

Secrecy in Cooperative Relay Broadcast Channels

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu ulukus@umd.edu

Abstract—We investigate the effects of user cooperation on the secrecy of broadcast channels by considering a cooperative relay broadcast channel. We show that user cooperation can increase the achievable secrecy region. We propose an achievable scheme that combines Marton’s coding scheme for broadcast channels and Cover and El Gamal’s compress-and-forward scheme for relay channels. We derive outer bounds for the rate-equivocation region using auxiliary random variables for single-letterization. Finally, we consider a Gaussian channel and show that both users can have positive secrecy rates, which is not possible for scalar Gaussian broadcast channels without cooperation.

I. INTRODUCTION

The open nature of wireless communications facilitates cooperation by allowing users to exploit the over-heard information to increase achievable rates. However, the same open nature of wireless communications makes it vulnerable to security attacks such as eavesdropping and jamming. In this paper, we investigate the interaction of these two phenomena, namely cooperation and secrecy. In particular, we investigate the effects of cooperation on secrecy.

The eavesdropping attack was first studied from an information theoretic point of view by Wyner in [1], where he established the secrecy capacity for a *single-user degraded* wire-tap channel. Later, Csiszar and Korner [2] studied the general, not necessarily degraded, *single-user* eavesdropping channel, and found the secrecy capacity. More recently *multi-user* versions of the secrecy problem have been considered for various channel models. References [3], [4], [5], [6] consider multiple access channels (MAC), where in [3], [4] the eavesdropper is an external entity, while in [5], [6] the users in the MAC act as eavesdroppers on each other. References [7], [8] consider broadcast channels (BC) where both receivers want to have secure communication with the transmitter; in here as well, each receiver of the BC is an eavesdropper for the other user. References [9], [10], [11], [12] consider secrecy in relay channels, where in [9], [10], the relay is the eavesdropper, while in [11], [12] there is an external eavesdropper.

In a wireless medium, since all users receive a version of all signals transmitted, they can cooperate to improve their communication rates. The simplest example of a cooperative system is the relay channel [13] where the relay helps increase the communication rate of a single-user channel using its over-heard information. Multi-user versions of cooperative

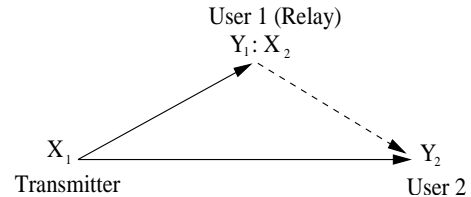


Fig. 1. The cooperative relay broadcast channel.

communication have been studied more recently. In [14], a MAC is considered where both users over-hear a noisy version of the signal transmitted by the other user, and transmit in such a way to increase their achievable rates. In [15], [16], [17], cooperation is done on the receiver side, where in a BC, one or both of the receivers transmit cooperative signals to improve the achievable rates of both users.

Our goal is to study the effects cooperation on the secrecy of *multiple users* where secrecy refers to individual confidentiality of each user. One of the simplest models to study this interaction is the cooperative relay broadcast channel (CRBC), where there is a single transmitter and two receivers, and each receiver would like to keep its message secret from the other user; see Fig. 1. In this model, in order to incorporate the effects of cooperation, there is a single-sided cooperation link from the first user to the second user. We note that if we remove the cooperation link, our model reduces to the BC with confidential messages in [7], [8], and if we set the rate of the first user to zero, our model reduces to the relay channel with confidential messages in [9], [10], and if we both set the rate of the first user to zero and remove the cooperation link between the users, our model reduces to the single-user eavesdropper channel in [1], [2]. Our model is the simplest model (except perhaps for the “dual” model of cooperating transmitters in a MAC with per-user secrecy constraints [18]) that allows us to study the effects of cooperation (or lack thereof) of the first user (the transmitting end of the cooperative link) on its own equivocation rate as well as on the equivocation rate of the other user (receiving end of the cooperative link).

