Multiple Access Channels with Generalized Feedback and Confidential Messages

Xiaojun Tang*, Ruoheng Liu†, Predrag Spasojević*, and H. Vincent Poor†
*WINLAB, Rutgers University, North Brunswick, NJ 08902
Email: {xtang, spasojev}@winlab.rutgers.edu
†Princeton University, Princeton, NJ 08544
Email: {rliu, poor}@princeton.edu

***Abstract*—This paper considers the problem of secret communication over a multiple access channel with generalized feedback. Two trusted users send independent confidential messages to an intended receiver, in the presence of a passive eavesdropper. In this setting, an active cooperation between two trusted users is enabled through using channel feedback in order to improve the communication efficiency. Based on rate-splitting and decode-and-forward strategies, achievable secrecy rate regions are derived for both discrete memoryless and Gaussian channels. Results show that channel feedback improves the achievable secrecy rates.**

I. Introduction

The broadcast nature of wireless medium poses both benefits and penalties for secret communication. The openness of wireless medium provides opportunities for cooperation between trusted users, which improves the communication efficiency. On the other hand, it makes the transmission extremely susceptible to eavesdropping. Anyone within communication range can listen and possibly extract information.

Those two opposite aspects are reflected in the system model as shown in Fig. 1, where we consider a multiple access channel in which two mutually trusted users communicate confidential messages to an intended receiver, in the presence of a passive eavesdropper. Channel feedback enables cooperation between two trusted users and consequently a higher communication efficiency. We refer to this channel as the *multiple access channel with generalized feedback and confidential messages* (MAC-GF-CM). The level of ignorance of the eavesdropper with respect to the confidential messages is measured by the equivocation rate. This approach was first introduced by Wyner for the wiretap channel [1], in which a single source-destination communication is eavesdropped upon via a degraded channel. Wyner's formulation was generalized by Csiszár and Körner who determined the capacity region of the broadcast channel with confidential messages [2]. The Gaussian wiretap channel was considered in [3]. More recently, multi-terminal communication with confidential messages has been studied further. This work is related to prior works on the multiple access channel with confidential messages [4], [5], the Gaussian multiple access wiretap channel [6], the interference channel with confidential messages [7], and the relay-eavesdropper channel [8], [9].

This research was supported by the National Science Foundation under Grants ANI-03-38807 and CNS-06-25637.

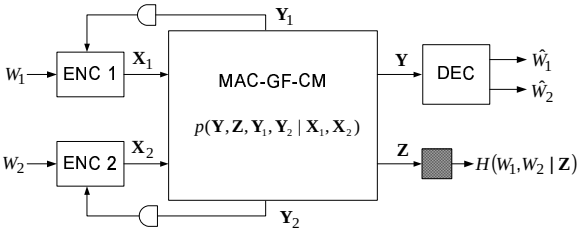

Fig. 1. The two-transmitter multiple access channel with generalized feedback and confidential messages.

The multiple access channel with generalized feedback (MAC-GF) without secrecy consideration was studied in [10]–[15]. The terminology "generalized feedback" refers to the wide range of possible situations, including the MAC without feedback, the MAC with output feedback, the MAC-GF with independent noise, the MAC with conferencing encoders, the relay channel and many others. A special case of the Gaussian fading MAC-GF is the so-called *user cooperation diversity* model proposed in [16].

In this work, we study secret communication over a multiple access channel with generalized feedback. Based on rate-splitting and decode-and-forward strategies, achievable secrecy rate regions are derived for both discrete memoryless and Gaussian MAC-GF-CMs. Several special cases of the derived achievable secrecy rate region include the rate regions of the two-user Gaussian multiple access wiretap channel [6], the relay-eavesdropper channel [8], [9], and the MISO wiretap model [17].

The remainder of the paper is organized as follows. Section II describes the system model. Section III states our main results on achievable rate regions for the discrete memoryless MAC-GF-CM. Some implications of the results are given in Section IV. Section V states our results for a Gaussian MAC-GF-CM with two numerical examples.

II. System Model

A two-user multiple access channel with generalized feedback and confidential messages consists of two transmitters, an intended receiver, and an eavesdropper, as depicted in Fig. 1. The channel is denoted by $(\mathcal{X}_1 \times \mathcal{X}_2,\ p(y_1, y_2, y, z|x_1, x_2),$

$\mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y} \times \mathcal{Z}$), where $\mathcal{X}_1$ and $\mathcal{X}_2$ are input alphabets; $\mathcal{Y}$ and $\mathcal{Z}$ are output alphabets at the intended receiver and the eavesdropper, respectively; $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are the feedback channel output alphabets; and $p(y_1, y_2, y, z|x_1, x_2)$ is the transition probability matrix. The channel is memoryless and time-invariant in the sense that

$$p(y_{1i}, y_{2i}, y_i, z_i|\mathbf{x}_1^i, \mathbf{x}_2^i, \mathbf{y}_1^{i-1}, \mathbf{y}_2^{i-1}) = p(y_{1i}, y_{2i}, y_i, z_i|x_{1i}, x_{2i})$$

where $\mathbf{x}_t^i = [x_{t1}, x_{t2}, \ldots, x_{ti}]$ for $t = 1, 2$. The superscript will be dropped when $i = n$ in order to simplify notations.

