ISIT'2013 1569719575

Secrecy capacity region of a class of two-user Gaussian MIMO BC with degraded message sets

Hon-Fah Chong and Ying-Chang Liang
1 Fusionopolis Way, #21-01 Connexis (South Tower),
Institute for Infocomm Research, Singapore 138632.
E-mail: chong.hon.fah@ieee.org, ycliang@i2r.a-star.edu.sg

***Abstract*—We consider a two-user broadcast channel (BC) with two-degraded message sets where a common message M_2 is intended for both receivers and a private message M_1 is intended for receiver one. There is an eavesdropper whose channel is stochastically degraded with respect to both receivers and both messages must be kept confidential from the eavesdropper. However, we do not assume any form of degradedness between the two receivers. We first characterize the capacity region of this class of discrete memoryless BC. Next, we consider the two-user Gaussian MIMO BC with two-degraded message sets and an eavesdropper. We characterize the capacity region for the case where the eavesdropper is only required to be stochastically degraded with respect to receiver one. We make use of the channel enhancement technique as well as an extremal entropy inequality of Liu et al. that was derived using the generalized Costa's entropy power inequality (EPI).**

I. Introduction

In [1], Liu et al. considered the following Gaussian MIMO BC with two receivers and an eavesdropper (see Figure 1):

$$\begin{aligned} \boldsymbol{Z} &= \boldsymbol{X} + \boldsymbol{N}^{(z)} \\ \boldsymbol{Y} &= \boldsymbol{X} + \boldsymbol{N}^{(y)} \\ \boldsymbol{W} &= \boldsymbol{X} + \boldsymbol{N}^{(w)} \end{aligned} \tag{1}$$

where $\mathbf{X}$ is a real input vector of size $t \times 1$; $\boldsymbol{N}^{(w)}$, $\boldsymbol{N}^{(y)}$ and $\boldsymbol{N}^{(z)}$ are real Gaussian random vectors of size $t \times 1$ with zero mean and covariance matrices (assumed to be strictly positive-definite) $\mathbf{N}^{(w)}$, $\mathbf{N}^{(y)}$ and $\mathbf{N}^{(z)}$, respectively; and $\boldsymbol{Z}$, $\boldsymbol{Y}$ and $\boldsymbol{W}$ are real output vectors of receiver 1, receiver 2 and the eavesdropper, respectively. A matrix constraint is imposed on the input $\mathbb{E}\left[\mathbf{X}\mathbf{X}^T\right] \preceq \mathbf{S}$, where $\mathbf{S} \succeq 0$.

The transmitter has a common message intended for both receivers and a private message intended for receiver 1. Both messages are to be kept perfectly secret from the eavesdropper. Furthermore, Liu et al. imposed the following constraint on the noise covariance matrices: $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(y)} \preceq \mathbf{N}^{(w)}$.

The secrecy capacity region [1, Theorem 6] is then given by the convex hull of the closure of all non-negative rate pairs (R_1, R_2) such that

$$R_1 \leq \frac{1}{2}\log\left|\frac{\mathbf{Q}+\mathbf{N}^{(z)}}{\mathbf{N}^{(z)}}\right| - \frac{1}{2}\log\left|\frac{\mathbf{Q}+\mathbf{N}^{(w)}}{\mathbf{N}^{(w)}}\right| \tag{2}$$

$$R_2 \leq \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}^{(y)}}{\mathbf{Q}+\mathbf{N}^{(y)}}\right| - \frac{1}{2}\log\left|\frac{\mathbf{S}+\mathbf{N}^{(w)}}{\mathbf{Q}+\mathbf{N}^{(w)}}\right| \tag{3}$$

for some $0 \preceq \mathbf{Q} \preceq \mathbf{S}$. In [2] and [3], it is shown that the same secrecy capacity region holds as long as the second receiver is degraded with respect to (w.r.t) the first receiver, i.e., $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(y)}$.

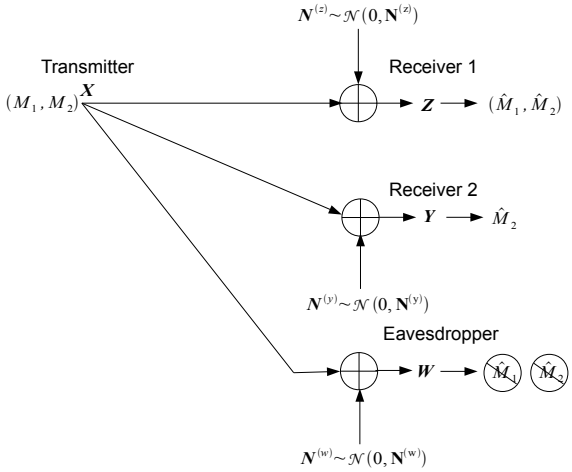

Fig. 1. Two-user Gaussian MIMO BC with degraded confidential messages.