Our motivation to study this problem can be best explained in a Gaussian example. Imagine a two-user Gaussian BC. This BC is degraded in one direction, hence both users cannot have positive secrecy rates simultaneously [1], [7], [8]. This has motivated [8] to use multiple antennas at the transmitter in order to remove this degradedness in either of

the directions and provide positive secrecy rates to both users simultaneously. We wish to achieve the same effect with a single transmitter antenna, by introducing cooperation from one user to the other. Imagine now a Gaussian CRBC [15], [16] as in Fig. 1, where user 1 acts as a relay for user 2's message, i.e., that there is a cooperative link from user 1 to user 2. Let us assume that in the underlying BC, user 1 has a better channel. Without the cooperative link, user 2 cannot have secure communication with the transmitter. We show that user 1 can transmit cooperative signals and improve the secrecy rate of user 2, while not compromising its own secret communication. Our main idea is that user 1 can use a compress-and-forward (CAF) based relaying scheme for the message of user 2, and increase user 2's rate to a level which is not decodable at user 1 [18]. This improves user 2's secrecy. Now, let us assume that in the underlying BC, user 1 has the worse channel. Without cooperation, user 1 cannot have secure communication with the transmitter. We show that user 1 can transmit a jamming signal in the cooperative channel first to guarantee a positive secrecy rate for itself assuming it has enough power. This essentially brings the system to the setting described in the previous case, and now user 1 can send a cooperative signal to user 2 to help it achieve a positive secrecy rate as well.

In this paper, we propose an achievable scheme that combines Marton's coding scheme for BCs [19] and Cover and El Gamal's CAF scheme for relay channels [13]. A similar achievable scheme has appeared in [20]; here we extend it to include the secrecy rates of the users. Then, we develop a single-letter outer bound on the rate-equivocation region; we accomplish single-letterization by using tools proposed in [2], namely by determining suitable auxiliary random variables. Besides this outer bound, for the second user, that is being helped, we develop another single-letter outer bound which depends only on the channel inputs and outputs.

Finally, we consider a Gaussian CRBC and show that both users can have positive secrecy rates through user cooperation. To obtain positive secrecy rates for both users, we provide different assignments for the auxiliary random variables appearing in the achievable rates. These auxiliary random variable assignments have dirty paper coding (DPC) interpretations [21]. In addition, we combine jamming and relaying to provide secrecy for both users when the relaying user is weak.

II. THE CHANNEL MODEL AND DEFINITIONS

The CRBC can be viewed as a relay channel where the transmitter sends messages both to the relay node and the destination. Therefore, one of the users, user 1 in our case, in a CRBC both decodes its own message and also helps the other user. A CRBC consists of two message sets $w_1 \in \mathcal{W}_1, w_2 \in \mathcal{W}_2$, two input alphabets, one at the transmitter $x_1 \in \mathcal{X}_1$ and one at user 1 $x_2 \in \mathcal{X}_2$, and two output alphabets $y_1 \in \mathcal{Y}_1, y_2 \in \mathcal{Y}_2$, where the former is for user 1 and the latter is for user 2. The channel is assumed to be memoryless and its transition probability distribution is $p(y_1, y_2 | x_1, x_2)$.

A $(2^{nR_1}, 2^{nR_2}, n)$ code for this channel consists of two message sets as $\mathcal{W}_1 = \{1, \dots, 2^{nR_1}\}$ and $\mathcal{W}_2 = \{1, \dots, 2^{nR_2}\}$, an encoder at the transmitter with mapping $\mathcal{W}_1 \times \mathcal{W}_2 \rightarrow \mathcal{X}_1^n$, a set of relay functions at user 1, $x_{2,i} = f_i(y_{1,1}, \dots, y_{1,i-1})$ for $1 \leq i \leq n$, two decoders, one at each user with the mappings $g_1 : \mathcal{Y}_1^n \rightarrow \mathcal{W}_1$ and $g_2 : \mathcal{Y}_2^n \rightarrow \mathcal{W}_2$. The probability of error is defined as $P_e^n = \max\{P_{e,1}^n, P_{e,2}^n\}$ where $P_{e,1}^n = \Pr(g_1(Y_1^n) \neq W_1)$, $P_{e,2}^n = \Pr(g_2(Y_2^n) \neq W_2)$. The secrecy of the users are measured by the normalized entropy of their messages conditioned on the other user's channel observation, $\frac{1}{n}H(W_1|Y_2^n)$ and $\frac{1}{n}H(W_2|Y_1^n)$ which hereafter will be called the equivocation rates.

