The Discrete Memoryless Multiple Access Channel with Confidential Messages

Ruoheng Liu, Ivana Marić, Roy D. Yates and Predrag Spasojević
WINLAB, Rutgers University
Email: {liurh,ivanam,ryates,spasojev}@winlab.rutgers.edu

***Abstract*— A multiple-access channel is considered in which messages from one encoder are confidential. Confidential messages are to be transmitted with perfect secrecy, as measured by equivocation at the other encoder. The upper bounds and the achievable rates for this communication situation are determined.**

I. Introduction

We consider a two-user discrete multiple-access channel in which one user wishes to communicate confidential messages to a common receiver while the other user is permitted to eavesdrop. We refer to this channel as the *multiple access channel with confidential messages* (MACC) and denote it $(\mathcal{X}_1 \times \mathcal{X}_2, p(y, y_1|x_1, x_2), \mathcal{Y} \times \mathcal{Y}_1)$. The communications system is shown in Figure 1. The ignorance of the other user is measured by equivocation. This approach was introduced by Wyner [1] for the wiretap channel, a scenario in which a single source-destination communication is eavesdropped. Under the assumption that the channel to the wire-tapper is a degraded version of that to the receiver, Wyner determined the capacity-secrecy tradeoff. This result was generalized by Csiszár and Körner who determined the capacity region of the broadcast channel with confidential messages [2]. The Gaussian wire-tap channel was considered in [3].

In this paper, we determine the bounds on the capacity region of the MACC, under the requirement that the eavesdropping user is kept in total ignorance. The results characterize the rate penalty when compared to the conventional MAC [4], [5] due to the requirement that one message is kept secret.

It is apparent from the results that eavesdropping by user 1 will hurt the achievable rate of user 2. As illustrated in the last section by an example in which the half-duplex constraint is imposed, the eavesdropper should give up on listening all together, thus maximizing rates of both users. The moral of the example is that either user 1 will make both himself and the other user miserable by eavesdropping more and thus reducing both its own and other user's ability to transmit; or, it will make both of them happy if it decides not to listen. We note that, although user 2 cannot know exact times when user 1 is eavesdropping, it is enough for user 2 to know the eavesdropping probability (or equivalently, the fraction of time user 1 is listening), to adjust its code rate accordingly. This information can be considered public, since it is known to the common receiver.

[1]This work was supported by NSF Grant NSF ANI 0338805.

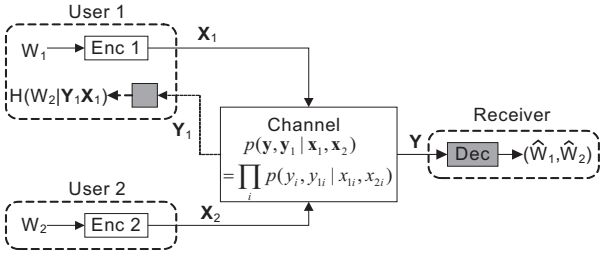

Fig. 1. System Model

II. Channel model and statement of result

A discrete memoryless MAC with confidential messages consists of finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}, \mathcal{Y}_1$ and a conditional probability distribution $p(y, y_1|x_1, x_2)$. Symbols $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$ are channel inputs and $(y, y_1) \in \mathcal{Y} \times \mathcal{Y}_1$ are channel outputs at the receiver and encoder 1, respectively. The channel $p(y|x_1, x_2)$ is a MAC channel, and the channel $p(y, y_1|x_1, x_2)$ is a wire-tap channel. Each encoder t, $t = 1, 2$, wishes to send an independent message $W_t \in \{1, \ldots, M_t\}$ to a common receiver in n channel uses. The channel is memoryless and time-invariant in the sense that

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

where $\mathbf{x}_t^i = \begin{bmatrix} x_{t,1}, & \ldots, & x_{t,i} \end{bmatrix}$. To simplify notation, we drop the superscript when $i = n$. A deterministic encoder g for user 1 is a mapping $g : \mathcal{W}_1 \to \mathcal{X}_1^n$ generating codewords

$$\mathbf{x}_1 = g(w_1). \quad (2)$$

A stochastic encoder f for user 2 is specified by a matrix of conditional probabilities $f(\mathbf{x}_2|w_2)$, where $\mathbf{x}_2 \in \mathcal{X}_2^n$, $w_2 \in \mathcal{W}_2$, is the private message set, and

$$\sum_{\mathbf{x}_2} f(\mathbf{x}_2|w_2) = 1.$$

Note that $f(\mathbf{x}_2|w_2)$ is the probability that the message w_2 is encoded as channel input $\mathbf{x}_2$.

