Two Receiver Relay Broadcast Channel with Mutual Secrecy

Krishnamoorthy Iyer
Department of Electrical Engineering, Indian Institute of Technology Bombay
krishna@ee.iitb.ac.in

***Abstract*—We consider mutual secrecy requirements in a two receiver relay broadcast channel, where the dedicated relay is trusted by all parties. In our scheme, the relay decodes and forwards the respective messages to their intended destinations. Coherent transmission by the transmitter and relay is achieved by employing the Marton-Marton coding technique. Double random binning is then used to provide mutual secrecy. While our encoding is irregular, the decoding at the receivers employs forward sliding windows. This improves flexibility and reduces decoding delay when compared to backward decoding. This will be welcomed by wireless engineers. The multi-block equivocation calculation also has some features of interest.**

I. Introduction

We study a discrete memoryless relay broadcast channel (DM-RBC) with a dedicated relay and two receivers – to each, the source transmits an independent message. In a wireless scenario, it is possible for both receivers to attempt to snoop on the message intended for the other. Preventing successful eavesdropping by either receiver is the mutual secrecy requirement imposed on the model. The relay, an extension of the transmitter, is trusted by all parties. We study the "strong" relay scenario where the transmitter-to-relay (Tx→Rel) link is stronger than *both* transmitter-to-destination (Tx→Rx) links. Here decode-forward (DF) is indicated [1]. The trusted relay decodes-forwards both messages to their respective destinations and assists the Tx in maintaining mutual confidentiality.

Both Tx and relay are used as broadcast channels *in their own right*. This is in contrast to [2], who used the relay in an RBC as a point-to-point channel to increase the common message rate. Wireless networks are inherently broadcast – [2]'s strategy is likely suboptimal. Coherent transmission between Tx and relay is obtained by the Marton-Marton coding technique developed by [3], who introduced the modified mutual covering lemma [3, Lemma 1] that we also use. (In a Gaussian setting, [4] also uses the relay as a broadcast channel).

The double random binning technique of [5] was the first achievable scheme for mutual secrecy in a two-Rx broadcast setup. [6] studied an extension of [5] wherein dedicated secure Tx-Rx links carrying fixed-rate secret keys were present. The model studied in this paper can be seen as another extension of [5] with the introduction of a dedicated relay trusted by all parties. It can also be seen as an extension of relay-eavesdropper with a "strong" relay studied by [7, Theorem 2] to a situation where both Rxs have legitimate message requirements and mutual secrecy is desired.

978-1-5386-3821-7/18/$31.00 © 2018 IEEE

[8, Chapter 7] indicate that for secrecy to be obtainable via DF in relay-eavesdropper, the Rel→Rx link must be stronger than the Rel→Eve link. Naively, this may lead one to conclude that mutual secrecy is unobtainable with a relay that performs DF. *Our results indicate that this intuition may be incorrect.*

The RBC with mutual secrecy was also studied by [9]. Their achievable scheme – like [7] (and unlike ours) – uses backward decoding and regular encoding, which respectively incurs large delay and is inflexible. They have not used the relay as a broadcast channel in its own right. The secret message is carried on the Tr→Rx link, which is problematic in DF based scenarios because this link is weaker than the Tr→Rel link.

Paper organization: Section II describes the model. Section III states the main theorems. Sections IV through VII respectively contain the achievable scheme, error probability analysis and equivocation calculation, and the conclusion. *Note:* For definitions of regular and irregular encoding, backward and forward sliding window decoding, see [1].

II. The Model: RBC with Mutual Secrecy

We assume a two-Rx discrete memoryless relay broadcast channel (DM-RBC) with two confidential messages. The finite sets $\mathcal{X}_{t=1,2}$, $\mathcal{Y}_{t=2,3,4}$ respectively represent the input at node 1 (Tx), at node 2 (relay), the output at nodes 2, 3 (Rx 1) and 4 (Rx 2). The channel is described by the conditional probability distribution $P_{Y_2,Y_3,Y_4|X_1,X_2}$, where RVs $X_t \overset{t=1,2}{\in} \mathcal{X}_t$, $Y_t \overset{t=2,3,4}{\in} \mathcal{Y}_t$. The Tx sends $B-1$ independent messages $M_t \in \{1,2,\ldots,2^{nR_t}\} \triangleq \mathcal{M}_t$ to the respective Rx $t \in \{1,2\}$ in B blocks of n channel uses each, while ensuring information theoretic secrecy (see below). The channel is memoryless and without feedback i.e. $\forall (\mathbf{x}_1,\mathbf{x}_2) \in \prod_{t=1}^{2} \mathcal{X}_t^n, \mathbf{y}_t \overset{t=2,3,4}{\in} \mathcal{Y}_t^n$:

$$P(\mathbf{y}_2,\mathbf{y}_3,\mathbf{y}_4|\mathbf{x}_1,\mathbf{x}_2) = \prod_{i=1}^{n} P_{Y_2,Y_3,Y_4|X_1,X_2}(y_{2i},y_{3i},y_{4i}|x_{1i},x_{2i})$$

The Tx channel input is obtained by passing satellite codewords $\mathbf{u}_t \equiv \mathbf{u}_t(|\mathbf{v}_t)_{t=1,2}$ through a stochastic encoder which generates $\mathbf{x}_1 \sim \prod_{i=1}^{n} P_{X_1|U_1,U_2}(x_{1i}|u_{1i},u_{2i})$. The relay channel input is obtained by passing codewords $\mathbf{v}_{t=1,2}$ through a stochastic encoder which generates $\mathbf{x}_2 \sim$

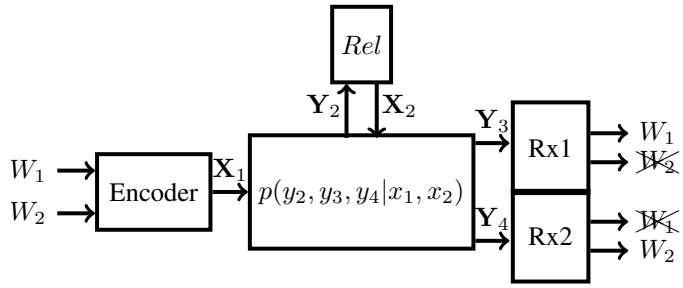

Fig. 1. Two Receiver Dedicated Relay Broadcast Channel with Trusted Relay (i.e. the relay is an extension of the transmitter, and is trusted by both Rxs) and Two Confidential Messages.