Encoder 1 and encoder 2 send independent messages $W_1 \in \mathcal{W}_1 = \{1, \ldots, M_1\}$ and $W_2 \in \mathcal{W}_2 = \{1, \ldots, M_2\}$ to the intended receiver in n channel uses, in a cooperative way by using the feedback signals $(\mathbf{y}_1, \mathbf{y}_2)$. For $t = 1, 2$, a stochastic encoder f_t for user t is specified by a matrix of conditional probabilities $f(x_{ti}|w_t, \mathbf{y}_t^{i-1})$, where $x_{ti} \in \mathcal{X}_t$, $w_t \in \mathcal{W}_t$, $\mathbf{y}_t^{i-1} \in \mathcal{Y}_t^{i-1}$ and $\sum_{x_{ti}} f(x_{ti}|w_t, \mathbf{y}_t^{i-1}) = 1$, for $i = 1, \ldots, n$, where $f(x_{ti}|w_t, \mathbf{y}_t^{i-1})$ is the probability that encoder t outputs x_{ti} when message w_t is being sent and $\mathbf{y}_t^{i-1}$ has been observed at encoder t.

The decoder uses the output sequence y^n to compute its estimate $(\hat{w}_1, \hat{w}_2)$ of (w_1, w_2). The decoding function is specified by a mapping $\phi : \mathcal{Y}^n \to \mathcal{W}_1 \times \mathcal{W}_2$.

An (M_1, M_2, n, P_e) code for the MAC with generalized feedback and confidential messages consists of two sets of n encoding functions f_{ti}, $t = 1, 2$, $i = 1, \ldots, n$ and a decoding function ϕ so that its average probability of error is

$$P_e = \sum_{(w_1, w_2)} \frac{1}{M_1 M_2} \Pr\{\phi(\mathbf{y}) \neq (w_1, w_2)|(w_1, w_2)\text{sent}\}. \tag{1}$$

The level of ignorance of the eavesdropper with respect to the confidential messages is measured by the equivocation rate $H(W_1, W_2|\mathbf{Z})/n$.

A rate pair (R_1, R_2) is achievable for the MAC with generalized feedback and confidential messages if, for any $\epsilon > 0$, there exists an (M_1, M_2, n, P_e) code so that

$$M_1 \geq 2^{nR_1},\ M_2 \geq 2^{nR_2},\ P_e \leq \epsilon \tag{2}$$

$$\text{and} \qquad R_1 + R_2 - H(W_1, W_2|\mathbf{Z})/n \leq \epsilon \tag{3}$$

for all sufficiently large n. The secrecy capacity region is the closure of the set of all achievable rate pairs (R_1, R_2).

We note that the perfect secrecy condition (3) implies

$$R_1 - \frac{1}{n} H(W_1|\mathbf{Z}) \leq \epsilon \ \text{ and } \ R_2 - \frac{1}{n} H(W_2|\mathbf{Z}) \leq \epsilon. \tag{4}$$

and therefore the *joint* perfect secrecy requirement is stronger than the *individual* perfect secrecy requirement.

This can be shown as follows:

$$\begin{aligned} H(W_1|\mathbf{Z}) &= H(W_1, W_2|\mathbf{Z}) - H(W_2|W_1, \mathbf{Z}) \\ &\geq H(W_1) + H(W_2) - n\epsilon - H(W_2|W_1, \mathbf{Z}) \\ &\geq H(W_1) - n\epsilon \\ &= n(R_1 - \epsilon). \end{aligned}$$

Similarly, we can show that (3) implies $H(W_2|\mathbf{Z}) \geq n(R_2 - \epsilon)$.

III. Discrete Memoryless Channels

We first state our results for discrete memoryless channels.

Theorem 1: (Partial Decode-and-Forward)

For a discrete memoryless MAC with generalized feedback and confidential messages, the secrecy rate region $\mathcal{R}(\pi_I)$ is achievable, where $\mathcal{R}(\pi_I)$ is the closure of the convex hull of all (R_1, R_2) satisfying

$$\begin{cases} R_1 = R_{10} + R_{12}, R_2 = R_{20} + R_{21} : \\ R_{10} + \tilde{R}_{10} \leq I(X_1; Y|X_2, V_1, U), \\ R_{20} + \tilde{R}_{20} \leq I(X_2; Y|X_1, V_2, U), \\ R_{10} + R_{20} + \tilde{R}_{10} + \tilde{R}_{20} \leq I(X_1, X_2; Y|V_1, V_2, U), \\ R_{12} + \tilde{R}_{12} \leq I(V_1; Y_2|X_2, U), \\ R_{21} + \tilde{R}_{21} \leq I(V_2; Y_1|X_1, U), \\ R_{10} + R_{20} + R_{12} + R_{21} \\ \qquad\qquad \leq I(X_1, X_2; Y) - I(X_1, X_2; Z). \\ R_{10}, R_{20}, R_{12}, R_{21} \geq 0, \\ (\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21}) \in \mathcal{C}(\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21}) \end{cases} \tag{5}$$

where

$$\mathcal{C}(\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21}) = \begin{cases} (\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21} \geq 0) : \\ \tilde{R}_{10} \leq I(X_1; Z|X_2, V_1, U), \\ \tilde{R}_{20} \leq I(X_2; Z|X_1, V_2, U), \\ \tilde{R}_{10} + \tilde{R}_{20} \leq I(X_1, X_2; Z|V_1, V_2, U), \\ \tilde{R}_{10} + \tilde{R}_{20} + \tilde{R}_{21} + \tilde{R}_{12} = I(X_1, X_2; Z). \end{cases} \tag{6}$$

and π_I denotes the class of joint probability mass functions $p(u, v_1, v_2, x_1, x_2, y_1, y_2, y, z)$ that factor as

$$p(u)p(v_1, x_1|u)p(v_2, x_2|u)p(y_1, y_2, y, z|x_1, x_2).$$

Theorem 1 illustrates a rate-splitting strategy. The rates R_1 and R_2 are split as $R_1 = R_{10} + R_{12}$ and $R_2 = R_{20} + R_{21}$, where R_{12} and R_{21} are the rates of information sent by both transmitters cooperatively to the intended receiver, while R_{10} and R_{20} are the rates of non-cooperative information sent by user 1 and user 2 individually to the receiver. The random variable U represents cooperative resolution information sent by both transmitters. V_1 represents information (at rate R_{12}) that user 1 sends to user 2 to enable cooperation. V_2 represents information (at rate R_{21}) that user 2 sends to user 1 to enable cooperation.