A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $(2^{nR_1}, 2^{nR_2}, n)$ code with $\lim_{n \rightarrow \infty} P_e^n = 0$ and

$$\lim_{n \rightarrow \infty} \frac{1}{n}H(W_1|Y_2^n) \geq R_{e,1}, \quad \lim_{n \rightarrow \infty} \frac{1}{n}H(W_2|Y_1^n) \geq R_{e,2}$$

III. AN ACHIEVABLE SCHEME

We now provide an achievable scheme which combines Marton's coding scheme for BCs [19] and Cover and El Gamal's CAF scheme for relay channels [13]. The scheme presented here extends the one in [20] to include the equivocation rates. In this scheme, user 1 sends a quantized version of its observation to user 2, which uses this information to decode its own message. The corresponding achievable rate-equivocation region is given by the following theorem.

Theorem 1 *The rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying*

$$\begin{aligned} R_1 &\leq I(V_1; Y_1 | X_2) \\ R_2 &\leq I(V_2; Y_2, \hat{Y}_1 | X_2) \\ R_1 + R_2 &\leq I(V_1; Y_1 | X_2) + I(V_2; Y_2, \hat{Y}_1 | X_2) - I(V_1; V_2) \\ R_{e,1} &\leq I(V_1; Y_1 | X_2) - I(V_1; Y_2, \hat{Y}_1 | V_2, X_2) - I(V_1; V_2) \\ R_{e,2} &\leq I(V_2; Y_2, \hat{Y}_1 | X_2) - I(V_2; Y_1 | V_1, X_2) - I(V_1; V_2) \\ R_{e,1} &\leq R_1, \quad R_{e,2} \leq R_2 \end{aligned} \quad (1)$$

are achievable for any distribution of the form

$$p(v_1, v_2)p(x_2)p(x_1|v_1, v_2)p(\hat{y}_1|x_2, y_1, v_1)p(y_1, y_2|x_1, x_2) \quad (2)$$

subject to the constraint

$$I(\hat{Y}_1; Y_1 | X_2, V_1) \leq I(\hat{Y}_1, X_2; Y_2) \quad (3)$$

Remark 1 *We note that both the form of the probability distribution in (2) and the constraint in (3) in Theorem 1 are somewhat different than the classical CAF scheme in [13]. We condition the distribution of \hat{Y}_1 on V_1 to prevent the compressed version of Y_1 to leak any information on user 1's message. The constraint in (3) also reflects this concern.*

Remark 2 *If we disable the assistance of user 1 to user 2 by setting $X_2 = \hat{Y}_1 = \phi$, the channel model reduces to the standard BC, and the equivocation rates become*

$$\begin{aligned} R_{e,1}^{BC} &\leq I(V_1; Y_1) - I(V_1; Y_2 | V_2) - I(V_1; V_2) \\ R_{e,2}^{BC} &\leq I(V_2; Y_2) - I(V_2; Y_1 | V_1) - I(V_1; V_2) \end{aligned} \quad (4)$$

which were derived for standard BCs in [8].

Remark 3 If we disable both cooperation between receivers by setting $X_2 = \hat{Y}_1 = \phi$, and also the confidential messages sent to user 1 by setting $V_1 = \phi$, the channel model reduces to the single-user eavesdropper channel, and the equivocation rate constraint for the second user becomes

$$R_{e,2} \leq I(V_2; Y_2) - I(V_2; Y_1) \quad (5)$$

and the Markov chain $V_2 \rightarrow X_1 \rightarrow (Y_1, Y_2)$ is required by the probability distribution in (2). This is exactly the secrecy capacity of the single-user eavesdropper channel given in [2].