$\prod_{i=1}^{n} P_{X_2|V_1,V_2}(x_{2i}|v_{1i}, v_{2i})$. (See Section IV, encoding, for how $(\mathbf{u}_t, \mathbf{v}_t)_{t=1,2}$ are chosen). The sequences $\mathbf{x}_{t=1,2}$ are not part of code $\mathcal{C}$. They are generated at the time of transmission by choosing an appropriate quadruple $(\mathbf{u}_t, \mathbf{v}_t)_{t=1,2}$. The relay decoding function is a map $\phi_2 : \mathcal{Y}_2^n \to \mathcal{M}_1 \times \mathcal{S}_1 \times \mathcal{M}_2 \times \mathcal{S}_2$. In the preceding, the subbin index $S_t \in \{1, 2, \ldots, 2^{n[R_{2t}-R_t]}\} \triangleq \mathcal{S}_t$. (See Section IV). The decoding map at Rx $1 \equiv Y_3$ (resp. Rx $2 \equiv Y_4$) is $\phi_3 : \mathcal{Y}_3^n \times \mathcal{Y}_3^n \to \mathcal{M}_1 \times \mathcal{S}_1$ (resp. $\phi_4 : \mathcal{Y}_4^n \times \mathcal{Y}_4^n \to \mathcal{M}_2 \times \mathcal{S}_2$). (See Remark 9 for why S_ts are decoded). A $(2^{nR_1}, 2^{nR_2}, n, P_e^{(n)})$ code for the RBC consists of the stochastic encoding functions, decoding functions $\phi_{t=2,3,4}$, and the error probability $P_e^{(n)} \triangleq \max\{P_{e,2}^{(n)}, P_{e,3}^{(n)}, P_{e,4}^{(n)}\}$:

$$P_{e,2}^{(n)} = \sum_{(m_t,s_t)_{t=1,2}} \frac{\Pr[\phi_2(\mathbf{Y}_2) \neq (m_t, s_t)_{t=1,2}|(m_t, s_t)_{t=1,2}]}{2^{nR_1} \times 2^{n[R_{21}-R_1]} \times 2^{nR_2} \times 2^{n[R_{22}-R_2]}}$$

$$P_{\substack{e,t+2 \\ t=1,2}}^{(n)} = \sum_{(m_t,s_t)} \frac{\Pr[\phi_{t+2}(\mathbf{Y}_{t+2} \times \mathbf{Y}_{t+2}) \neq (m_t, s_t)|m_t, s_t]}{2^{nR_t} \times 2^{n[R_{2t}-R_t]}}$$

Rates (R_1, R_2) achievable for the DM-RBC with confidential messages if, for any $\epsilon_0 > 0, \exists(2^{nR_1}, 2^{nR_2}, n, P_e^{(n)})$ code s.t.:

$$\begin{aligned}
&P_e^{(n)} \leq \epsilon_0 \text{ reliability requirement} \\
&n(B-1)R_1 - H(M_1^{[B-1]}|\mathbf{Y}_4^{[B]}) \leq n(B-1)\epsilon_0 \\
&n(B-1)R_2 - H(M_2^{[B-1]}|\mathbf{Y}_3^{[B]}) \leq n(B-1)\epsilon_0
\end{aligned}$$

The last two constraints are the weak secrecy constraints [5]. We use the notation $\bar{t} \triangleq \{1,2\}\backslash\{t\}$, and $t^{[j]} \triangleq \{t_1, t_2, \ldots, t_j\}$.

III. Inner Bound

Theorem 1. *A (pure secrecy) rate pair (R_1, R_2) is achievable if there exist distributions $P_Q P_{V_1,V_2|Q}, P_{U_1,U_2|V_1,V_2,Q}, P_{X_1|U_1,U_2,Q}, P_{X_2|V_1,V_2,Q}$, so that the following inequalities are satisfied.*

$$\begin{aligned}
R_1 &\leq \min\{I(U_1, V_1; Y_3|Q), I(U_1; U_2, V_2, Y_2|V_1, Q)\} \\
&\quad - I(U_1, V_1; U_2, V_2, Y_4|Q) \\
R_2 &\leq \min\{I(U_2, V_2; Y_4|Q), I(U_2; U_1, V_1, Y_2|V_2, Q)\} \\
&\quad - I(U_2, V_2; U_1, V_1, Y_3|Q) \\
R_1 + R_2 &\leq I(U_1; V_2, Y_2|V_1, Q) + I(U_2; V_1, Y_2|V_2, Q) \\
&\quad + I(U_1; U_2|V_1, V_2, Y_2, Q) \\
&\quad - I(U_1, V_1; U_2, V_2, Y_4|Q) - I(U_2, V_2; U_1, V_1, Y_3|Q)
\end{aligned}$$

(R_1, R_2) is obtained by Fourier-Motzkin (FM) elimination of the following inequalities, followed by convexification via a time-sharing random variable (RV) Q. In the doubly subscripted quantities below, the first subscript refers to the node index; the second to the intended Rx. Thus R_{12} refers to the rate of the codebook at the Tx intended for Rx 2.

