# Effects of Cooperation on the Secrecy of Multiple Access Channels with Generalized Feedback

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 multiple access channels with generalized feedback (MAC-GF). We show that cooperation can increase the achievable secrecy region. We propose achievable schemes which use compress-and-forward (CAF) based transmission strategies. CAF based strategies allow users to increase their rates up to levels which are not decodable by the cooperating partners, consequently improving the secrecy of the users. We also provide outer bounds on the achievable equivocation rates. The outer bounds we derive depend only on the channel inputs and outputs, and hence, are easily computable. Finally, we specialize our results to a Gaussian MAC-GF, and present numerical results which demonstrate the beneficial effects of cooperation on secrecy.**

## I. Introduction

The broadcast nature of wireless communications enables the communicating parties to increase their achievable rates by exploiting over-heard information, i.e., cooperation. A major concern in this setting is the potential of compromising the confidentiality of transmitted information, i.e., secrecy. In this work, we aim to gain an understanding on the interaction of these two phenomena, i.e., cooperation and secrecy, and more specifically, the effects of cooperation on secrecy.

The first information theoretic treatment of the wire-tap channel appeared in [1], where the wire-tapper's signal was assumed to be a degraded version of the main receiver's signal, and the secrecy capacity of this channel was established. Later [2] determined the secrecy capacity of the general, not necessarily degraded, wire-tap channel. More recently, secrecy of multiple-user channels have been studied under various different models. References [3]–[6] focus on the secrecy of multiple access channels (MAC), where in [3], [4], the eavesdropper is an external entity, while in [5], [6], users are the eavesdroppers. The secrecy of broadcast channels (BC) is studied in [7], where each user wants to have secure communication with the transmitter while the other user eavesdrops. In [8]–[11], relay channels are considered, where in [8], [9], there is an external wire-tapper and the relay helps either the legitimate receiver [8] or the wire-tapper [9]. In [10], [11], the relay itself is considered an eavesdropper.

The simplest model of a cooperative network is the relay channel, where the sole role of the relay node is to help the ongoing communication [12]. The two basic achievable schemes for the relay channel, decode-and-forward (DAF) and compress-and-forward (CAF), were both proposed in [12]. These schemes were utilized later in MAC with generalized feedback (MAC-GF) [13], [14] and BC with cooperating receivers (BC-CR) [15]–[17]. In MAC-GF, cooperation is done at the transmitter side using the feedback signals at each transmitter, while in BC-CR, cooperation is done at the receiver side through a link between the receivers.

Our goal is to study the effects of cooperation on the secrecy of users in a multi-user network, where users are willing to help each other, but also want to keep their information as secret as possible from the other users. For such a goal, the simplest channel models to study are BC-CR and MAC-GF, where multiple users have their individual rates, and there is opportunity for cooperation through feedback signals, which also leak information. We studied the effects of cooperation on secrecy in BC-CR in [18], and here, we focus on the secrecy of MAC-GF.

Our work differs significantly from previous works [5], [6] which also examined secrecy of MAC-GF. In [5], [6] feedback signals, which are available at the transmitters, are not used in the encoding functions, i.e., the users are not allowed to cooperate. Our motivation for this work, and the differences of our work and [5], [6], can be explained more effectively with a Gaussian MAC-GF example. In a Gaussian MAC-GF, if feedback signals are not used in encoding, e.g., as in [5], [6], the users would have positive secrecy rates only when the inter-user links between them are noisier than their main links to the receiver. Here, we show that, if the users are willing to cooperate using a CAF-based scheme, then they can achieve positive secrecy rates, even when the channels between them are stronger than their main links. The basic enabling factor for this is that, when a cooperating partner uses CAF, it helps the other user increase its rate to levels which are no longer decodable at the cooperating partner.

In this paper, we present two achievable schemes which are based on CAF strategy [12]. CAF has been used before in the context of increasing rates in MAC-GF [19], [20]; here we use CAF to provide secrecy to cooperating users, and determine achievable equivocation rates. We also present outer bounds on the achievable equivocation rates. The outer bounds we derive depend only on the channel inputs and outputs, and hence are easily computable. Finally, we present numerical results for Gaussian MAC-GF.

This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

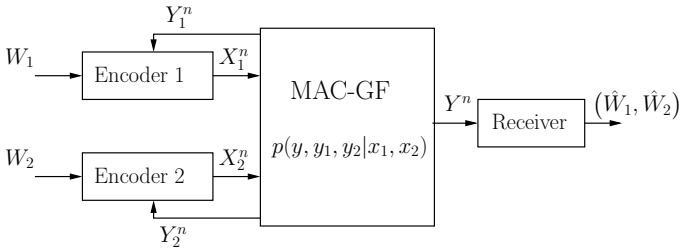


Fig. 1. The MAC-GF channel model.