Remark 4 If we disable the confidential messages sent to user 1 by setting $V_1 = \phi$, the channel model reduces to a standard relay channel with secrecy constraints, and the equivocation rate constraint for the second user becomes

$$R_{e,2} \leq I(V_2; Y_2, \hat{Y}_1 | X_2) - I(V_2; Y_1 | X_2) \quad (6)$$

subject to

$$I(\hat{Y}_1; Y_1 | X_2) \leq I(\hat{Y}_1, X_2; Y_2) \quad (7)$$

which was found in [9] as an achievable secrecy rate.

IV. AN OUTER BOUND

We now provide an outer bound for the rate-equivocation region. Our first outer bound in Theorem 2 uses auxiliary random variables. Next, in Corollary 1 we provide a simpler outer bound for user 2 using only the channel inputs and outputs, without employing any auxiliary random variables.

Theorem 2 The rate-equivocation region of the CRBC lies in the union of the following rate tuples,

$$\begin{aligned} R_1 &\leq I(V_1; Y_1 | X_2) \\ R_2 &\leq I(X_2, V_2; Y_2) \\ R_{e,1} &\leq \min \left\{ R_{e,1}^{U,1}, R_{e,1}^{U,2}, R_1 \right\} \\ R_{e,2} &\leq \min \left\{ R_{e,2}^{U,1}, R_{e,2}^{U,2}, R_2 \right\} \end{aligned} \quad (8)$$

where

$$\begin{aligned} R_{e,1}^{U,1} &= I(V_1; Y_1 | X_2, U) - I(V_1; Y_2 | X_2, U) \\ R_{e,2}^{U,1} &= I(V_2; Y_2 | X_2, U) - I(V_2; Y_1 | X_2, U) \\ R_{e,1}^{U,2} &= I(V_1; Y_1 | X_2, V_2) - I(V_1; Y_2 | X_2, V_2) \\ R_{e,2}^{U,2} &= I(V_2; Y_2 | X_2, V_1) - I(V_2; Y_1 | X_2, V_1) \end{aligned} \quad (9)$$

where the union is taken over all joint probability distributions satisfying the following Markov chain

$$U \rightarrow (V_1, V_2) \rightarrow (X_1, X_2, Y_1) \rightarrow Y_2 \quad (10)$$

Remark 5 The bounds on the equivocation rates in Theorem 2 and those in [8], where the outer bounds are for the equivocation rates in a two-user BC, have the same expressions. The only difference between the two outer bounds

is in the Markov chain over which the union is taken. The Markov chain in (10) contains the one in [8], which is

$$U \rightarrow (V_1, V_2) \rightarrow X_1 \rightarrow (Y_1, Y_2) \quad (11)$$

which means that our outer bound here evaluates to a larger region than the one in [8]. This should be expected since the achievable rate-equivocation region here in our CRBC contains the achievable region in the BC.

Corollary 1 A simpler outer bound for the equivocation rate of user 2 can be obtained by the union of the rates

$$R_{e,2} \leq I(X_1; Y_2 | X_2, Y_1) \quad (12)$$

V. AN EXAMPLE: GAUSSIAN CHANNELS

We now provide an example to show how the proposed achievable scheme can enlarge the secrecy region for a Gaussian BC. The channel outputs of a Gaussian CRBC are $Y_1 = X_1 + Z_1, Y_2 = X_1 + X_2 + Z_2$ where $Z_1 \sim \mathcal{N}(0, N_1), Z_2 \sim \mathcal{N}(0, N_2)$ and independent, $E\{X_1^2\} \leq P, E\{X_2^2\} \leq aP$. We also assume that $N_2 > N_1$, i.e., user 1 has a stronger channel in the corresponding BC. Note that, in this case, if user 1 does not help user 2, e.g., in the corresponding BC, $R_{e,2} = 0$. We present two different achievable schemes for this channel where each one corresponds to a particular selection of the underlying random variables in Theorem 1 satisfying the probability distribution condition in (2). Proposition 1 assigns independent channel inputs for each user, whereas Proposition 2 uses a DPC. For simplicity, we provide only the achievable equivocation region in the following propositions.