In this paper, we characterize the capacity region for the case where the eavesdropper is degraded w.r.t. the first receiver, i.e.,

$$\mathbf{N}^{(z)} \preceq \mathbf{N}^{(w)}. \tag{4}$$

We first consider the discrete memoryless case where the eavesdropper is stochastically degraded w.r.t. both receivers and prove the capacity region in Section II.

In Section III, we consider the equivalent two-user Gaussian MIMO BC with two-degraded message sets and an eavesdropper, where the eavesdropper is stochastically degraded w.r.t. both receivers, i.e.,

$$\left\{\mathbf{N}^{(y)}, \mathbf{N}^{(z)}\right\} \preceq \mathbf{N}^{(w)}. \tag{5}$$

However, no order of degradedness is assumed between receivers 1 and 2. To prove that Gaussian inputs attain the capacity region, we make use of an extremal entropy inequality by Liu et al. [1, Theorem 2] that was proved using a vector generalization of Costa's EPI.

Finally, in Section IV, we prove the capacity region for the Gaussian MIMO case where the eavesdropper is only stochastically degraded w.r.t. the first receiver, i.e., (4). We make use of the channel enhancement technique [4] in which we enhance the channel of the second user.

II. Secrecy capacity region of a class of discrete memoryless two-user BC with two-degraded message sets

In this section, we consider the discrete memoryless case where the eavesdropper is stochastically degraded w.r.t. both the receivers, i.e., there exists distributions $p^{'}(w|z)$ and $p^{'}(w|y)$ such that

$$p(w|x) = \sum_{z} p^{'}(w|z)\, p(z|x)$$
$$p(w|x) = \sum_{y} p^{'}(w|y)\, p(y|x).$$

The confidentiality of the messages at the eavesdropper is measured using the normalized information-theoretic criteria [5], [6], [1]

$$\frac{1}{n} I(M_1, M_2; W^n) \leq \epsilon^{(n)} \tag{6}$$

where $\epsilon^{(n)} \to 0$ as $n \to \infty$. We have the following single-letter characterization of the secrecy capacity region:

***Theorem** 1:* The secrecy capacity region of the two-user BC with two-degraded message sets, where the eavesdropper is stochastically degraded with respect to *both* receivers, is given by the convex hull of the closure of all non-negative rate pairs (R_1, R_2) where

$$R_2 \leq I(U;Y) - I(U;W) \tag{7}$$
$$R_1 + R_2 \leq I(X;Z) - I(X;W) \tag{8}$$
$$R_1 + R_2 \leq I(U;Y) + I(X;Z|U) - I(X;W) \tag{9}$$

for some input probability distribution $p(u,x)$.

A. Achievability

Our codebook generation is similar to that in [7, Appendix 1], where Bagherikaram et al. introduced a coding scheme for the general two-user BC with common and private messages to be kept perfectly secure from the eavesdropper. However, we employ joint decoding at receiver 1 rather than sequential decoding as the achievable rate region so derived allows us to readily prove the converse as well as to readily characterize the capacity region of the Gaussian MIMO case. For completeness sake, we describe the coding scheme.

Fix $p(u)\,p(x|u)$. Split the private message $M_1 \in \left\{1, \ldots, 2^{nR_1}\right\}$ into $M_{1,1} \in \left\{1, \ldots, 2^{nR_{1,1}}\right\}$ and $M_{1,2} \in \left\{1, \ldots, 2^{nR_{1,2}}\right\}$ and let

$$R_1^{'} = I(X;W|U) - \epsilon_1 \tag{10}$$
$$R_2^{'} = I(U;W) - \epsilon_1 \tag{11}$$

for some $\epsilon_1 > 0$.

1) Codebook generation: Generate $2^{n\left(R_{1,1}+R_2+R_2^{'}\right)}$ independent codewords u^n of length n according to $\prod_{i=1}^{n} p(u_i)$ and label them as $u^n(m_{1,1}, m_2, j_2)$, where $m_{1,1} \in \left\{1, \ldots, 2^{nR_{1,1}}\right\}$, $m_2 \in \left\{1, \ldots, 2^{nR_2}\right\}$ and $j_2 \in \left\{1, \ldots, 2^{nR_2^{'}}\right\}$.

For each codeword $u^n(m_{1,1}, m_2, j_2)$, generate $2^{n\left(R_{1,2}+R_1^{'}\right)}$ codewords according to $\prod_{i=1}^{n} p(x_i|u_i(m_{1,1}, m_2, j_2))$ and label them as

$$x^n(m_{1,1}, m_{1,2}, m_2, j_1, j_2),$$

where $m_{1,2} \in \left\{1, \ldots, 2^{nR_{1,2}}\right\}$ and $j_1 \in \left\{1, \ldots, 2^{nR_1^{'}}\right\}$.

