Cooperation with an Untrusted Relay in Broadcast Channels

Liang Chen

***Abstract*—This paper studies secure communication over the broadcast channels with an untrusted relay. The relay helps users with transmission in broadcast channels, but we also wish to keep the information secret against the relay. Compress-and-forward relaying is a potential strategy to achieve secrecy. We obtain the achievable rate-equivocation regions by combining it with Marton's coding scheme and Cover's superposition coding scheme respectively. The secrecy rate region based on Marton's coding scheme provides a general result, without knowing information regarding two users. If we know which user is better (i.e. receiving more information), we can design a simpler scheme with superposition encoding. Outer bound to the rate-equivocation regions is also provided in this paper.**

I. Introduction

Wireless channel is broadcast by nature. This open nature facilitates cooperation in wireless communications by allowing users to relay information. However, the same nature induces security issues such as eavesdropping. Cooperation and security are two sides of a coin.

The effects of user cooperation in secret communication have been studied in [1], [2] for some cases. In [1], He and Yener consider a relay channel where the relay has a lower security clearance than the destination and is therefore untrusted. The relay is regarded as an eavesdropper. In [2], Ekrem and Ulukus consider the two-user broadcast channels where a relay link is introduced between two users. Each user wishes to keep its own information secret against the other.

In this paper, we consider a different scenario for two-user broadcast channels (see Fig. 1). A relay is introduced to assist both users. In [3], Liang and Veeravalli showed that we could obtain significant gain in capacity region by using such a relay in broadcast channels. However, the relay may have a lower level of security clearance than the destinations. For example, in a military network, not every node is supposed to have the same level of access information, despite serving as a relay through agreed protocols. If the decode-and-forward strategy [3] is used to assist users, there is no secrecy for the messages of both users at the relay since the relay first decodes them before forwarding. We hope the relay assists us in transmission. At the same time, we also wish to keep the information secret against the relay. In this paper, we adopt the compress-and-forward strategy [4] for cooperation. The relay compresses the received signals but does not decode them. With this cooperative protocol, we may achieve secrecy. We provide the rate-equivocation regions for the broadcast channels with an untrusted relay based on this strategy.

II. The Channel Model and Definitions

The broadcast channel with an untrusted relay consists of a channel input alphabet $\mathcal{X}$, a relay input alphabets $\mathcal{X}_r$, a relay output alphabet $\mathcal{Y}_r$, two channel output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$, and a probability transition function $p(y_1, y_2, y_r \mid x, x_r)$.

A $(2^{nR_1}, 2^{nR_2}, n)$ code for a broadcast channel with an untrusted relay consists of:

Two message sets: $\mathcal{W}_1 = \{1, 2, ..., 2^{nR_1}\}, \mathcal{W}_2 = \{1, 2, ..., 2^{nR_2}\}$;

An encoder: $\mathcal{W}_1 \times \mathcal{W}_2 \to \mathcal{X}^n$, which maps each message tuple $(W_1, W_2) \in \mathcal{W}_1 \times \mathcal{W}_2$ to a codeword $x \in \mathcal{X}^n$;

A set of relay functions: $\{f_i\}_{i=1}^n$ such that

$$x_{r,i} = f_i(y_{r,1}, y_{r,2}, ..., y_{r,i-1}), \quad 1 \le i \le n;$$

Two decoders: one at user 1, $\mathcal{Y}_1^n \to \mathcal{W}_1$, which maps a received sequence y_1^n to a message $\hat{W}_1$; the other at user 2, $\mathcal{Y}_2^n \to \mathcal{W}_2$, which maps y_2^n to a message $\hat{W}_2$.

The probability of error is defined as

$$P_e^{(n)} = \max\{P_{e1}^{(n)}, P_{e2}^{(n)}\}$$

where $P_{e1}^{(n)} = \Pr(\hat{W}_1 \ne W_1)$, $P_{e2}^{(n)} = \Pr(\hat{W}_2 \ne W_2)$.

The secrecy of the messages W_1 and W_2 are measured at the relay by three equivocation rates $\frac{1}{n} H(W_1 \mid Y_r^n, X_r^n)$, $\frac{1}{n} H(W_2 \mid Y_r^n, X_r^n)$ and $\frac{1}{n} H(W_1, W_2 \mid Y_r^n, X_r^n)$.

A rate tuple $(R_1, R_2, R_{e1}, R_{e2}, R_{e12})$ is said to be achievable if there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code with $\lim_{n\to\infty} P_e^{(n)} = 0$ and

$$\lim_{n\to\infty} \tfrac{1}{n} H(W_1 \mid Y_r^n, X_r^n) \ge R_{e1}$$

$$\lim_{n\to\infty} \tfrac{1}{n} H(W_2 \mid Y_r^n, X_r^n) \ge R_{e2}$$

$$\lim_{n\to\infty} \tfrac{1}{n} H(W_1, W_2 \mid Y_r^n, X_r^n) \ge R_{e12}$$

If the relay uses the decode-and-forward scheme to assist users, there is no secrecy of the messages W_1 and W_2 since the relay knows these messages, i.e. $R_{e1} = R_{e2} = R_{e12} = 0$. For the purpose of secrecy, we design the cooperative protocols with compress-and-forward relaying to help users.

III. An Achievable Rate Region Based on Marton's Coding Scheme

First, we provide a general achievable scheme which combines Marton's coding scheme for broadcast channels [5], the random binning scheme for wiretap channels [6], and the compress-and-forward scheme for relay channels.