Theorem 2. *A (pure secrecy) rate pair (R_1, R_2) is achievable if $\exists R_{11}, R_{12}, R_{21}, R_{22}$, and distributions $P_{V_1V_2}, P_{U_1U_2|V_1V_2}, P_{X_1|U_1U_2}, P_{X_2|V_1V_2}$, so that the following inequalities are satisfied.*

$$\begin{aligned}
&R_{11} \leq \min\{I(U_1, V_1; Y_3), I(U_1; U_2, V_2, Y_2|V_1)\} \qquad (1) \\
&R_{12} \leq \min\{I(U_2, V_2; Y_4), I(U_2; U_1, V_1, Y_2|V_2)\} \\
&R_{11} + R_{12} \leq I(U_1; V_2, Y_2|V_1) + I(U_2; V_1, Y_2|V_2) \\
&\qquad\qquad + I(U_1; U_2|V_1, V_2, Y_2) \\
&R_{21} - R_1 > I(V_1; U_2, V_2, Y_4) \qquad (2) \\
&R_{22} - R_2 > I(V_2; U_1, V_1, Y_3) \\
&R_{11} - R_1 = I(U_1, V_1; U_2, V_2, Y_4) - \epsilon_{11} \\
&R_{12} - R_2 = I(U_2, V_2; U_1, V_1, Y_3) - \epsilon_{12}
\end{aligned}$$

$$\begin{aligned}
&R_{11} - R_{21} > I(U_1; V_2|V_1); \;\; R_{12} - R_{22} > I(U_2; V_1|V_2) \quad (3) \\
&[R_{11} - R_{21}] + [R_{12} - R_{22}] > I(U_1; V_2|V_1) + I(U_2; V_1|V_2) \\
&\qquad\qquad + I(U_1; U_2|V_1, V_2)
\end{aligned}$$

Remark 3. *From the above, we can obtain: $R_{1t} \geq R_{2t} \geq R_t, \;\; t = 1, 2$, indicating the ordering between the corresponding codebook sizes at the Tx, the relay, and the (pure secrecy) message rate intended for Rxs $1, 2$.*

Remark 4. *In the inequalities (1) on R_{1t}, $t = 1, 2$, the first term inside the* min *arises from decoding at the intended Rxs $t = 1, 2$ and second term from decoding at the relay. The sum-rate constraint $R_{11} + R_{12}$ arises from (nonunique) decoding at the relay. The following redundant constraints also arise from nonunique decoding at the relay.*

$$R_{11} + R_{12} - \underset{t=1,2}{R_{2t}} \leq I(U_1; V_2, Y_2|V_1) + I(U_2; U_1, V_1, Y_2|V_2)$$

Remark 5. *The four inequalities (2) are packing constraints on the bins at the relay and the transmitter that arise due to secrecy requirements. ϵ_{1j}s satisfy $n\epsilon_{1j} \overset{n\uparrow\infty}{\to} 0$.*

Remark 6. *Slack variables $\Delta_{t=1,2} > 0$ can be used to rewrite the first two inequalities in (2) as equalities and obtain, after appropriate manipulations, the following constraints: $\Delta_1 < I(U_1; U_2, Y_4|V_1, V_2)$, $\Delta_2 < I(U_2; U_1, Y_3|V_1, V_2)$, $\Delta_1 + \Delta_2 < I(U_1; U_2, Y_4|V_1, V_2) + I(U_2; U_1, Y_3|V_1, V_2) - I(U_1; U_2|V_1, V_2)$.*

IV. Achievability Scheme

In decode-forward scenarios, the relay and transmitter must transmit coherently. This is enabled in our achievability scheme by the Marton-Marton technique developed by [3]. Mutual secrecy is obtained by means of double random binning developed by [5]. The employed coding structure is

$$\mathcal{C}_{1j}^{(b)} = \left\{ \mathbf{u}_j^{(b)}(m_j, s_j, t_j, m_j', s_j') | m_j, m_j' \in \left[2^{nR_j}\right], s_j, s_j' \in \left[2^{n(R_{2j}-R_j)}\right], t_j \in \left[2^{n(R_{1j}-R_{2j})}\right] \right\} \tag{4}$$

shown below. Let us consider rates $R_1, R_2, R_{11}, R_{12}, R_{21}, R_{22}$ satisfying the constraints in Theorem 2 for some distributions $P_{V_1,V_2}, P_{U_1,U_2|V_1,V_2}, P_{X_1|U_1,U_2}, P_{X_2|V_1,V_2}$.

Codebook Generation: The Tx uses two codes, $\mathcal{C}_{11}, \mathcal{C}_{12}$, one intended for each Rx. Similarly, the relay uses two codes, $\mathcal{C}_{21}, \mathcal{C}_{22}$, one intended for each Rx. Our achievable scheme is over B blocks of n channel uses each. So each code $\mathcal{C}_{ij}$ has B parts: $\mathcal{C}_{ij} = (\mathcal{C}_{ij}^{(1)}, \ldots, \mathcal{C}_{ij}^{(B)})$. We now describe what these codes contain, and how they are generated. The size of the codes used by the relay are given by

$$|\mathcal{C}_{2j}^{(k)}| = 2^{nR_{2j}} \qquad \text{for } j = 1, 2; k \in [1:B].$$

- For blocks $b \in [1:B], j = 1, 2$, relay codebooks $\mathcal{C}_{2j}^{(b)}$:

$$\mathcal{C}_{2j}^{(b)} = \left\{ \mathbf{v}_j^{(b)}(m_j', s_j') | m_j' \in \left[2^{nR_j}\right], s_j' \in \left[2^{n(R_{2j}-R_j)}\right] \right\}$$

- For blocks $b \in [1:B], j = 1, 2$, Tx codebooks $\mathcal{C}_{1j}^{(b)}$: See the equation (4) at the top of the page.