The decoding function is given by a mapping $\phi : \mathcal{Y}^n \to \mathcal{W}_1 \times \mathcal{W}_2$.

The implicit assumption in our model is that user 1 observes the sequence $\mathbf{Y}_1$ in block fashion. This prevents user 1 from using symbols Y_1 for encoding its own messages, as reflected in the encoding function (2). This restriction of our model is

made for the sole purpose of making the problem easier to solve and understand.

An (M_1, M_2, n, P_e) code for the channel consists of two encoding functions f, g, decoding function ϕ such that the *average probability of error* of the code is

$$P_e = \sum_{(w_1,w_2)} \frac{1}{M_1 M_2} P\{\phi(\mathbf{y}) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}\} \quad (3)$$

The level of ignorance of user 1 with respect to the confidential message is measured by the normalized equivocation $(1/n)H(W_2|\mathbf{X}_1, \mathbf{Y}_1)$.

A rate pair (R_1, R_2) is achievable for the MACC if, for any $\epsilon > 0$, there exists a (M_1, M_2, n, P_e) code such that

$$M_t \geq 2^{nR_t} \quad t = 1, 2, \quad P_e \leq \epsilon \quad (4)$$

$$R_2 - \frac{1}{n} H(W_2|\mathbf{X}_1, \mathbf{Y}_1) \leq \epsilon. \quad (5)$$

The capacity region of the MACC is the closure of the set of all achievable rate pairs (R_1, R_2).

The next two theorems show the outer bound and the achievable rates and are the main results of this paper.

Let $\mathcal{C}_U$ be a closure of the union of all (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2) \\ R_2 &\leq I(V; Y|U, X_1) - I(V; Y_1|U, X_1) \\ R_1 + R_2 &\leq I(X_1, V; Y) - I(V; Y_1|U, X_1) \end{aligned} \quad (6)$$

for some joint distribution

$$\begin{aligned} &p(u, v, x_1, x_2, y, y_1) \\ &= p(u)p(v|u)p(x_1|u)p(x_2|v)p(y, y_1|x_1, x_2) \end{aligned} \quad (7)$$

where U and V are auxiliary random variables satisfying $U \to V \to (X_1, X_2) \to (Y, Y_1)$.

Theorem 1: (Outer Bound) For any achievable rate pair (R_1, R_2) in MACC it holds that $(R_1, R_2) \in \mathcal{C}_U$.

Theorem 2: (Achievability) The rates in the closure of the union of all (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\leq I(X_1; Y|U, V) \\ R_2 &\leq I(V; Y|U, X_1) - I(V; Y_1|U, X_1) \\ R_1 + R_2 &\leq I(X_1, V; Y|U) - I(V; Y_1|U, X_1) \end{aligned} \quad (8)$$

for a joint distribution $p(u, v, x_1, x_2, y, y_1)$ that factors as (7).

III. Outer Bound

Proof: (Theorem 1)

We next show that any achievable rate pair satisfies

$$R_1 \leq I(X_1; Y|X_2, Q) \quad (9)$$

$$R_2 \leq I(V; Y|U, X_1, Q) - I(V; Y_1|U, X_1, Q) \quad (10)$$

$$R_1 + R_2 \leq I(U, X_1, V; Y|Q) - I(V; Y_1|U, X_1, Q) \quad (11)$$

for some product distribution $U \to V \to (X_1, X_2) \to (Y, Y_1)$ that factor as (7) and an independent timesharing random variable Q. Then, the approach of [6, Thm. 14.3.3] and the observation that Markovity $U \to V \to (X_1, X_2) \to Y$ implies $U \to (V, X_1) \to Y$, will prove the claim.