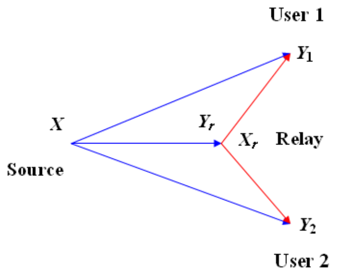

Fig 1. Broadcast Channel with an Untrusted Relay

Theorem 1: An achievable rate-equivocation region $\mathscr{R}_1$ for the broadcast channel with an untrusted relay is given by

$$\bigcup_{p(u_1,u_2)p(x|u_1,u_2)p(v_1,v_2)p(x_r|v_1,v_2)p(y_1,y_2,y_r|x,x_r)p(\hat{y}_1|y_r,v_1,v_2)p(\hat{y}_2|y_r,v_1,v_2)} \left\{ \begin{array}{l} (R_1,R_2,R_{e1},R_{e2},R_{e12}): \\ R_1 \le I(U_1;\hat{Y}_1,Y_1 \mid V_1) \\ R_2 \le I(U_2;\hat{Y}_2,Y_2 \mid V_2) \\ R_1+R_2 \le I(U_1;\hat{Y}_1,Y_1 \mid V_1)+I(U_2;\hat{Y}_2,Y_2 \mid V_2)-I(U_1;U_2) \\ R_{e1} \le R_1 \\ R_{e1} \le [I(U_1;\hat{Y}_1,Y_1 \mid V_1)-I(U_1;Y_r \mid U_2,X_r)-I(U_1;U_2)]^+ \\ R_{e2} \le R_2 \\ R_{e2} \le [I(U_2;\hat{Y}_2,Y_2 \mid V_2)-I(U_2;Y_r \mid U_1,X_r)-I(U_1;U_2)]^+ \\ R_{e12} \le R_1+R_2 \\ R_{e12} \le [I(U_1;\hat{Y}_1,Y_1 \mid V_1)+I(U_2;\hat{Y}_2,Y_2 \mid V_2) \\ \qquad -I(U_1,U_2;Y_r \mid X_r)-I(U_1;U_2)]^+ \\ \text{subject to:} \\ I(\hat{Y}_1;Y_r \mid V_1) \le I(V_1,\hat{Y}_1;Y_1) \\ I(\hat{Y}_2;Y_r \mid V_2) \le I(V_2,\hat{Y}_2;Y_2) \\ I(\hat{Y}_1;Y_r \mid V_1)+I(\hat{Y}_2;Y_r \mid V_2) \le \\ \qquad I(V_1,\hat{Y}_1;Y_1)+I(V_2,\hat{Y}_2;Y_2)-I(V_1;V_2) \end{array} \right\}$$

where U_1,U_2,V_1,V_2 are auxiliary random variables.

Proof: We consider a transmission over *B* blocks, each with length *n*.

Random Codebook Generation:

1. Generate $2^{nR(U_1)}$ independent identically distributed (i.i.d.) $\underline{u}_1$ each with distribution $\prod_{i=1}^{n} p(u_{1,i})$. Index them as $\underline{u}_1(w_1,\tilde{w}_1,w_1')$, $w_1 \in [1,2^{nR_1}]$, $\tilde{w}_1 \in [1,2^{n\tilde{R}_1}]$, $w_1' \in [1,2^{nR_1'}]$. R_1, $\tilde{R}_1$, R_1' and $R(U_1)$ are related through

$$R(U_1)=R_1+\tilde{R}_1+R_1'. \tag{1}$$

2. Generate $2^{nR(U_2)}$ i.i.d. $\underline{u}_2$ each with distribution $\prod_{i=1}^{n} p(u_{2,i})$. Index them as $\underline{u}_2(w_2,\tilde{w}_2,w_2')$, $w_2 \in [1,2^{nR_2}]$, $\tilde{w}_2 \in [1,2^{n\tilde{R}_2}]$, $w_2' \in [1,2^{nR_2'}]$. R_2, $\tilde{R}_2$, R_2' and $R(U_2)$ are related through

$$R(U_2)=R_2+\tilde{R}_2+R_2'. \tag{2}$$

3. For each (w_1,w_2), randomly picks $(\tilde{w}_1,\tilde{w}_2)$. For given pairs $(w_1,\tilde{w}_1)$ and $(w_2,\tilde{w}_2)$, we can find an appropriate pair (w_1',w_2') with high probability so that the pair $(\underline{u}_1(w_1,\tilde{w}_1,w_1'),\underline{u}_2(w_2,\tilde{w}_2,w_2'))$ is jointly typical, as long as

$$R_1'+R_2' > I(U_1,U_2). \tag{3}$$

Then, given this pair of $(\underline{u}_1,\underline{u}_2)$, the transmitter generates its channel inputs $\underline{x}$ through

$$\prod_{i=1}^{n} p(x_i \mid u_{1,i}(w_1,\tilde{w}_1,w_1'),u_{2,\mathrm{i}}(w_2,\tilde{w}_2,w_2')).$$