Proposition 1 The following equivocation rates are achievable for $\forall \alpha \in [0, 1]$ ($\bar{\alpha} = 1 - \alpha$)

$$\begin{aligned} R_{e,1} &\leq \frac{1}{2} \log \left(1 + \frac{\alpha P}{\bar{\alpha} P + N_1} \right) - \frac{1}{2} \log \left(1 + \frac{\alpha P}{N_2} \right) \\ R_{e,2} &\leq \frac{1}{2} \log \left(1 + \bar{\alpha} P \left(\frac{1}{\alpha P + N_2} + \frac{1}{N_1 + N_c} \right) \right) \\ &\quad - \frac{1}{2} \log \left(1 + \frac{\bar{\alpha} P}{N_1} \right) \end{aligned} \quad (13)$$

where N_c is subject to

$$N_c \geq \frac{N_2(\bar{\alpha} P + N_1) + P(\alpha \bar{\alpha} P + N_1)}{aP} \quad (14)$$

Proof: This achievable region can be obtained by selecting $V_1 \sim \mathcal{N}(0, \alpha P), V_2 \sim \mathcal{N}(0, \bar{\alpha} P), X_1 = V_1 + V_2, X_2 \sim \mathcal{N}(0, aP), \hat{Y}_1 = Y_1 - V_1 + Z_c = V_2 + Z_1 + Z_c$ and $Z_c \sim \mathcal{N}(0, N_c)$, where V_1, V_2, X_2 and Z_c are independent. ■

This achievable region can be enlarged by introducing correlation between V_1, V_2 . Since a joint encoding is performed at the transmitter, one of the users' signals can be treated as a non-causally known interference, and DPC [21] can be used. In the following proposition, transmitter treats user 2's signal as a non-causally known interference.

Proposition 2 The following equivocation rates are achiev-

able for any γ and $\forall \alpha \in [0, 1]$

$$\begin{aligned}
R_{e,1} &\leq \frac{1}{2} \log \left(1 + \frac{(\bar{\alpha}\gamma + \alpha)^2 P}{(\alpha + \gamma^2 \bar{\alpha})N_1 + (\gamma - 1)^2 \alpha \bar{\alpha} P} \right) \\
&\quad - \frac{1}{2} \log \left(1 + \frac{\alpha P}{N_2} \right) - \frac{1}{2} \log \left(1 + \gamma^2 \frac{\bar{\alpha}}{\alpha} \right) \\
R_{e,2} &\leq \frac{1}{2} \log \left(1 + \frac{\bar{\alpha} P (N_1 + N_c) + \bar{\alpha} (1 - \gamma)^2 P (\alpha P + N_2)}{(\alpha P + N_2)(N_1 + N_c)} \right) \\
&\quad - \frac{1}{2} \log \left(1 + \frac{\alpha \bar{\alpha} (\gamma - 1)^2 P}{(\alpha + \gamma^2 \bar{\alpha})N_1} \right) - \frac{1}{2} \log \left(1 + \gamma^2 \frac{\bar{\alpha}}{\alpha} \right)
\end{aligned} \tag{15}$$

where N_c is subject to

$$N_c \geq \frac{-\eta + \sqrt{\eta^2 + 4\theta\omega}}{2\theta} \tag{16}$$

where

$$\begin{aligned}
\eta &= (\alpha + \gamma^2 \bar{\alpha}) P [aN_1 + (1 - \gamma)^2 \bar{\alpha} P (a + \bar{\alpha})] \\
&\quad - (P + N_2) [N_1 (\alpha + \gamma^2 \bar{\alpha}) + \alpha \bar{\alpha} (\gamma - 1)^2 P] \\
\omega &= [N_1 (\alpha + \gamma^2 \bar{\alpha}) + P \alpha \bar{\alpha} (\gamma - 1)^2] \\
&\quad \times [(P + N_2) ((1 - \gamma)^2 \bar{\alpha} P + N_1) - (1 - \gamma)^2 \bar{\alpha}^2 P^2] \\
\theta &= a(\alpha + \bar{\alpha} \gamma^2) P
\end{aligned} \tag{17}$$

