \times \mathcal{Y}_3^n$  is given by

$$\begin{aligned} & p(w_{12}, w_{13}, w_{23}, \mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_2, \mathbf{y}_3) \\ &= p(w_{12})p(w_{13})p(w_{23}) \\ & \quad \times p(\mathbf{x}_1 | w_{12}, w_{13}) \prod_{i=1}^n p(x_{2,i} | w_{23}, y_2^{i-1}) \\ & \quad p(y_{2,i} y_{3,i} | x_{1,i} x_{2,i}). \end{aligned} \quad (41)$$

Now, based on Fano's inequality, we have

$$H(W_{12} | Y_2^n) \leq nR_{12} P_{e,R}^{(n)} + 1 = n\delta_{R,n} \quad (42)$$

$$H(W_{13}, W_{23} | Y_3^n) \leq n(R_{13} + R_{23}) P_{e,D}^{(n)} + 1 = n\delta_{D,n} \quad (43)$$

where  $\delta_{R,n}, \delta_{D,n} \rightarrow 0$  as  $P_e^{(n)} \rightarrow 0$ .

$R_{13}$  can be upper bounded as follows:

$$\begin{aligned} nR_{13} &= H(W_{13}) \\ &= I(W_{13}; Y_3^n) + H(W_{13} | Y_3^n) \\ &\stackrel{(a)}{\leq} I(W_{13}; Y_3^n) + n\delta_{D,n} \\ &= \sum_{i=1}^n I(W_{13}; Y_{3,i} | Y_3^{i-1}) + n\delta_{D,n} \\ &= \sum_{i=1}^n H(Y_{3,i} | Y_3^{i-1}) - H(Y_{3,i} | Y_3^{i-1}, W_{13}) + n\delta_{D,n} \\ &\leq \sum_{i=1}^n H(Y_{3,i}) - H(Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}) + n\delta_{D,n} \\ &= \sum_{i=1}^n H(Y_{3,i}) - H(Y_{3,i} | U_i, V_i) + n\delta_{D,n} \\ &= \sum_{i=1}^n I(U_i, V_i; Y_{3,i}) + n\delta_{D,n} \end{aligned} \quad (44)$$

where (a) follows from Fano's inequality since  $H(W_{13} | Y_3^n) \leq H(W_{13}, W_{23} | Y_3^n)$  and we define  $U_i = (Y_2^{i-1}, Y_3^{i-1})$  and  $V_i = Y_2 = \dots = Y_n = W_{13}$ .

And  $R_{12}$  can be upper bounded as follows:

$$\begin{aligned} nR_{12} &= H(W_{12}) \\ &= I(W_{12}; Y_2^n) + H(W_{12} | Y_2^n) \\ &\leq I(W_{12}; Y_2^n, Y_3^n, W_{13}, W_{23}) + n\delta_{R,n}, \\ &\stackrel{(b)}{=} I(W_{12}; Y_2^n, Y_3^n | W_{13}, W_{23}) + n\delta_{R,n} \\ &= \sum_{i=1}^n H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}, W_{23}) \\ & \quad - H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{12}, W_{13}, W_{23}) + n\delta_{R,n} \\ &\stackrel{(c)}{=} \sum_{i=1}^n H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}, W_{23}, X_{2,i}) \\ & \quad - H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{12}, W_{13}, W_{23}, X_{2,i}) \\ & \quad + n\delta_{R,n} \\ &\leq \sum_{i=1}^n H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}, W_{23}, X_{2,i}) \\ & \quad - H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{12}, W_{13}, W_{23}, X_{1,i}, X_{2,i}) \\ & \quad + n\delta_{R,n} \\ &\stackrel{(d)}{\leq} \sum_{i=1}^n H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}, X_{2,i}) \\ & \quad - H(Y_{2,i}, Y_{3,i} | X_{1,i}, X_{2,i}) + n\delta_{R,n}, \\ &\leq \sum_{i=1}^n H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}, X_{2,i}) \\ & \quad - H(Y_{2,i}, Y_{3,i} | Y_2^{i-1}, Y_3^{i-1}, W_{13}, X_{1,i}, X_{2,i}) + n\delta_{R,n} \\ &= \sum_{i=1}^n I(X_{1,i}; Y_{2,i} Y_{3,i} | U_i, V_i, X_{2,i}) + n\delta_{R,n}. \end{aligned} \quad (45)$$

(b) follows from independence of  $W_{13}$ ,  $W_{13}$ , and  $W_{23}$ , (c) is due to the fact that  $X_{2,i}$  is a function of  $Y_2^{i-1}$  and  $W_{23}$ , and (d) is justified because of removing  $W_{23}$  from the conditioning of the first term and by noting that  $(W_{12}, W_{13}, W_{23}, Y_2^{i-1}, Y_3^{i-1}) \rightarrow (X_{1,i}, X_{2,i}) \rightarrow (Y_{2,i}, Y_{3,i})$  form a Markov chain from the memoryless property of the channel.