All the codewords are generated independently, and the components of $\mathbf{u}_j^{(b)}(m_j, s_j, t_j, m_j', s_j')$ are generated independently as a satellite of $\mathbf{v}_j^{(b)}(m_j', s_j')$ using the conditional distribution $P_{U_j|V_j}$, i.e. $\mathbf{u}_j^{(b)}(m_j, s_j, t_j, m_j', s_j') \sim \prod_{i=1}^n P_{U_j|V_j}(\mathbf{u}_{ji}^{(b)} | \mathbf{v}_{ji}^{(b)}(m_j', s_j'))$. The code can be thought as the union of satellite codebooks for each relay codeword $\mathbf{v}_j^{(b)}(m_j', s_j')$ (m', s' corresponds to the previous block). Each satellite codebook has 2^{nR_j} bins ($\equiv$ messages) indexed by m_j, $2^{n(R_{2j}-R_j)}$ subbins indexed by s_j in each bin, and $2^{n(R_{1j}-R_{2j})}$ codewords indexed by t_j in each subbin. Each relay codebook has 2^{nR_j} bins indexed by m_j'; each relay bin has $2^{n[R_{2j}-R_j]}$ codewords, indexed by s_j'. *This is identical to the number of subbins per bin in each satellite codebook, enabling a one-to-one correspondence to be set up*. The codebooks to be used in the B blocks are supplied to all users.

Encoding at the transmitter: To transmit $(m_1^{(b)}, m_2^{(b)})$ in block b, the Tx finds a pair $(s_1^{(b)}, s_2^{(b)})$ s.t.:

$$\left(\mathbf{v}_1^{(b+1)}(m_1^{(b)}, s_1^{(b)}), \mathbf{v}_2^{(b+1)}(m_2^{(b)}, s_2^{(b)})\right) \in T_\epsilon. \tag{5}$$

Remark 7. *The Tx looks inside the appropriate bins in the relay codebooks in the **next** block $b+1$. Thus the codebooks must be known at least one block in advance.*

If there is no such pair, then the encoder chooses $(1, 1)$, and if there is more than one, then it chooses the least such pair in lexicographical order. It then picks $(t_1^{(b)}, t_2^{(b)})$ s.t.:

$$\Big(\mathbf{u}_1^{(b)}(m_1^{(b)}, s_1^{(b)}, t_1^{(b)}, m_1^{(b-1)}, s_1^{(b-1)}), \mathbf{v}_1^{(b)}(m_1^{(b-1)}, s_1^{(b-1)}), \mathbf{u}_2^{(b)}(m_2^{(b)}, s_2^{(b)}, t_2^{(b)}, m_2^{(b-1)}, s_2^{(b-1)}), \mathbf{v}_2^{(b)}(m_2^{(b-1)}, s_2^{(b-1)})\Big) \tag{6}$$

is typical where $s_1^{(b-1)}||_{b=1} = m_1^{(b-1)}|_{b=1} = m_2^{(b-1)}|_{b=1} = 1$. Also, $s_2^{(0)} = 1'$ is the least index s.t. $(\mathbf{v}_1^{(1)}(1,1), \mathbf{v}_2^{(1)}(1,1'))$ is jointly typical. By appropriate relabelling of the indexes we can take $m_2^{(b-1)} = 1$ itself, a convention followed below. The codeword $\mathbf{x}_1^{(b)}$ is generated from $\mathbf{u}_1^{(b)}(m_1^{(b)}, s_1^{(b)}, t_1^{(b)}, m_1^{(b-1)}, s_1^{(b-1)})$ and $\mathbf{u}_2^{(b)}(m_2^{(b)}, s_2^{(b)}, t_2^{(b)}, m_2^{(b-1)}, s_2^{(b-1)})$ component-wise using $\prod_{i=1}^n p_{X_1|U_1,U_2}(x_{1i}|u_{1i}^{(b)}, u_{2i}^{(b)})$.

Decoding at the relay: The relay knows $m_1^{(0)} = m_2^{(0)} = s_1^{(0)} = s_2^{(0)} = 1$ and assigns the same decoded values $\widetilde{m}_1^{(0)} = \widetilde{m}_2^{(0)} = \widetilde{s}_1^{(0)} = \widetilde{s}_2^{(0)} = 1$. In block b, the relay chooses the quadruple $(\widetilde{m}_1^{(b)}, \widetilde{s}_1^{(b)}, \widetilde{m}_2^{(b)}, \widetilde{s}_2^{(b)})$ if it is the unique one s.t.:

$$\Big(\mathbf{u}_1^{(b)}(\widetilde{m}_1^{(b)}, \widetilde{s}_1^{(b)}, \tilde{t}_1^{(b)}, \widetilde{m}_1^{(b-1)}, \widetilde{s}_1^{(b-1)}), \mathbf{v}_1^{(b)}(\widetilde{m}_1^{(b-1)}, \widetilde{s}_1^{(b-1)}), \mathbf{v}_2^{(b)}(\widetilde{m}_2^{(b-1)}, \widetilde{s}_2^{(b-1)}), \mathbf{u}_2^{(b)}(\widetilde{m}_2^{(b)}, \widetilde{s}_2^{(b)}, \tilde{t}_2^{(b)}, \widetilde{m}_2^{(b-1)}, \widetilde{s}_2^{(b-1)}), \mathbf{y}_2^{(b)}\Big)$$

is typical for some $\tilde{t}_1^{(b)}, \tilde{t}_2^{(b)}$. This is the value of the tuple $(m_1^{(b)}, s_1^{(b)}, t_1^{(b)}, m_2^{(b)}, s_2^{(b)}, t_2^{(b)})$ decoded by the relay. We only require that $(\tilde{m}_1^{(b)}, \tilde{s}_1^{(b)}, \tilde{m}_2^{(b)}, \tilde{s}_2^{(b)})$ be unique. $(\tilde{t}_1^{(b)}, \tilde{t}_2^{(b)})$ need not be. If no such quadruple exists or there is more than one, the relay chooses $(\widetilde{m}_1^{(b)}, \widetilde{s}_1^{(b)}, \widetilde{m}_2^{(b)}, \widetilde{s}_2^{(b)}) = (1, 1, 1, 1)$.