## II. Channel Model and Definitions

The two-user MAC-GF (see Figure 1) consists of two input alphabets $\mathcal{X}_1, \mathcal{X}_2$ and three output alphabets $\mathcal{Y}, \mathcal{Y}_1, \mathcal{Y}_2$. The channel is memoryless and is characterized by $p(y, y_1, y_2|x_1, x_2)$.

A $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code for this channel consists of two message sets $\mathcal{W}_1 = \left\{1, \ldots, 2^{nR_1}\right\}, \mathcal{W}_2 = \left\{1, \ldots, 2^{nR_2}\right\}$, two encoder functions

$$x_{1,i} = f_1\left(w_1, y_{1,1}, \ldots, y_{1,i-1}\right), \qquad i = 1, \ldots, n$$
$$x_{2,i} = f_2\left(w_2, y_{2,1}, \ldots, y_{2,i-1}\right), \qquad i = 1, \ldots, n$$

and a decoder function $g : \mathcal{Y} \to \mathcal{W}_1 \times \mathcal{W}_2$. The probability of error is defined as $P_e^n = \Pr\left(g(Y^n) \neq (W_1, W_2)\right)$.

The secrecy of each user is measured by the normalized entropy of its message conditioned on the random variables available at the other user, the other user's observation, channel input and message, i.e.,

$$\frac{1}{n} H(W_1|Y_2^n, X_2^n, W_2) \quad \text{and} \quad \frac{1}{n} H(W_2|Y_1^n, X_1^n, W_1)$$

which will hereafter be called equivocation rates. A rate tuple $(R_1, R_2, R_{e,1}, R_{e,2})$ is said to be achievable if there exists a $\left(2^{nR_1}, 2^{nR_2}, n\right)$ code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(W_1|Y_2^n, X_2^n, W_2) \geq R_{e,1} \tag{2}$$
$$\lim_{n\to\infty} \frac{1}{n} H(W_2|Y_1^n, X_1^n, W_1) \geq R_{e,2} \tag{3}$$

**Remark 1** We note that our coding scheme is different than those in previous works [5], [6], which also considered secrecy in MAC-GF. In [5], [6], the encoding functions are restricted to be of the form

$$f_i : \mathcal{W}_i \to \mathcal{X}_i^n, \qquad i = 1, 2$$

i.e., the feedback signals that are available at the transmitters are not utilized in the encoding functions.

## III. Achievable Schemes

We present our first achievable scheme in the following theorem. In this achievable scheme, even though both users receive feedback signals in the MAC-GF, only one of them, user 1, utilizes the feedback signal in its encoding function and sends a compressed version of its observation to the main receiver. This achievable scheme is based on CAF strategy [12].

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

$$R_1 \leq I(X_1; Y, \hat{Y}_1|U, X_2) \tag{4}$$
$$R_2 \leq I(X_2; Y, \hat{Y}_1|U, X_1) \tag{5}$$
$$R_1 + R_2 \leq I(X_1, X_2; Y, \hat{Y}_1|U) \tag{6}$$
$$R_{e,1} \leq \min\left\{R_1' - \tilde{R}_{e,1}, R_1\right\} \tag{7}$$
$$R_{e,2} \leq \min\left\{R_2' - I(X_2; Y_1|U, X_1), R_2\right\} \tag{8}$$

where the pairs $(R_1', R_2')$ belong to

$$\mathcal{C}_1\left(R_1, R_2\right) = \left\{ \begin{array}{rcl} R_1 & \leq & R_1' \\ R_2 & \leq & R_2' \\ R_1' & \leq & I(X_1; Y, \hat{Y}_1|U, X_2) \\ R_2' & \leq & I(X_2; Y, \hat{Y}_1|U, X_1) \\ R_1' + R_2' & \leq & I(X_1, X_2; Y, \hat{Y}_1|U) \end{array} \right\} \tag{9}$$

and $\tilde{R}_{e,1}$ is given by

$$\tilde{R}_{e,1} = \left\{ \begin{array}{ll} I(X_1; Y_2, \hat{Y}_1|U, X_2) & \text{if} \quad \mathcal{S}_1 \\ \\ I(X_1; Y_2|U, X_2) & \text{otherwise} \end{array} \right. \tag{10}$$

are achievable for any distribution of the form

$$p(u)p(x_1|u)p(\hat{y}_1|u, x_1, y_1)p(x_2)p(y, y_1, y_2|x_1, x_2) \tag{11}$$

subject to the constraint

$$I(\hat{Y}_1; Y_1|U, X_1) \leq I(U, \hat{Y}_1; Y) \tag{12}$$

where

$$\begin{aligned} \mathcal{S}_1 = \big\{ & I(U; Y) \leq I(U; Y_2|X_2), \\ & I(\hat{Y}_1; Y|U) \leq I(\hat{Y}_1; Y_2|U, X_2) \big\} \end{aligned} \tag{13}$$

**Remark 2** The achievable region given in Theorem 1 can be enlarged by using the channel prefixing technique introduced in [2]. In Theorem 1, we did not use channel prefixing for the clarity of presentation. If we want to use it, we need to replace all occurrences of $X_1$ (resp. $X_2$) with $V_1$ (resp. $V_2$), and change the joint distribution in (11) to $p(u)p(v_1|u)p(x_1|v_1)p(\hat{y}_1|u, v_1, y_1)p(v_2)p(x_2|v_2)$ $p(y, y_1, y_2|x_1, x_2)$.