In case of degraded RCPM,  $X_{1,i} \rightarrow (U_i, V_i, X_{2,i}, Y_{2,i}) \rightarrow Y_{3,i}$  form a Markov chain and so

$$\sum_{i=1}^n I(X_{1,i}; Y_{3,i} | U_i, V_i, X_{2,i}, Y_{2,i}) = 0. \quad (46)$$

Hence  $R_{12}$  is upper bounded by

$$nR_{12} \leq \sum_{i=1}^n I(X_{1,i}; Y_{2,i} | U_i, V_i, X_{2,i}) + n\delta_{R,n}. \quad (47)$$

Finally, the single letter characterization for the two previous bounds can be obtained by introducing a time-sharing random variable  $Q$  which is uniformly distributed over the  $n$  symbols and independent of  $W_{12}, W_{13}, W_{23}, X_1, X_2, Y_2$  and  $Y_3$ . Next, define  $U = (Q, U_Q)$ ,  $V = V_Q$ ,  $X_1 = X_Q$ ,  $X_2 = X_{2,Q}$ ,  $Y_2 = Y_{2,Q}$ , and  $Y_3 = Y_{3,Q}$ . Following steps similar to those in [16, Ch. 14.3.4] the bounds can be reduced to the single letter form given by

$$R_{13} < I(U, V; Y_3) \quad (48)$$

$$R_{12} < I(X_1; Y_2 | U, V, X_2). \quad (49)$$

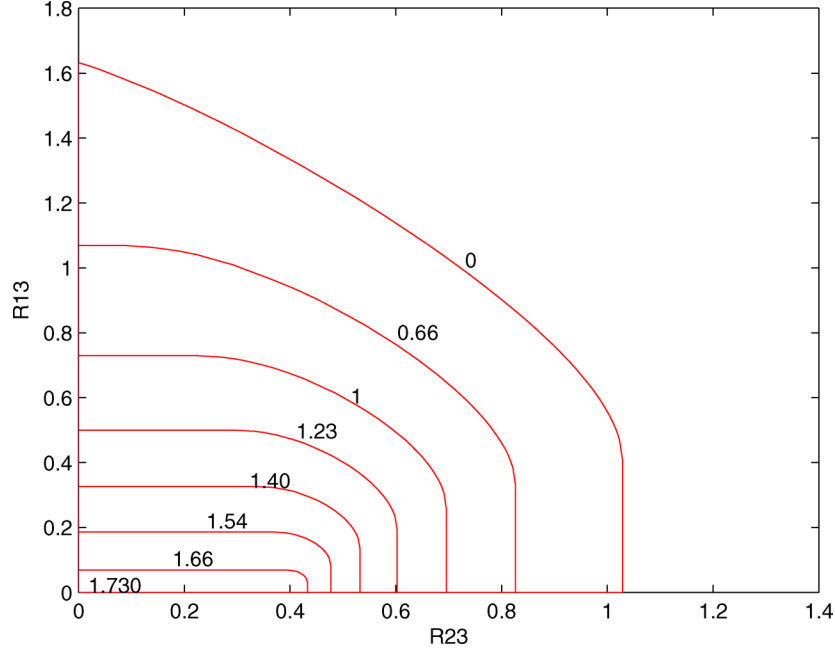


Fig. 5. Cross sections of achievable rate region of the degraded Gaussian relay channel with private messages, parameterized by the private rate  $R_{12}$ .

It can be easily shown that for the degraded RCPM, the bound on  $R_{12}$  is tighter than the cut-set bound of (39) and in fact comparing (12) and (49), the bound is tight.

*Remark 4:* The auxiliary random variables  $U$  and  $V$  are not independent, therefore their cardinality cannot be bounded using existing methods (e.g., [18]). This problem has been previously noted in [6, Comment 4.1].