$\tilde{R}_{10}$, $\tilde{R}_{20}$, $\tilde{R}_{12}$ and $\tilde{R}_{21}$ represent the rates sacrificed in order to confuse the eavesdropper completely. The sum rate loss is $I(X_1, X_2; Z)$. When we set $Z = \varnothing$ (in the case of no eavesdropper), $\tilde{R}_{10} = \tilde{R}_{20} = \tilde{R}_{12} = \tilde{R}_{21} = 0$, and hence, our result becomes the rate region of the MAC with general feedback as given in [14].

The achievability scheme is based on the combination of superposition block Markov encoding [13], backward decoding [15] and random binning [1], [18]. We outline the proof in the Appendix.

Remark 1: The rate region may be enlarged by using the channel prefixing technique in [2, Lemma 4]. However, we do

not follow this approach in this paper to avoid its complicated notation and the intractability of its evaluation.

If we require that $R_1 = R_{12}$ and $R_2 = R_{21}$, that is, all information is sent cooperatively and each user can fully decode the other user's message, we have the following result.

Theorem 2: (Full Decode-and-Forward)

The secrecy rate region $\mathcal{R}(\pi_{II})$ is achievable, where $\mathcal{R}(\pi_{II})$ is the closure of the convex hull of all (R_1, R_2) satisfying

$$\begin{cases} (R_1, R_2 \geq 0): \\ R_1 \leq I(X_1; Y_2|X_2, U), \\ R_2 \leq I(X_2; Y_1|X_1, U), \\ R_1 + R_2 \leq \min\{I(X_1; Y_2|X_2, U) \\ \qquad\qquad +I(X_2; Y_1|X_1, U),\ I(X_1, X_2; Y)\} \\ \qquad\qquad -I(X_1, X_2; Z). \end{cases} \tag{7}$$

where π_{II} denotes the class of joint probability mass functions $p(u, x_1, x_2, y_1, y_2, y, z)$ that factor as

$$p(u)p(x_1|u)p(x_2|u)p(y_1, y_2, y, z|x_1, x_2).$$

IV. Some Implications of the Results

Next, we discuss some implications of our main result. We consider several special cases of Theorems 1 and 2, which are consistent with the recent results in [6], [8], [9], [17].

A. Multiple Access Wiretap Channel

An achievable rate region for the Gaussian multiple access wiretap channel is given in [6], which is the special case when neither user can obtain feedback, i.e., $Y_1 = \varnothing$ and $Y_2 = \varnothing$. We set $V_1 = V_2 = U = \varnothing$ in Theorem 1 and have the achievable region $\mathcal{R}(\pi_{MAC-WT})$, which is the closure of the convex hull of all (R_1, R_2) satisfying

$$\begin{cases} (R_1, R_2 \geq 0): \\ R_1 \leq I(X_1; Y|X_2) - I(X_1; Z), \\ R_2 \leq I(X_2; Y|X_1) - I(X_2; Z), \\ R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_1, X_2; Z), \end{cases} \tag{8}$$

where π_{MAC-WT} is the class of all distributions that factor as $p(x_1, x_2, y, z) = p(x_1)p(x_2)p(y, z|x_1, x_2)$.

B. Relay-Eavesdropper Channel

An achievable rate region for the relay-eavesdropper channel is given in [8], [9], which is the case when only user 1 has confidential messages to send and user 2 is a relay to help with the decode-and-forward strategy; therefore $R_2 = 0$ and $Y_1 = \varnothing$. We set $V_2 = \varnothing$ and $U = X_2$ in Theorem 2 and the achievable rate satisfies

$$R_1 \leq [\min\{I(X_1; Y_2|X_2), I(X_1, X_2; Y)\} - I(X_1, X_2; Z)]^+, \tag{9}$$

for all distributions that factor as $p(x_1, x_2, y_2, y, z) = p(x_1, x_2)p(y_2, y, z|x_1, x_2)$. This result is consistent with [8, Theorem 2].

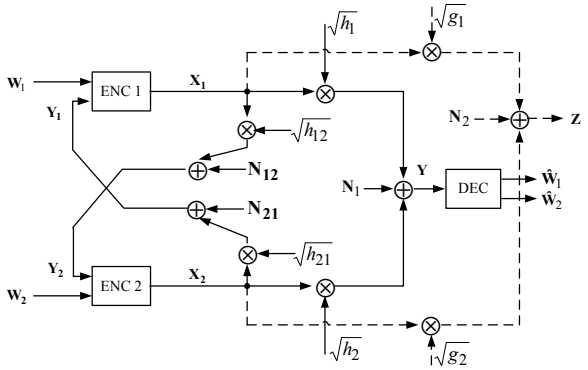

Fig. 2. A Gaussian MAC-GF with confidential messages

C. MISO Wiretap Channel

When each transmitter can obtain perfect channel feedback, i.e., $Y_2 = V_1$ and $Y_1 = V_2$, we have a virtual MISO wiretap channel. We set $V_1 = X_1$ and $V_2 = X_2$ in Theorem 1. The achievable secrecy rate of the MISO channel is given by

$$R = R_1 + R_2 \leq [I(X_1, X_2; Y) - I(X_1, X_2; Z)]^+, \tag{10}$$

for all distributions that factor as $p(x_1, x_2, y, z) = p(x_1, x_2)p(y, z|x_1, x_2)$. This result is consistent with [17].