2) Encoding: To transmit the message $(m_{1,1}, m_{1,2}, m_2)$, the transmitter randomly chooses a pair (j_1, j_2) and sends the corresponding codeword $x^n(m_{1,1}, m_{1,2}, m_2, j_1, j_2)$ through the channel.

3) Decoding: Receiver 2 determines the unique $(m_{1,1}, m_2, j_2)$ such that

$$\left(u^n(m_{1,1}, m_2, j_2), y^n\right) \in A_\epsilon^{(n)}(U,Y).$$

Receiver 1 determines the unique $(m_{1,1}, m_{1,2}, m_2, j_1, j_2)$ such that

$$\begin{pmatrix} u^n(m_{1,1}, m_2, j_2), \\ x^n(m_{1,1}, m_{1,2}, m_2, j_1, j_2), z^n \end{pmatrix} \in A_\epsilon^{(n)}(U,X,Z).$$

1) Error analysis: Using standard analysis, it can be shown that correct decoding can be carried out with high probability as long as the following holds:

$$R_{1,1} + R_2 \leq I(U;Y) - I(U;W) + \epsilon_1$$
$$R_{1,1} + R_{1,2} + R_2 \leq I(X;Z) - I(X;W) + 2\epsilon_1$$
$$R_{1,2} \leq I(X;Z|U) - I(X;W|U) + \epsilon_1$$

Using Fourier-Motzkin elimination as well as the fact that ϵ_1 can be chosen to be arbitrarily small, we can show that (7)-(9) is achievable.

2) Equivocation rate calculation: Let us consider the following lower bound on the equivocation:

$$\begin{aligned}
&H(M_1, M_2|W^n, \mathcal{C}) \\
&= H(M_{1,1}, M_{1,2}, M_2|W^n, \mathcal{C}) \\
&= H(M_{1,1}, M_{1,2}, M_2, W^n|\mathcal{C}) - H(W^n|\mathcal{C}) \\
&= H(M_{1,1}, M_{1,2}, M_2, J_1, J_2, W^n|\mathcal{C}) \\
&\quad - H(J_1, J_2|M_{1,1}, M_{1,2}, M_2, W^n, \mathcal{C}) - H(W^n|\mathcal{C}) \\
&= H(M_{1,1}, M_{1,2}, M_2, J_1, J_2, W^n|\mathcal{C}) \\
&\quad - H(J_2|M_{1,1}, M_{1,2}, M_2, W^n, \mathcal{C}) \\
&\quad - H(J_1|M_{1,1}, M_{1,2}, M_2, J_2, W^n, \mathcal{C}) - H(W^n|\mathcal{C}) \\
&\overset{(a)}{\geq} H(M_{1,1}, M_{1,2}, M_2, J_1, J_2, W^n|\mathcal{C}) \\
&\quad - H(W^n|\mathcal{C}) - 2n\epsilon_2 \\
&= H(M_{1,1}, M_{1,2}, M_2, J_1, J_2|\mathcal{C}) \\
&\quad + H(W^n|M_{1,1}, M_{1,2}, M_2, J_1, J_2, \mathcal{C}) - H(W^n|\mathcal{C}) - 2n\epsilon_2 \\
&= H(M_{1,1}, M_{1,2}, M_2, J_1, J_2|\mathcal{C}) \\
&\quad - I(M_{1,1}, M_{1,2}, M_2, J_1, J_2; W^n|\mathcal{C}) - 2n\epsilon_2 \\
&\geq H(M_{1,1}, M_{1,2}, M_2, J_1, J_2|\mathcal{C}) - I(X^n; W^n|\mathcal{C}) - 2n\epsilon_2 \\
&\overset{(b)}{=} H(M_{1,1}, M_{1,2}, M_2|\mathcal{C}) + nI(X;W) \\
&\quad - nI(X;W) - 2n(\epsilon_1 + \epsilon_2) \\
&\overset{(c)}{=} H(M_{1,1}, M_{1,2}, M_2|\mathcal{C}) - n\epsilon_3
\end{aligned}$$

where (a) follows from Fano's inequality

$$\begin{aligned} H\left(J_2|M_{1,1},M_{1,2},M_2,W^n,\mathcal{C}\right) &\leq H\left(P_{w,2}^n\right)+nP_{w,2}^nR_2^{'} \\ &\leq n\epsilon_2 \\ H\left(J_1|M_{1,1},M_{1,2},M_2,J_2,W^n,\mathcal{C}\right) &\leq H\left(P_{w,1}^n\right)+nP_{w,1}^nR_1^{'} \\ &\leq n\epsilon_2 \end{aligned}$$

and the fact that the eavesdropper can decode j_1 and j_2 with arbitrarily small probability of error if it knows the message $(m_{1,1},m_{1,2},m_2)$ since we have chosen $R_1^{'}$ and $R_2^{'}$ to satisfy (10)-(11); (b) follows from the fact that we are averaging over all possible codebooks as well as the fact that we have chosen $R_1^{'}$ and $R_2^{'}$ to satisfy (10)-(11); and (c) follows from defining $\epsilon_3=2\left(\epsilon_1+\epsilon_2\right)$. Thus, we obtain

$$\Rightarrow \frac{1}{n}I\left(M_{1,1},M_{1,2},M_2;W^n|\mathcal{C}\right)=\epsilon_3.$$