## V. APPLICATION TO GAUSSIAN CHANNELS

Characterizing the capacity region in Gaussian channels is of high interest as Gaussian channel provide approximation to realistic wireless channel models. Moreover, the DMC bounds developed in the previous sections are incomputable due to the problem of bounding the cardinality of the auxiliary random variables. Nevertheless, by applying previous results in Gaussian RCPM channel we can obtain some numerical results and assess the behavior of various rates in our three-node network. For simplicity, the following results assume the input distributions to be Gaussian. Although, Gaussian inputs may not be optimal, however, searching over all possible distributions is a tedious task. All rate values in this section are expressed in (bps/Hz).

### A. Decode-and-Forward

The following result applies to the Gaussian RCPM of Definition 4 and to its degraded form given by Definition 5.

*Corollary 1:* An achievable rate region for the AWGN relay channel with private messages is the convex hull of the rates  $(R_{12}, R_{23}, R_{13})$  satisfying

$$R_{13} < \min \left\{ \mathcal{C} \left( \frac{\bar{\alpha}P_1 + \bar{\gamma}P_2 + 2\sqrt{\bar{\alpha}\bar{\beta}\bar{\gamma}P_1P_2}}{\alpha P_1 + \gamma P_2 + N_3} \right), \mathcal{C} \left( \frac{\beta \bar{\alpha}P_1}{\alpha P_1 + N_2} \right) \right\} \quad (50)$$

$$R_{23} < \mathcal{C} \left( \frac{\gamma P_2}{\alpha P_1 + N_3} \right) \quad (51)$$

$$R_{12} < \mathcal{C} \left( \frac{\alpha P_1}{N_2} \right) \quad (52)$$

for some  $\alpha, \beta$  and  $\gamma \in [0, 1]$ .

Here  $\alpha$  indicates the fraction of the source's power allocated to convey its private message to the relay,  $\beta$  controls the power allocated to the source-to-destination message in the previous block and in the current block and finally,  $\gamma$  indicates the part of the power allocated to convey the private message from the relay to the destination.

*Proof:* This rate region is achieved via the coding strategy described in Theorem 1 and then evaluating mutual informations using the following independent distributions:

- $U \sim \mathcal{N}(0, P_u), V' \sim \mathcal{N}(0, \beta \bar{\alpha} P_1)$ .
- $X'_1 \sim \mathcal{N}(0, \alpha P_1), X'_2 \sim \mathcal{N}(0, \gamma P_2)$ .

Furthermore, we let  $V = \sqrt{\frac{\bar{\alpha}\beta P_1}{P_u}}U + V', X_1 = V + X'_1$  and  $X_2 = \sqrt{\frac{\bar{\gamma}P_2}{P_u}}U + X'_2$ .  $\square$

*Remark 5:* When setting  $\alpha = 0$  and  $\gamma = 0$ , the rate  $R_{13}$  obtained in this case is the capacity of the degraded Gaussian relay channel defined in [2, Theorem 5].

*Example 1:* Consider the degraded Gaussian RCPM with  $\frac{P_1}{N_2} = 10$  dB,  $\frac{P_2}{N_3} = 5$  dB. Fig. 5 shows contour plots of the achievable rate region in the  $R_{13}$ - $R_{23}$  plane to demonstrate the trade-off between the relayed rate and one of the private rates.

### B. Compress-and-Forward

We consider a general (nondegraded) Gaussian RCPM. In addition to the channel outputs relations given in Section II, the random variable representing the compressed channel output of the relay is chosen as

$$\hat{Y}_2 = U_1 + Z_2 + Z_c \quad (53)$$

where  $Z_c$  refers to the compression noise whose variance  $N_c$  is determined by the constraint given in Theorem 2. Then, the following result applies.

*Corollary 2:* An achievable rate region for the AWGN relay channel with private messages is given by (54)–(57) shown at the top of the following page, subject to

$$N_c \geq \left( \frac{P_{u1}P_{u2}(1 - \rho^2) + P_{u1}N_3 + N_2(P_1 + N_3)}{\bar{\gamma}P_2} \right) \quad (58)$$

$$R_{13} < \mathcal{C} \left( \frac{P_{u_1} P_{u_2} (1 - \rho^2) + (P_{u_1} + 2\rho\sqrt{P_{u_1} P_{u_2}})(N_2 + N_c) + P_{u_1} N_3}{P_{u_2}(N_2 + N_c) + N_3(N_2 + N_c)} \right) \quad (54)$$