V. Gaussian Channels

In this section, we consider a Gaussian MAC-GF-CM, as depicted in Fig. 2. Each mutually trusted user receives an attenuated and noisy version of the partner's signal and uses that signal, in conjunction with its own message, to construct the transmit signal. The intended receiver and a passive eavesdropper each get a noisy version of the sum of the attenuated signals of both users. The signal model is therefore

$$\begin{aligned} Y_1 &= \sqrt{h_{21}}X_2 + N_{21} \\ Y_2 &= \sqrt{h_{12}}X_1 + N_{12} \\ Y &= \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_1 \\ Z &= \sqrt{g_1}X_1 + \sqrt{g_2}X_2 + N_2. \end{aligned} \tag{11}$$

where h_i, g_i for $i = 1, 2$ are main and eavesdropper channel gains respectively; h_{12} and h_{21} are feedback channel gains, as shown in Fig. 2. We assume the following: the transmitted signal X_t has an average power constraint

$$\frac{1}{n}\sum_{i=1}^{n} E[X_{ti}^2] \leq P_t, \quad t = 1, 2; \tag{12}$$

and the noise terms N_1, N_2, N_{12}, and N_{21} are independent white zero-mean unit-variance complex Gaussian, i.e., $N_1 \sim \mathcal{N}(0, 1)$, $N_2 \sim \mathcal{N}(0, 1)$, $N_{12} \sim \mathcal{N}(0, 1)$, and $N_{21} \sim \mathcal{N}(0, 1)$.

Let V_1, V_2, X_1, and X_2 be jointly Gaussian with

$$\begin{aligned} V_1 &= \sqrt{P_{U1}}U + \sqrt{P_{12}}U_1' \\ V_2 &= \sqrt{P_{U2}}U + \sqrt{P_{21}}U_2' \\ X_1 &= V_1 + \sqrt{P_{10}}U_1'' \\ X_2 &= V_2 + \sqrt{P_{20}}U_2'' \end{aligned} \tag{13}$$

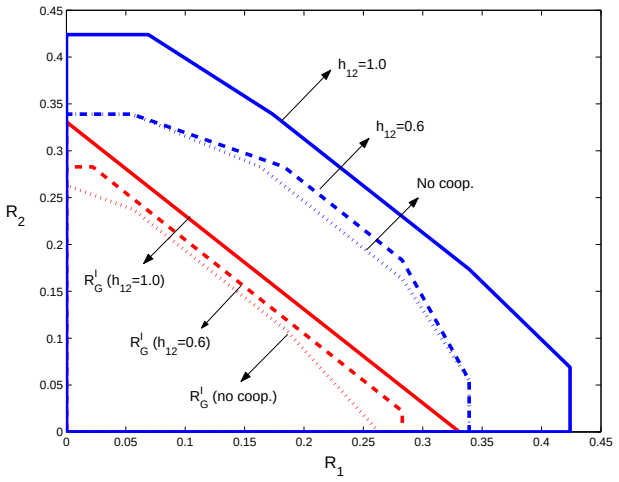

Fig. 3. Regular Rate regions and secrecy rate regions $\mathcal{R}_G^I$ for $h_1 = 0.6$, $h_2 = 0.6$, $g_1 = 0.2$, $g_2 = 0.1$, $P_1 = 1$, $P_2 = 1$ under different cooperation conditions $h_{12} = h_{21} \in [0, 0.6, 1.0]$, where $h_{12} = h_{21} = 0$ means no cooperation.

where U, U_1', U_2', U_1'', and U_2'' are independent zero mean unit variance Gaussian. The terms P_{U1}, P_{12}, P_{10}, P_{U2}, P_{21} and P_{20} denote the corresponding power allocation, where

$$P_1 = P_{U1} + P_{12} + P_{10} \quad \text{and} \quad P_2 = P_{U2} + P_{21} + P_{20}. \tag{14}$$

Following the achievability proof for the discrete memoryless channel, we have the following result for the Gaussian multiple access channel with feedback.

Theorem 3: (Partial Decode-and-Forward)

An achievable secrecy rate region $\mathcal{R}_G^I$ is the closure of the convex hull of all rate pairs (R_1, R_2) with

$$\begin{cases} R_1 = R_{10} + R_{12}, R_2 = R_{20} + R_{21}: \\ R_{10} + \tilde{R}_{10} \le C(h_1 P_{10}), \\ R_{20} + \tilde{R}_{20} \le C(h_2 P_{20}), \\ R_{10} + R_{20} + \tilde{R}_{10} + \tilde{R}_{20} \le C(h_1 P_{10} + h_2 P_{20}), \\ R_{12} + \tilde{R}_{12} \le C(\frac{h_{12} P_{12}}{1 + h_{12} P_{10}}), \\ R_{21} + \tilde{R}_{21} \le C(\frac{h_{21} P_{21}}{1 + h_{21} P_{20}}), \\ R_{10} + R_{20} + R_{12} + R_{21} \le \\ \quad C\left(h_1 P_1 + h_2 P_2 + 2\sqrt{h_1 h_2 P_{U1} P_{U2}}\right) \\ \quad -C\left(g_1 P_1 + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U1} P_{U2}}\right). \\ R_{10}, R_{20}, R_{12}, R_{21} \ge 0, \\ (\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21}) \in \mathcal{C}(\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21}) \end{cases} \tag{15}$$