Hence, there exists a codebook that can attain arbitrarily small probability of error as well as arbitrarily small $\frac{1}{n}I\left(M_1,M_2;W^n\right)$ as $n\to\infty$.

B. Converse

Let us first prove the bound (7). We define $\tilde{W}$ to be a physically degraded version of Y and $\overline{W}$ to be a physically degraded version of Z, where $p\left(\tilde{w}|x\right)=p\left(\overline{w}|x\right)=p\left(w|x\right)$.

We note from the secrecy constraint and Fano's inequality that

$$\begin{aligned} nR_2 &\leq H\left(M_2|W^n\right)-H\left(M_2|Y^n\right)+n\epsilon+n\delta_1 \\ &= I\left(M_2;Y^n\right)-I\left(M_2;W^n\right)+n\left(\epsilon+\delta_1\right). \end{aligned}$$

Next, we note that

$$\begin{aligned} &I\left(M_2;Y^n\right)-I\left(M_2;W^n\right) \\ &=\sum_{i=1}^{n}\left[I\left(M_2;Y_i|Y_1^{i-1}\right)-I\left(M_2;W_i|W_{i+1}^n\right)\right] \\ &=\sum_{i=1}^{n}\left[I\left(M_2,W_{i+1}^n;Y_i|Y_1^{i-1}\right)-I\left(M_2,Y_1^{i-1};W_i|W_{i+1}^n\right)\right] \\ &-\sum_{i=1}^{n}\left[I\left(W_{i+1}^n;Y_i|Y_1^{i-1},M_2\right)-I\left(Y_1^{i-1},;W_i|W_{i+1}^n,M_2\right)\right] \\ &\overset{(a)}{=}\sum_{i=1}^{n}\left[I\left(M_2;Y_i|Y_1^{i-1},W_{i+1}^n\right)-I\left(M_2,;W_i|W_{i+1}^n,Y_1^{i-1}\right)\right] \\ &\quad+\sum_{i=1}^{n}\left[I\left(W_{i+1}^n;Y_i|Y_1^{i-1}\right)-I\left(Y_1^{i-1};W_i|W_{i+1}^n\right)\right] \\ &\overset{(a)(b)}{=}\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2;Y_i|Y_1^{i-1},\overline{W}_{i+1}^n\right)\\-I\left(M_2,;W_i|\overline{W}_{i+1}^n,Y_1^{i-1}\right)\end{bmatrix} \\ &=\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,\overline{W}_{i+1}^n,Y_1^{i-1};Y_i\right)\\-I\left(M_2,\overline{W}_{i+1}^n,Y_1^{i-1};W_i\right)\end{bmatrix} \\ &\quad-\sum_{i=1}^{n}\left[I\left(\overline{W}_{i+1}^n,Y_1^{i-1};Y_i\right)-I\left(\overline{W}_{i+1}^n,Y_1^{i-1};W_i\right)\right] \\ &\overset{(c)}{\leq}\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,\overline{W}_{i+1}^n,Y_1^{i-1};Y_i\right)\\-I\left(M_2,\overline{W}_{i+1}^n,Y_1^{i-1};W_i\right)\end{bmatrix} \\ &=\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,Z_{i+1}^n,\overline{W}_{i+1}^n,Y_1^{i-1};Y_i\right)\\-I\left(M_2,Z_{i+1}^n,\overline{W}_{i+1}^n,Y_1^{i-1};W_i\right)\end{bmatrix} \\ &\quad-\sum_{i=1}^{n}\begin{bmatrix}I\left(Z_{i+1}^n;Y_i|M_2,\overline{W}_{i+1}^n,Y_1^{i-1}\right)\\-I\left(Z_{i+1}^n;W_i|M_2,\overline{W}_{i+1}^n,Y_1^{i-1}\right)\end{bmatrix} \\ &\overset{(c)}{\leq}\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,Z_{i+1}^n,\overline{W}_{i+1}^n,Y_1^{i-1};Y_i\right)\\-I\left(M_2,Z_{i+1}^n,\overline{W}_{i+1}^n,Y_1^{i-1};W_i\right)\end{bmatrix} \\ &\overset{(d)}{\leq}\sum_{i=1}^{n}\left[I\left(M_2,Z_{i+1}^n,Y_1^{i-1};Y_i\right)-I\left(M_2,Z_{i+1}^n,Y_1^{i-1};W_i\right)\right] \end{aligned}$$

where (a) follows from the Csiszár sum lemma; (b) follows from the fact that the channel is memoryless; (c) follows from the fact that W is stochastically degraded w.r.t Y; and (d) follows from the fact that $\overline{W}$ is a physically degraded version of Z.