Consider a code (M_1, M_2, n, P_e) for the MACC. Applying Fano's inequality results in

$$H(W_1, W_2|\mathbf{Y}) \leq P_e \log(M_1 M_2 - 1) + h(P_e) \triangleq n\delta_n \quad (12)$$

where $\delta_n \to 0$ as $P_e \to 0$. It follows that

$$H(W_1, W_2|\mathbf{Y}) = H(W_1|\mathbf{Y}) + H(W_2|\mathbf{Y}, W_1) \leq n\delta_n \quad (13)$$

We first consider the bound on R_1.

$$\begin{aligned} nR_1 &= H(W_1) \\ &= I(W_1; \mathbf{Y}) + H(W_1|\mathbf{Y}) \\ &\leq^{(a)} I(W_1; \mathbf{Y}) + n\delta_n \\ &\leq^{(b)} I(\mathbf{X}_1(W_1); \mathbf{Y}) + n\delta_n \\ &\leq^{(c)} I(\mathbf{X}_1; \mathbf{Y}|\mathbf{X}_2) + n\delta_n \\ &=^{(d)} \sum_{i=1}^{n} H(Y_i|\mathbf{X}_2, \mathbf{Y}^{i-1}) - \sum_{i=1}^{n} H(Y_i|\mathbf{Y}^{i-1}, \mathbf{X}_1, \mathbf{X}_2) \\ &\quad + n\delta_n \\ &\leq^{(e)} \sum_{i=1}^{n} H(Y_i|X_{2i}) - \sum_{i=1}^{n} H(Y_i|X_{1i}, X_{2i}) + n\delta_n \\ &= \sum_{i=1}^{n} I(X_{1,i}; Y_i|X_{2,i}) + n\delta_n \end{aligned} \quad (14)$$

where (a) follows from from Fano's inequality (13); (b) from (2); (c) from the independence of $\mathbf{X}_1, \mathbf{X}_2$; (d) from the chain rule; (e) from the fact that the conditioning decreases entropy and from the memoryless property of the channel (1).

Following the approach in [6, Sec. 14.3.4], we introduce a uniformly distributed random variable $Q, Q \in \{1, \ldots, n\}$. Equation (14) becomes

$$\begin{aligned} nR_1 &\leq \sum_{i=1}^{n} I(X_{1,i}; Y_i|X_{2,i}) + n\delta_n \\ &= \sum_{i=1}^{n} I(X_{1,i}; Y_i|X_{2,i}, Q = i) + n\delta_n \\ &= nI(X_{1,Q}; Y_Q|X_{2,Q}, Q) + n\delta_n \\ &= nI(X_1; Y|X_2, Q) + n\delta_n \end{aligned} \quad (15)$$

where $X_1 = X_{1,Q}, X_2 = X_{2,Q}, Y = Y_Q$. Distributions of new variables depend on Q in the same way as the distributions of $X_{1,i}, X_{2,i}, Y_i$ depend on i.

Next, we derive the bound on R_2. Note that the perfect security (5) implies

$$nR_2 - n\epsilon \leq H(W_2|\mathbf{X}_1, \mathbf{Y}_1). \quad (16)$$

Hence, we consider the bound on $H(W_2|\mathbf{X}_1, \mathbf{Y}_1)$.

$$\begin{aligned} &H(W_2|\mathbf{X}_1, \mathbf{Y}_1) \\ &\quad = H(W_2|\mathbf{X}_1) - I(W_2; \mathbf{Y}_1|\mathbf{X}_1) \\ &\quad = I(W_2; \mathbf{Y}|\mathbf{X}_1) + H(W_2|\mathbf{Y}, \mathbf{X}_1) - I(W_2; \mathbf{Y}_1|\mathbf{X}_1) \\ &\quad \leq I(W_2; \mathbf{Y}|\mathbf{X}_1) - I(W_2; \mathbf{Y}_1|\mathbf{X}_1) + n\delta_n \end{aligned} \quad (17)$$

where the inequality follows from Fano's inequality (13). We next use a similar approach as in [2, Sect.V] to bound equivocation $H(W_2|\mathbf{X}_1, \mathbf{Y}_1)$ in (17).