4. The relay generates $2^{nR(V_1)}$ i.i.d. $\underline{v}_1$ each with distribution $\prod_{i=1}^{n} p(v_{1,i})$. Index them as $\underline{v}_1(s_1,s_1')$, $s_1' \in [1,2^{nR_{r1}'}]$, $s_1 \in [1,2^{nR_{r1}}]$. R_{r1}, R_{r1}' and $R(V_1)$ are related through

$$R(V_1)=R_{r1}+R_{r1}'. \tag{4}$$

5. The relay generates $2^{nR(V_2)}$ i.i.d. $\underline{v}_2$ each with distribution $\prod_{i=1}^{n} p(v_{2,i})$. Index them as $\underline{v}_2(s_2,s_2')$, $s_2 \in [1,2^{nR_{r2}}]$, $s_2' \in [1,2^{nR_{r2}'}]$. R_{r2}, R_{r2}' and $R(V_2)$ are related through

$$R(V_2)=R_{r2}+R_{r2}'. \tag{5}$$

6. For each (s_1,s_2), the relay can find an appropriate pair (s_1',s_2') with high probability so that $(\underline{v}_1(s_1,s_1'),\ \underline{v}_2(s_2,s_2'))$ that is jointly typical as long as

$$R_{r1}'+R_{r2}' > I(V_1,V_2). \tag{6}$$

Then, given this pair of $(\underline{v}_1,\underline{v}_2)$, the relay generates its relay inputs $\underline{x}_r$ through

$$\prod_{i=1}^{n} p(x_{r,i} \mid v_{1,i}(s_{1,i},s_{1,i}'),v_{2,\mathrm{i}}(s_{2,i},s_{2,i}')).$$

7. For each $\underline{v}_1(s_1,s_1')$, generates $2^{n\hat{R}_{r1}}$ i.i.d. $\underline{\hat{y}}_1$ each with distribution $\prod_{i=1}^{n} p(\hat{y}_{1,i} \mid v_{1,i}(s_1,s_1'))$. Index them as $\underline{\hat{y}}_1(t_1 \mid s_1,s_1')$, $t_1 \in [1,2^{n\hat{R}_{r1}}]$. Partition $2^{n\hat{R}_{r1}}$ into cells A_{s_1} where $s_1 \in [1,2^{nR_{r1}}]$.

8. For each $\underline{v}_2(s_2,s_2')$, generate $2^{n\hat{R}_{r2}}$ i.i.d. $\underline{\hat{y}}_2$ each with distribution $\prod_{i=1}^{n} p(\hat{y}_{2,i} \mid v_{2,i}(s_2,s_2'))$. Index them as $\underline{\hat{y}}_2(t_2 \mid s_2,s_2')$, $t_2 \in [1,2^{n\hat{R}_{r1}}]$. Partition $2^{n\hat{R}_{r2}}$ into cells B_{s_2} where $s_2 \in [1,2^{nR_{r2}}]$.

Encoding: At the source, let $(w_{1,i},w_{2,i})$ be the new message pair to be sent in block *i*. It first finds a pair $(\underline{u}_1(w_1,\tilde{w}_1,w_1'),\underline{u}_2(w_2,\tilde{w}_2,w_2'))$ that is jointly typical. (3) guarantees that such a pair exists with high probability. The source then sends the codeword $\underline{x}$ corresponding to the tuple $(w_{1,i},\tilde{w}_{1,i},w_{1,i}',w_{2,i},\tilde{w}_{2,i},w_{2,i}')$.

At the beginning of block *i*, the relay should have estimations $\hat{s}_{1,i-1}$, $\hat{s}_{1,i-1}'$, $\hat{s}_{2,i-1}$ and $\hat{s}_{2,i-1}'$. It then sends the codeword $\underline{x}_r$ corresponding to the tuple $(\hat{s}_{1,i-1},\hat{s}_{1,i-1}',\hat{s}_{2,i-1},\hat{s}_{2,i-1}')$ if the estimation $\hat{t}_{1,i-1}$ of the index $t_{1,i-1}$ of the compressed signal $\underline{\hat{y}}_1(i-1)$ falls into $A_{\hat{s}_{1,i-1}}$ and the estimation $\hat{t}_{2,i-1}$ of the index $t_{2,i-1}$ of the compressed signal $\underline{\hat{y}}_2(i-1)$ falls into $B_{\hat{s}_{2,i-1}}$.

Decoding: The decoding procedures at the end of block *i* are as follows:

1. The relay determines that the estimate signal $\underline{\hat{y}}_1$ for $\underline{y}_r(i)$ is indexed by $\hat{t}_{1,i}$ if there is a unique $\hat{t}_{1,i}$ such that

$$\left(\underline{v}_1(s_{1,i-1},s_{1,i-1}'),\underline{\hat{y}}_1(\hat{t}_{1,i} \mid s_{1,i-1},s_{1,i-1}'),\underline{y}_r(i)\right) \in \mathbf{A}_\varepsilon^n$$

There exists such an $\hat{t}_{1,i}$ with high probability for sufficiently large *n* if

$$\hat{R}_1 \ge I(\hat{Y}_1;Y_r \mid V_1) \tag{7}$$

2. The relay determines that the estimate signal $\underline{\hat{y}}_2$ for $\underline{y}_r(i)$ is indexed by $\hat{t}_{2,i}$ if there is a unique $\hat{t}_{2,i}$ such that

$$\left(\underline{v}_2(s_{2,i-1},s_{2,i-1}'),\underline{\hat{y}}_2(\hat{t}_{2,i} \mid s_{2,i-1},s_{2,i-1}'),\underline{y}_r(i)\right) \in \mathbf{A}_\varepsilon^n$$