Similarly, we may note from the secrecy constraint and Fano's inequality that

$$\begin{aligned} &n\left(R_1+R_2\right) \\ &\leq H\left(M_1,M_2|W^n\right)-H\left(M_1,M_2|Z^n\right)+n\epsilon+n\delta_2 \\ &= I\left(M_1,M_2;Z^n\right)-I\left(M_1,M_2;W^n\right)+n\left(\epsilon+\delta_2\right). \end{aligned}$$

Next, we note that

$$\begin{aligned} &I\left(M_1,M_2;Z^n\right)-I\left(M_1,M_2;W^n\right) \\ &\leq I\left(X^n;Z^n\right)-I\left(X^n;W^n\right) \\ &\quad-\left[I\left(X^n;Z^n|M_1,M_2\right)-I\left(X^n;W^n|M_1,M_2\right)\right] \\ &\overset{(a)}{\leq} I\left(X^n;Z^n\right)-I\left(X^n;W^n\right) \\ &=\sum_{i=1}^{n}\left[I\left(X_i;Z_i|Z^{i-1}\right)-I\left(X_i;W_i|W^{i-1}\right)\right] \\ &=\sum_{i=1}^{n}\left[I\left(X_i;Z_i\right)-I\left(X_i;W_i\right)\right] \\ &\quad-\sum_{i=1}^{n}\left[I\left(Z^{i-1};Z_i\right)-I\left(W^{i-1};W_i\right)\right] \\ &\overset{(a)}{\leq}\sum_{i=1}^{n}\left[I\left(X_i;Z_i\right)-I\left(X_i;W_i\right)\right] \end{aligned}$$

where (a) follows from the fact that W is stochastically degraded w.r.t Z.

Similarly, we may note from the secrecy constraint and Fano's inequality that

$$\begin{aligned} &n\left(R_1+R_2\right) \\ &\leq H\left(M_1,M_2|W^n\right)-H\left(M_2|Y^n\right)-H\left(M_1|Z^n,M_2\right) \\ &\quad+n\left(\epsilon+\delta_1+\delta_2\right) \\ &= I\left(M_2;Y^n\right)+I\left(M_1;Z^n|M_2\right)-I\left(M_1,M_2;W^n\right) \\ &\quad+n\left(\epsilon+\delta_1+\delta_2\right). \end{aligned}$$

We note that

$$
\begin{aligned}
&I\left(M_2;Y^n\right)+I\left(M_1;Z^n|M_2\right)-I\left(M_1,M_2;W^n\right)\\
&=I\left(M_2;Y^n\right)+I\left(M_1;Z^n|M_2\right)\\
&\quad-I\left(M_2;W^n\right)-I\left(M_1;W^n|M_2\right)\\
&=I\left(M_2;Y^n\right)+I\left(X^n;Z^n|M_2\right)\\
&\quad-I\left(M_2;W^n\right)-I\left(X^n;W^n|M_2\right)\\
&\quad-\left[I\left(X^n;Z^n|M_1,M_2\right)-I\left(X^n;W^n|M_1,M_2\right)\right]\\
&\overset{(a)}{=}I\left(M_2;Y^n\right)+I\left(X^n;Z^n|M_2\right)-I\left(X^n;W^n\right)\\
&=\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2;Y_i|Y^{i-1}\right)+I\left(X_i;Z_i|M_2,Z_{i+1}^n\right)\\-I\left(X_i;W_i|W_1^{i-1}\right)\end{bmatrix}\\
&=\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,Z_{i+1}^n;Y_i|Y^{i-1}\right)\\+I\left(X_i;Z_i|M_2,Z_{i+1}^n,Y^{i-1}\right)\\-I\left(Z_{i+1}^n;Y_i|M_2,Y^{i-1}\right)+I\left(Y^{i-1};Z_i|M_2,Z_{i+1}^n\right)\\-I\left(X_i;W_i|W_1^{i-1}\right)\end{bmatrix}\\
&\overset{(b)}{=}\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,Z_{i+1}^n;Y_i|Y^{i-1}\right)\\+I\left(X_i;Z_i|M_2,Z_{i+1}^n,Y^{i-1}\right)-I\left(X_i;W_i|W_1^{i-1}\right)\end{bmatrix}\\
&=\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,Y^{i-1},Z_{i+1}^n;Y_i\right)\\+I\left(X_i;Z_i|M_2,Z_{i+1}^n,Y^{i-1}\right)-I\left(X_i;W_i\right)\\-I\left(Y^{i-1};Y_i\right)+I\left(W^{i-1};W_i\right)\end{bmatrix}\\
&\overset{(c)}{\leq}\sum_{i=1}^{n}\begin{bmatrix}I\left(M_2,Y^{i-1},Z_{i+1}^n;Y_i\right)\\+I\left(X_i;Z_i|M_2,Z_{i+1}^n,Y^{i-1}\right)-I\left(X_i;W_i\right)\end{bmatrix}
\end{aligned}
$$

