Gaussian Two-Way Relay Channel with Private Information for the Relay

Chin Keong Ho, Kiran T. Gowda, and Sumei Sun

Abstract—We introduce a generalized two-way relay channel where two sources exchange information (not necessarily of the same rate) with help from a relay, and each source additionally sends private information to the relay. We consider the Gaussian setting where all point-to-point links are Gaussian channels. For this channel, we consider a two-phase protocol consisting of a multiple access channel (MAC) phase and a broadcast channel (BC) phase. We propose a general decode-and-forward (DF) scheme where the MAC phase is related to computation over MAC, while the BC phase is related to BC with receiver side information. In the MAC phase, we time share a capacity-achieving code for the MAC and a superposition code with a lattice code as its component code. We show that the proposed DF scheme is near optimal for any channel conditions, in that it achieves rates within half bit of the capacity region of the two-phase protocol.

Index Terms—Two-way relay channel, private information for relay, computation over multiple access channel, broadcast channel with side information, lattice code, superposition code.

I. INTRODUCTION

TWO-WAY relaying is an effective means of exchanging information between two sources $S_1, S_2$ with help from a relay $R$ [1]–[8]. While more phases can be used [1], a two-phase protocol that is relevant when the sources cannot listen to each other is typically considered: the relay listens in the first phase, then performs relaying in the second phase. Two relaying schemes are widely studied. In the decode-and-forward (DF) scheme [1]–[6], the relay first decodes some or all of the information bits from both sources, while in the amplify-and-forward scheme [6], [7], the relay simply forwards the received symbols. In both schemes, each source removes the self-interference that originates from itself in the first phase, so as to decode the desired message in the second phase.

In the current literature for two-way relaying, e.g., [1]–[8], the relay does not recover any information from the sources explicitly for its own use. In practice, the relay may require side information from the sources to facilitate two-way relaying, e.g., to achieve phase or frequency synchronization, or to update channel state information or queue information. For simplicity, we model the required side information as private messages $W_{1r}, W_{2r}$ to be communicated from sources $S_1, S_2$.

Fig. 1. A generalized two-way relay. Each dotted arrow represents the flow of information, via a message $W_{ij}$, from source $S_i$ to its final destination, namely, source $S_j$ or relay $R$. respectively, to the relay, see Fig. 1. In general, common (i.e., non-private) information may also be sent to all the other nodes, e.g., in [5] the relay sends a common message to both sources, but such a multicast scenario is not covered here.

In this paper, we consider a generalized two-way relay channel where two sources exchange information (not necessarily of the same rate) and each source sends private information to the relay. We consider the Gaussian setting where all point-to-point channels are Gaussian channels. We focus on the two-phase protocol shown in Fig. 2. In the multiple access channel (MAC) phase, the sources transmit, while in the broadcast channel (BC) phase, the relay transmits. Both phases are carried out over orthogonal radio resources. This protocol is relevant if the communication link between $S_1$ and $S_2$ is weak or absent.

We view the generalized two-way relay channel as an amalgam of a conventional two-way relay channel where no private information is sent, and a conventional MAC where only private information is sent by the sources to the relay. With this view, we propose a DF scheme for the two-phase protocol. This DF scheme corresponds closely to computation over MAC [9], [10] in the MAC phase, and to the BC with receiver side information [11]–[13] in the BC phase. Specifically, in the MAC phase we propose an equal-exchange-rate with bit relabeling (EER-BR) scheme that involves two steps. First, some of the exchange message bits are relabeled as private information bits such that the messages to be exchanged are of equal rates. Second, to transmit the relabeled messages, we time share two coding schemes, namely a capacity-achieving code for the conventional MAC and a superposition code with a lattice code as its component code. The overall DF scheme is near optimal in that reliable decoding is possible if $(R_{12}, R_{21}, R_{1r}, R_{2r})$ lies within half bit of the capacity region of the two-phase protocol, where $R_{ij}$ is the achievable rate of the message from node $i$ to node $j$. This holds for arbitrary transmission powers and channel conditions in the MAC and BC phases, e.g., channel reciprocity may not hold in general. Our result may be treated as a generalization of the result in [4], where the conventional two-way relay with $R_{1r} = R_{2r} = 0$ and $R_{12} = R_{21}$ is considered. Key to our DF
scheme is the lattice code used for computation over MAC that is introduced in [4, 10].