**Remark 3** In (11), we condition $\hat{Y}_1$ on $X_1$ because user 1's feedback signal can be correlated with $X_1$. The conditioning on $X_1$ in (12) is for the same reason as well. By these conditionings, we implicitly assume that, if the feedback signal of user 1 has a self-interference term, user 1 cancels it out. If user 1 does not want to cancel it out hoping that this may increase the achievable region, then the pdf in (11) and the constraint in (12) should be replaced with $p(\hat{y}_1|u, y_1)$ and $I(\hat{Y}_1; Y_1|U) \leq I(U, \hat{Y}_1; Y)$, respectively. Both choices are optional, and neither of them provides an achievable region that includes the one provided by the other. For a similar discussion, please see Remark 2 of [21].

**Remark 4** User 2 may want to decode the compressed version of user 1's observation, $\hat{Y}_1$, hoping that it may find additional useful information on user 1's message, besides

what it gets through its own observation $Y_2$. Equations (10) and (13) are a result of this.

**Remark 5** If we disable user cooperation via setting $U = \hat{Y}_1 = \phi$, the achievable rate region for the pairs $(R_1, R_2)$ reduce to the capacity region of the MAC [22].

**Remark 6** If we set $U = X_1 = \hat{Y}_1 = Y_2 = \phi$, then the channel becomes a wire-tap channel, and the achievable rate region reduces to

$$R_2 \leq I(X_2;Y) \tag{14}$$
$$R_{e,2} \leq \min\{I(X_2;Y) - I(X_2;Y_1), R_2\} \tag{15}$$

which, after channel prefixing, becomes the same as the one in [2].

**Remark 7** If we disable the assistance of user 1 by setting $U = \hat{Y}_1 = \phi$, then we have the following achievable region

$$R_1 \leq I(X_1;Y|X_2) \tag{16}$$
$$R_2 \leq I(X_2;Y|X_1) \tag{17}$$
$$R_1 + R_2 \leq I(X_1,X_2;Y) \tag{18}$$
$$R_{e,1} \leq \min\{R_1' - I(X_1;Y_2|X_2), R_1\} \tag{19}$$
$$R_{e,2} \leq \min\{R_2' - I(X_2;Y_1|X_1), R_2\} \tag{20}$$

where the pairs $(R_1', R_2')$ belong to

$$\left\{ \begin{array}{rcl} R_1 & \leq & R_1' \\ R_2 & \leq & R_2' \\ R_1' & \leq & I(X_1;Y|X_2) \\ R_2' & \leq & I(X_2;Y|X_1) \\ R_1'+R_2' & \leq & I(X_1,X_2;Y) \end{array} \right\} \tag{21}$$

for any distribution of the form

$$p(x_1)p(x_2)p(y,y_1,y_2|x_1,x_2) \tag{22}$$

which, after channel prefixing, becomes the same as the one in [5], where feedback signals are not utilized in the encoding functions.

**Remark 8** If we disable the confidential messages of user 1 by setting $U = X_1$, the channel model becomes a relay channel with secrecy constraints, and the achievable region reduces to

$$R_2 \leq I(X_2;Y,\hat{Y}_1|X_1) \tag{23}$$
$$R_{e,2} \leq \min\left\{I(X_2;Y,\hat{Y}_1|X_1) - I(X_2;Y_1|X_1), R_2\right\} \tag{24}$$

for any distribution

$$p(x_1)p(\hat{y}_1|x_1,y_1)p(x_2)p(y,y_1,y_2|x_1,x_2) \tag{25}$$

subject to the constraint

$$I(\hat{Y}_1;Y_1|X_1) \leq I(X_1,\hat{Y}_1;Y) \tag{26}$$

which was proposed in [10].

We state our second achievable scheme in the following theorem. In this achievable scheme, both users utilize the feedback signals they receive in their encoding functions, and send compressed versions of their observations to the main receiver.