Encoding at the relay: In block b, the relay transmits $\mathbf{x}_2\left(\mathbf{v}_1^{(b)}(\widetilde{m}_1^{(b-1)}, \widetilde{s}_1^{(b-1)}), \mathbf{v}_2^{(b)}(\widetilde{m}_2^{(b-1)}, \widetilde{s}_2^{(b-1)})\right)$, where $\mathbf{x}_2$ is a stochastic mapping, according to $\prod_{i=1}^n p(x_{2i}|v_{1i}^{(b)}(\widetilde{m}_1^{(b-1)}, \widetilde{s}_1^{(b-1)}), v_{2i}^{(b)}(\widetilde{m}_2^{(b-1)}, \widetilde{s}_2^{(b-1)}))$.

Decoding at the receivers: The Rxs know $m_1^{(0)} = m_2^{(0)} = s_1^{(0)} = s_2^{(0)} = 1$ and assign $\widehat{m}_1^{(0)} = \widehat{m}_2^{(0)} = \widehat{s}_1^{(0)} = \widehat{s}_2^{(0)} = 1$. We assume that the Rx 1 has correctly decoded $(\hat{m}_1^{(b-1)}, \hat{s}_1^{(b-1)})$. To decode $m_1^{(b)}$, Rx 1 performs sliding window decoding and looks for a unique tuple $(\hat{m}_1^{(b)}, \hat{s}_1^{(b)})$ s.t.: $\left(\mathbf{v}_1^{(b+1)}(\widehat{m}_1^{(b)}, \widehat{s}_1^{(b)}), \mathbf{y}_3^{(b+1)}\right) \in T_\epsilon$ and

$$\left(\mathbf{u}_1^{(b)}(\widehat{m}_1^{(b)}, \widehat{s}_1^{(b)}, \hat{t}_1^{(b)}, \widehat{m}_1^{(b-1)}, \widehat{s}_1^{(b-1)}), \mathbf{v}_1^{(b)}(\widehat{m}_1^{(b-1)}, \widehat{s}_1^{(b-1)}), \mathbf{y}_3^{(b)}\right)$$

is typical for some $\hat{t}_1^{(b)}$. If a unique such $(\hat{m}_1^{(b)}, \hat{s}_1^{(b)})$ is found, then $\hat{m}_1^{(b)}$ is declared as the decoded message, else an error is declared. Rx 2 decodes $m_2^{(b)}$ in a similar manner.

Remark 8. *$\hat{t}_k^{(b)}$ is decoded nonuniquely by Rx k, $k = 1, 2$.*

Remark 9. *Decoding $\hat{m}_t^{(b)}$ correctly and $\hat{s}_t^{(b)}$ incorrectly ($t = 1, 2$) gives the correct block b message, but leads (w.h.p) to error in block $b+1$ as the relay codeword will have been decoded incorrectly. Hence this is also considered an error.*

V. Probability of Error Analysis

A. Probability of encoding error:

The modified mutual covering lemma [3, Lemma 1] ensures that probability of success in the encoding step at the Tx given

in (6), can be made arbitrarily close to one for large enough n by choosing, for $t = 1, 2: \ R_{1t} - R_{2t} > I(U_t; V_{\bar{t}}|V_t)$ and

$$\sum_{t=1,2} [R_{1t} - R_{2t}] > \sum_{t=1,2} I(U_t; V_{\bar{t}}|V_t) + I(U_1; U_2|V_1, V_2)$$

Success in the encoding step (5) is ensured by the condition $[R_{21} - R_1] + [R_{22} - R_2] > I(V_1; V_2)$ which follows from the standard mutual covering lemma [1, Lemma 8.1]. Note that the first two constraints in (2) in Theorem 2 make this redundant.

B. Probability of decoding error:

Under random coding arguments, assume w.l.o.g that the transmitted indices are $(1, 1, 1, 1)$ for all $b \in [1 : B]$.

- *Decoding at the relay:* We list three kinds of error events.
  - $E_r(e, 1)$: The tuple $(m_1, s_1, 1, 1)$ satisfies the typicality test for $(m_1, s_1) \neq (1, 1)$. The number of possibilities is $(2^{nR_{11}} - 2^{n[R_{11}-R_{12}]}) \times 1$. *The second factor* 1 *hides a crucial subtlety*. See remark 10.
  - $E_r(1, e)$: The tuple $(1, 1, m_2, s_2)$ satisfies the typicality test for $(m_2, s_2) \neq (1, 1)$. $P(E_r(1, e))$ can be obtained as above with a change of variables.
  - $E_r(e, e)$: The tuple (m_1, s_1, m_2, s_2) satisfies the typicality test for $(m_1, s_1) \neq (1, 1)$ and $(m_2, s_2) \neq (1, 1)$. The number of possibilities is $(2^{nR_{11}} - 2^{n[R_{11}-R_{12}]}) \times (2^{nR_{12}} - 2^{n[R_{12}-R_{22}]})$.