We denote $\tilde{\mathbf{Y}}_1^{i+1} = [Y_{1,i+1}, \ldots, Y_{1,n}]$ and use the chain rule to obtain

$$\begin{aligned} &I(W_2; \mathbf{Y}|\mathbf{X}_1) \\ &\quad= \sum_{i=1}^{n} I(W_2; Y_i|\mathbf{Y}^{i-1}, \mathbf{X}_1) \\ &\quad= \sum_{i=1}^{n} I(W_2, ; Y_i|\tilde{\mathbf{Y}}_1^{i+1}, \mathbf{Y}^{i-1}, \mathbf{X}_1) + \Sigma_1 - \Sigma_2 \quad (18) \\ &I(W_2; \mathbf{Y}_1|\mathbf{X}_1) \\ &\quad= \sum_{i=1}^{n} I(W_2; Y_{1i}|\tilde{\mathbf{Y}}_1^{i+1}, \mathbf{X}_1) \\ &\quad= \sum_{i=1}^{n} I(W_2, ; Y_{1,i}|\tilde{\mathbf{Y}}_1^{i+1}, \mathbf{Y}^{i-1}, \mathbf{X}_1) + \hat{\Sigma}_1 - \hat{\Sigma}_2 \quad (19) \end{aligned}$$

where

$$\begin{aligned} \Sigma_1 &= \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_1^{i+1}; Y_i|\mathbf{Y}^{i-1}, \mathbf{X}_1) \\ \Sigma_2 &= \sum_{i=1}^{n} I(\tilde{\mathbf{Y}}_1^{i+1}; Y_i|\mathbf{Y}^{i-1}, \mathbf{X}_1, W_2) \\ \hat{\Sigma}_1 &= \sum_{i=1}^{n} I(\mathbf{Y}^{i-1}; Y_{1,i}|\tilde{\mathbf{Y}}_1^{i+1}, \mathbf{X}_1) \\ \hat{\Sigma}_2 &= \sum_{i=1}^{n} I(\mathbf{Y}^{i-1}; Y_{1,i}|\tilde{\mathbf{Y}}_1^{i+1}, \mathbf{X}_1, W_2). \end{aligned}$$

Lemma 1: $\Sigma_1 = \hat{\Sigma}_1$ and $\Sigma_2 = \hat{\Sigma}_2$.

Proof: Proof follows the approach in [2, Lemma 7]. ∎

We let

$$U_i = (\mathbf{Y}^{i-1}\tilde{\mathbf{Y}}_1^{i+1}\mathbf{X}_1^{i-1}\tilde{\mathbf{X}}_1^{i+1}) \quad (20)$$

$$V_i = (W_2, U_i) \quad (21)$$

in (18) and (19) and obtain respectively

$$I(W_2; \mathbf{Y}|\mathbf{X}_1) = \sum_{i=1}^{n} I(V_i; Y_i|U_i, X_{1,i}) + \Sigma_1 - \Sigma_2 \quad (22)$$

$$I(W_2; \mathbf{Y}_1|\mathbf{X}_1) = \sum_{i=1}^{n} I(V_i; Y_{1,i}|U_i, X_{1,i}) + \hat{\Sigma}_1 - \hat{\Sigma}_2 \quad (23)$$

We follow the same approach as in (15) to obtain

$$\begin{aligned} \frac{1}{n}\sum_{i=1}^{n} I(V_i; Y_i|U_i, X_{1,i}) &= \frac{1}{n}\sum_{i=1}^{n} I(V_i; Y_i|U_i, X_{1,i}, Q = i) \\ &= I(V_Q; Y_Q|U_Q, X_{1,Q}, Q) \\ &= I(V; Y|U, X_1, Q) \quad (24) \end{aligned}$$

where $V = V_Q, Y = Y_Q, X_1 = X_{1,Q}, U = U_Q$. Similarly,

$$\frac{1}{n}\sum_{i=1}^{n} I(V_i; Y_{1,i}|U_i, X_{1,i}) = I(V; Y_1|U, X_1, Q) \quad (25)$$

where $Y_1 = Y_{1,Q}$. From the memoryless property of the channel (1), it follows that $V \to (X_1, X_2) \to (Y, Y_1)$.