where (a) follows from the fact that W is a stochastically degraded w.r.t. Z; (b) follows from the Csiszár sum lemma; and (c) follows from the fact that W is stochastically degraded w.r.t. Y.

Finally, we define $U_i \triangleq \left(M_2, Z_{i+1}^n, Y^{i-1}\right)$ and following the standard single-letterization process, we have the desired converse result.

III. Secrecy capacity region of a class of two-user Gaussian MIMO BC with two-degraded message sets, $\left\{\mathbf{N}^{(y)},\mathbf{N}^{(z)}\right\}\preceq\mathbf{N}^{(w)}$

In this section, we consider the equivalent class of two-user Gaussian MIMO BC with two-degraded message sets, where the eavesdropper is stochastically degraded w.r.t both receivers (see (5)). The capacity region is given by the following theorem:

***Theorem** 2:* The secrecy capacity region, $\mathcal{C}_1\left(\mathbf{S}\right)$, of the two-user Gaussian MIMO BC with two-degraded message sets under the input matrix power constraint $\mathbb{E}\left[\boldsymbol{X}\boldsymbol{X}^T\right]\preceq\mathbf{S}$, and where $\left\{\mathbf{N}^{(y)},\mathbf{N}^{(z)}\right\}\preceq\mathbf{N}^{(w)}$, is given by the convex hull of the closure of all non-negative rate pairs (R_1,R_2) such that

$$R_2\leq\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}+\mathbf{N}^{(y)}\right|}-\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{Q}+\mathbf{N}^{(w)}\right|}\tag{12}$$

$$R_1+R_2\leq\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|}-\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|}\tag{13}$$

$$R_1+R_2\leq\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}+\mathbf{N}^{(y)}\right|}+\frac{1}{2}\log\frac{\left|\mathbf{Q}+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|}-\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|}\tag{14}$$

for some $0\preceq\mathbf{Q}\preceq\mathbf{S}$.

A. Proof

Since the capacity region $\mathcal{C}_1\left(\mathbf{S}\right)$ is convex due to time-sharing, it may be described by the following optimization problem:

$$(P1):\sup_{\substack{(R_1,R_2)\\P_{U,\boldsymbol{X}}:\mathbb{E}[\boldsymbol{X}\boldsymbol{X}]\preceq\mathbf{S}}}\mu_1R_1+\mu_2R_2$$

and $R_1,R_2\geq0$ satisfy (7)-(9). If $\mu_2\leq\mu_1$, we note that

$$\max_{(R_1,R_2)\in\mathcal{C}_1(\mathbf{S})}\mu_1R_1+\mu_2R_2\leq\max_{(R_1+R_2,0)\in\mathcal{C}_1(\mathbf{S})}\mu_1\left(R_1+R_2\right)$$

since for any $(R_1,R_2)\in\mathcal{C}_1\left(\mathbf{S}\right)$, we also have $(R_1+R_2,0)\in\mathcal{C}_1\left(\mathbf{S}\right)$. Hence, for $\mu_2\leq\mu_1$, we transmit at maximum secrecy rate to receiver one. We consider the case for $\mu_1<\mu_2$.

***Remark** 1:* We may readily verify that the explicit constraint $R_2\geq0$ is unnecessary when $\mu_1<\mu_2$.

Assuming Gaussian inputs given by $\boldsymbol{V}\sim\mathcal{N}\left(0,\mathbf{Q}\right)$, $\boldsymbol{U}\sim\mathcal{N}\left(0,\mathbf{S}-\mathbf{Q}\right)$, $\boldsymbol{X}=\boldsymbol{U}+\boldsymbol{V}$, we consider the following optimization problem:

$$(P1-G):\max_{\substack{(R_1,R_2)\\0\preceq\mathbf{Q}\preceq\mathbf{S}}}\mu_1R_1+\mu_2R_2$$

where $R_1\geq0$ and (R_1,R_2) satisfy (12)-(14). The KKT conditions for the optimization problem $(P1-G)$ is given by