Notations: Let $C(x) = 1/2 \log (1 + x), D(x) = 1/2 \max \{0, \log (1/2 + x)\}, x \geq 0$. Logarithms are of base two. Rates are expressed in bit/symbol. Upper case letters denote random variables. Lower case letters denote the values of random variables. We collect $n$ elements $X_1, \cdots, X_n$ as a vector $X^n$.

II. SYSTEM MODEL

The generalized two-way relay channel is shown in Fig. 1. Two sources $S_1, S_2$ exchange messages $W_{12} \in \{1, \cdots, 2^{nR_{12}}\}$ and $W_{21} \in \{1, \cdots, 2^{nR_{21}}\}$, respectively. In addition, $S_1$ sends a message $W_{1r} \in \{1, \cdots, 2^{nR_{1r}}\}$ to the relay, $i = 1, 2$. The messages are generated independently with a uniform distribution.

A. Two-Phase Protocol

We consider the two-phase protocol as shown in Fig. 2, which consists of a MAC phase and a BC phase. In each phase, $n$ channel symbols are transmitted; the extension for different number of channel symbols in both phases is straightforward. The discrete time index $m$ ranges from 1 to $n$ in both phases. MAC phase: $S_1$ encodes both messages $W_{12}, W_{1r}$, to form the codeword $X^n_1$ for transmission in the MAC phase. Similarly, $S_2$ encodes $W_{21}, W_{2r}$, to form the codeword $X^n_2$. The relay thus receives at time $m$

$$Y_{1m} = X_{1m}(W_{12}, W_{1r}) + X_{2m}(W_{21}, W_{2r}) + Z_m,$$

where $Z_m \sim \mathcal{N}(0, 1)$ is zero-mean unit-variance i.i.d. Gaussian noise. All signals are real-valued. We impose the power constraints $\sum_{m=1}^{n} |x_{1m}|^2 \leq nP_1, i = 1, 2$. Without loss of generality, let $P_1 \leq P_2$.

BC phase: The relay uses the received signal $Y^n_1$ to decode for its private messages as $\hat{W}_{1r}, \hat{W}_{2r}$, and also to form a codeword $X^n_r$ for transmission in the BC phase. Source $S_i, i = 1, 2$, thus receives at time $m$

$$Y_{im} = \sqrt{P_{ir}}X_{rm}(Y^n_r) + \mathcal{Z}'_{im},$$

where $Z'_{im} \sim \mathcal{N}(0, 1)$ is i.i.d. Gaussian noise and $P_{ir}$ is the SNR from the relay to source $S_i$. Without loss of generality, we impose the power constraint $\sum_{m=1}^{n} |x_{rm}|^2/n \leq 1$. Using $Y^n_r$, as well as the previously transmitted messages $W_{12}, W_{1r}$, as side information, $S_1$ decodes its desired message as $\hat{W}_{21}$. Note that $X^n_1$ can be constructed from $W_{12}, W_{1r}$, by the source $S_1$ (during decoding) and hence is also implicitly available as side information. Similarly, using $Y^n_2$ and side information ($W_{21}, W_{2r}$), $S_2$ decodes its desired message as $\hat{W}_{12}$.

An error event is said to occur if at least one of the messages in $W \triangleq (W_{12}, W_{21}, W_{1r}, W_{2r})$ is not decoded correctly by the intended final destination at the end of a protocol cycle. Thus, it is not necessary for the relay to decode $W_{12}$ or $W_{21}$. The rate tuple $(R_{12}, R_{21}, R_{1r}, R_{2r}) \in \mathbb{R}_+^4$ is said to be achievable if the average probability of error $P_e$ can be driven to zero for $n \to \infty$. An achievable rate region $\mathcal{R}$ is a collection of achievable rate tuples. The capacity region $\mathcal{C}$ is the closure of the set of all achievable rate tuples, and its outer bound is denoted as $\overline{\mathcal{C}}$. Thus, $\mathcal{R} \subseteq \mathcal{C} \subseteq \overline{\mathcal{C}} \subseteq \mathbb{R}_+^4$.

B. An Outer Bound for the Capacity Region

Theorem 1 states an outer bound $\overline{\mathcal{C}}$ for the two-phase protocol, which holds for any source and relay processing, and for any Gaussian channels in the MAC and BC phases, i.e., $P_1, P_2, P_{1r}, P_{2r}$ are arbitrary and so channel reciprocity is not assumed.