Using (24) in (22), we obtain

$$I(W_2; \mathbf{Y}|\mathbf{X}_1) = nI(V; Y|U, X_1, Q) + \Sigma_1 - \Sigma_2. \quad (26)$$

Similarly, using (25) in (23)

$$I(W_2; \mathbf{Y}_1|\mathbf{X}_1) = nI(V; Y_1|U, X_1, Q) + \hat{\Sigma}_1 - \hat{\Sigma}_2. \quad (27)$$

Substituting (26) and (27) in (17) results in

$$\begin{aligned} &\frac{1}{n}H(W_2|\mathbf{X}_1, \mathbf{Y}_1) \\ &\quad\le I(V; Y|U, X_1, Q) - I(V; Y_1|U, X_1, Q) + \delta_n. \quad (28) \end{aligned}$$

Using (16) in (28), we obtain the desired the bound (10) on rate R_2.

We next prove the bound on the sum rate (11).

$$\begin{aligned} n(R_1 + R_2) &= I(W_1, W_2; \mathbf{Y}) + H(W_1, W_2|\mathbf{Y}) \\ &\le I(\mathbf{X}_1, W_2; \mathbf{Y}) + n\delta_n \\ &\le I(\mathbf{X}_1, W_2; \mathbf{Y}) - [H(W_2) \\ &\quad - H(W_2|\mathbf{X}_1, \mathbf{Y}_1) - n\epsilon] + n\delta_n \\ &= I(\mathbf{X}_1; \mathbf{Y}) + I(W_2; \mathbf{Y}|\mathbf{X}_1) \\ &\quad - I(W_2; \mathbf{Y}_1|\mathbf{X}_1) + n(\delta_n + \epsilon) \end{aligned} \quad (29)$$

where the second inequality follows from the perfect secrecy (5). Using (22), (23) and Lemma 1, we have

$$\begin{aligned} &I(W_2; \mathbf{Y}|\mathbf{X}_1) - I(W_2; \mathbf{Y}_1|\mathbf{X}_1) \\ &\quad= \sum_{i=1}^{n}\big[I(W_2; Y_i|U_i, X_{1,i}) - I(W_2; Y_{1,i}|U_i, X_{1,i})\big] \quad (30) \end{aligned}$$

Hence, (29) can be rewritten as

$$\begin{aligned} &n(R_1 + R_2) \\ &\le \sum_{i=1}^{n}\big[I(\mathbf{X}_1; Y_i|\mathbf{Y}^{i-1}) + I(W_2; Y_i|U_i, X_{1,i}) \\ &\quad - I(W_2; Y_{1,i}|U_i, X_{1,i})\big] + n(\delta_n + \epsilon) \\ &\le \sum_{i=1}^{n}\big[I(\mathbf{X}_1, \mathbf{Y}^{i-1}, \tilde{\mathbf{Y}}_1^{i+1}; Y_i) + I(W_2; Y_i|U_i, X_{1,i}) \\ &\quad - I(W_2; Y_{1,i}|U_i, X_{1,i})\big] + n(\delta_n + \epsilon) \\ &= \sum_{i=1}^{n}\big[I(V_i, X_{1,i}; Y_i) - I(V_i; Y_{1,i}|U_i, X_{1,i})\big] + n(\delta_n + \epsilon) \\ &\le \sum_{i=1}^{n}\big[I(V_i, U_i, X_{1,i}; Y_i) - I(V_i; Y_{1,i}|U_i, X_{1,i})\big] + n(\delta_n + \epsilon) \end{aligned}$$

where U_i and V_i are defined in (20) and (21). Using the same time-sharing variable approach as before we obtain the sum rate bound (11). Moreover, the Markovity $X_{1,i} - U_i - V_i$ can easily be verified. ∎

IV. Achievability

Proof: (Theorem 2)

Fix $p(u)$, $p(x_1|u)$, $p(v|u)$ and $p(x_2|v)$. Let

$$R_3 = R_2 + I(V; Y_1|X_1, U). \tag{31}$$

Codebook generation: Generate a random typical sequence $\mathbf{u}$, with probability $p(\mathbf{u}) = \prod_{i=1}^{n} p(u_i)$. We assume that both transmitters and the common receiver know the sequence $\mathbf{u}$.

Generate $M_1 = 2^{nR_1}$ sequences $\mathbf{x}_1$, each with probability $p(\mathbf{x}_1|\mathbf{u}) = \prod_{i=1}^{n} p(x_{1,i}|u_i)$. Label them $\mathbf{x}_1(w_1)$, $w_1 \in \{1, \ldots, M_1\}$.