  By standard calculations, the relay's decoding error probability can be made arbitrarily small if:

$$\begin{aligned} R_{11} &\leq I(U_1; V_2, U_2, Y_2|V_1) - \epsilon \\ R_{12} &\leq I(U_2; V_1, U_1, Y_2|V_2) - \epsilon \\ R_{11} + R_{12} &\leq I(U_1; V_2, Y_2|V_1) + I(U_2; U_1, V_1, Y_2|V_2) - \epsilon. \end{aligned}$$

  Remark 10. *In computing the number of possibilities above for error event $E_r(e, 1)$, we have written the second factor as* 1*. It means that the relay has decoded not just the indices (m_2, s_2) correctly as $(1, 1)$, but also t_2 correctly. But if (m_2, s_2) is decoded correctly as $(1, 1)$ and t_2 is decoded incorrectly within the correct subbin, then the second factor above becomes $2^{n[R_{12}-R_{22}]} - 1$. In this case, the RHS will be identical to the error event $E_r(e, e)$; the LHS will have an extra term $[R_{12} - R_{22}]$, giving a constraint redundant w.r.t the one on $R_{11} + R_{12}$:*

$$R_{11} + R_{12} - R_{22} \leq I(U_1; V_2, Y_2|V_1) + I(U_2; U_1, V_1, Y_2|V_2) - \epsilon$$

  A similar remark w.r.t. $E_r(1, e)$ gives the other redundant constraint with $[R_{11} - R_{21}] + R_{12}$ on the LHS.

- *Decoding at the Rxs:* We show that we can guarantee successful decoding at Rxs by choosing $R_{11} \leq I(U_1, V_1; Y_3) - \epsilon$ and $R_{12} \leq I(U_2, V_2; Y_4) - \epsilon$. Using $\mathbf{y}_3^{(b+1)}$, Rx 1 list decodes to reduce the size of the ambiguity set of possible $\mathbf{v}_1^{(b+1)}$ from $2^{nR_{21}}$ to $2^{n[R_{21}-I(V_1;Y_3)]}$. Each $\mathbf{v}_1$ corresponds to a previous block subbin of size $2^{n[R_{11}-R_{21}]}$. Thus the search space of possible $\mathbf{u}_1^{(b)}$ is now of size $2^{n[R_{11}-I(V_1;Y_3)]}$ – assuming that the relay codeword in block b has already been correctly decoded (in the previous step). If so, the information obtained from the other JT condition is $2^{nI(U_1;Y_3|V_1)}$. If $R_{11} - I(V_1; Y_3) < I(U_1; Y_3|V_1) \equiv R_{11} < I(U_1, V_1; Y_3)$, then we can decode $\mathbf{u}_1^{(b)}$ correctly w.h.p., and thus also $\mathbf{v}_1^{(b+1)}$, as it's a function of $\mathbf{u}_1^{(b)}$. Rx 2 performs likewise.

VI. Equivocation Calculations

We denote the RVs for the messages in block b for the two Rxs by $M_t^{(b)}$, $t = 1, 2$. The codewords chosen by the Tx and the relay in block b are denoted by $\mathbf{U}_1^{(b)}, \mathbf{U}_2^{(b)}, \mathbf{V}_1^{(b)}, \mathbf{V}_2^{(b)}$ respectively. The block b sequences inputted by Tx and relay are denoted by $\mathbf{X}_1^{(b)}$ and $\mathbf{X}_2^{(b)}$ respectively. We will show that the multi-block equivocation of the message $M_1^{[B-1]}$ intended for Rx 1 given the observation of the Rx 2 satisfies:

$$H(M_1^{[B-1]}|\mathbf{Y}_4^{[B]}, \mathcal{C}) \geq n(B-1)(R_1 - \epsilon_0)$$

Since the relay always chooses $m_1^{(0)} = m_2^{(0)} = s_1^{(0)} = s_2^{(0)} = 1$, all parties know that $\mathbf{V}_t^{(1)} = \mathbf{v}_t^{(1)}(1, 1)$, $t = 1, 2$. We have:

$$\begin{aligned} &H(M_1^{[B-1]}|\mathbf{Y}_4^{[B]}, \mathcal{C}) \\ &\geq H(M_1^{[B-1]}|(\mathbf{U}_2, \mathbf{V}_2, \mathbf{Y}_4)^{[B]}, \mathcal{C}) \\ &\geq I((\mathbf{U}_1, \mathbf{V}_1)^{[B]}; M_1^{[B-1]}|(\mathbf{U}_2, \mathbf{V}_2, \mathbf{Y}_4)^{[B]}, \mathcal{C}) \\ &= H((\mathbf{U}_1, \mathbf{V}_1)^{[B]}|(\mathbf{U}_2, \mathbf{V}_2, \mathbf{Y}_4)^{[B]}, \mathcal{C}) \\ &\quad - H((\mathbf{U}_1, \mathbf{V}_1)^{[B]}|(\mathbf{U}_2, \mathbf{V}_2, \mathbf{Y}_4)^{[B]}, M_1^{[B-1]}, \mathcal{C}) \\ &= H((\mathbf{U}_1, \mathbf{V}_1)^{[B]}|(\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}) \\ &\quad - I((\mathbf{U}_1, \mathbf{V}_1)^{[B]}; \mathbf{Y}_4^{[B]}|(\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}) \\ &\quad - H(\mathbf{U}_1^{[B]}, \mathbf{V}_1^{[B]}|(\mathbf{U}_2, \mathbf{V}_2, \mathbf{Y}_4)^{[B]}, M_1^{[B-1]}, \mathcal{C}) \end{aligned} \quad (7)$$