where

$$\mathcal{C}(\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21}) = \begin{cases} (\tilde{R}_{10}, \tilde{R}_{20}, \tilde{R}_{12}, \tilde{R}_{21} \ge 0): \\ \tilde{R}_{10} \le C(g_1 P_{10}), \\ \tilde{R}_{20} \le C(g_2 P_{20}), \\ \tilde{R}_{10} + \tilde{R}_{20} \le C(g_1 P_{10} + g_2 P_{20}), \\ \tilde{R}_{10} + \tilde{R}_{20} + \tilde{R}_{21} + \tilde{R}_{12} = \\ \quad C\left(g_1 P_1 + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U1} P_{U2}}\right), \end{cases} \tag{16}$$

and $C(x) \triangleq (1/2)\log(1 + x)$.

As a numerical example, we show in Fig. 3 the "regular" rate region (without the secrecy constraint) and the secrecy rate region $\mathcal{R}_G^I$ for $h_1 = 0.6$, $h_2 = 0.6$, $g_1 = 0.2$, $g_2 = 0.1$, $P_1 = 1$ and $P_2 = 1$ under different cooperation conditions $h_{12} = h_{21} \in [0, 0.6, 1.0]$. When $h_{12} = h_{21} = 0$, there is no cooperation between the two encoders, which corresponds to the multiple access wiretap channel. Both the regular rate region and the secrecy rate region are significantly enlarged when the channel gains between the two users (h_{21} and h_{12}) become larger, which shows the benefits due to cooperation. Comparing with the regular rate region, the secrecy rate region suffers rate loss due to the secrecy constraint and furthermore, the secrecy rate region is increasingly dominated by the sum rate constraint, as depicted in Fig. 3.

Next, we give the secrecy rate region when each user can fully decode the message sent by the other user.

Theorem 4: (Full Decode-and-Forward)

An achievable secrecy rate region $\mathcal{R}_G^{II}$ is the closure of the convex hull of all rate pairs (R_1, R_2) with

$$\begin{cases} (R_1, R_2 \ge 0): \\ R_1 \le C(h_{12} P_{12}), \\ R_2 \le C(h_{21} P_{21}), \\ R_1 + R_2 \le \min\{C(h_{12} P_{12}) + C(h_{21} P_{21}), \\ \quad C\left(h_1 P_1 + h_2 P_2 + 2\sqrt{h_1 h_2 P_{U1} P_{U2}}\right)\} \\ \quad -C\left(g_1 P_1 + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U1} P_{U2}}\right). \end{cases} \tag{17}$$

We summarize the secrecy sum rates of partial and full decode-and-forward strategies in the following theorem.

Theorem 5: (Sum Rate) The maximal achievable sum rate in $\mathcal{R}_G^I$ is

$$\begin{aligned} R^I = \min\Big\{ & C\left(h_1 P_1 + h_2 P_2 + 2\sqrt{h_1 h_2 P_{U1} P_{U2}}\right), \\ & C\left(\frac{h_{12} P_{12}}{1 + h_{12} P_{10}}\right) + C\left(\frac{h_{21} P_{21}}{1 + h_{21} P_{20}}\right) \\ & + C\left(h_1 P_{10} + h_2 P_{20}\right)\Big\} \\ & - C\left(g_1 P_1 + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U1} P_{U2}}\right); \end{aligned} \tag{18}$$

the maximum achievable sum rate in $\mathcal{R}_G^{II}$ is

$$\begin{aligned} R^{II} = \min\Big\{ & C\left(h_1 P_1 + h_2 P_2 + 2\sqrt{h_1 h_2 P_{U1} P_{U2}}\right), \\ & C(h_{12} P_{12}) + C(h_{21} P_{21})\Big\} \\ & - C\left(g_1 P_1 + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U1} P_{U2}}\right). \end{aligned} \tag{19}$$

Furthermore, $R^I = R^{II}$ when $h_{12} \ge h_1$ and $h_{21} \ge h_2$.

The proof of Theorem 5 is provided in the Appendix.

In Fig. 4, we illustrate secrecy rate regions $\mathcal{R}_G^I$ and $\mathcal{R}_G^{II}$ for $h_1 = 0.6$, $h_2 = 0.6$, $g_1 = 0.2$, $g_2 = 0.1$, $P_1 = 1$ and $P_2 = 1$ under different cooperation conditions $h_{12} = h_{21} \in [0.2, 0.55, 1.0]$. Comparing with $\mathcal{R}_G^I$, $\mathcal{R}_G^{II}$ suffers a significant rate loss when h_{12} and h_{21} are small ($h_{12} = h_{21} = 0.2$) as expected. When h_{12} and h_{21} increase, the rate loss is reduced. When h_{12} and h_{21} are large enough, $\mathcal{R}_G^{II}$ and $\mathcal{R}_G^I$ coincide. This observation is partially verified by Theorem 5.