$$\begin{aligned}\frac{\alpha_1^*}{2}\left(\mathbf{Q}^*+\mathbf{N}^{(w)}\right)^{-1}+\frac{\alpha_3^*}{2}\left(\mathbf{Q}^*+\mathbf{N}^{(z)}\right)^{-1}+\mathbf{M}\\=\frac{\alpha_1^*+\alpha_3^*}{2}\left(\mathbf{Q}^*+\mathbf{N}^{(y)}\right)^{-1}+\mathbf{M}_S\end{aligned}\tag{15}$$

$$\mathbf{Q}^*\mathbf{M}=0\tag{16}$$

$$\left(\mathbf{S}-\mathbf{Q}^*\right)\mathbf{M}_S=0.\tag{17}$$

$$\alpha_1^*+\alpha_2^*+\alpha_3^*=\mu_2\tag{18}$$

$$\alpha_2^*+\alpha_3^*=\mu_1+\gamma_1^*\tag{19}$$

where $\alpha_1^*,\alpha_2^*,\alpha_3^*,\gamma_1^*\geq0$. We note that (15)-(17) satisfy the conditions of the extremal entropy inequality of Liu et al. (see [1, Theorem 2]).

The optimal value of $(P1)$ can be readily shown to be upper bounded by

$$\begin{aligned}&\sup_{\substack{P_{U,\boldsymbol{X}}\\\mathbb{E}[\boldsymbol{X}\boldsymbol{X}]\preceq\mathbf{S}}}\begin{matrix}\alpha_1^*\left[I\left(U;\boldsymbol{Y}\right)-I\left(U;\boldsymbol{W}\right)\right]\\+\alpha_2^*\left[I\left(\boldsymbol{X};\boldsymbol{Z}\right)-I\left(\boldsymbol{X};\boldsymbol{W}\right)\right]\\+\alpha_3^*\left[I\left(U;\boldsymbol{Y}\right)+I\left(\boldsymbol{X};\boldsymbol{Z}|U\right)-I\left(\boldsymbol{X};\boldsymbol{W}\right)\right]\end{matrix}\\
&=\sup_{\substack{P_{U,\boldsymbol{X}}\\\mathbb{E}[\boldsymbol{X}\boldsymbol{X}]\preceq\mathbf{S}}}\begin{matrix}\alpha_1^*h\left(\boldsymbol{W}|U\right)+\alpha_3^*h\left(\boldsymbol{Z}|U\right)\\-\left(\alpha_1^*+\alpha_3^*\right)h\left(\boldsymbol{Y}|\boldsymbol{U}\right)\end{matrix}\\
&\quad+\sup_{\substack{P_{U,\boldsymbol{X}}\\\mathbb{E}[\boldsymbol{X}\boldsymbol{X}]\preceq\mathbf{S}}}\begin{matrix}\left(\alpha_1^*+\alpha_3^*\right)\left[h\left(\boldsymbol{Y}\right)-h\left(\boldsymbol{W}\right)\right]\\+\alpha_2^*\left[h\left(\boldsymbol{Z}\right)-h\left(\boldsymbol{W}\right)\right]\end{matrix}\\
&\quad+\left(\alpha_2^*+\alpha_3^*\right)\left[h\left(\boldsymbol{N}^{(w)}\right)-h\left(\boldsymbol{N}^{(z)}\right)\right]\end{aligned}\tag{20}$$

$$\stackrel{(a)}{\leq} \frac{\alpha_1^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(y)}\right|} - \frac{\alpha_1^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(w)}\right|} + \frac{\alpha_2^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|} - \frac{\alpha_2^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|} + \frac{\alpha_3^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(y)}\right|} + \frac{\alpha_3^*}{2}\log\frac{\left|\mathbf{Q}^*+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|} - \frac{\alpha_3^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|} \quad (21)$$

where (a) follows from [1, Theorem 2] and from the worst additive noise lemma (see [8, Lemma 2]) since $\boldsymbol{W}$ is stochastically degraded w.r.t $\boldsymbol{Y}$ and $\boldsymbol{Z}$.

Finally, we note that (21) is achievable. We note that the following optimization problem is linear:

$$\begin{aligned}(P2): \max_{R_1,R_2}\ & \mu_1 R_1 + \mu_2 R_2 \\ R_2 &\leq \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(y)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(w)}\right|} \\ R_1+R_2 &\leq \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|} \\ R_1+R_2 &\leq \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(y)}\right|} + \frac{1}{2}\log\frac{\left|\mathbf{Q}^*+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|} \\ -R_1 &\leq 0.\end{aligned}$$

We may easily verify that the optimal value of $(P2)$ is given by (21).