We recall that all messages are mutually independent. The $S_1$-and-$S_2$-to-$R$ channel, as well as the $R$-to-$S_1$ and $R$-to-$S_2$ channels, are memoryless with Gaussian transition probabilities given by $p_1(x_{1m}|x_{2m}, x_{2m})$, $p_2(x_{1m}|x_{2m}), p_1(y_{2m}|x_{2m})$, respectively. In general, we express the encoding functions for $S_1, S_2$ and $R$ as $p(x^n_1|w_{1r}, w_{12}), p(x^n_2|w_{2r}, w_{21}), p(y^n_r|y^n_1, y_2^n)$, and their decoding functions as $p(\hat{w}_{12}|y^n_1, w_{12}, w_{1r}), p(\hat{w}_{12}|y^n_2, w_{2r}, w_{21}), p(\hat{w}_{1r}, \hat{w}_{2r}|y^n_r)$, respectively. Note that each source can use its previously transmitted messages as side information for decoding. Thus, the joint distribution factorizes as

$$p(w, x^n_1, x^n_2, y^n_1, y^n_2, y^n_r, \hat{w}) = p(w_1)p(w_{12})p(w_{1r})p(w_{2r})p(w_{21}) \times p(x^n_1|w_{1r}, w_{12})p(x^n_2|w_{2r}, w_{21})p(y^n_r|y^n_1, y^n_2)p(\hat{w}_{1r}, \hat{w}_{2r}|y^n_r) \times p(x^n_1|y^n_r)p(y^n_1|x^n_r)p(y^n_2|x^n_r)p(\hat{w}_{21}|y^n_2, w_{1r}, w_{12}) \times p(\hat{w}_{12}|y^n_2, w_{2r}, w_{21})$$

Fig. 3. Dependence diagram for the generalized two-way relay channel.
where \( w = (w_{1r}, w_{12}, w_{2r}, w_{21}) \) and \( \hat{w} \) denotes the decoded message of \( w \). Fig. 3 relates the random variables by a dependence diagram.

**Theorem 1:** Consider the Gaussian two-way relay channel with distribution (3). If \( P_e^{(n)} \to 0 \) for \( n \to \infty \), then \( (R_{12}, R_{21}, R_{1r}, R_{2r}) \) is achievable for communication over MAC [9], [10], see Fig. 4. For a given function \( f \), an error event is said to occur if at least one of \( W_{1r}, W_{2r} \) is not decoded correctly. The rate tuple \((R_{12}, R_{21})\) is said to be achievable if the error probability can be driven to zero for \( n \to \infty \). The achievable rate region in the BC phase is denoted as \( \mathcal{R}_{bc} \).

Now if \( r = (R_{12}, R_{21}, R_{1r}, R_{2r}) \) is achievable for communication over MAC and the same \((R_{12}, R_{21})\) is achievable for BC with receiver side information, then each message \( W_{12}, W_{21}, W_{1r}, W_{2r} \) is decoded correctly by the intended final destination. Thus, \( r \) is achievable for the two-phase protocol of the generalized two-way relay channel. An achievable rate region is thus

\[
\mathcal{R}(\mathcal{R}_{bc}, \mathcal{R}_{ma}) \triangleq \{(R_{12}, R_{21}, R_{1r}, R_{2r}) \subseteq \mathbb{R}^4_+ : (R_{12}, R_{21}) \in \mathcal{R}_{bc}, (R_{12}, R_{21}, R_{1r}, R_{2r}) \in \mathcal{R}_{ma}\}.
\] (8)

Next, we consider two specific schemes based on the DF strategy and quantify their optimality in terms of the achievable rate regions.

**A. Conventional MAC Scheme**

In our first scheme, we define \( W_0 = (W_{12}, W_{21}) \). Thus, the relay decodes for \( W = (W_{12}, W_{21}, W_{1r}, W_{2r}) \) in the MAC phase, then a codeword based on \( W_0 \) is transmitted in the BC phase. We call this the conventional MAC approach, as it can be implemented in the MAC phase using the classical MAC [14]. Theorem 2 gives the achievable rate region \( \mathcal{R}_1 \).