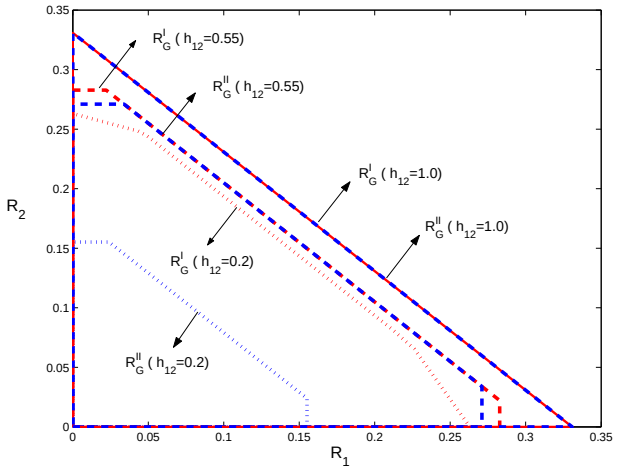

Fig. 4. Secrecy rate regions $\mathcal{R}_G^I$ and $\mathcal{R}_G^{II}$ for $h_1 = 0.6$, $h_2 = 0.6$, $g_1 = 0.2$, $g_2 = 0.1$, $P_1 = 1$, $P_2 = 1$ under different cooperation conditions: $h_{12} = h_{21} \in [0.2, 0.55, 1.0]$.

APPENDIX

Proof: (**Theorem 1**) The transmission is performed for $B+1$ blocks of length n_1, where both B and n_1 are sufficiently large and $n = (B+1)n_1$.

The random code generation is described as follows.

We fix $p(u)$, $p(v_1, x_1|u)$ and $p(v_2, x_2|u_2)$ and split the rate pair (R_1, R_2) as $R_1 = R_{12} + R_{10}$ and $R_2 = R_{21} + R_{20}$. Let

$$\tilde{R}_{12} + \tilde{R}_{10} + \tilde{R}_{21} + \tilde{R}_{20} = I(X_1, X_2; Z) - \epsilon_1 \qquad (20)$$

where $\epsilon_1 > 0$ and $\epsilon_1 \to 0$ as $n_1 \to \infty$. Let $R'_1 = R_{12} + \tilde{R}_{12}$, $R''_1 = R_{10} + \tilde{R}_{10}$, $R'_2 = R_{21} + \tilde{R}_{21}$ and $R''_2 = R_{20} + \tilde{R}_{20}$.

Code Construction:

- Generate $2^{n_1(R'_1+R'_2)}$ codewords $u^{n_1}(\mathbf{w}_0)$ by choosing the $u_i(\mathbf{w}_0)$ independently according to $p(u)$ for $i = 1, 2, \ldots, n_1$, where $\mathbf{w}_0 = 1, 2, \ldots, 2^{n_1(R'_1+R'_2)}$.
- For each $\mathbf{w}_0$, generate $2^{n_1 R'_1}$ codewords $v_1^{n_1}(\mathbf{w}_0, \mathbf{w}'_1)$ by choosing the $v_{1i}(\mathbf{w}_0, \mathbf{w}'_1)$ independently according to $p(v_1|u)$ for $i = 1, 2, \ldots, n_1$, where $\mathbf{w}'_1 = 1, 2, \ldots, 2^{n_1 R'_1}$.
- For each tuple $(\mathbf{w}_0, \mathbf{w}'_1)$, generate $2^{n_1 R''_1}$ codewords $x_1^{n_1}(\mathbf{w}_0, \mathbf{w}'_1, \mathbf{w}''_1)$ by choosing the $x_{1i}(\mathbf{w}_0, \mathbf{w}'_1, \mathbf{w}''_1)$ independently according to $p(x_1|u, v_1)$ for $i = 1, 2, \ldots, n_1$, where $\mathbf{w}''_1 = 1, 2, \ldots, 2^{n_1 R''_1}$.

The codebooks for user 2 are generated in the same way, except that there are $2^{n_1 R'_2}$ and $2^{n_1 R''_2}$ codewords in each of the $v_2^{n_1}$ and $x_2^{n_1}$ codebooks, respectively. The same codebooks will be used for all $B+1$ blocks during the encoding.

Encoding: Message w_1 has $n_1(R_1 B + R_{10})$ bits and is split into two parts: w'_1 with $n_1 R_{12} B$ bits and w''_1 with $n_1 R_{10}(B+1)$ bits, respectively. Message w_2 is similarly divided into w'_2 and w''_2. Each of the four messages w'_1, w''_1, w'_2 and w''_2 is further divided into B sub-blocks of equal lengths for each message. They are denoted by $w'_{1,b}$, $w''_{1,b}$, $w'_{2,b}$ and $w''_{2,b}$, respectively, for $b = 1, 2, \ldots, B+1$. Let

$$\mathbf{w}'_{1,b} = (w'_{1,b}, \tilde{w}'_{1,b}), \text{ and } \mathbf{w}''_{1,b} = (w''_{1,b}, \tilde{w}''_{1,b}), \qquad (21)$$

where $\tilde{w}'_{1,b}$ and $\tilde{w}''_{1,b}$ are uniformly and independently chosen at random from $\{1, 2, \ldots, 2^{n_1 \tilde{R}_{12}}\}$ and $\{1, 2, \ldots, 2^{n_1 \tilde{R}_{10}}\}$ respectively. We also choose $\mathbf{w}'_{1,0} = (1, 1)$ and $\mathbf{w}'_{1,B+1} = (1, 1)$. The $\mathbf{w}'_{2,b}$ and $\mathbf{w}''_{2,b}$ for $b = 1, \ldots, B+1$ are formed in the same way.

Suppose that encoder 1 has obtained $\mathbf{w}'_{2,b-1}$ and encoder 2 has obtained $\mathbf{w}'_{1,b-1}$ before block b. By forming $\mathbf{w}_{0,b} = (\mathbf{w}'_{1,b-1}, \mathbf{w}'_{2,b-1})$, encoder 1 transmits $x_1^n(\mathbf{w}_{0,b}, \mathbf{w}'_{1,b}, \mathbf{w}''_{1,b})$; encoder 2 transmits $x_2^n(\mathbf{w}_{0,b}, \mathbf{w}'_{2,b}, \mathbf{w}''_{2,b})$ in block b.