There exists such an $\hat{t}_{2,i}$ with high probability for sufficiently large *n* if

$$\hat{R}_2 \ge I(\hat{Y}_2;Y_r \mid V_2) \tag{8}$$

3. User 1 seeks a unique jointly typical pair of $(\underline{v}_1(s_{1,i-1},s_{1,i-1}'),\underline{y}_1(i))$, which can be found with vanishingly small error probability if

$$R(V_1)=R_{r1}+R_{r1}' \le I(V_1;Y_1) \tag{9}$$

4. User 1 uses list decoding to decode $\underline{\hat{y}}_1(t_{1,i-1} \mid s_{1,i-1},s_{1,i-1}')$. It first calculates its ambiguity set as

$$\mathscr{L}_1(\underline{\hat{y}}_1(t_{1,i} \mid s_{1,i-1}, s'_{1,i-1})) = \{\underline{\hat{y}}_1(t_{1,i} \mid s_{1,i-1}, s'_{1,i-1}) : \\ \big(\underline{v}_1(s_{1,i-1}, s'_{1,i-1}), \underline{\hat{y}}_1(t_{1,i} \mid s_{1,i-1}, s'_{1,i-1}), \underline{y}_1(i)\big) \in \mathbf{A}_\varepsilon^n\}$$

and takes its intersection with A_{s_1} which results in a unique and correct intersection point of

$$\begin{aligned} \hat{R}_1 &\le I(\hat{Y}_1; Y_1 \mid V_1) + R_{r1} \\ &\le I(\hat{Y}_1; Y_1 \mid V_1) + I(V_1; Y_1) - R'_{r1} \\ &\le I(V_1, \hat{Y}_1; Y_1) - R'_{r1} \end{aligned} \tag{10}$$

5. User 1 determines that $\underline{u}_1(w_{1,i}, \tilde{w}_{1,i}, w'_{1,i})$ is received if there exists a unique jointly typical tuple $\big(\underline{u}_1(w_{1,i}, \tilde{w}_{1,i}, w'_{1,i}), \underline{v}_1(s_{1,i-1}, s'_{1,i-1}), \underline{\hat{y}}_1(t_{1,i} \mid s_{1,i-1}, s'_{1,i-1}), \underline{y}_1(i)\big)$, which can be found with vanishingly small error probability if

$$R(U_1) = R_1 + \tilde{R}_1 + R'_1 \le I(U_1; \hat{Y}_1, Y_1 \mid V_1) \tag{11}$$

6. User 2 seeks a unique jointly typical pair of $(\underline{v}_2(s_{2,i-1}, s'_{2,i-1}), \underline{y}_2(i))$, which can be found with vanishingly small error probability if

$$R(V_2) = R_{r2} + R'_{r2} \le I(V_2; Y_2) \tag{12}$$

7. User 2 uses list decoding to decode $\underline{\hat{y}}_2(t_{2,i-1} \mid s_{2,i-1}, s'_{2,i-1})$. It first calculates its ambiguity set as

$$\mathscr{L}_2(\underline{\hat{y}}_2(t_{2,i-1} \mid s_{2,i-1}, s'_{2,i-1})) = \{\underline{\hat{y}}_2(t_{2,i-1} \mid s_{2,i-1}, s'_{2,i-1}) : \\ \big(\underline{v}_2(s_{2,i-1}, s'_{2,i-1}), \underline{\hat{y}}_2(t_{2,i-1} \mid s_{2,i-1}, s'_{2,i-1}), \underline{y}_2(i-1)\big) \in \mathbf{A}_\varepsilon^n\}$$

and takes its intersection with B_{s_2} which results in a unique and correct intersection point of

$$\hat{R}_2 \le I(\hat{Y}_2; Y_2 \mid V_2) + R_{r2} \le I(V_2, \hat{Y}_2; Y_2) - R'_{r2} \tag{13}$$

8. User 2 determines that $\underline{u}_2(w_{2,i-1}, \tilde{w}_{2,i-1}, w'_{2,i-1})$ is received if there is a unique jointly typical tuple $\big(\underline{u}_2(w_{2,i-1}, \tilde{w}_{2,i-1}, w'_{2,i-1}), \underline{v}_2(s_{2,i-1}, s'_{2,i-1}), \underline{\hat{y}}_2(t_{2,i-1} \mid s_{2,i-1}, s'_{2,i-1}), \underline{y}_2(i-1)\big)$, which can be found with vanishingly small error probability if

$$R(U_2) = R_2 + \tilde{R}_2 + R'_2 \le I(U_2; \hat{Y}_2, Y_2 \mid V_2) \tag{14}$$

Equivocation computation: We now show that R_{e1}, R_{e2} and R_{e12} satisfying the bounds in Theorem 1 are achievable with the coding scheme presented.

We consider the equivocation

$$\begin{aligned} &H(W_1 \mid Y_r^n, X_r^n) \\ &\ge H(W_1 \mid Y_r^n, X_r^n, U_2^n) \\ &= H(W_1, Y_r^n \mid X_r^n, U_2^n) - H(Y_r^n \mid X_r^n, U_2^n) \\ &= H(W_1, Y_r^n, U_1^n \mid X_r^n, U_2^n) - H(U_1^n \mid W_1, Y_r^n, X_r^n, U_2^n) \\ &\quad - H(Y_r^n \mid X_r^n, U_2^n) \\ &= H(U_1^n \mid X_r^n, U_2^n) + H(W_1, Y_r^n \mid X_r^n, U_1^n, U_2^n) \\ &\quad - H(U_1^n \mid W_1, Y_r^n, X_r^n, U_2^n) - H(Y_r^n \mid X_r^n, U_2^n) \\ &= H(U_1^n) + H(W_1, Y_r^n \mid X_r^n, U_1^n, U_2^n) - H(U_1^n \mid W_1, Y_r^n, X_r^n, U_2^n) \\ &\quad - H(Y_r^n \mid X_r^n, U_2^n) \\ &\ge H(U_1^n) + H(Y_r^n \mid X_r^n, U_1^n, U_2^n) - H(Y_r^n \mid X_r^n, U_2^n) \\ &\quad - H(U_1^n \mid W_1, Y_r^n, X_r^n, U_2^n) \\ &= H(U_1^n) - I(U_1^n; Y_r^n \mid X_r^n, U_2^n) - H(U_1^n \mid W_1, Y_r^n, X_r^n, U_2^n) \end{aligned} \tag{15}$$

We treat two cases separately, like in proving Theorem 4 of [2].