We expand the first term in (7) by the chain rule to obtain:

$$\begin{aligned} &\sum_{j=1}^{B} H((\mathbf{U}_1, \mathbf{V}_1)^{(j)}|(\mathbf{U}_1, \mathbf{V}_1)^{[j-1]}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}) \\ &\geq \sum_{j=1}^{B} H(\mathbf{U}_1^{(j)}|\mathbf{V}_1^{(j)}, (\mathbf{U}_1, \mathbf{V}_1)^{[j-1]}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}) \\ &\overset{(a)}{=} \sum_{j=1}^{B-1} H(\mathbf{U}_1^{(j)}|\mathbf{V}_1^{(j)}, (\mathbf{U}_1, \mathbf{V}_1)^{[j-1]}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}) \\ &\overset{(b)}{=} \sum_{j=1}^{B-1} H(\mathbf{U}_1^{(j)}, \mathbf{V}_1^{(j+1)}|\mathbf{V}_1^{(j)}, (\mathbf{U}_1, \mathbf{V}_1)^{[j-1]}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}), \end{aligned}$$

where (a) follows because $\mathbf{U}_1^{(B)} = \mathbf{u}_1^{(B)}(1, 1, 1, m^{(B-1)}, s^{(B-1)})$, (b) because $\mathbf{V}_1^{(j+1)}$ is determined by $\mathbf{U}_1^{(j)}$. Consider $j = 1$. The number of $\mathbf{v}_1^{(2)}$s typical with a given $(\mathbf{v}_2, \mathbf{u}_2)^{(2)}$ pair is $\approx 2^{n(R_{21}-I(V_1;U_2,V_2))}$. For each possible $\mathbf{v}_1^{(2)}$, the encoder can choose uniformly from among $2^{n(R_{11}-R_{21})}\mathbf{u}_1^{(1)}$ sequences. The number of possible choices for $\mathbf{u}_1^{(1)}$ is thus $2^{n[R_{11}-I(V_1;U_2,V_2)]}$. Note that since $\mathbf{v}_1^{(1)}$ and $(\mathbf{u}_2, \mathbf{v}_2)^{(1)}$ are in the conditioning, we can further reduce the number of possibilities for $\mathbf{u}_1^{(1)}$ by a factor $2^{nI(U_1;U_2,V_2|V_1)}$ down to $2^{n[R_{11}-I(U_1,V_1;U_2,V_2)]}$. In terms of equivocation, this contributes a term $n(R_{11} - I(U_1, V_1; U_2, V_2) - \epsilon_1)$. The same argument

applies for $j = 2, 3, \ldots, B-1$, and so we can lower bound the first term as:

$$n(B-1)\left(R_{11} - I(U_1, V_1; U_2, V_2) - \epsilon_1\right) \tag{8}$$

To upper bound the second term of (7), we use the chain rule:

$$\begin{aligned}
&\sum_{j=1}^{B} I((\mathbf{U}_1, \mathbf{V}_1)^{[B]}; \mathbf{Y}_4^{(j)} | \mathbf{Y}_4^{[j-1]}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}) \\
&\overset{(a)}{\leq} \sum_{j=1}^{B} I((\mathbf{U}_1, \mathbf{V}_1)^{(j)}; \mathbf{Y}_4^{(j)} | (\mathbf{U}_2, \mathbf{V}_2)^{(j)}) \\
&\overset{(b)}{\leq} n(B-1)[I(Y_4; U_1, V_1 | U_2, V_2) + \epsilon_2]
\end{aligned}$$

for large enough n for any $\epsilon > 0$. Here, (a) follows because

$$\mathbf{Y}_4^{(j)} \leftrightarrow (\mathbf{U}_1^{(j)}, \mathbf{V}_1^{(j)}, \mathbf{U}_2^{(j)}, \mathbf{V}_2^{(j)}) \leftrightarrow \left((\mathbf{U}_1, \mathbf{V}_1, \mathbf{U}_2, \mathbf{V}_2)^{[j-1]}, (\mathbf{U}_1, \mathbf{V}_1, \mathbf{U}_2, \mathbf{V}_2)^{[j+1:B]}, \mathbf{Y}_4^{[j-1]}, \mathcal{C}\right)$$

forms a Markov chain. In (b) we have a factor $B-1$ and not B because $\mathbf{V}_1^{(1)}$ and $\mathbf{U}_1^{(B)}$ do not contribute. See [5] for a similar calculation bounding each individual term.

We define the RV $\mathbb{I}_{\mathcal{R}} = 0$ if the relay makes a decoding error in some block and $\mathbb{I}_{\mathcal{R}} = 1$ if it decodes correctly in all B blocks. Now we upper bound the third term of (7)

$$\begin{aligned}
&H((\mathbf{U}_1, \mathbf{V}_1)^{[B]} | (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}, M_1^{[B-1]}, \mathbf{Y}_4^{[B]}) \\
&= H((\mathbf{U}_1, \mathbf{V}_1)^{[B]} | \mathbb{I}_{\mathcal{R}}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}, M_1^{[B-1]}, \mathbf{Y}_4^{[B]}) \\
&\quad + I(\mathbb{I}_{\mathcal{R}}; (\mathbf{U}_1, \mathbf{V}_1)^{[B]} | (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}, M_1^{[B-1]}, \mathbf{Y}_4^{[B]}) \\
&\overset{(a)}{\leq} H((\mathbf{U}_1, \mathbf{V}_1)^{[B]} | \mathbb{I}_{\mathcal{R}}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}, M_1^{[B-1]}, \mathbf{Y}_4^{[B]}) + 1 \\
&\leq H((S_1, T_1)^{[B]} | \mathbb{I}_{\mathcal{R}}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}, M_1^{[B-1]}, \mathbf{Y}_4^{[B]}) + 1 \\
&= \sum_{b=1}^{B-1} \big[H((S_1, T_1)^{(b)} | (S_1, T_1)^{[b-1]}, \mathbb{I}_{\mathcal{R}}, \ldots \\
&\qquad \ldots (\mathbf{U}_2, \mathbf{V}_2)^{[B]}, \mathcal{C}, M_1^{[B-1]}, \mathbf{Y}_4^{[B]})\big] + 1
\end{aligned}$$

where (a) follows because the conditional mutual information term is upper bounded by $H(\mathbb{I}_{\mathcal{R}}) \leq 1$, as $\mathbb{I}_{\mathcal{R}}$ is a binary RV.