Generate $M_3 = 2^{nR_3}$ sequences $\mathbf{v}$ with probability $p(\mathbf{v}|\mathbf{u}) = \prod_{i=1}^{n} p(v_i|u_i)$. Label them $\mathbf{v}(w_2, l)$, $w_2 \in \{1, \ldots, 2^{nR_2}\}$, $l \in \{1, \ldots, 2^{nI(V;Y_1|X_1,U)}\}$.

Encoding: To send message $w_1 \in \mathcal{W}_1$, user 1 sends codeword $\mathbf{x}_1(w_1)$. To send message $w_2 \in \mathcal{W}_2$, user 2 uses stochastic encoder f, and encoder 2 uniformly randomly chooses an codeword $\mathbf{v}(w_2, l)$. That is, the encoder chooses randomly a codeword $\mathbf{v}(w_2, l)$ from a bin w_2. Finally, user 2 generates the channel input sequences $\mathbf{x}_2$ according to $p(x_2|v)$.

Decoding: Let $A_\epsilon^{(n)}$ denote the set of typical $(\mathbf{u}, \mathbf{x}_1, \mathbf{v}, \mathbf{y})$ sequences. Decoder chooses the pair (w_1, w_2) such that $(\mathbf{u}, \mathbf{x}_1(w_1), \mathbf{v}(w_2, l), \mathbf{y}) \in A_\epsilon^{(n)}$ if such a pair (w_1, w_2) exists and is unique; otherwise, an error is declared.

Probability of error: Define the events

$$E_{w_1,w_2} = \{(\mathbf{u}, \mathbf{x}_1(w_1), \mathbf{v}(w_2, l), \mathbf{y}) \in A_\epsilon^{(n)}\}. \tag{32}$$

Without loss of generality, we can assume that $(w_1, w_2) = (1, 1)$ was sent. From the union bound, the error probability is given by

$$\begin{aligned} P_e \leq & P\{E_{1,1}^c|(1,1)\} + \sum_{w_1 \neq 1} P\{E_{w_1,1}|(1,1)\} \\ & + \sum_{w_2 \neq 1} \sum_{l} P\{E_{1,w_2}|(1,1)\} \\ & + \sum_{w_1 \neq 1} \sum_{w_2 \neq 1} \sum_{l} P\{E_{w_1,w_2}|(1,1)\} \end{aligned} \tag{33}$$

From the AEP and [6, Thm. 14.2.1, 14.2.3], it follows that

$$P\{E_{1,1}^c|(1,1)\} \leq \delta \tag{34}$$

$$P\{E_{w_1,1}|(1,1)\} \leq 2^{-n[I(X_1;Y|V,U)-\delta]} \tag{35}$$

$$P\{E_{1,w_2}|(1,1)\} \leq 2^{-n[I(V;Y|X_1,U)-\delta]} \tag{36}$$

$$P\{E_{w_1,w_2}|(1,1)\} \leq 2^{-n[I(X_1,V;Y|U)-\delta]} \tag{37}$$

where $\delta \to 0$ as $n \to \infty$. Hence, (33) is bounded by

$$\begin{aligned} P_e \leq & \delta + 2^{nR_1} 2^{-n(I(X_1;Y|V,U)-\delta)} + 2^{nR_3} 2^{-n(I(V;Y|X_1,U)-\delta)} \\ & + 2^{n(R_1+R_3)} 2^{-n(I(X_1,V;Y|U)-\delta)} \end{aligned} \tag{38}$$

implying that we must choose

$$R_1 \leq I(X_1; Y|V, U) \tag{39}$$

$$R_3 \leq I(V; Y|X_1, U) \tag{40}$$

$$R_1 + R_3 \leq I(X_1, V; Y|U) \tag{41}$$

to guarantee $P_e \to 0$ as n gets large.