**Theorem 2:** The achievable rate region of the conventional MAC scheme is

\[
\mathcal{R}_{1, ma} = \{(R_{12}, R_{21}, R_{1r}, R_{2r}) \subseteq \mathbb{R}^4_+ : R_{1r} + R_{12} \leq C(P_1), R_{2r} + R_{21} \leq C(P_2), R_{1r} + R_{2r} + R_{12} + R_{21} \leq C(P_1 + P_2)\}.
\] (9c)

**Proof:** In the classical Gaussian MAC described by \( Y_{rm} = X_{1m}(W_{1}) + X_{2m}(W_{2}) + Z_{m} \), where \( Z_{m} \) is Gaussian noise and \( \sum_i |x_{im}|^2 \leq nP_i \) for \( i = 1, 2 \), a destination decodes messages \( W_1, W_2 \) at rate \( \hat{R}_1, \hat{R}_2 \) respectively. The capacity region is \( C_{ma} \triangleq \{(R_1, R_2) \subseteq \mathbb{R}^2_+: \sum_i \hat{R}_i \leq C(\sum_i P_i) \forall S \subseteq \{1, 2\}\} [14] \). In the conventional MAC approach, the relay becomes the destination with \( W = (W_{1r}, W_{12}), W_{2} = (W_{2r}, W_{21}) \). Substituting \( \hat{R}_1 = R_{1r} + R_{12} \) and \( \hat{R}_2 = R_{2r} + R_{21} \) into \( C_{ma} \) then gives \( \mathcal{R}_{1, ma} \) in (9).

Suppose \( \hat{W}_0 = W_0 \), which occurs with high probability if the rate tuple lies in \( \mathcal{R}_{1, ma} \). Then the relay knows all messages in \( W \). In this case, the BC capacity with receiver side information is known [11], [12] and meets the outer bound in the BC phase in Theorem 1, i.e., \( \mathcal{R}_{bc} = \mathcal{C}_{bc} \).

**Remark 2:** The conventional MAC scheme is optimal with respect to the BC phase, in the sense that every point in \( \mathcal{C}_{bc} \) can be achieved in the BC phase assuming the messages are always correctly decoded in the MAC phase. However, comparing the MAC phase region \( \mathcal{R}_{1, ma} \) with the corresponding upper bound \( \mathcal{C}_{ma} \) shows that the difference of (9c) and (6c) can be arbitrarily large at high SNR.
B. Equal-Exchange-Rate with Bit Relabeling Scheme

Next, we propose the EER-BR scheme and show that it achieves near-optimal performance.

In this scheme, we use the nested lattice code $\mathcal{L}$ [15], associated with a finite lattice $\Lambda_f$ for lattice decoding and a coarse lattice $\Lambda \subseteq \Lambda_f$ for signal shaping and constraining the power. In [4], the lattice code is used for two-way relaying for the case of $R_{12} = R_{21}$ and $R_{1r} = R_{2r} = 0$. Every lattice codeword $T^n \in \mathcal{L}$ is transmitted over $n$ symbols, and is mapped one-to-one to message $W$ of rate $R_{\mathcal{L}}$ via the mapping $g$ such that $T^n = g(W)$ and $W = g^{-1}(T^n)$. Define the operation $\oplus$ according to $T^n_1 \oplus T^n_2 \triangleq T^n_1 + T^n_2 \mod \Lambda$ where $T^n_1, T^n_2 \in \mathcal{L}$ and mod $\Lambda$ is the modulo operation over $\Lambda$.

1) Equal Exchange Rates: We first consider the EER scheme where we assume $R_{12} = R_{21} = R'_{0}$. We propose time sharing of Schemes 1 and 2 which are described below.

Scheme I (Conventional MAC): Both sources send only their respective private messages $W_{12}, W_{21}$ to the relay. The messages $W_{12}, W_{21}$ to be exchanged are not sent, i.e., $R'_{0} = 0$. In Scheme 1, the sources use independent Gaussian codes, which allows any rate pair in the capacity region $\mathcal{C}_{ma}$ to be achieved in the MAC phase. Thus, any rate tuple $r_1 = (0, 0, R_{1r}, R_{2r})$ is achievable for $(R_{1r}, R_{2r}) \in \mathcal{C}_{ma}$.

Scheme 2 (Superposition): Recall that $P_1 \leq P_2$. To send message $W_{12}$, the (weaker) source $S_1$ transmits $X_{12r}$ with power $P_1$. $S_1$ does not transmit any private message, i.e., $R_{1r} = 0$. To send message $W_{21}$, $S_2$ transmits $X_{21r}$ at the same power of $P_1$. Moreover, to send its private message $W_{2r}$, source $S_2$ employs the superposition technique to transmit $X_{22r}$ with power $P_2$. That is,