If $R_1 \ge I(U_1; \hat{Y}_1, Y_1 \mid V_1) - I(U_1; Y_r \mid U_2, V_1, V_2) - I(U_1; U_2)$, we select $R(U_1) = I(U_1; \hat{Y}_1, Y_1 \mid V_1)$.

With this selection, we have

$$\tilde{R}_1 + R'_1 \le I(U_1; Y_r \mid U_2, V_1, V_2) + I(U_1; U_2) \tag{16}$$

The first term in (15) is

$$H(U_1^n) = nR(U_1) = nI(U_1; \hat{Y}_1, Y_1 \mid V_1) \tag{17}$$

The second term can be bounded as

$$I(U_1^n; Y_r^n \mid X_r^n, U_2^n) \le nI(U_1; Y_r \mid U_2, X_r) + n\varepsilon_n \tag{18}$$

using the method devised in Lemma 3 of [7].

As for the third term, we consider the following case. Given $W_1 = w_1$, the relay can decode U_1^n with small error probability since U_1^n can only take $2^{n(\tilde{R}_1 + R'_1)}$ values while $\tilde{R}_1 + R'_1$ has the upper bound (16). From Fano's inequality, we know

$$H(U_1^n \mid W_1, Y_r^n, X_r^n, U_2^n) \le n\varepsilon'_n \tag{19}$$

Combining (17)-(19), we conclude

$$\begin{aligned} R_{e1} &\le I(U_1; \hat{Y}_1, Y_1 \mid V_1) - I(U_1; Y_r, U_2 \mid X_r) \\ &= I(U_1; \hat{Y}_1, Y_1 \mid V_1) - I(U_1; Y_r \mid U_2, X_r) - I(U_1; U_2) \end{aligned}$$

is achievable.

If $R_1 \le I(U_1; \hat{Y}_1, Y_1 \mid V_1) - I(U_1; Y_r \mid U_2, V_1, V_2) - I(U_1; U_2)$, we select $R(U_1) = R_1 + I(U_1; Y_r \mid U_2, V_1, V_2) + I(U_1; U_2)$, which is equivalent to

$$\tilde{R}_1 + R'_1 = I(U_1; Y_r \mid U_2, V_1, V_2) + I(U_1; U_2).$$

The first term in (15) is now

$$H(U_1^n) = nR(U_1) = n(R_1 + I(U_1; Y_r \mid U_2, V_1, V_2) + I(U_1; U_2)) \tag{20}$$

An upper bound on the second term has been already obtained in (18).

As for the third term, we also have (19) from Fano's inequality. Given $W_1 = w_1$, the relay can decode U_1^n with small error probability since U_1^n can take only $2^{n(\tilde{R}_1 + R'_1)} = 2^{n[I(U_1; Y_r | U_2, V_1, V_2) + I(U_1; U_2)]}$ values.

Combining (18)-(20), we conclude that $R_{e1} \le R_1$ is achievable. Therefore,

$$R_{e1} \le \min\{R_1; I(U_1; \hat{Y}_1, Y_1 \mid V_1) - I(U_1; Y_r \mid U_2, X_r) - I(U_1; U_2)\}$$

is always achievable for any case.

Similarly, we can prove the achievable range of R_{e2} and R_{e12}.

Thus, we complete the proof. □

IV. Achievable Rate Region Based on Cover's Superposition Coding Scheme

The achievable rate region based on Marton's coding scheme provides a general result for the broadcast channels with an untrusted relay, without knowing the information regarding two users. If we know which user is better (i.e. receiving more information), we can design a simpler scheme. Here we provide another secrecy rate region based on the scheme which combines Cover's superposition coding scheme [8] for broadcast channels, the random binning scheme for wiretap channels, and compress-and-forward scheme for relay channels. We suppose user 2 is the better user.

Theorem 2: An achievable rate-equivocation region $\mathscr{R}_2$ for the broadcast channel with an untrusted relay is given by

$$\bigcup_{p(u)p(x|u)p(v)p(x_r|v)p(y_1, y_2, y_r|x, x_r)p(\hat{y}_1|y_r, v)p(\hat{y}_2|y_r, v, \hat{y}_1, x_r)}$$

$$\left\{\begin{array}{l}(R_1, R_2, R_{e1}, R_{e2}, R_{e12}): \\ R_1 \le \min\{I(U;\hat{Y}_1, Y_1 \mid V), I(U;\hat{Y}_2, Y_2 \mid V, X_r, \hat{Y}_1)\} \\ R_2 \le I(X;\hat{Y}_2, Y_2 \mid U, V, X_r, \hat{Y}_1) \\ R_{e1} \le R_1 \\ R_{e1} \le \min\{I(U;\hat{Y}_1, Y_1 \mid V), I(U;\hat{Y}_2, Y_2 \mid V, X_r, \hat{Y}_1)\} \\ \qquad - I(U;Y_r \mid V, X_r) \\ R_{e2} \le R_2, \\ R_{e2} \le I(X;\hat{Y}_2, Y_2 \mid U, V, X_r, \hat{Y}_1) - I(X;Y_r \mid U, V, X_r) \\ R_{e12} \le R_1 + R_2 \\ R_{e12} \le \min\{I(U;\hat{Y}_1, Y_1 \mid V), I(U;\hat{Y}_2, Y_2 \mid V, X_r, \hat{Y}_1)\} \\ \qquad + I(X;\hat{Y}_2, Y_2 \mid U, V, X_r, \hat{Y}_1) - I(U, X;Y_r \mid V, X_r) \\ \text{subject to:} \\ I(\hat{Y}_1;Y_r \mid V, X_r, Y_1) \le I(V;Y_1) \\ I(\hat{Y}_1;Y_r \mid V, X_r, Y_2) \le I(V;Y_2) \\ I(\hat{Y}_2;Y_r \mid V, X_r, \hat{Y}_1, Y_2) \le I(X_r;Y_2 \mid V) \end{array}\right\}$$