Equivocation: We consider the normalized equivocation.

$$\begin{aligned} & H(W_2|\mathbf{Y}_1, \mathbf{X}_1) \\ & \quad \geq H(W_2|\mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) \\ & \quad = H(W_2, \mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) - H(\mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) \\ & \quad = H(W_2, \mathbf{Y}_1, \mathbf{V}|\mathbf{X}_1, \mathbf{U}) - H(\mathbf{V}|W_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) \\ & \qquad - H(\mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) \\ & \quad = H(W_2, \mathbf{V}|\mathbf{X}_1, \mathbf{U}) + H(\mathbf{Y}_1|W_2, \mathbf{V}, \mathbf{X}_1, \mathbf{U}) \\ & \qquad - H(\mathbf{V}|W_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) - H(\mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) \\ & \quad \geq H(\mathbf{V}|\mathbf{X}_1, \mathbf{U}) + H(\mathbf{Y}_1|\mathbf{V}, \mathbf{X}_1, \mathbf{U}) \\ & \qquad - H(\mathbf{V}|W_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) - H(\mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) \\ & \quad = H(\mathbf{V}|\mathbf{X}_1, \mathbf{U}) - H(\mathbf{V}|W_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) \\ & \qquad - I(\mathbf{V}; \mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) \end{aligned} \tag{42}$$

The first term in (42) is given by

$$H(\mathbf{V}|\mathbf{X}_1, \mathbf{U}) = H(\mathbf{V}|\mathbf{U}) = nR_3 \tag{43}$$

where the first equality follows from the Markov chain $\mathbf{V} - \mathbf{U} - \mathbf{X}_1$, and the second equality because given $\mathbf{U} = \mathbf{u}$, $\mathbf{V}$ has 2^{nR_3} possible values with equal probability.

We next show that $H(\mathbf{V}|W_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) \leq n\delta_1$, where $\delta_1 \to 0$ as $n \to \infty$. Let $W_2 = w_2$. User 2 then sends a codeword $\mathbf{v}(w_2, l)$. Let λ_{w_2} denote the average probability of error that user 1 does not decode $\mathbf{v}(w_2, l)$ correctly given the information $W_2 = w_2$. Following the joint typical decoding approach, we have $\lambda_{w_2} \to 0$ as $n \to \infty$. Therefore, Fano's inequality implies that

$$H(\mathbf{V}|W_2 = w_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) \leq 1 + \lambda_{w_2}(nR_3 - nR_2) \triangleq n\delta_1.$$

Hence

$$\begin{aligned} & H(\mathbf{V}|W_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) = \\ & \qquad \sum_{w_2 \in \mathcal{W}_2} p(W_2 = w_2) H(\mathbf{V}|W_2 = w_2, \mathbf{Y}_1, \mathbf{X}_1, \mathbf{U}) \leq n\delta_1. \end{aligned} \tag{44}$$

Finally, the third term in (42) can be bounded by

$$I(\mathbf{V}; \mathbf{Y}_1|\mathbf{X}_1, \mathbf{U}) \leq nI(V; Y_1|X_1, U) + n\delta_2 \tag{45}$$

where $\delta_2 \to 0$ as $n \to \infty$. The proof follows the proof in [1, Lemma 8].

Therefore, by using (31), (43), (44), and (45), we can rewrite (42) as

$$\begin{aligned} H(W_2|\mathbf{X}_1, \mathbf{Y}_1) & \geq nR_3 - nI(V; Y_1|X_1, U) - n(\delta_1 + \delta_2) \\ & = nR_2 - n\epsilon \end{aligned} \tag{46}$$

where $\epsilon \triangleq \delta_1 + \delta_2$. ■

V. Discussion and Implications

To show the impact of secret communication on the achievable rates in MACC, we present two examples: the half-duplex MACC and the Gaussian MACC. To simplify calculations, we consider the following corollary which gives a weaker inner bound used in the rest of the paper.

Corollary 1: The rates in the closure of the convex hull of all (R_1, R_2) satisfying

$$R_1 \leq I(X_1; Y|X_2) \tag{47}$$
$$R_2 \leq I(X_2; Y|X_1) - I(X_2; Y_1|X_1) \tag{48}$$
$$R_1 + R_2 \leq I(X_1, X_2; Y) - I(X_2; Y_1|X_1) \tag{49}$$

for fixed product distribution $p(x_1)p(x_2)$ on $\mathcal{X}_1 \times \mathcal{X}_2$ is achievable in MACC.