$$X_{1m} = \sqrt{P_1}X_{12m}(W_{12}),$$

$$X_{2m} = \sqrt{P_1}X_{21m}(W_{21}) + \sqrt{P_2 - P_1}X_{22m}(W_{2r}).$$

where each codeword is subject to unit power constraints, i.e., $\sum_{m=1}^{n}|x_{12m}|^2/n \leq 1$, $\sum_{m=1}^{n}|x_{22m}|^2/n \leq 1$, and $\sum_{m=1}^{n}|x_{21m}|^2/n \leq 1$. Here, $X_{12m}$ is transmitted using a Gaussian code. The remaining signals use the same lattice code $\mathcal{L}$ of rate $R_{\mathcal{L}} = R'_{0}$ to give $X_{12}(W_{21}) = g(W_{21}) = T_{21}^{1}$ and $X_{12}(W_{12}) = g(W_{12}) = T_{12}^{2}$. For decoding, the relay employs successive decoding. Specifically, the relay first decodes for $W_{2r}$ of signal power $P_2 - P_1$, treating $\sqrt{P_1}(T_{12}^{1} + T_{21}^{2})$ as interference of power $P_1$. The zero-mean Gaussian distribution (with the same interference power) is the worst-case interference distribution, hence the rate $R_{2r} = C((P_2 - P_1)/(1 + 2P_1))$ is achievable. After reliably decoding $W_{2r}$, $X_{22m}$ is removed from $X_{2m}$. The received signal after interference cancelation is thus $\sqrt{P_1}(T_{12}^{1} + T_{21}^{2} + Z^n)$. Then, following the approach in [4], the relay decodes for $T_{12}^{1} \oplus T_{21}^{2}$, which allows $W_{1r} = g^{-1}(T_{12}^{1})$ to be obtained. The rate $R'_{0}$ is achieved by lattice decoding [4], thus $r_2 = (D(P_1), D(P_1), 0, C((P_2 - P_1)/(1 + 2P_1)))$ is achievable for the MAC phase.

EER Scheme: We take share Schemes 1 and 2 so that $(1 - \alpha)r_1 + \alpha r_2$ is achievable for $0 \leq \alpha \leq 1$. The achievable rate region for the EER scheme is then given by

$$\mathcal{R}_2 = \{(R_0, R_0, R_{1r}, R_{2r}) : R_0 = \alpha D(P_1), (R_{1r}, R_{2r}) \in \mathcal{R}_2'(\alpha), 0 \leq \alpha \leq 1\}$$

and $\mathcal{R}_2'(\alpha)$ denotes the region of $(R_{1r}, R_{2r})$ such that

$$0 \leq R_{1r} \leq (1 - \alpha)C(P_1),$$

$$0 \leq R_{2r} \leq (1 - \alpha)C(P_2) + \alpha C\left(\frac{P_2 - P_1}{1 + 2P_1}\right) = C(P_2) - \alpha G,$$

$$R_{1r} + R_{2r} \leq (1 - \alpha)C(P_1 + P_2) + \alpha C\left(\frac{P_2 - P_1}{1 + 2P_1}\right) = C(P_1 + P_2) - \alpha C(2P_1).$$

where $G \triangleq C(2P_1) + C(P_2) - C(P_1 + P_2)$.

2) Arbitrary Exchange Rates: Denote the messages in the EER scheme as $W \triangleq (W_{12}, W_{21}, W_{1r}, W_{2r})$ where $W_{12}, W_{21}$ are at the same rate of $R'_{0}$. Denote the messages in the EER-BR scheme as $W' \triangleq (W_{12}, W_{21}, W_{1r}, W_{2r})$ where $R_{12}, R_{21}$ can be different. For arbitrary $R_{12}, R_{21}$, we build on the EER scheme with the bit-relabeling technique. The key idea is to use the EER scheme to transmit the exchange messages at a common rate of $R'_{0} = \min\{R_{12}, R_{21}\}$, and transmit the remaining $\delta \triangleq |R_{12} - R_{21}|$ bits of the (longer) exchange message together with the private messages. First, suppose $R_{12} \leq R_{21}$. We split the message as $W_{12} = (W'_{12}, W''_{12})$, where $W''_{12}$ and $W''_{21}$ have respective rates $R_{12}$ and $\delta$. We use the EER scheme by relabeling the messages as $W_{12} = W'_1 W_{21}, W_{1r} = W_{1r}', W_{2r} = (W_{2r}' W_{2r}'')$. That is, $W_{12}, W_{21}$ become the messages to be exchanged, while $W''_{21}$ is sent as additional "private" message to the relay (although the relay does not need this message). Thus, if $(R_{12}, R_{12}, R_{31}, R_{2r})$ is achievable with the EER scheme, then $(R_{12}, R_{12} + \delta, R_{1r}, R_{2r} - \delta)$ for $0 \leq \delta \leq R_{2r}$ is also achievable with the EER-BR scheme. From (12), the achievable rate region for $R_{12} \leq R_{21}$ is thus