$$R_{12} < \mathcal{C} \left( \frac{P_{u_2} + 2\rho\sqrt{P_{u_1} P_{u_2}}}{P_{u_1} + N_2} \right) \quad (55)$$

$$R_{13} + R_{12} < \mathcal{C} \left( \frac{(P_{u_1} + 2\rho\sqrt{P_{u_1} P_{u_2}})(N_2 + N_3 + N_c)}{P_{u_2}(N_2 + N_3 + N_c) + N_3(N_2 + N_c)} \right) + \mathcal{C} \left( \frac{P_{u_2} + 2\rho\sqrt{P_{u_1} P_{u_2}}}{P_{u_1} + N_2} \right) + \mathcal{C}(-\rho^2) \quad (56)$$

$$R_{23} < \mathcal{C} \left( \frac{\gamma P_2}{P_1 + \bar{\gamma} P_2 + N_3} \right) \quad (57)$$

for some  $\alpha$  and  $\gamma \in [0, 1]$  and  $0 < \rho < 1$ .

$$P_{u_1} \leq \left( \sqrt{P_1(1 - \alpha(1 - \rho^2))} - \rho\sqrt{\alpha P_1} \right)^2 \quad (59)$$

$$P_{u_2} \leq \alpha P_1. \quad (60)$$

We shall see that the variable  $\rho$  denotes the correlation coefficient between the two Gaussian codebooks  $U_1$  and  $U_2$  used by the source,  $\alpha$  is the fraction of source power dedicated to its private message, and  $\gamma$  is the fraction of relay power dedicated to relay's private message.

*Proof:* We attempt to find attractive compress-and-forward achievable rates, according to (17)–(20), by finding suitable  $X_1$ ,  $X_2$ ,  $U_1$ ,  $U_2$ , and  $V$ , and their distributions. The extension of compress-and-forward DMC to the Gaussian channel faces two main problems.

- The proof of achievability requires strong typicality. In general, strong typicality does not apply to continuous random variables. However, for Gaussian input distributions the problem can be solved, as explained in [8, Remark 30].
- Every time we wish to extend DMC results to Gaussian channels, we need to find optimal codebooks which are often left unspecified in the DMC developments. In some early cases, e.g., dirty paper coding of Costa [19], the optimum codebook was correctly guessed, and the guess was verified by tightness against upper bounds. In many cases, such as ours, it is not feasible to verify optimality of the guesses. We use jointly Gaussian  $U_1$  and  $U_2$  with correlation  $\rho$  as our guess, where  $\rho$  will be optimized.

The codebook is therefore as follows.

- $U_1 \sim \mathcal{N}(0, P_{u_1})$ ,  $U_2 \sim \mathcal{N}(0, P_{u_2})$  with correlation coefficient  $\rho$ .
- $V \sim \mathcal{N}(0, \gamma P_2)$  and  $X_2' \sim \mathcal{N}(0, \bar{\gamma} P_2)$ .

The transmit signals are  $X_1 = U_1 + U_2$  and  $X_2 = V + X_2'$ . The achievability of (54)–(57) follows from this choice of codebooks (the details of proof appear in the Appendix). The power constraint of  $X_1$  gives rise to power constraints (59) and (60) for  $U_1$  and  $U_2$ , respectively. Equation (58) gives  $N_c$ , the compression noise variance, in terms of other variables in the system.  $\square$

*Remark 6:* One would recover the compress-and-forward rate in a nondegraded Gaussian relay channel provided in [8] by setting  $\alpha = 0$  and  $\gamma = 0$ .

Note that the above achievable rate was obtained by successive nulling and cancellation in a particular order, namely, the private messages are decoded first. Other achievable rates can be obtained by different orderings of nulling and canceling the codeword components representing  $Z$  and  $W_{12}$  at the relay, and  $W_{13}$  and  $W_{23}$  at the destination. This leads to a total of four possibilities. Each of the decoding orders gives one achievable rate region, and naturally the overall

achievable rate region is the convex hull of the four (the remaining rate regions can be similarly derived as Corollary 2).

We briefly comment on the various orderings possible for nulling and canceling. Consider the achievable region in Corollary 2 where the private messages are decoded first and peeled off, following by the decoding of relayed message at rate  $R_{13}$ . It is known that for successive decoding to work well, one must start with the dominant signal in the superposition. However, at least at some operating points we may have very low rates for private messages, which translates into low power allocated for these messages. Therefore the remainder of the power will be available for relaying. This means that the private messages do not always correspond to the dominant signal.