Proof: Corollary follows by choosing $V = X_2$ and U independent from X_1 and X_2 in Theorem 2. ∎

Binary inputs are to be communicated from the both users under a half-duplex model in which user 1 cannot listen and transmit at the same time. Therefore $X_2 \in \{0, 1\}$ and $X_1 \in \{\varnothing, 0, 1\}$. Null symbol $\varnothing$ models the listening period of user 1. When $X_1 = \varnothing$, user 1 observes the output $Y_1 = Y$; when user 1 transmits, $X_1 \in \{0, 1\}$, the output Y_1 is the null symbol, no matter what user 2 sends. When both users transmit, the MAC channel to the destination is given by the mod 2 sum $Y = X_1 \oplus X_2$. Otherwise, $Y = X_2$. In summary,

$$Y = X_1 \oplus X_2, \quad Y_1 = \varnothing, \qquad \text{if } X_1 \neq \varnothing \tag{50}$$
$$Y = X_2, \quad Y_1 = Y, \qquad \text{if } X_1 = \varnothing \tag{51}$$

Denote $P = P[X_1 = 1]$ and $D = P[X_1 = \varnothing]$. Rates (47)-(49) for this channel can be shown to be

$$R_1 \leq h(P) \tag{52}$$
$$R_2 \leq H(X_2)(1 - D) \tag{53}$$
$$R_1 + R_2 \leq H(Y) - H(X_2)D. \tag{54}$$

If we assume the inputs at user 2 are equally likely, then $H(Y) = 1$. The rates (52)-(54) become

$$R_1 \leq h(P) \tag{55}$$
$$R_2 \leq 1 - D \tag{56}$$
$$R_1 + R_2 \leq 1 - D \tag{57}$$

and the secrecy constraint (56) becomes irrelevant. The achievable rates are determined by the amount of time user 1 listens: the more user 1 listens, the more user 2 must equivocate rather than communicate. The best strategy is then for user 1 to transmit all the time $(D = 0)$, thus achieving the full capacity region of the conventional MAC.

In the other limiting case in which user 1 only listens ($D = 1$), user 2 cannot send information because user 1 hears it ($Y_1 = X_2$). In fact, the channel reduces to the special case of the channel considered in [2] and the conclusion is agreeable with that of [2]. In the example, the fact that $R_2 = 0$ is due to the very special channel $Y_1 = Y$. In the more general case in which Y_1 is a noiser observation of X_2 than Y, user 2 can still "squeeze" some information through even if user 1 listens all the time. Nonetheless, this example illustrates the fundamental behavior in the MACC, that can be observed from Corollary 1, Eq. (48): the more user 1 decides to listen, the more user 2 has to equivocate and his achievable rate is lower.

We next consider the Gaussian channel

$$Y = X_1 + X_2 + Z \tag{58}$$
$$Y_1 = X_2 + Z_1 \tag{59}$$

where Z and Z_1 are independent zero-mean Gaussian random variables with variance N and N_1, respectively. The code definition is the same as given in Section II with the addition of the power constraints

$$\frac{1}{n}\sum_{i=1}^{n} E[X_{ti}^2] \leq P_t, \qquad t = 1, 2. \tag{60}$$

Corollary 2: The rates in the closure of the convex hull of all (R_1, R_2) satisfying

$$R_1 \leq C\left(\frac{P_1}{N}\right) \tag{61}$$
$$R_2 \leq C\left(\frac{P_2}{N}\right) - C\left(\frac{P_2}{N_1}\right) \tag{62}$$
$$R_1 + R_2 \leq C\left(\frac{P_1 + P_2}{N}\right) - C\left(\frac{P_2}{N_1}\right). \tag{63}$$

Corollary follows from Theorem 2 by independently choosing $X_t \sim \mathcal{N}[0, P_t]$ for $t = 1, 2$.

Future Work

It is conceivable that the outer bounds given in Theorem 1 can be strengthened to coincide with the lower bounds of Theorem 2. Investigating this possibility and determining the MACC capacity are the subjects of our future work. Moreover, the formulation of this problem in which the objective is to maximize rates under the secrecy constraint follows the definition of Wyner [1]. However, different objectives can be envisioned, in which user 1 is more interested in eavesdropping than in maximizing its rate. It would be interesting to compare the conclusions that follow from the two problem formulations.

References

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

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

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

[4] H. Liao, "Multiple access channels," *Ph.D. Thesis, University of Hawaii*, 1972.

[5] R. Ahlswede, "Multi-way communication channels," in *Int. Symp. Inf, Th.*, 1971, pp. 23–52.

[6] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley Sons, Inc., 1991.