Decoding: All decodings are based on the typical set decoding. After the transmission of block b is completed, user 1 has seen $y_{1,b}^{n_1}$. It tries to decode $\mathbf{w}'_{2,b}$. User 2 operates in the same way.

The intended receiver waits until all $B+1$ blocks of transmission are completed and performs backward decoding. Given $y_{B+1}^{n_1}$, it tries to decode $(\mathbf{w}_{B+1}, \mathbf{w}''_{1,B+1}, \mathbf{w}''_{2,B+1})$. Assuming that the decoding for block $B+1$ is correct, the decoder next considers $y_B^{n_1}$ to decode $(\mathbf{w}_B, \mathbf{w}''_{1,B}, \mathbf{w}''_{2,B})$. The decoder continues until it decodes all blocks.

Error Analysis: Following similar steps to the error analysis for the MAC-GF in [14], we found that the intended receiver can decode all $\mathbf{w}'_b, \mathbf{w}''_b$ and therefore w_1, w_2 with error probability less than any $\epsilon > 0$ if

$$\begin{aligned}
R_{21} + \tilde{R}_{21} = R'_2 &\le I(V_2; Y_1|X_1, U),\\
R_{12} + \tilde{R}_{12} = R'_1 &\le I(V_1; Y_2|X_2, U),\\
R_{10} + \tilde{R}_{10} = R''_1 &\le I(X_1; Y|X_2, V_1, U),\\
R_{20} + \tilde{R}_{20} = R''_2 &\le I(X_2; Y|X_1, V_2, U),\\
R_{10} + R_{20} + \tilde{R}_{10} + \tilde{R}_{20} &\le I(X_1, X_2; Y|V_1, V_2, U),
\end{aligned}$$

and

$$R_{10} + R_{20} + R_{12} + R_{21} \le I(X_1, X_2; Y) - I(X_1, X_2; Z),$$

for sufficiently large n_1, where we also used (20).

Equivocation: Now we consider the equivocation,

$$\begin{aligned}
&H(W_1, W_2|\mathbf{Z})\\
&\quad = H(W_1, W_2, \mathbf{Z}) - H(\mathbf{Z})\\
&\quad = H(W_1, W_2, \mathbf{Z}, \mathbf{X}_1, \mathbf{X}_2) - H(\mathbf{X}_1, \mathbf{X}_2|W_1, W_2, \mathbf{Z}) - H(\mathbf{Z})\\
&\quad = H(\mathbf{X}_1, \mathbf{X}_2) + H(W_1, W_2, \mathbf{Z}|\mathbf{X}_1, \mathbf{X}_2) - H(Z)\\
&\qquad - H(\mathbf{X}_1, \mathbf{X}_2|W_1, W_2, \mathbf{Z})\\
&\quad \ge H(\mathbf{X}_1, \mathbf{X}_2) + H(\mathbf{Z}|\mathbf{X}_1, \mathbf{X}_2) - H(\mathbf{Z})\\
&\qquad - H(\mathbf{X}_1, \mathbf{X}_2|W_1, W_2, \mathbf{Z})\\
&\quad = H(\mathbf{X}_1, \mathbf{X}_2) - I(\mathbf{X}_1, \mathbf{X}_2; \mathbf{Z}) - H(\mathbf{X}_1, \mathbf{X}_2|W_1, W_2, \mathbf{Z}), \qquad (22)
\end{aligned}$$

and we can bound each term in the above.

The first term in (22) is given by

$$\begin{aligned}
&H(\mathbf{X}_1, \mathbf{X}_2)\\
&\quad = n_1 B(R_{10} + R_{20} + R_{12} + R_{21}) + n_1(R_{10} + R_{20})\\
&\qquad + n_1 B(\tilde{R}_{10} + \tilde{R}_{20} + \tilde{R}_{12} + \tilde{R}_{21}) + n_1(\tilde{R}_{10} + \tilde{R}_{20})\\
&\quad \ge n_1 B(R_1 + R_2) + n_1 B\left[I(X_1, X_2; Z) - \epsilon_1\right]. \qquad (23)
\end{aligned}$$

Since the channel is memoryless, the second term in (22) can be bounded by

$$I(\mathbf{X}_1, \mathbf{X}_2; \mathbf{Z}) \leq n_1(B+1)\left[I(X_1, X_2; Z) - \delta_1\right] \qquad (24)$$

where $\delta_1 \to 0$ as $n_1 \to \infty$.

We next show that the third term can be bounded by

$$H(\mathbf{X}_1, \mathbf{X}_2 | W_1, W_2, \mathbf{Z}) \leq n_1(B+1)\delta_2. \qquad (25)$$

In order to calculate $H(\mathbf{X}_1, \mathbf{X}_2 | W_1, W_2, \mathbf{Z})$, we consider the following situation: the transmitters send fixed messages $W_1 = w_1, W_2 = w_2$. Now, the eavesdropper also performs backward decoding to decode all ($\mathbf{w}_{0,b}, \mathbf{w}''_{1,b}$ and $\mathbf{w}''_{2,b}$). We can show that the error probability is less than any $\epsilon > 0$ if

$$\tilde{R}_{10} \leq I(X_1; Z | X_2, V_1, U), \qquad (26)$$

$$\tilde{R}_{20} \leq I(X_2; Z | X_1, V_2, U), \qquad (27)$$

$$\text{and} \qquad \tilde{R}_{10} + \tilde{R}_{20} \leq I(X_1, X_2; Z | V_1, V_2, U), \qquad (28)$$

for sufficiently large n_1. In other words, given message (w_1, w_2), the eavesdropper can decode $(\mathbf{X}_1, \mathbf{X}_2)$ under conditions (26), (27) and (28). Therefore, Fano's inequality implies that

$$H(\mathbf{X}_1, \mathbf{X}_2 | W_1 = w_1, W_2 = w_2, \mathbf{Z}) \leq n_1(B+1)\delta_2. \qquad (29)$$