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

$$R_1 \leq I(X_1;Y,\hat{Y}_1,\hat{Y}_2|U_1,U_2,X_2) \tag{27}$$
$$R_2 \leq I(X_2;Y,\hat{Y}_1,\hat{Y}_2|U_1,U_2,X_1) \tag{28}$$
$$R_1 + R_2 \leq I(X_1,X_2;Y,\hat{Y}_1,\hat{Y}_2|U_1,U_2) \tag{29}$$
$$R_{e,1} \leq \min\left\{R_1' - \tilde{R}_{e,1}, R_1\right\} \tag{30}$$
$$R_{e,2} \leq \min\left\{R_2' - \tilde{R}_{e,2}, R_2\right\} \tag{31}$$

where the pairs $(R_1', R_2')$ belong to

$$\mathcal{C}_2(R_1,R_2) = \left\{ \begin{array}{rcl} R_1 & \leq & R_1' \\ R_2 & \leq & R_2' \\ R_1' & \leq & I(X_1;Y,\hat{Y}_1,\hat{Y}_2|U_1,U_2,X_2) \\ R_2' & \leq & I(X_2;Y,\hat{Y}_1,\hat{Y}_2|U_1,U_2,X_1) \\ R_1'+R_2' & \leq & I(X_1,X_2;Y,\hat{Y}_1,\hat{Y}_2|U_1,U_2) \end{array} \right\} \tag{32}$$

and $(\tilde{R}_{e,1}, \tilde{R}_{e,2})$ are given by

$$\tilde{R}_{e,1} = \left\{ \begin{array}{ll} I(X_1;Y_2,\hat{Y}_1|U_1,U_2,X_2) & \text{if} \quad \mathcal{S}_{2,1} \\ I(X_1;Y_2|U_1,U_2,X_2) & \text{otherwise} \end{array} \right. \tag{33}$$

$$\tilde{R}_{e,2} = \left\{ \begin{array}{ll} I(X_2;Y_1,\hat{Y}_2|U_1,U_2,X_1) & \text{if} \quad \mathcal{S}_{2,2} \\ I(X_2;Y_1|U_1,U_2,X_1) & \text{otherwise} \end{array} \right. \tag{34}$$

are achievable for any distribution of the form

$$p(u_1)p(x_1|u_1)p(\hat{y}_1|u_1,x_1,y_1)p(u_2)p(x_2|u_2) \\ p(\hat{y}_2|u_2,x_2,y_2)p(y,y_1,y_2|x_1,x_2) \tag{35}$$

subject to the constraints

$$I(\hat{Y}_1;Y_1|U_1,X_1) \leq I(U_1,\hat{Y}_1;Y|U_2) \tag{36}$$
$$I(\hat{Y}_2;Y_2|U_2,X_2) \leq I(U_2,\hat{Y}_2;Y|U_1) \tag{37}$$
$$I(\hat{Y}_1;Y_1|U_1,X_1) + I(\hat{Y}_2;Y_2|U_2,X_2) \leq \\ I(U_1,U_2;Y) + I(\hat{Y}_1;Y|U_1,U_2) + I(\hat{Y}_2;Y|U_1,U_2) \tag{38}$$

where

$$\mathcal{S}_{2,1} = \Big\{I(U_1;Y) \leq I(U_1;Y_2|U_2,X_2), \\ I(\hat{Y}_1;Y|U_1,U_2) \leq I(\hat{Y}_1;Y_2|U_1,U_2,X_2)\Big\} \tag{39}$$

$$\mathcal{S}_{2,2} = \Big\{I(U_2;Y) \leq I(U_2;Y_1|U_1,X_1), \\ I(\hat{Y}_2;Y|U_1,U_2) \leq I(\hat{Y}_2;Y_1|U_1,U_2,X_1)\Big\} \tag{40}$$

**Remark 9** Remarks 2, 3, 4 apply to Theorem 2, as well. As in Remark 3, if users do not want to cancel their own signals out from their observations while compressing, the conditioning of $\hat{Y}_1$ (resp. $\hat{Y}_2$) on $X_1$ (resp. $X_2$) and conditionings on the left hand sides of inequalities (36), (37), (38) on $X_1, X_2$ should be removed. Similar to Remark 4, each user may want to decode the compressed signal of the other user in hopes of decreasing the secrecy of the other user. This is reflected in (33), (34), (39) and (40).

**Remark 10** In Theorem 2, the receiver jointly decodes $U_1, U_2$ which, as seen in (38), results in a sum constraint on the qualities of the observations sent to the receiver.

**Remark 11** If we set $U_2 = \hat{Y}_2 = \phi$ in Theorem 2, we recover Theorem 1.

## IV. Outer Bound

We now present an outer bound on the equivocation rates. This outer bound depends only on the channel inputs and outputs, and hence is computable.

**Theorem 3** The equivocation rate pairs $(R_{e,1}, R_{e,2})$ are contained in the union of

$$R_{e,1} \leq I(X_1, Y_1; Y|X_2, Y_2) \tag{41}$$

$$R_{e,2} \leq I(X_2, Y_2; Y|X_1, Y_1) \tag{42}$$

This bound is obtained by considering the best possible scenario for each user, e.g., the bound for user 1 assumes that user 2's observation is made available to the main receiver.