We will examine the ambiguity about $(S_1, T_1)^{(b)}$ at the Rx 2 $\equiv$ Y_4 if it is additionally provided $M_1^{[B-1]}, S_1^{[b-1]}, T_1^{[b-1]}, (\mathbf{U}_2, \mathbf{V}_2)^{[B]}$ and also assuming that the relay decodes correctly. Consider $b = 1$.

1) From $(\mathbf{U}_2, \mathbf{V}_2, \mathbf{Y}_4)^{(2)}$ Rx 2 gets $\approx nI(V_1; Y_4, U_2, V_2)$ bits of information about $\mathbf{V}_1^{(2)} = \mathbf{v}_1^{(2)}(M_1^{(1)}, S_1^{(1)})$. Since $W_1^{(1)}$ is known to Rx 2, its remaining uncertainty about $S_1^{(1)}$ is $\leq n(R_{21} - R_1) - nI(V_1; Y_4, U_2, V_2)$. Here note that $R_{21} - R_1 > I(V_1; Y_4, U_2, V_2)$ by the conditions of Theorem 2.
2) The remaining uncertainty in $(S_1^{(1)}, T_1^{(1)})$ is thus $\leq n(R_{21} - R_1) - nI(V_1; Y_4, U_2, V_2) + n(R_{11} - R_{21}) = n(R_{11} - R_1) - nI(V_1; Y_4, U_2, V_2)$. So, there is a list of about $2^{n((R_{11}-R_1) - I(V_1; Y_4, U_2, V_2))}$ pairs $(S_1^{(1)}, T_1^{(1)})$ pairs. This includes the uncertainty in $T_1^{(1)}$.
3) All the possible codewords in the list are from the satellite codebook of $\mathbf{V}_1^{(1)}$. So, a randomly chosen codeword from the list has a probability of about $2^{-nI(U_1; U_2, V_2, Y_4 | V_1)}$ of being jointly typical with $(\mathbf{U}_2^{(1)}, \mathbf{V}_2^{(1)}, \mathbf{Y}_4^{(1)})$. So, the number of codewords from the list that are jointly typical with $\mathbf{U}_2^{(1)}, \mathbf{V}_2^{(1)}, \mathbf{Y}_4^{(1)}$ is $\approx 2^{n((R_{11}-R_1) - I(V_1; U_2, V_2, Y_4) - I(U_1; U_2, V_2, Y_4 | V_1))}$. So the uncertainty remaining in $(S_1^{(1)}, T_1^{(1)})$ is $\leq n\left((R_{11} - R_1) - I(U_1, V_1; U_2, V_2, Y_4) - \epsilon_{11}\right)$ But we have packed each transmitter bin with $R_{11} - R_1 \approx I(U_1, V_1; U_2, V_2, Y_4)$ and by our choice $n\epsilon_{11} \overset{n\uparrow\infty}{\to} 0$, and so each term can be made as small as desired and we can upper bound each term by $n\epsilon_3$.
4) Each term $j = 1, 2, \ldots, B-1$ contributes at most $n\epsilon_3$.
5) In the last block $b = B$, $S_1^{(B)} = T_1^{(B)} = 1$. So there is no uncertainty and the last block does not contribute.

We can upper bound the third term as the sum of $B-1$ terms: $\leq n(B-1)\epsilon_3 + 1 = n(B-1)\epsilon_3'$ (with $\epsilon_3' \overset{\text{def}}{=} \epsilon + 1/n$).

Finally, the upper and lower bounds for terms in (7) give:

$$\begin{aligned}
H(M_1^{[B-1]} | \mathbf{Y}_4^{[B]}, \mathcal{C}) &\geq n(B-1)(R_{11} - I(U_1, V_1; V_2, U_2) - \epsilon_1) \\
&\quad - n(B-1)(I(Y_4; U_1, V_1 | U_2, V_2) + \epsilon_2) - n(B-1)\epsilon_3' \\
&= n(B-1)[R_{11} - I(U_1, V_1; U_2, V_2, Y_4) - \epsilon_5] \\
&\overset{\because R_{11} - R_1 = I(U_1, V_1; U_2, V_2, Y_4)}{=} n(B-1)[R_1 - (\epsilon_{1j} + \epsilon_5)]
\end{aligned}$$

VII. Conclusion and Future Work

We have some preliminary results for the "weak" relay using compress-forward in the pure eavesdropper case. Our approach provides a novel perspective distinct from [7, Theorems 3, 4], and is an initial step to studying an RBC with mutual secrecy with a relay "strong" wrt one Rx and "weak" wrt the other.

VIII. Acknowledgements

The author is thankful to S. R. B. Pillai and B. K. Dey for constructive discussions. The support of the Bharti Centre for Communication, IIT Bombay is gratefully acknowledged.

References

[1] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. Cambridge University Press, 2011.
[2] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative Strategies and Capacity Theorems for Relay Networks," *IEEE Transactions on Information Theory*, vol. 51, no. 9, pp. 3037–3063, Sept 2005.
[3] L. Zhao and S. Y. Chung, "Marton-Marton Coding for a Broadcast Relay Network," in *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, July 2013, pp. 1282–1286.
[4] S. R. Bhaskaran, "Gaussian Degraded Relay Broadcast Channel," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3699–3709, Aug 2008.
[5] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete Memoryless Interference and Broadcast Channels With Confidential Messages: Secrecy Rate Regions," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2493–2507, June 2008.
[6] K. Iyer, "Broadcast Channel with Confidential Messages and Secret Keys," in *2016 National Conference on Communications*, March 2016.
[7] L. Lai and H. E. Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, Sept 2008.
[8] R. Liu and W. Trappe, Eds., *Securing Wireless Communications at the Physical Layer*. Springer, 2010.
[9] B. Dai, L. Yu, and Z. Ma, "Relay Broadcast Channel with Confidential Messages," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 410–425, Feb 2016.