$$\mathcal{R}_{2,ma} = \{(R_0, R_0 + \delta, R_{1r}, R_{2r} - \delta) : R_0 = \alpha D(P_1), (R_{1r}, R_{2r}) \in \mathcal{R}_2'(\alpha), 0 \leq \alpha \leq 1, 0 \leq \delta \leq R_{2r}\}.$$
3) Near Optimality: The near-optimality of the EER-BR scheme is characterized in Theorem 4. First, Lemma 1 establishes the near-optimality of the proposed scheme for the MAC phase.

Lemma 1: If \((R_{12}, R_{21}, R_{1r}, R_{2r}) \in \mathcal{C}_\text{max}\), then \((R_{12} - 1/2, R_{21} - 1/2, R_{1r} - 1/2, R_{2r} - 1/2) \in \mathcal{R}_{2,\text{ma}}\).

Proof: See proof in Appendix B. ■

Theorem 4: The EER-BR scheme achieves any rate within half bit of the capacity region for the two-phase protocol, i.e., if \((R_{12}, R_{21}, R_{1r}, R_{2r}) \in \mathcal{C}\), then \((R_{12} - 1/2, R_{21} - 1/2, R_{1r} - 1/2, R_{2r} - 1/2) \in \mathcal{R}_2\).

Proof: Comparing the the outer bound \(\mathcal{C}\) in Theorem 1 with the achievable rate region \(\mathcal{R}_2\) in Theorem 3, and using Lemma 1, we get \((R_{12}, R_{21}, R_{1r}, R_{2r}) \in \mathcal{C} \Rightarrow (R_{12} - 1/2, R_{21} - 1/2, R_{1r} - 1/2, R_{2r} - 1/2) \in \mathcal{R}_2\). Since \(\mathcal{C} \supseteq \mathcal{C}_\text{max}\), the desired result follows. ■

Remark 3: Since \(\mathcal{R}_{bc} = \mathcal{C}_{bc}\), there is no loss in optimality of the EER-BR scheme for the BC phase, as also observed for the conventional MAC scheme. Hence, the proof of the near-optimality of the EER-BR scheme for the two-phase protocol lies mainly in Lemma 1.

Remark 4: A larger rate region, especially at low SNR, is given by \(\text{conv}\{\mathcal{R}_2 \cup \mathcal{R}_1\}\), where \(\text{conv}\) is the convex hull operation. This is obtained by time sharing the EER-BR scheme with the scheme based on the conventional MAC approach. Nevertheless, the EER-BR scheme with achievable rate region \(\mathcal{R}_2\) is sufficient to achieve near-optimality.

IV. CONCLUSION

We have introduced a generalized two-way relay channel, which models a three-node communication scenario where each of two nodes sends different messages to the remaining two nodes, while the third node assists. We focused on the Gaussian setting and employs a two-phase protocol. We proposed a coding scheme based on time sharing Gaussian codes and lattice codes as well as a bit relabeling technique, which achieves within half bit of the capacity region for any channel conditions. In a separate work [16], we have also applied the lattice coding schemes to a multi-carrier system with optimization of the time-sharing variables.

APPENDIX

A. Proof for Theorem 1

Let \(E_1, E_2, E_3\) be the error events \(\{(\hat{W}_{1r}, \hat{W}_{2r}) \neq (W_{1r}, W_{2r})\}\) \(\{\hat{W}_{12} \neq W_{12}\}\) and \(\{W_{21} \neq W_{21}\}\), respectively. Then the error probability \(P_e^{(n)}\) is lower bounded as:

\[ P_e^{(n)} = \Pr(E_1 \cup E_2 \cup E_3) \geq \max_{i=1,2,3} \Pr(E_i). \]

If \(P_e^{(n)}\) approaches zero, each \(\Pr(E_i)\) also goes to zero. Then we have

\[ H(W_{1r}, W_{2r}|Y^n_1) \leq n\epsilon_n, \]
\[ H(W_{12}|Y^n_2, W_{21}, W_{2r}) \leq n\epsilon_n, \]
\[ H(W_{21}|Y^n_1, W_{1r}, W_{12}) \leq n\epsilon_n, \]

where \(\epsilon_n = 0\) as \(n \to \infty\). Here, (15) follows from Fano’s inequality [14], while (16) and (17) follow from Fano’s inequality with the fact that the sources can use their previously transmitted messages as side information for decoding [13, Lemma 2.5].