where U and V are two auxiliary random variables.

Proof: The detailed proof is omitted due to space limit. The encoding and decoding procedures are as follows:

At the source, let $(w_{1,i}, w_{2,i})$ be the new message pair to be sent in block *i*. The source then sends the codeword $\underline{x}(w_{1,i}, \tilde{w}_{1,i}, w_{2,i}, \tilde{w}_{2,i})$ which also includes the message pair in the last block.

At the beginning of block *i*, the relay should have an estimation $\hat{s}_{i-1}$ of the index s_{i-1} of the compressed signal $\underline{\hat{y}_1}$ for $\underline{y_r}(i-1)$, and an estimation $\hat{t}_{i-1}$ of $\underline{\hat{y}_2}$ that including additional information about $\underline{y_r}(i-1)$. It then sends the codeword $\underline{x_r}(\hat{s}_{i-1}, \hat{t}_{i-1})$ to two users.

At the end of block *i*, the relay, having known s_{i-1} and t_{i-1}, determines that the estimate signal $\underline{\hat{y}_1}$ for $\underline{y_r}(i)$ is indexed by $\hat{s}_i$. Then, having known s_{i-1}, s_i and t_{i-1}, it determines that the estimate signal $\underline{\hat{y}_2}$ is indexed by $\hat{t}_i$.

At the end of block *i*, user 1, having known s_{i-2}, determines that $\underline{\hat{y}_1}$ indexed by $\hat{s}_{i-1}$ is picked to compress $\underline{y_r}(i-1)$ by the relay based on the information received in blocks $i-1$ and *i*. Then, having known both s_{i-1} and s_{i-2}, it determines the message pair $(\hat{w}_{1,i-1}, \hat{\tilde{w}}_{1,i-1})$ based on the information received in block $i-1$.

At the end of block *i*, user 2, having known s_{i-2}, determines that $\underline{\hat{y}_1}$ indexed by $\hat{s}_{i-1}$ is picked to compress $\underline{y_r}(i-1)$ by the relay based on the information received in blocks $i-1$ and *i*. then, having known s_{i-1}, s_{i-2} and t_{i-2}, it determines that $\underline{\hat{y}_2}$ indexed by $\hat{t}_{i-1}$ is picked to compress $\underline{y_r}(i-1)$ by the relay based on the information received in blocks $i-1$ and *i*. Next, having known s_{i-1}, s_{i-2}, t_{i-1} and t_{i-2}, it determines the message pair $(\hat{w}_{1,i-1}, \hat{\tilde{w}}_{1,i-1})$ based on the information received in block $i-1$. Finally, having known $w_{1,i-1}$, s_{i-1}, s_{i-2}, t_{i-1} and t_{i-2}, it determines the message pair $(\hat{w}_{2,i-1}, \hat{\tilde{w}}_{2,i-1})$ based on the information received in block $i-1$.

Using this scheme, we can obtain the achievable rate-equivocation region in theorem 2.

V. An Outer Bound

We also provide an outer bound for the rate-equivocation region.

Theorem 3: The rate-equivocation region of the broadcast channels with an untrusted relay lies in the union of the following rate tuples

$$\begin{array}{l} R_1 \le \min\{I(U_1;Y_1), I(U_1';Y_1, Y_r \mid X_r)\} \\ R_2 \le \min\{I(U_2;Y_2), I(U_2';Y_2, Y_r \mid X_r)\} \\ R_{e1} \le R_1 \\ R_{e1} \le I(U_1;Y_1 \mid V_1) - I(U_1;Y_r \mid V_1) \\ R_{e2} \le R_2 \\ R_{e2} \le I(U_2;Y_2 \mid V_2) - I(U_2;Y_r \mid V_2) \\ R_{e12} \le R_1 + R_2 \\ R_{e12} \le I(U_1;Y_1 \mid V_1) + I(U_2;Y_2 \mid V_2) \\ \qquad - I(U_1;Y_r \mid V_1) - I(U_2;Y_r \mid V_2) \end{array}$$

where the union is taken over all joint distributions satisfying the Markov chains

$$V_1 \to U_1 \to X$$
$$V_2 \to U_2 \to X$$
$$(V_1, V_2) \to (U_1, U_2) \to (X, X_r, Y_r) \to (Y_1, Y_2)$$
$$X_r \to (V_1', V_2') \to X$$
$$(V_1', V_2') \to (X, X_r) \to (Y_1, Y_2, Y_r).$$

Proof: First, define the following auxiliary random variables

$$\begin{array}{l} V_{1,j} = Y_1^{j-1} Y_{r,j+1}^n \\ V_{2,j} = Y_2^{j-1} Y_{r,j+1}^n \\ U_{1,j} = W_1 V_{1,j} = W_1 Y_1^{j-1} Y_{r,j+1}^n \\ U_{2,j} = W_2 V_{2,j} = W_2 Y_2^{j-1} Y_{r,j+1}^n \\ U_{1,j}' = W_1 Y_1^{j-1} Y_r^{j-1} \\ U_{2,j}' = W_2 Y_2^{j-1} Y_r^{j-1}. \end{array}$$

Consider a sequence of codes for the channel with $P_e^{(n)} \to 0$.