## V. Gaussian Channels

A Gaussian MAC-GF may be described by [5]:

$$Y_{1,i} = X_{1,i} + X_{2,i} + Z_{1,i} \tag{43}$$

$$Y_{2,i} = X_{1,i} + X_{2,i} + Z_{2,i} \tag{44}$$

$$Y_i = X_{1,i} + X_{2,i} + Z_i \tag{45}$$

where $Z_{1,i} \sim \mathcal{N}(0, N_1), Z_{2,i} \sim \mathcal{N}(0, N_2), Z_i \sim \mathcal{N}(0, N)$ and are all i.i.d. In addition, we have the following power constraints: $\frac{1}{n}\sum_{i=1}^{n} E[X_{1,i}^2] \leq P_1$ and $\frac{1}{n}\sum_{i=1}^{n} E[X_{2,i}^2] \leq P_2$.

In Section V-A, we present results on degraded channels. This section is designed to identify cases where the use of feedback signals in the encoding, i.e., cooperation, is needed for positive secrecy rates. In Section V-B, we present achievable regions for Gaussian channels with some particular selections for random variables involved in Theorems 1, 2.

### A. Degraded Channels and Implications

We first note that, for a given channel $p(y, y_1, y_2|x_1, x_2)$, depending on whether the feedback signals are used in the encoding or not, we obtain different $n$-letter joint distributions $p(w_1, w_2, x_1^n, x_2^n, y_1^n, y_2^n, y^n)$, and observe different characteristics. In this section, we focus on MAC-GFs where the feedback signals are not used in the encoding functions, e.g., [5], [6]. For such channels, we have the following outer bound.

**Theorem 4** The equivocation rate pairs $(R_{e,1}, R_{e,2})$ of MAC-GFs where feedback signals are not used in the encoding functions, are contained in the union of

$$R_{e,1} \leq I(X_1; Y|X_2, Y_2) \tag{46}$$

$$R_{e,2} \leq I(X_2; Y|X_1, Y_1) \tag{47}$$

Motivated with this outer bound, we define degradedness.

**Definition 1** If the channel satisfies the Markov chain $X_1 \to (X_2, Y_2) \to Y$ (resp. $X_2 \to (X_1, Y_1) \to Y$), then it is said to be type-I (resp. type-II) degraded.

Theorem 4 together with Definition 1 implies the following.

**Corollary 1** If the channel is type-I (resp. type-II) degraded, then we have $R_{e,1} = 0$ (resp. $R_{e,2} = 0$).

Corollary 1 can be specialized to degraded Gaussian channels.

**Corollary 2** For Gaussian channels with $Z = Z_1 + Z'$ (resp. $Z = Z_2 + Z'$), we have $R_{e,2} = 0$ (resp. $R_{e,1} = 0$) where $Z' \sim \mathcal{N}(0, N')$ and independent of $Z_1, Z_2$.

The following lemma is from [5].

**Lemma 1** All channels having the same marginal distributions $p(y_1|x_1, x_2), p(y_2|x_1, x_2), p(y|x_1, x_2)$ as the original channel have the same capacity-equivocation regions.

We are now ready to consider the broader class of stochastically degraded channels.

**Definition 2** A channel is said to be stochastically type-I degraded, if its conditional marginal distribution $p(y|x_1, x_2)$ is the same as that of a type-I degraded channel, i.e., there exists a distribution $p'(y|y_2, x_2)$ which satisfies

$$p(y|x_1, x_2) = \sum_{y_2} p(y_2|x_1, x_2) p'(y|y_2, x_2) \tag{48}$$

Stochastically type-II degradedness is defined similarly.

Using Lemma 1, we have the following corollary.

**Corollary 3** If a channel is stochastically type-I (resp. type-II) degraded, then we have $R_{e,1} = 0$ (resp. $R_{e,2} = 0$).

In Gaussian MAC-GFs, stochastically degradedness is characterized by receiver noise variances, as stated next.

**Corollary 4** For Gaussian channels, if $N_1 < N$ (resp. $N_2 < N$), then $R_{e,2} = 0$ (resp. $R_{e,1} = 0$).

This corollary is proved by showing that there always exists a degraded channel with the same conditional marginal distributions as the original channel.

To sum up, in this section we showed that, for Gaussian MAC-GF, if the feedback signals are not utilized in the encoding functions and if $N_1 < N$ (resp. $N_2 < N$), then $R_{e,1} = 0$ (resp. $R_{e,2} = 0$). However, if the feedback signals are utilized in the encoding functions, then we may have positive secrecy rates for both users as will be shown next.

### B. Achievable Schemes for Gaussian Channels

We now provide achievable regions for Gaussian MAC-GF. The following propositions characterize achievable regions using Theorems 1, 2 with certain selections for the involved random variables. We define $\mathrm{C}(x) = \frac{1}{2}\log(1 + x)$.