IV. Secrecy capacity region of a class of two-user Gaussian MIMO BC with two-degraded message sets, $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(w)}$

Finally, we consider the case where the eavesdropper is stochastically degraded w.r.t. receiver 1, i.e., $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(w)}$. The capacity region is given by the following theorem:

***Theorem** 3:* The secrecy capacity region, $\mathcal{C}_2(\mathbf{S})$, of the two-user Gaussian MIMO BC with two-degraded message sets under the input matrix power constraint $\mathbb{E}\left[\boldsymbol{X}\boldsymbol{X}^T\right] \preceq \mathbf{S}$, and where $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(w)}$, is given by the convex hull of the closure of all non-negative rate pairs (R_1, R_2) such that (12)-(14) is satisfied for some $0 \preceq \mathbf{Q} \preceq \mathbf{S}$.

Proof: Similar to the previous section, we only consider the case where $\mu_1 < \mu_2$. We first note that any (R_1, R_2) satisfying (12)-(14) is achievable as long as

$$\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}+\mathbf{N}^{(y)}\right|} \geq \frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{Q}+\mathbf{N}^{(w)}\right|}. \quad (22)$$

Next, we consider the optimization problem $(P1-G)$ (without imposing the constraint that $R_2 \geq 0$) for the case where $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(w)}$. We note that the KKT conditions (15)-(19) hold as well. We may enhance the second receiver and obtain

$$\begin{matrix}\frac{\alpha_1^*+\alpha_3^*}{2}\left(\mathbf{Q}^*+\mathbf{N}^{(y)}\right)^{-1} \\ +\mathbf{M}_S\end{matrix} = \frac{\alpha_1^*+\alpha_3^*}{2}\left(\mathbf{Q}^*+\hat{\mathbf{N}}^{(y)}\right)^{-1}.$$

We may readily verify that $\left\{\hat{\mathbf{N}}^{(y)}, \mathbf{N}^{(z)}\right\} \preceq \mathbf{N}^{(w)}$ and $\hat{\mathbf{N}}^{(y)} \preceq \mathbf{N}^{(y)}$. Furthermore, we note that (see [4])

$$\frac{1}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(y)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(y)}\right|} = \frac{1}{2}\log\frac{\left|\mathbf{S}+\hat{\mathbf{N}}^{(y)}\right|}{\left|\mathbf{Q}^*+\hat{\mathbf{N}}^{(y)}\right|}. \quad (23)$$

We now consider the enhanced channel where $\left\{\hat{\mathbf{N}}^{(y)}, \mathbf{N}^{(z)}\right\} \preceq \mathbf{N}^{(w)}$. The weighted sum-rate for the non-enhanced channel may be upper bounded by the weighted sum-rate of the enhanced channel since $\hat{\mathbf{N}}^{(y)} \preceq \mathbf{N}^{(y)}$. Furthermore, the weighted sum-rate of the enhanced channel is given in the previous section as

$$\frac{\alpha_1^*}{2}\log\frac{\left|\mathbf{S}+\hat{\mathbf{N}}^{(y)}\right|}{\left|\mathbf{Q}^*+\hat{\mathbf{N}}^{(y)}\right|} - \frac{\alpha_1^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{Q}^*+\mathbf{N}^{(w)}\right|} + \frac{\alpha_2^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|} - \frac{\alpha_2^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|} + \frac{\alpha_3^*}{2}\log\frac{\left|\mathbf{S}+\hat{\mathbf{N}}^{(y)}\right|}{\left|\mathbf{Q}^*+\hat{\mathbf{N}}^{(y)}\right|} + \frac{\alpha_3^*}{2}\log\frac{\left|\mathbf{Q}^*+\mathbf{N}^{(z)}\right|}{\left|\mathbf{N}^{(z)}\right|} - \frac{\alpha_3^*}{2}\log\frac{\left|\mathbf{S}+\mathbf{N}^{(w)}\right|}{\left|\mathbf{N}^{(w)}\right|}.$$

The weighted sum-rate for the enhanced channel above is also achievable by the non-enhanced channel as (23) holds (hence, (22) is satisfied). Therefore, the capacity region of the channel where $\mathbf{N}^{(z)} \preceq \mathbf{N}^{(w)}$ is given by Theorem 3. ■

References

[1] R. Liu, T. Liu, H. V. Poor and S. Shamai, "A vector generalization of Costa's entropy-power inequality with applications," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1865–1879, 2010.

[2] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "The secrecy capacity region of the Gaussian MIMO broadcast channel," *IEEE Trans. Inf. Theory*, accepted for publication. [Online]. Available: http://arxiv.org/pdf/0903.3261v2.pdf

[3] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.

[4] H. Weingarten, Y. Steinberg and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936 – 3964, Sep. 2006.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.

[6] I. Csiszár and J. Körner, "The wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 339–348, May 1978.

[7] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," *IEEE Trans. Inf. Theory*, submitted for publication. [Online]. Available: http://arxiv.org/pdf/0910.3658v1.pdf

[8] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information-theoretic problems," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1839–1851, May 2007.