For example, consider the case where  $R_{23}$  is small, that is, the signal corresponding to the private message from relay to destination has small power. If we insist on decoding the private message first, it will limit the power and hence the rate associated with  $R_{13}$  below the levels possible in the system, and hence is very suboptimal. It is then reasonable to proceed with decoding as follows.

At the destination, we start by considering the signal component of  $R_{23}$  as “noise” and decode the relayed signal at rate  $R_{13}$ . This will allow us to know (part of) the signal transmitted by the source, which can now be peeled off. Note that the relay's transmission cannot be peeled off in general, because the system is not degraded. Now, the private message from the relay is decoded.

As yet another example, consider that  $R_{12}$  is much smaller than the other rates in the system. Therefore, if the relay wishes to peel off  $W_{12}$  from its input, this will severely limit the amount of information that can be relayed in a decode-and-forward protocol, since this assumes  $R_{12}$  is the dominant signal at the relay input. Once again, by reversing the order of nulling and canceling whenever appropriate, one may be able to obtain better achievable rates.

## VI. CONCLUSIONS AND FUTURE DIRECTIONS

We present a general form of the relay channel with private messages from source to relay and from relay to destination. Coding strategies are developed for this channel. Three-dimensional rate regions are characterized in both DMC and Gaussian channels. Also, numerical results are obtained that shed light on the trade-off between private messaging and relaying in a hybrid relay system. Many of the previous results for the original relay and relay-broadcast channels can be recovered as special cases of the results presented in this correspondence.

Extensions to this work include developing tight outer bounds for the Gaussian RCPM, inclusion of a common message from the source to relay and destination, and finally, studying RCPM in fading channels is a natural direction to follow. Specifically, power allocation policies at the source and relay are worth studying.

APPENDIX  
DERIVATION OF (54)–(58)

Given the input–output relationship between different random variables in Gaussian channels, the rate region represented by (54)–(57) is obtained as follows:

$$\begin{aligned} R_{13} &\leq I(U_1; \hat{Y}_2, Y_3 | V, X_2) \\ &= h(\hat{Y}_2, Y_3 | V, X_2) - h(\hat{Y}_2, Y_3 | U_1, V, X_2). \end{aligned} \quad (61)$$

Now

$$\begin{aligned} &h(\hat{Y}_2, Y_3 | V, X_2) \\ &= h(U_1 + Z_2 + Z_c, X_1 + X_2 + Z_3 | V, X_2) \\ &= h(U_1 + Z_2 + Z_c, U_1 + U_2 + Z_3) \\ &= \frac{1}{2} \log(2\pi e)^2 \left| \begin{array}{cc} P_{u_1} + N_2 + N_c & \rho\sqrt{P_{u_1}P_{u_2}} \\ \rho\sqrt{P_{u_1}P_{u_2}} & P_1 + N_3 \end{array} \right| \\ &= \frac{1}{2} \log(2\pi e)^2 \left( P_{u_1}P_{u_2}(1 - \rho^2) + P_1(N_2 + N_c) + P_{u_1}N_3 \right. \\ &\quad \left. + N_3(N_2 + N_c) \right) \end{aligned} \quad (62)$$

while

$$\begin{aligned} &h(\hat{Y}_2, Y_3 | U_1, V, X_2) \\ &= h(Z_2 + Z_c, U_2 + Z_3) \\ &= \frac{1}{2} \log(2\pi e)^2 \left| \begin{array}{cc} N_2 + N_c & 0 \\ 0 & P_{u_2} + N_3 \end{array} \right| \\ &= \frac{1}{2} \log(2\pi e)^2 \left( (P_{u_2} + N_3)(N_2 + N_c) \right). \end{aligned} \quad (63)$$

After straightforward simplifications we get (64) shown at the bottom of the page. Next

$$\begin{aligned} R_{12} &\leq I(U_2; Y_2 | X_2) \\ &= h(Y_2 | X_2) - h(Y_2 | U_2, X_2) \\ &= \frac{1}{2} \log(2\pi e)(P_1 + N_2) - \frac{1}{2} \log(2\pi e)(P_{u_1} + N_2) \end{aligned} \quad (65)$$

simplifying we get

$$R_{12} < \mathcal{C} \left( \frac{P_{u_2} + 2\rho\sqrt{P_{u_1}P_{u_2}}}{P_{u_1} + N_2} \right). \quad (66)$$