**Proposition 1** For any $\bar{\alpha} = 1 - \alpha \in [0, 1]$, rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying

$$R_1 \leq R_1' \leq \mathrm{C}\left(\bar{\alpha}\frac{P_1}{N}\right) \tag{49}$$

$$R_2 \leq R_2' \leq \mathrm{C}\left(P_2\frac{N + N_1 + N_c}{N(N_1 + N_c)}\right) \tag{50}$$

$$R_1' + R_2' \leq \mathrm{C}\left(\bar{\alpha}\frac{P_1}{N} + P_2\frac{N+N_1+N_c}{N\left(N_1+N_c\right)} + \frac{\bar{\alpha}P_1P_2}{N(N_1+N_c)}\right) \tag{51}$$

$$R_{e,1} \leq \min\left\{R_1' - \mathrm{C}\left(\bar{\alpha}\frac{P_1}{N_2}\right), R_1\right\} \tag{52}$$

$$R_{e,2} \leq \min\left\{R_2' - \mathrm{C}\left(\frac{P_2}{N_1}\right), R_2\right\} \tag{53}$$

are achievable, subject to the constraint

$$N_c \geq \frac{-\beta + \sqrt{\beta^2 + 4\theta\gamma}}{2\theta} \tag{54}$$

where

$$\begin{aligned}
\theta &= \alpha P_1 \\
\beta &= P_2\left[(2\alpha-1)P_1 - N - N_1\right] - N_1\left[(1-2\alpha)P_1 + N\right] \\
\gamma &= (P_2+N_1)\left[N_1\left(\bar{\alpha}P_1 + P_2 + N\right) + P_2\left(\bar{\alpha}P_1 + N\right)\right]
\end{aligned}$$

*Proof:* This region is obtained via direct calculation of the rates in Theorem 1 with the following selection of the random variables: $X_2 \sim \mathcal{N}(0, P_2), U \sim \mathcal{N}(0, \alpha P_1)$, $U' \sim \mathcal{N}(0, \bar{\alpha}P_1)$ and $X_1 = U + U'$. $\hat{Y}_1 = Y_1 - X_1 + Z_c = X_2 + Z_1 + Z_c$ where $Z_c$ is the compression noise with distribution $Z_c \sim \mathcal{N}(0, N_c)$. $X_2, U', Z_c$ are all independent. ■

**Proposition 2** For any $\left(\bar{\alpha} = 1-\alpha, \bar{\beta} = 1-\beta\right) \in [0,1] \times [0,1]$, rate tuples $(R_1, R_2, R_{e,1}, R_{e,2})$ satisfying

$$R_1 \leq R_1' \leq \mathrm{C}\left(\bar{\alpha}P_1\frac{N+N_2+N_{c,2}}{N\left(N_2+N_{c,2}\right)}\right) \tag{55}$$

$$R_2 \leq R_2' \leq \mathrm{C}\left(\bar{\beta}P_2\frac{N+N_1+N_{c,1}}{N(N_1+N_{c,1})}\right) \tag{56}$$

$$\begin{aligned}
R_1' + R_2' \leq \mathrm{C}\Bigg(&\bar{\alpha}P_1\frac{N+N_2+N_{c,2}}{N(N_2+N_{c,2})} + \bar{\beta}P_2\frac{N+N_1+N_{c,1}}{N(N_1+N_{c,1})} \\
&+ \bar{\alpha}\bar{\beta}P_1P_2\frac{N+N_1+N_{c,1}+N_2+N_{c,2}}{N(N_1+N_{c,1})(N_2+N_{c,2})}\Bigg)
\end{aligned} \tag{57}$$

$$R_{e,1} \leq \min\left\{R_1' - \mathrm{C}\left(\bar{\alpha}\frac{P_1}{N_2}\right), R_1\right\} \tag{58}$$

$$R_{e,2} \leq \min\left\{R_2' - \mathrm{C}\left(\bar{\beta}\frac{P_2}{N_1}\right), R_2\right\} \tag{59}$$

are achievable, subject to the constraints

$$\frac{-\beta_1 + \sqrt{\beta_1^2 + 4\theta_1\gamma_1}}{2\theta_1} \leq N_{c,1} \tag{60}$$

$$\frac{-\beta_2 + \sqrt{\beta_2^2 + 4\theta_2\gamma_2}}{2\theta_2} \leq N_{c,2} \tag{61}$$

$$\begin{aligned}
&\left(1 + \frac{P_2+N_1}{N_{c,1}}\right)\left(1 + \frac{P_1+N_2}{N_{c,2}}\right) \leq \\
&\qquad (1+\omega_1)(1+\omega_2)\left(1 + \frac{\alpha P_1 + \bar{\beta}P_2}{\bar{\alpha}P_1 + \bar{\beta}P_2 + N}\right)
\end{aligned} \tag{62}$$