By Fano's inequality, we have

$$H(W_1 \mid Y_1^n) \le 1 + nR_1 P_e^{(n)}$$

Let $n\delta_n \triangleq 1 + nR_1 P_e^{(n)}$. Clearly, $\delta_n \to 0$ if $P_e^{(n)} \to 0$.

Further, we have

$$H(W_1 \mid Y_1^n, Y_r^n) \le H(W_1 \mid Y_1^n) = n\delta_n$$

We can bound the rate R_1 as

$$\begin{array}{l} nR_1 = H(W_1) \\ = I(W_1;Y_1^n) + H(W_1 \mid Y_1^n) \\ \le I(W_1;Y_1^n) + n\delta_n \\ = \sum_{j=1}^{n} I(W_1;Y_{1,j} \mid Y_1^{j-1}) + n\delta_n \\ = \sum_{j=1}^{n} [H(Y_{1,j} \mid Y_1^{j-1}) - H(Y_{1,j} \mid Y_1^{j-1}, W_1)] + n\delta_n \\ \le \sum_{j=1}^{n} [H(Y_{1,j}) - H(Y_{1,j} \mid Y_1^{j-1}, Y_{r,j+1}^n, W_1)] + n\delta_n \\ = \sum_{j=1}^{n} [H(Y_{1,j}) - H(Y_{1,j} \mid U_{1,j})] + n\delta_n \\ = \sum_{j=1}^{n} I(U_{1,j};Y_{1,j}) + n\delta_n \end{array}$$

We also have

$$\begin{array}{l} nR_1 = H(W_1) \\ = I(W_1;Y_1^n, Y_r^n) + H(W_1 \mid Y_1^n, Y_r^n) \\ \le I(W_1;Y_1^n, Y_r^n) + n\delta_n \\ = \sum_{j=1}^{n} I(W_1;Y_{1,j}, Y_{r,j} \mid Y_1^{j-1}, Y_r^{j-1}) + n\delta_n \end{array}$$

$$
\begin{aligned}
&= \sum_{j=1}^{n} [H(W_1 \mid Y_1^{j-1}, Y_r^{j-1}) - H(W_1 \mid Y_1^{j}, Y_r^{j})] + n\delta_n \\
&= \sum_{j=1}^{n} [H(W_1 \mid Y_1^{j-1}, Y_r^{j-1}, X_r) - H(W_1 \mid Y_1^{j}, Y_r^{j})] + n\delta_n \\
&\le \sum_{j=1}^{n} [H(W_1 \mid Y_1^{j-1}, Y_r^{j-1}, X_r) - H(W_1 \mid Y_1^{j}, Y_r^{j}, X_r)] + n\delta_n \\
&= \sum_{j=1}^{n} I(W_1; Y_{1,j}, Y_{r,j} \mid Y_1^{j-1}, Y_r^{j-1}, X_r) + n\delta_n \\
&= \sum_{j=1}^{n} [H(Y_{1,j}, Y_{r,j} \mid Y_1^{j-1}, Y_r^{j-1}, X_r) - H(Y_{1,j}, Y_{r,j} \mid W_1, Y_1^{j-1}, Y_r^{j-1}, X_r)] \\
&+ n\delta_n \\
&\le \sum_{j=1}^{n} [H(Y_{1,j}, Y_{r,j} \mid X_r) - H(Y_{1,j}, Y_{r,j} \mid W_1, Y_1^{j-1}, Y_r^{j-1}, X_r)] + n\delta_n \\
&= \sum_{j=1}^{n} [H(Y_{1,j}, Y_{r,j} \mid X_r) - H(Y_{1,j}, Y_{r,j} \mid U'_{1,j}, X_r)] + n\delta_n \\
&= \sum_{j=1}^{n} I(U'_{1,j}; Y_{1,j}, Y_{r,j} \mid X_r) + n\delta_n
\end{aligned}
$$

We can change the bounds into single-letter characterization, thus obtaining

$$R_1 \le \min\{I(U_1;Y_1), I(U'_1;Y_1,Y_r \mid X_r)\}$$

Similarly, we can obtain the upper bounds on R_2.

For the upper bounds on the equivocation rates, it is obvious that $R_{e1} \le R_1$, $R_{e2} \le R_2$ and $R_{e12} \le R_1 + R_2$ due to the definitions.