Proof: The rates are obtained by applying DPC for user 1. The channel input of the transmitter is $X_1 = U_1 + U_2$ where $U_1 \sim \mathcal{N}(0, \alpha P)$, $U_2 \sim \mathcal{N}(0, \bar{\alpha} P)$. The other selections are $V_2 = U_2$, $V_1 = U_1 + \gamma U_2$, where for user 1, the signal of user 2 is treated as non-casually known interference at the transmitter. The compressed signal is $\hat{Y}_1 = Y_1 - V_1 + Z_c = (1 - \gamma)U_2 + Z_1 + Z_c$ where $Z_c \sim \mathcal{N}(0, N_c)$ is the compression noise. The channel input of user 1 is selected as $X_2 \sim \mathcal{N}(0, aP)$. Here, again, U_1, U_2, Z_c and X_2 are all independent. ■

Each rate region is evaluated for $P = 8, N_1 = 1, N_2 = 2$ and corresponding plots are given in Figs. 2, 3. Note that since $N_2 > N_1$, if there was no cooperation between the users, user 2 could not have a positive secrecy rate. We observe from these figures that, thanks to the cooperation of the users, both users enjoy positive secrecy rates. Moreover, by comparing Fig. 2 with Fig. 3, we observe that inducing correlation between V_1, V_2 improves the rates.

VI. JOINT JAMMING AND RELAYING

The proposed achievability scheme and its application to a Gaussian example show us that user cooperation can enlarge the secrecy region. However, this achievability scheme and the Gaussian example provide us with only a limited picture of what can be achieved. In particular, the proposed achievability scheme is designed with the cooperating user (user 1) being the stronger of the two users in mind. Next, we want to explore what can be done when the cooperating user (user 1) is the weaker of the two users. In this case, without the cooperative link, user 1 cannot have a positive secrecy rate. Therefore, the first question to ask is, whether user 1 can have a positive secrecy rate by utilizing the cooperative link. The answer is positive if user 1 uses the cooperative link to

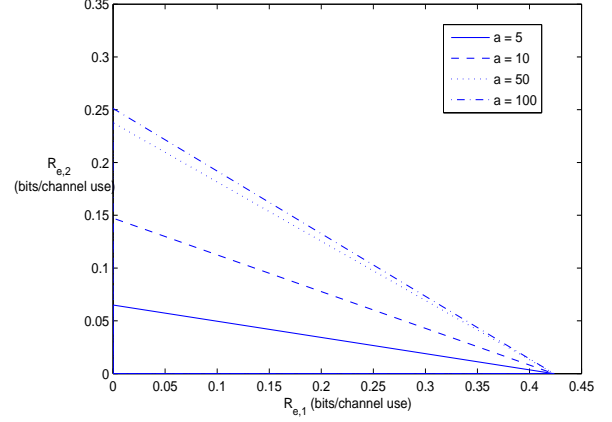


Fig. 2. Achievable equivocation region using Proposition 1.

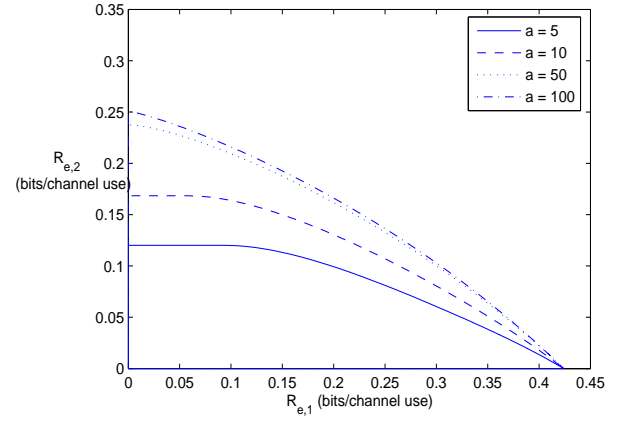


Fig. 3. Achievable equivocation region using Proposition 2.

send a jamming signal to user 2. However, a more interesting question is whether both users can achieve positive secrecy rates simultaneously. The following theorem provides an achievable scheme, where user 1 performs a combination of jamming and relaying, to provide both users with positive secrecy rates.