where

$$\begin{aligned}
\theta_1 &= \alpha P_1 \\
\theta_2 &= \beta P_2 \\
\beta_1 &= \alpha P_1(\bar{\beta}P_2 + N_1) + (\bar{\beta}P_2)^2 \\
&\qquad - (P_2+N_1)(\bar{\beta}P_2 + \bar{\alpha}P_1 + N) \\
\beta_2 &= \beta P_2(\bar{\alpha}P_1 + N_2) + (\bar{\alpha}P_1)^2 \\
&\qquad - (P_1+N_2)(\bar{\alpha}P_1 + \bar{\beta}P_2 + N) \\
\gamma_1 &= (P_2+N_1)\left((\bar{\alpha}P_1 + N)(\bar{\beta}P_2 + N_1) + \bar{\beta}P_2N_1\right) \\
\gamma_2 &= (P_1+N_2)\left((\bar{\beta}P_2 + N)(\bar{\alpha}P_1 + N_2) + \bar{\alpha}P_1N_2\right) \\
\omega_1 &= \frac{(\bar{\alpha}P_1)^2}{\bar{\alpha}P_1(\bar{\beta}P_2 + N + N_2 + N_{c,2}) + (\bar{\beta}P_2 + N)(N_2 + N_{c,2})} \\
\omega_2 &= \frac{\left(\bar{\beta}P_2\right)^2}{\bar{\beta}P_2(\bar{\alpha}P_1 + N + N_1 + N_{c,1}) + (\bar{\alpha}P_1 + N)(N_1 + N_{c,1})}
\end{aligned}$$

*Proof:* This region is obtained via direct calculation of the rates in Theorem 2 with the following selection of the random variables: $X_2 = U_2 + U_2'$ where $U_2 \sim \mathcal{N}(0, \beta P_2), U_2' \sim \mathcal{N}(0, \bar{\beta}P_2)$; $X_1 = U_1 + U_1'$ where $U_1 \sim \mathcal{N}(0, \alpha P_1)$, $U_1' \sim \mathcal{N}(0, \bar{\alpha}P_1)$; $\hat{Y}_1 = Y_1 - X_1 + Z_{c,1} = X_2 + Z_1 + Z_{c,1}$ where $Z_{c,1}$ is the compression noise with distribution $Z_{c,1} \sim \mathcal{N}(0, N_{c,1})$ $\hat{Y}_2 = Y_2 - X_2 + Z_{c,2} = X_1 + Z_2 + Z_{c,2}$ where $Z_{c,2}$ is the compression noise with distribution $Z_{c,2} \sim \mathcal{N}(0, N_{c,2})$; and $U_1, U_1', U_2, U_2', Z_{c,1}, Z_{c,2}$ are all independent. ■

Graphical illustrations of Propositions 1, 2 are given in Figures 2, 3, 4. In all these figures, we use $P_1 = P_2 = 50$. In Figure 2, equivocation regions are plotted for $N_1 = 0.75, N_2 = 1.25, N = 1$. Since $N_1 < N$, if cooperation is not allowed for this channel, we have $R_{e,2} = 0$. Due to user cooperation, we have a positive secrecy rate for user 2. If Proposition 1 (i.e., one-sided cooperation) is used, then we provide a positive secrecy rate for user 2 at the expense of the secrecy of user 1. However, if Proposition 2 (i.e., two-sided cooperation) is used, then user 2 can have positive secrecy without any cost, i.e., without any decrease in the secrecy of user 1. For both propositions, maximum secrecy rate for user 2 is achieved if user 1 does not transmit any confidential messages and acts as a relay for user 2. In Proposition 1, the maximum secrecy for user 1 is achieved when user 1 does not help user 2, and in Proposition 2, the maximum secrecy for user 1 is achieved when user 2 does not transmit any confidential messages and acts as a relay for user 1.

Secondly, we consider a case where neither user can achieve positive secrecy rates without cooperation, i.e., $N_1 < N, N_2 < N$. We select the parameters as $N_1 = 0.75, N_2 = 0.75, N = 1$. As we see in Figure 3, both users are able to have positive secrecy rates through cooperation. Again, in this case as well, the maximum secrecy rate for each user is obtained when the other user acts as a pure relay.

Finally, we consider a system with $N_1 = 1.25, N_2 = 1.25, N = 1$, where we can have positive secrecy rates for both users without cooperation. We observe from Figure 4 that user cooperation increases the achievable secrecy rates.

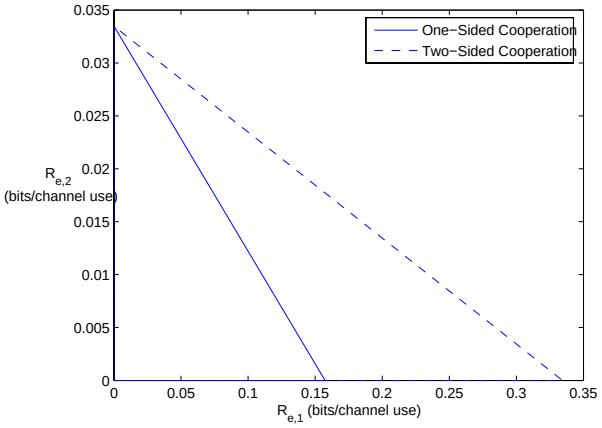


Fig. 2. The equivocation regions given in Propositions 1,2.