Hence,

$$\begin{aligned} & H(\mathbf{X}_1, \mathbf{X}_2 | W_1, W_2, \mathbf{Z}) \\ = & \sum_{w_1}\sum_{w_2} p(W_1 = w_1)p(W_2 = w_2) \\ & H(\mathbf{X}_1, \mathbf{X}_2 | W_1 = w_1, W_2 = w_2, \mathbf{Z}) \\ \leq & n_1(B+1)\delta_2. \end{aligned}$$

By using (23), (24) and (25), we can rewrite (22) as

$$\begin{aligned} & H(W_1, W_2 | \mathbf{Z}) \\ \geq & n_1 B(R_1 + R_2) + n_1 B\left[I(X_1, X_2; Z) - \epsilon_1\right] \\ & - n_1(B+1)\left[I(X_1, X_2; Z) - \delta_1\right] - n_1(B+1)\delta_2 \\ \geq & n_1 B(R_1 + R_2) - n_1 I(X_1, X_2; Z) - n(B+1)\epsilon. \end{aligned}$$

The equivocation rate is therefore

$$\begin{aligned} & \frac{1}{n}H(W_1, W_2 | \mathbf{Z}) = \frac{1}{n_1(B+1)}H(W_1, W_2 | \mathbf{Z}) \\ & \geq (1 - \frac{1}{B+1})(R_1 + R_2) - \frac{1}{B+1}I(X_1, X_2; Z) - \epsilon. \end{aligned}$$

For sufficiently large B, we have

$$\frac{1}{n}H(W_1, W_2 | \mathbf{Z}) \geq R_1 + R_2 - \epsilon, \qquad (30)$$

which is the perfect secrecy requirement defined by (3).

Proof: (**Theorem 5**) The sum rates (18) and (19) can be derived based on Theorems 3 and 4, respectively. Hence, we need only to show that $P_{10} = P_{20} = 0$ in (18) is optimal to maximize R^I, when $h_{12} \geq h_1$ and $h_{21} \geq h_2$.

It is easy to show that R^I can be written as

$$R^I = \frac{1}{2}\min\{\log(T_1), \log(T_2) + \log(T_3)\},$$

where

$$T_1 = \frac{1 + h_1P_1 + h_2P_2 + 2\sqrt{h_1h_2P_{U1}P_{U2}}}{1 + g_1P_1 + g_2P_2 + 2\sqrt{g_1g_2P_{U1}P_{U2}}},$$

$$T_2 = \frac{[1 + h_{12}(P_{10} + P_{12})][1 + h_{21}(P_{20} + P_{21})]}{1 + g_1P_1 + g_2P_2 + 2\sqrt{g_1g_2P_{U1}P_{U2}}},$$

$$\text{and} \qquad T_3 = \frac{1 + h_1P_{10} + h_2P_{20}}{(1 + P_{10}h_{12})(1 + P_{20}h_{21})}.$$

Note that $P_{10} + P_{12} = P_1 - P_{U1}$ and $P_{20} + P_{21} = P_2 - P_{U2}$. Hence, given P_1, P_2, P_{U1} and P_{U2}, T_1 and T_2 are not related to P_{10} and P_{20}.

When $h_{12} \geq h_1$ and $h_{21} \geq h_2$, $T_3 \leq 1$ for any power allocation pair (P_{10}, P_{20}). Furthermore, $T_3 = 1$ can be achieved only when $P_{10} = P_{20} = 0$. Therefore, we have the desired result.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–138, Oct. 1975.

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

[3] S. K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[4] Y. Liang and H. Vincent Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, Apr. 2006, submitted.

[5] R. Liu, I. Maric, R. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory, ISIT*, July 2006.

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

[7] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions," *IEEE Trans. Inf. Theory*, Feb 2007, submitted.

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

[9] M. Yusel and E. Erkip, "The relay channel with a wire-tapper," in *Proc. 41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[10] R. King, "Multiple access channels with generalized feedback," Ph.D. dissertation, Stanford University, Stanford, CA, March 1978.

[11] A. Carleial, "Multiple access channels with different generalized feedback signals," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 841–850, Nov 1982.

[12] L. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. Inf. Theory*, vol. 30, pp. 623–629, July 1984.

[13] T. Cover and C. Leung, "An achievable rate region for the multiple access channel with feedback," *IEEE Trans. Inf. Theory*, vol. 27, pp. 292–298, May 1981.

[14] F. Willems, E. van der. Meulen, and J. Schalkwijk, "Achievable rate region for the multiple access channel with generalized feedback," in *Proc. 21st Annnal Allerton Conference on Commun. Contr. Computing*, Monticello, IL, USA, 1983, pp. 284–292.

[15] F. Willems and E. van der Meulen, "The discrete memoryless multiple access channel with cribbing encoders," *IEEE Trans. Inf. Theory*, vol. 31, pp. 313–327, May 1985.

[16] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity - part I: System description," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 1927–1938, November 2003.

[17] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Annual Conference on Information Sciences and Systems*, Baltimore, MD, March 2007.

[18] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 3, pp. 471–480, 1973.