First, we prove \(R_{12} \leq C(P_{12})\) if \(P_e^{(n)} \to 0\). The proof for \(R_{21} \leq C(P_{11})\) is similar. We have

\[ nR_{12} = H(W_{12}|W_{21}, W_{2r}) = I(W_{12}; Y^n_2 | W_{21}, W_{2r}) + H(W_{12}|Y^n_2, W_{21}, W_{2r}) \leq I(W_{12}; Y^n_2 | W_{21}, W_{2r}) + n\epsilon_n \]
\[ \leq I(W_{12}; Y^n_2 | W_{21}, W_{2r}) + n\epsilon_n \]
\[ = H(Y^n_2 | W_{21}, W_{2r}, W_{12}) + n\epsilon_n \]
\[ \leq H(Y^n_2 | X^n_1, X^n_2, W_{21}, W_{2r}, W_{12}) + n\epsilon_n \]
\[ \leq H(X^n_1; Y^n_2) + n\epsilon_n \]

where (a) follows from the independence of the messages; (b) follows from (16); (c) follows from the chain rule of mutual information and \(I(\cdot;\cdot) \geq 0\); (d) follows as conditioning reduces entropy; (e) follows because \((W_{12}, W_{1r}, W_{2r})\) forms a Markov chain. Note steps (d) and (e) together show that the data processing inequality holds even if side information is available to decode \(\hat{W}_{12}\). Following standard steps for the converse proof of the capacity of Gaussian channels [14], we obtain \(R_{12} \leq C(P_{12})\).

Next, we prove \(R_{1r} + R_{12} \leq C(P_1)\) if \(P_e^{(n)} \to 0\). The proof for \(R_{2r} + R_{21} \leq C(P_2)\) is similar. Let \(\epsilon'_n = 2\epsilon_n\). We have

\[ n(R_{1r} + R_{12}) \leq H(W_{1r}|W_{21}, W_{2r}) + H(W_{12}|W_{1r}, W_{21}, W_{2r}) \leq I(W_{1r}; Y^n_1 | W_{21}, W_{2r}) + I(W_{12}; Y^n_2 | W_{1r}, W_{21}, W_{2r}) + n\epsilon'_n \]
\[ = I(W_{1r}; Y^n_1 | W_{21}, W_{2r}) + I(W_{12}; Y^n_2 | W_{1r}, W_{21}, W_{2r}) + n\epsilon'_n \]
\[ = H(Y^n_1 | W_{21}, W_{2r}, W_{1r}, W_{12}) + H(Y^n_2 | W_{1r}, W_{21}, W_{2r}) + n\epsilon'_n \]
\[ = H(Y^n_1 | X^n_1, X^n_2, W_{1r}, W_{12}, W_{2r}) + n\epsilon'_n \]
\[ \leq X^n_1; Y^n_2) + n\epsilon'_n \]

where (a) follows from the independence of the messages; (b) follows from the following inequalities

\[ H(W_{1r}|Y^n_1, W_{21}, W_{2r}) \leq H(W_{1r}|Y^n_1) \leq H(W_{1r}, W_{2r}|Y^n_1) \]
\[ H(W_{12}|Y^n_2, W_{1r}, W_{21}, W_{2r}) \leq H(W_{12}|Y^n_2, W_{21}, W_{2r}) \]

and by applying Fano’s inequality (15) and (16); (c) follows from the data processing inequality (which can be shown to hold even if \(W_{12}, W_{1r}, W_{2r}\) are given); (d) follows from the fact that \(X^n_1\) is a function of only \(W_{1r}, W_{12}\) and \(X^n_2\) is a function of only \(W_{2r}, W_{21}\); (e) follows from conditioning reduces entropy and because \((W_{1r}, W_{12}, W_{2r}) - (X^n_1, X^n_2) - Y^n_2\) forms a Markov chain. Following standard steps for the converse proof of the capacity of Gaussian MAC channels [14], we obtain \(R_{1r} + R_{12} \leq C(P_1)\).
Before we prove (6c), we first prove that $R_{1r} + R_{2r} + R_{12} \leq C(P_1 + P_2)$ holds if $P_c^{(n)} \to 0$. We have

$$n(R_{1r} + R_{2r} + R_{12})$$

(a) $\leq H(W_{1r}, W_{2r}, W_{21}) + H(W_{12}, W_{1r}, W_{2r}, W_{21})$ (b) $\leq I(W_{1r}, W_{2r}, Y^n_{1r}|W_{21}) + I(W_{12}; Y^n_{2r}|W_{1r}, W_{2r}, W_{21}) + \epsilon'_n$