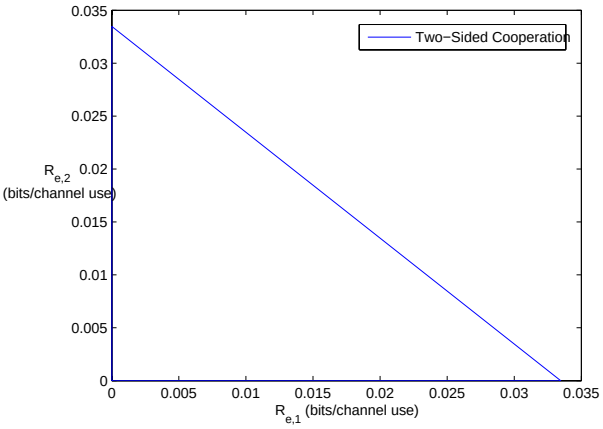


Fig. 3. The equivocation region given in Proposition 2.

## VI. Conclusions

In this paper, we showed that, in a MAC-GF, CAF-based cooperation can improve the secrecy of users, when the users are viewed as also eavesdropping on each other. This might seem expected at first, as feedback is known to increase the achievable rates of a MAC [14]. It is important to note however that, the improvement on the secrecy region is not only a consequence of the improvement on the achievable rate region through utilization of feedback (i.e., cooperation), but also how this improvement is obtained. For example, DAF or partial-DAF could improve the achievable rate region in MAC-GF, as CAF does, however, DAF or partial-DAF could not improve the secrecy region. The important point to note here is that, a cooperating partner, using CAF, can increase the rate to beyond its own decoding capability (thereby improving the secrecy of the user it helps), but it cannot do the same using DAF or partial DAF.

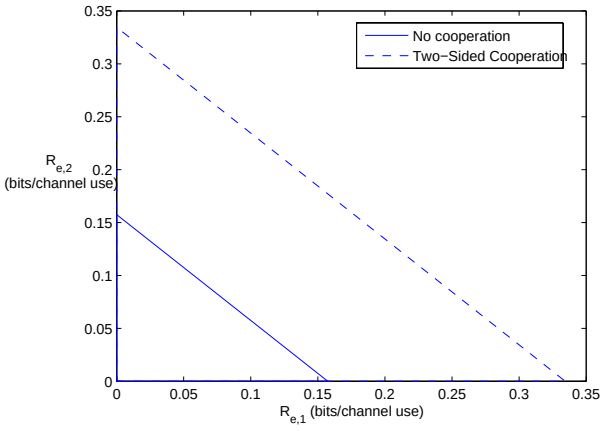


Fig. 4. Comparison of equivocation regions with and without cooperation.

## 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.

[3] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. Submitted to *IEEE Trans. Inf. Theory*, May 2006.

[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, 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.

[8] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. Submitted to *IEEE Trans. Inf. Theory*, Dec. 2006.

[9] M. Yuksel and E. Erkip. Secure communication with a relay helping the wiretapper. In *IEEE Inf. Theory Workshop*, Sep. 2007.

[10] 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.

[11] Y. Oohama. Relay channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory*, Mar. 2007.

[12] T. M. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory*, IT-25(5):572–584, Sep. 1979.

[13] F. Willems, E. van der Meulen, and J. Schalkwijk. Achievable rate region for the multiple access channel with generalized feedback. In *41th Asilomar Conf. Signals, Syst. and Comp.*, Nov. 1983.

[14] T. Cover and C. Leung. An achievable rate region for the multiple access channel with feedback. *IEEE Trans. Inf. Theory*, 27(5):292–298, May 1981.

[15] R. Dabora and S. Servetto. Broadcast channels with cooperating decoders. *IEEE Trans. Inf. Theory*, 52(12):5438–5454, Dec. 2006.

[16] Y. Liang and V. V. Veeravalli. Cooperative relay broadcast channels. *IEEE Trans. Inf. Theory*, 53(3):900–928, Mar. 2007.

[17] Y. Liang and G. Kramer. Rate regions for relay broadcast channel. *IEEE Trans. Inf. Theory*, 53(10):3517–3535, October 2007.

[18] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. Submitted to *IEEE ISIT 2008*, Jan. 2008.

[19] L. Ong and M. Motani. Coding strategies for multiple-access channels with feedback and correlated sources. *IEEE Trans. Inf. Theory*, 53(10):3476–3497, Oct. 2007.

[20] M. A. Khojastepour, A. Sabharwal, and B. Aazhang. Improved achievable rates for user cooperation and relay channels. In *IEEE Int. Symp. Inf. Theory*, Jun. 2004.

[21] R. Tanniuos and A. Nosratinia. Relay channels with private messages. *IEEE Trans. Inf. Theory*, 53(10):3777–3785, Oct. 2007.

[22] T. Cover and J. Thomas. *Elements of Information Theory*. Wiley & Sons, 2006. 2nd edition.