We also have

$$
\begin{aligned}
& nR_{e1} \le H(W_1 \mid Y_r^n) \\
&= H(W_1) - I(W_1; Y_r^n) \\
&= I(W_1; Y_1^n) + H(W_1 \mid Y_1^n) - I(W_1; Y_r^n) \\
&\le I(W_1; Y_1^n) - I(W_1; Y_r^n) + n\delta_n \\
&= \sum_{j=1}^{n} [I(W_1; Y_{1,j} \mid Y_1^{j-1}) - I(W_1; Y_{r,j} \mid Y_{r,j+1}^{n})] + n\delta_n \\
&= \sum_{j=1}^{n} [I(W_1, Y_{r,j+1}^{n}; Y_{1,j} \mid Y_1^{j-1}) - I(Y_{r,j+1}^{n}; Y_{1,j} \mid Y_1^{j-1}, W_1) \\
&\quad - I(W_1, Y_1^{j-1}; Y_{r,j} \mid Y_{r,j+1}^{n}) + I(Y_1^{j-1}; Y_{r,j} \mid Y_{r,j+1}^{n}, W_1)] + n\delta_n \\
&= \sum_{j=1}^{n} [I(W_1, Y_{r,j+1}^{n}; Y_{1,j} \mid Y_1^{j-1}) - I(W_1, Y_1^{j-1}; Y_{r,j} \mid Y_{r,j+1}^{n})] \\
&\quad + n\delta_n \qquad (21) \\
&= \sum_{j=1}^{n} [I(W_1; Y_{1,j} \mid Y_1^{j-1}, Y_{r,j+1}^{n}) + I(Y_{r,j+1}^{n}; Y_{1,j} \mid Y_1^{j-1}) \\
&\quad - I(W_1; Y_{r,j} \mid Y_{r,j+1}^{n}, Y_1^{j-1}) - I(Y_1^{j-1}; Y_{r,j} \mid Y_{r,j+1}^{n})] + n\delta_n \\
&= \sum_{j=1}^{n} [I(W_1; Y_{1,j} \mid Y_1^{j-1}, Y_{r,j+1}^{n}) - I(W_1; Y_{r,j} \mid Y_{r,j+1}^{n}, Y_1^{j-1})] \\
&\quad + n\delta_n \qquad (22) \\
&= \sum_{j=1}^{n} [I(W_1; Y_{1,j} \mid V_{1,j}) - I(W_1; Y_{r,j} \mid V_{1,j})] + n\delta_n \\
&= \sum_{j=1}^{n} [I(W_1, V_{1,j}; Y_{1,j} \mid V_{1,j}) - I(W_1, V_{1,j}; Y_{r,j} \mid V_{1,j})] + n\delta_n \\
&= \sum_{j=1}^{n} [I(U_{1,j}; Y_{1,j} \mid V_{1,j}) - I(U_{1,j}; Y_{r,j} \mid V_{1,j})] + n\delta_n
\end{aligned}
$$

in which the derivations of (21) and (22) are due to Lemma 7 of [9].

Similarly, we have

$$
\begin{aligned}
& nR_{e2} \le H(W_2 \mid Y_r^n) = H(W_2) - I(W_2; Y_r^n) \\
&\le \sum_{j=1}^{n} [I(U_{2,j}; Y_{2,j} \mid V_{2,j}) - I(U_{2,j}; Y_{r,j} \mid V_{2,j})] + n\delta_n
\end{aligned}
$$

Next, we bound R_{e12} as

$$
\begin{aligned}
& nR_{e12} \le H(W_1, W_2 \mid Y_r^n) \\
&= H(W_1, W_2) - I(W_1, W_2; Y_r^n) \\
&\le H(W_1) + H(W_2) - [I(W_1; Y_r^n) + I(W_2; Y_r^n \mid W_1)] \\
&= H(W_1) + H(W_2) - I(W_1; Y_r^n) - [H(W_2 \mid W_1) - H(W_2 \mid W_1, Y_r^n)] \\
&\le H(W_1) - I(W_1; Y_r^n) + H(W_2) - [H(W_2) - H(W_2 \mid Y_r^n)] \\
&= H(W_1) - I(W_1; Y_r^n) + H(W_2) - I(W_2; Y_r^n) \\
&\le \sum_{j=1}^{n} [I(U_{1,j}; Y_{1,j} \mid V_{1,j}) - I(U_{1,j}; Y_{r,j} \mid V_{1,j}) \\
&\quad + I(U_{2,j}; Y_{2,j} \mid V_{2,j}) - I(U_{2,j}; Y_{r,j} \mid V_{2,j})] + n\delta_n
\end{aligned}
$$

Changing all bounds to single-letter characterization, we complete the proof, which uses some important techniques developed to prove the converse given in [9]. Note that the outer bound in [9] is tight for the wiretap channel, but here the bounds are generally not tight.

VI. Conclusions

In this paper, secrecy rate regions for the broadcast channels with an untrusted relay are studied. Secrecy can be achieved when using the compress-and-forward scheme. We obtain the achievable rate-equivocation regions by combining it with Marton's coding scheme and Cover's superposition coding scheme. The secrecy rate region based on Marton's coding scheme provides a general result, without knowing information regarding two users. When we know which user is better, we can design a simpler scheme with superposition encoding. However, in general, this scheme does not necessarily perform better. Outer bound to the rate-equivocation regions is also provided in the paper.

References

[1] X. He and A. Yener, "Cooperation with an untrusted relay: a secrecy perspective," *IEEE Trans. Inform. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.

[2] E. Ersen and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inform. Theory*, vol. 57, no. 1, pp. 137–155, Jan. 2011.

[3] Y. Liang and V. V. Veeravalli, "The impact of relaying on the capacity of broadcast channels," in *Proc. IEEE ISIT*, Chicago, IL, Jun./Jul. 2004, pp. 403.

[4] T. M. Cover and A. A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 5, pp. 572–584, Sep. 1979.

[5] K. Marton, "A coding theorem for the discrete memoryless channels," *IEEE Trans. Inform. Theory*, vol. IT-25, no. 1, 1979, pp. 306–311.

[6] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[7] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[8] T. M. Cover, "Broadcast Channels," *IEEE Trans. Inform. Theory*, vol. IT-18, no. 1, pp. 2–14, Jan 1972.

[9] I. Csiszár, and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.