To compute  $I(U_1; U_2)$ , we have

$$\begin{aligned} I(U_1; U_2) &= h(U_1) + h(U_2) - h(U_1, U_2) \\ &= \frac{1}{2} \log(2\pi e)(P_{u_1}) + \frac{1}{2} \log(2\pi e)(P_{u_2}) \\ &\quad - \frac{1}{2} \log(2\pi e)^2 \left| \begin{array}{cc} P_{u_1} & \rho\sqrt{P_{u_1}P_{u_2}} \\ \rho\sqrt{P_{u_1}P_{u_2}} & P_{u_2} \end{array} \right|. \end{aligned} \quad (67)$$

Simplifying, we get

$$I(U_1; U_2) = -\mathcal{C}(-\rho^2). \quad (68)$$

Combining (64), (66), and (68), we have

$$\begin{aligned} R_{13} + R_{12} &< \mathcal{C} \left( \frac{(P_{u_1} + 2\rho\sqrt{P_{u_1}P_{u_2}})(N_2 + N_3 + N_c)}{P_{u_2}(N_2 + N_3 + N_c) + N_3(N_2 + N_c)} \right) \\ &\quad + \mathcal{C} \left( \frac{P_{u_2} + 2\rho\sqrt{P_{u_1}P_{u_2}}}{P_{u_1} + N_2} \right) + \mathcal{C}(-\rho^2). \end{aligned} \quad (69)$$

For  $R_{23}$ , we have

$$\begin{aligned} R_{23} &\leq I(V; Y_3) \\ &= h(Y_3) - h(Y_3 | V) \\ &= \mathcal{C} \left( \frac{\gamma P_2}{P_1 + \bar{\gamma} P_2 + N_3} \right). \end{aligned} \quad (70)$$

We are left with computing the constraint on the compression noise variance  $N_c$ . From (25),

$$\begin{aligned} \hat{R} &> I(\hat{Y}_2; Y_2 | U_2, V, X_2) \\ &= h(\hat{Y}_2 | U_2, V, X_2) - h(\hat{Y}_2 | U_2, V, X_2, Y_2) \\ &= \frac{1}{2} \log(2\pi e)(P_{u_1} + N_2 + N_c) - \frac{1}{2} \log(2\pi e)(N_c). \end{aligned} \quad (71)$$

Hence

$$\hat{R} > \mathcal{C} \left( \frac{P_{u_1} + N_2}{N_c} \right). \quad (72)$$

On the other hand, we have from (26)

$$\begin{aligned} \hat{R} &< I(X_2, \hat{Y}_2; Y_3 | V) \\ &= I(X_2; Y_3 | V) + I(\hat{Y}_2; Y_3 | V, X_2). \end{aligned} \quad (73)$$

Now

$$I(X_2; Y_3 | V) = \mathcal{C} \left( \frac{\bar{\gamma} P_2}{P_1 + N_3} \right). \quad (74)$$

Moreover, we have

$$\begin{aligned} I(\hat{Y}_2; Y_3 | V, X_2) &= h(\hat{Y}_2 | V, X_2) - h(\hat{Y}_2 | V, X_2, Y_3) \\ &= h(\hat{Y}_2) - h(\hat{Y}_2 | Y_3') \end{aligned} \quad (75)$$

where we defined

$$Y_3' = Y_3 - X_2 = U_1 + U_2 + Z_3.$$

Now

$$\begin{aligned} h(\hat{Y}_2) &= \frac{1}{2} \log(2\pi e)(P_{u_1} + N_2 + N_c) \\ h(\hat{Y}_2 | Y_3') &= h(\hat{Y}_2, Y_3') - h(Y_3') \\ &= \frac{1}{2} \log(2\pi e)^2 \left| \begin{array}{cc} P_{u_1} + N_2 + N_c & \rho\sqrt{P_{u_1}P_{u_2}} \\ \rho\sqrt{P_{u_1}P_{u_2}} & P_{u_2} \end{array} \right| \\ &\quad - \frac{1}{2} \log(2\pi e)(P_1 + N_3). \end{aligned} \quad (77)$$

$$R_{13} < \mathcal{C} \left( \frac{P_{u_1}P_{u_2}(1 - \rho^2) + (P_{u_1} + 2\rho\sqrt{P_{u_1}P_{u_2}})(N_2 + N_c) + P_{u_1}N_3}{P_{u_2}(N_2 + N_c) + N_3(N_2 + N_c)} \right). \quad (64)$$