Theorem 3 *The rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying*

$$\begin{aligned}
R_1 &\leq I(V_1; Y_1 | X_2, U) \\
R_2 &\leq I(V_2; \hat{Y}_1, Y_2 | U) \\
R_1 + R_2 &\leq I(V_2; \hat{Y}_1, Y_2 | U) + I(V_1; Y_1 | X_2, U) - I(V_1; V_2) \\
R_{e,1} &\leq I(V_1; Y_1 | X_2, U) - I(V_1; \hat{Y}_1, Y_2 | U, V_2) - I(V_1; V_2) \\
R_{e,2} &\leq I(V_2; \hat{Y}_1, Y_2 | U) - I(V_2; Y_1 | X_2, U, V_1) - I(V_1; V_2) \\
R_{e,1} &\leq R_1, \quad R_{e,2} \leq R_2
\end{aligned} \tag{18}$$

are achievable for any distribution of the form

$$p(v_1, v_2) p(x_1 | v_1, v_2) p(u) p(\hat{y}_1 | u, v_1, y_1) p(x_2 | u) \tag{19}$$

subject to the following constraint

$$I(\hat{Y}_1; Y_1 | U, V_1) \leq I(U, \hat{Y}_1; Y_2) \tag{20}$$

Remark 6 In Theorem 3, U denotes the actual help signal, while X_2 , which is correlated with U , may include an additional jamming attack. The intuition behind this scheme is that, although user 2 should be able to decode U , it cannot decode the entire X_2 . Hence, since user 2 cannot decode and subtract X_2 from Y_2 , its channel becomes an attacked one, where decoding V_1 may be impossible. Thus, here, user 1 first attacks user 2 to make its channel worse by associating U with many X_2 s, and then helps it to improve its secrecy rate.

Remark 7 This scheme is reminiscent of “cooperative jamming” [3] and “noise forwarding” [11]. However, in [3], [11], there is an external eavesdropper, and the jamming attack hurts both the eavesdropper and also the receiver, with the hope that it hurts the eavesdropper more, i.e., helps the receiver. Moreover, jamming codewords should be decoded by the receiver in [11], which is not the case here.

Now, we provide a Gaussian example. Consider again the Gaussian CRBC, now with $N_1 > N_2$. The proposed scheme works as follows: user 1 divides X_2 into two parts. The first part carries the noise and the second part carries the bin index of \hat{Y}_1 . Although Theorem 3 is valid for all cases, assume here that user 1 has large enough power. Then, the first part makes user 2’s channel noisier than user 1’s channel. This brings the situation to the case studied earlier. Consequently, we can now have a positive secrecy rate for user 1, and also provide a positive secrecy rate to user 2, by sending a compressed version of Y_1 to it, as in the previous section.

Proposition 3 The following equivocation rates are achievable $\forall (\alpha, \beta) \in [0, 1] \times [0, 1]$

$$\begin{aligned} R_{e,1} &\leq \frac{1}{2} \log \left(1 + \frac{\alpha P}{\bar{\alpha} P + N_1} \right) - \frac{1}{2} \log \left(1 + \frac{\alpha P}{a\bar{\beta} P + N_2} \right) \\ R_{e,2} &\leq \frac{1}{2} \log \left(1 + \bar{\alpha} P \left(\frac{1}{N_1 + N_c} + \frac{1}{\alpha P + N_2 + a\bar{\beta} P} \right) \right) \\ &\quad - \frac{1}{2} \log \left(1 + \frac{\bar{\alpha} P}{N_1} \right) \end{aligned} \quad (21)$$

where N_c is subject to

$$N_c \geq \frac{\bar{\alpha} P (\alpha P + N_2 + a\bar{\beta} P) + N_1 (P + N_2 + a\bar{\beta} P)}{a\bar{\beta} P} \quad (22)$$