(c) $\leq I(W_{1r}, W_{2r}, Y^n_{1r}|W_{21}) + I(W_{12}; Y^n_{2r}|W_{1r}, W_{2r}, W_{21}) + \epsilon'_n$

(d) $\leq I(W_{1r}, W_{2r}, W_{12}, W_{21}; Y^n_{1r}) + \epsilon'_n$

(e) $\leq I(X^n_{1r}, X^n_{2r}, Y^n_{1r}) + \epsilon'_n$

where (a) follows from the independence of the messages; (b) follows from conditioning reduces entropy and Fano’s inequality via (15) and (16); (c) follows from the data processing inequality (which can be shown to hold even if $W_{1r}, W_{2r}, W_{21}$ are given); (d) follows from the chain rule of mutual information and from $I(\cdot;\cdot) \geq 0$; (e) follows from the data processing inequality. Following standard steps for the converse proof of the capacity of Gaussian MACs [14], we obtain $R_{1r} + R_{2r} + R_{12} \leq C(P_1 + P_2)$ if $P_c^{(n)} \to 0$. Similarly, we can obtain $R_{1r} + R_{2r} + R_{21} \leq C(P_1 + P_2)$ if $P_c^{(n)} \to 0$. Thus, (6c) holds if $P_c^{(n)} \to 0$.

B. Proof for Lemma 1

Suppose $R_{12} \leq R_{21}$. The proof for $R_{12} \geq R_{21}$ is similar. Without loss of generality, we let the rate tuple $(R_{12}, R_{21}, R_{1r}, R_{2r})$ in $\mathcal{C}_{\text{ma}}$ in Theorem 1 be $(R_0, R_0 + \delta, R_{1r}' + R_{2r}' - \delta)$, where $R_0, R_{1r}', R_{2r}' \geq 0$ and $0 \leq \delta \leq R_{2r}'$ (a one-to-one mapping of four variables to another four). Since $R_0 \leq C(P_1)$ from (6a), without loss of generality, let $R_0 = \alpha C(P_1)$, where $0 \leq \alpha \leq 1$. Then, $\mathcal{C}_{\text{ma}}$ is alternatively given by

$$\mathcal{C}_{\text{ma}} = \{(R_0, R_0 + \delta, R_{1r}', R_{2r}' - \delta) :$$

$$R_0 = \alpha C(P_1)$$

$$0 \leq R_{1r}' \leq (1 - \alpha) C(P_1)$$

$$0 \leq R_{2r}' \leq C(P_2) - \alpha C(P_1)$$

$$R_{1r}' + R_{2r}' \leq C(P_1 + P_2)$$

$$0 \leq \alpha \leq 1, 0 \leq \delta \leq R_{2r}'\}.$$

Fix $\alpha$ and $\delta$, where $0 \leq \alpha \leq 1, 0 \leq \delta \leq R_{2r}'$. The rate $R_0 = \alpha D(P_1)$ in (12) differs from $R_0 = \alpha C(P_1)$ in $\mathcal{C}_{\text{ma}}$. By at most $C(P_1) - D(P_1) \leq 1/2 \log(3/2) < 1/2$. To see this, recall the definition $D(x) = 1/2 \log(1/2 + x)$ and note that $C(P_1) - D(P_1)$ is maximized when $P_1 = 1/2$. We now compare the inequalities (13a)–(13c) with (18a)–(18c), respectively. The first pair (13a), (18a) is the same. The second pair (13b), (18b) differs in the RHS by at most $\Gamma - C(P_1) \leq [C(P_2) - C(P_1 + P_2)] + [C(2P_2) - C(P_1)] \leq 1/2$ since $C(P_2) \leq C(P_1 + P_2)$ and $C(2P_2) - C(P_1) \leq 1/2$. The last pair (13c), (18c) differs in the RHS by at most $C(2P_2) - C(P_1) \leq 1/2$. Thus, each achievable rate is within half bit of its respective upper bound. Since this holds for arbitrary $0 \leq \alpha \leq 1, 0 \leq \delta \leq R_{2r}'$, we obtain Lemma 1.

REFERENCES