$$h(\hat{Y}_2|Y_3') = \frac{1}{2} \log(2\pi e) \left( \frac{P_{u_1}P_{u_2}(1-\rho^2) + P_1(N_2 + N_c) + P_{u_1}N_3 + N_3(N_2 + N_c)}{P_1 + N_3} \right). \quad (78)$$

$$I(\hat{Y}_2; Y_3|V, X_2) = C \left( \frac{P_1P_{u_1} - P_{u_1}P_{u_2}(1-\rho^2)}{P_{u_1}P_{u_2}(1-\rho^2) + P_1(N_2 + N_c) + P_{u_1}N_3 + N_3(N_2 + N_c)} \right). \quad (79)$$

$$\hat{R} = C \left( \frac{\bar{\gamma}P_2}{P_1 + N_3} \right) + C \left( \frac{P_1P_{u_1} - P_{u_1}P_{u_2}(1-\rho^2)}{P_{u_1}P_{u_2}(1-\rho^2) + P_1(N_2 + N_c) + P_{u_1}N_3 + N_3(N_2 + N_c)} \right). \quad (80)$$

Simplifying, we get (78) shown at the top of the page. Combining (76) and (78), we get (79) shown at the top of the page. Combining (74) and (79), we get (80) also shown at the top of the page. Finally, from (72) and (80), we have

$$\frac{P_{u_1} + N_2 + N_c}{N_c} \leq \left( \frac{\bar{\gamma}P_2 + P_1 + N_3}{P_1 + N_3} \right) \cdot \left( \frac{(P_1 + N_3)(P_{u_1} + N_2 + N_c)}{P_{u_1}P_{u_2}(1-\rho^2) + P_1(N_2 + N_c) + P_{u_1}N_3 + N_3(N_2 + N_c)} \right). \quad (81)$$

Solving (81) for  $N_c$  leads to

$$N_c \geq \left( \frac{P_{u_1}P_{u_2}(1-\rho^2) + P_{u_1}N_3 + N_2(P_1 + N_3)}{\bar{\gamma}P_2} \right). \quad (82)$$

## REFERENCES

- [1] E. C. van der Meulen, "Three-terminal communication channels," *Adv. Appl. Probab.*, vol. 3, pp. 120–154, 1971.
- [2] T. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sep. 1979.
- [3] Y. Liang and V. V. Veeravalli, "Cooperative relay broadcast channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 900–928, Mar. 2007.
- [4] Y. Liang and G. Kramer, "Rate regions for relay broadcast channels," *IEEE Trans. Inf. Theory*, to be published.
- [5] A. Reznik, S. R. Kulkarni, and S. Verdú, "Broadcast-relay channel: Capacity region bounds," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 820–824.
- [6] R. Dabora and S. D. Servetto, "Broadcast channels with cooperating decoders," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5438–5454, Dec. 2006.
- [7] L. Lai, K. Liu, and H. El Gamal, "The three node wireless network: Achievable rates and cooperation strategies," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 805–828, Mar. 2006.
- [8] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3037–3063, Sep. 2005.
- [9] C.-M. Zing, F. Kuhlmann, and A. Buzo, "Achievability proof of some multiuser channel coding theorems using backward decoding," *IEEE Trans. Inf. Theory*, vol. 35, no. 6, pp. 1160–1165, Nov. 1989.
- [10] H.-F. Chong, M. Motani, and K. H. Carg, "Generalized backward decoding strategies for the relay channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 394–401, Jan. 2007.
- [11] T. M. Cover, "Comments on broadcast channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2524–2530, Oct. 1998.
- [12] F. M. J. Willems, "Informationtheoretical Results for the Discrete Memoryless Multiple Access Channel," Ph.D. dissertation, Katholieke Univ. Leuven, Leuven, Belgium, 1982.
- [13] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 3, pp. 306–311, May 1979.
- [14] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.
- [15] R. W. Yeung, *A First Course in Information Theory*. New York: Springer-Verlag, 2002.
- [16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.
- [17] A. A. El Gamal and E. C. van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 120–122, Jan. 1981.
- [18] B. E. Hajek and M. B. Pursley, "Evaluation of an achievable rate region for the broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 36–46, Jan. 1979.
- [19] M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.