Proof: The rates are obtained by using the following assignments for the random variables in Theorem 3: $X_1 = V_1 + V_2$ where $V_1 \sim \mathcal{N}(0, \alpha P)$, $V_2 \sim \mathcal{N}(0, \bar{\alpha} P)$, $X_2 = U + Z_j$ where $U \sim \mathcal{N}(0, a\bar{\beta} P)$, $Z_j \sim \mathcal{N}(0, a\bar{\beta} P)$, $\hat{Y}_1 = Y_1 - V_1 + Z_c = V_2 + Z_1 + Z_c$ where $Z_c \sim \mathcal{N}(0, N_c)$. Moreover, V_1, V_2, U, Z_j, Z_c are all independent. Here, Z_j serves as the jamming signal, and U serves as the helper signal. ■

An example is given in Fig. 4 for $P = 8$, $N_1 = 2$, $N_2 = 1$.

REFERENCES

- [1] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.
- [2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

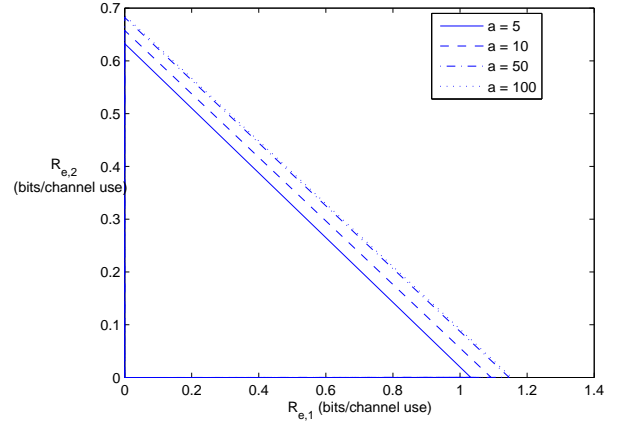


Fig. 4. Achievable equivocation region using Proposition 3.

- [3] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*. To appear.
- [4] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *IEEE Inf. Theory Workshop on Frontiers in Coding Theory*, Sep. 2007.
- [5] Y. Liang and H. V. Poor. Generalized multiple access channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Apr. 2006.
- [6] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE Int. Symp. Inf. Theory*, Jul. 2006.
- [7] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Sep. 2007.
- [8] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*. to appear, Jun. 2008.
- [9] X. He and A. Yener. On the equivocation region of relay channels with orthogonal components. In *41th Asilomar Conf. Signals, Syst. and Comp.*, Nov. 2007.
- [10] Y. Oohama. Relay channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2007.
- [11] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. Submitted to *IEEE Trans. Inf. Theory*, Dec. 2006.
- [12] M. Yuksel and E. Erkip. The relay channel with a wire-tapper. In *41st CISS*, Mar. 2007.
- [13] T. M. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory*, IT-25(5):572–584, Sep. 1979.
- [14] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity-part I: System description. *IEEE Trans. Commun.*, 51(11):1927–1938, Nov. 2003.
- [15] Y. Liang and G. Kramer. Rate regions for relay broadcast channel. *IEEE Trans. Inf. Theory*, 53(10):3517–3535, October 2007.
- [16] R. Dabora and S. Servetto. Broadcast channels with cooperating decoders. *IEEE Trans. Inf. Theory*, 52(12):5438–5454, Dec. 2006.
- [17] Y. Liang and V. V. Veeravalli. Cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 53(3):900–928, Mar. 2007.
- [18] E. Ekrem and S. Ulukus. Effects of cooperation on the secrecy of multiple access channels with generalized feedback. In *CISS*, Mar. 2008.
- [19] K. Marton. A coding theorem for the discrete memoryless channels. *IEEE Trans. Inf. Theory*, 25(1):306–311, May 1979.
- [20] R. Tanniuos and A. Nosratinia. Relay channels with private messages. *IEEE Trans. Inf. Theory*, 53(10):3777–3785, Oct. 2007.
- [21] M. H. M. Costa. Writing on dirty paper. *IEEE Trans. Inf. Theory*, IT-29(3):439–441, May 1983.