On the Individual Secrecy Rate Region for the Broadcast Channel with an External Eavesdropper

Yanling Chen*, O. Ozan Koyluoglu†, Aydin Sezgin*
* Institute for Digital Communication Systems, Ruhr University Bochum, Germany.
Email: {yanling.chen-q5g, aydin.sezgin}@rub.de.
† Department of Electrical and Computer Engineering, The University of Arizona.
Email: ozan@email.arizona.edu.

***Abstract*—This paper studies the problem of secure communication over broadcast channels under the lens of individual secrecy constraints (i.e., information leakage from each message to an eavesdropper is made vanishing). It is known that, for the communication over the degraded broadcast channels, the stronger receiver is able to decode the message of the weaker receiver. In the individual secrecy setting, the message for the weaker receiver can be further utilized to secure the partial message that is intended to the stronger receiver. With such a coding spirit, it is shown that more secret bits can be conveyed to the stronger receiver. In particular, for the corresponding Gaussian model, a constant gap (i.e., 0.5 bits within the individual secrecy capacity region) result is obtained. Overall, when compared with the joint secrecy constraint, the results allow for trading-off secrecy level and throughput in the system.**

I. Introduction

The broadcast channel (BC) is a fundamental communication model that involves transmission of independent messages to different users. The broadcast nature makes the communication susceptible to eavesdropping. Therefore, it is desirable to offer a reliable communication with a certain level of security guarantee, especially to ensure that sensitive information is protected from unauthorized parties.

The model of the discrete memoryless degraded broadcast channel (DM-DBC) with or without an external eavesdropper has been well studied. Both capacity regions have been determined for the cases without secrecy constraint [1]–[3], or subject to a *joint* secrecy constraint (whereby the information leakage from *both* messages to the eavesdropper is made vanishing) [4], [5]. Interestingly, superposition coding is optimal in both settings. Differently from the previous studies, we focus on the problem under the *individual* secrecy constraints, where the requirement is to minimize the information leakage from *each* message to the eavesdropper. Remarkably, these two secrecy notions are different. The joint secrecy constraint offers a higher secrecy level from the system design perspective but unfortunately not always affordable [6], while the individual secrecy constraint provides an acceptable security strength by keeping each legitimate receiver away from an invasion of secrecy. In communication networks, from the end user's point of view, this is a good option for trading-off of the throughput and secrecy [7].

The work of Yanling Chen and Aydin Sezgin is supported by the German Research Foundation, Deutsche Forschungsgemeinschaft (DFG), Germany, under grant SE 1697/11.

II. System model

Consider a discrete memoryless broadcast channel given by $p(y_1, y_2, z|x)$ with two legitimate receivers and one passive eavesdropper. The transmitter aims to send messages m_1, m_2 to receiver $1, 2$, respectively. Suppose x^n is the channel input, whilst y_1^n (at receiver 1), y_2^n (at receiver 2) and z^n (at eavesdropper), are the channel outputs.

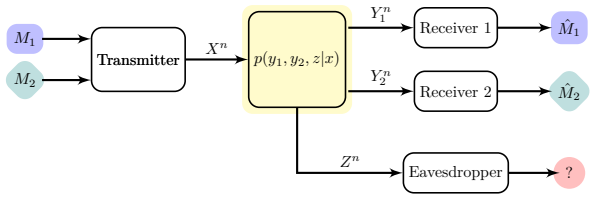

Fig. 1: DM-BC with an external eavesdropper.

Denote the average probability of decoding error at receiver i as $P_{e,i}$. The rate pair (R_1, R_2) is said to be *achievable*, if for any $\epsilon > 0$, there exists an encoder-decoder such that

$$\frac{1}{n}H(M_i) \geq R_i - \epsilon \tag{1}$$

$$P_{e,i} \leq \epsilon \tag{2}$$

$$\frac{1}{n}I(M_i; Z^n) \leq \epsilon, \tag{3}$$

for $i = 1, 2$ and for sufficiently large n. Note that (3) corresponds to the *individual* secrecy constraints. If the coding scheme fulfills a stronger condition that

$$\frac{1}{n}I(M_1, M_2; Z^n) \leq \epsilon, \tag{4}$$

then it is said to satisfy the *joint* secrecy constraint. Clearly, the joint secrecy constraint implies the individual secrecy constraints.

III. DM-BC with an external eavesdropper

In this section, we are interested in the DM-BC scenario where the individual secrecy constraint is employed. (The Gaussian counterpart of the model is the subject of Section IV.) Our first observation is that *positive rate pairs are not possible if the eavesdropper's channel is less noisy than either receiver's channel*, i.e., $I(U;Z) \geq I(U;Y_i)$ for $i \in \{1,2\}$ for all $p(u)$ such that $U \to X \to (Y_1, Y_2, Z)$. This is due to the fact that $nR_i = H(M_i) = I(M_i; Y_i^n) + H(M_i|Y_i^n) \leq I(M_i; Z^n) + nO(\epsilon) \leq nO(\epsilon)$, where the first inequality is due to the reliability constraint whilst the second inequality is due to the individual secrecy constraint. Therefore, we assume that both Y_1, Y_2 are less noisy than Z for the DM-BC under investigation. Utilizing the superposition coding with secrecy coding [8], we have the following theorem.

Theorem 1. *For DM-BC with an external eavesdropper such that Y_1 is less noisy than Y_2, an achievable individual secrecy rate region is given by the union of non-negative rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_2 &\leq I(U;Y_2) - I(U;Z), \\ R_1 &\leq I(V;Y_1|U) - I(V;Z|U) \\ &\quad + I(U;Y_2) - \max\{R_2, I(U;Z)\} \end{aligned}$$

over all $p(u)p(v|u)p(x|v)$.

Proof. Rate splitting: We split M_1 into (M_{1k}, M_{1s}). In particular, M_{1k}, M_{1s} are of entropy nR_{1k} and nR_{1s}, respectively; and M_2 is of entropy nR_2. That is,

$$R_1 = R_{1k} + R_{1s}. \tag{5}$$

Codebook generation: Fix $p(u), p(v|u)$. First, randomly generate $2^{n(R_2+R_{1k}+R_{2r})}$ i.i.d. sequences $u^n(m_2, m_{1k}, m_{2r})$, with $(m_2, m_{1k}, m_{2r}) \in [1 : 2^{nR_2}] \times [1 : 2^{nR_{1k}}] \times [1 : 2^{nR_{2r}}]$, according to $p(u)$. Secondly, for each $u^n(m_2, m_{1k}, m_{2r})$, randomly generate i.i.d. sequences $v^n(m_2, m_{1k}, m_{2r}, m_{1s}, m_{1r})$ with $(m_{1s}, m_{1r}) \in [1 : 2^{nR_{1s}}] \times [1 : 2^{nR_{1r}}]$, according to $p(v|u)$.

Encoding: To send messages (m_1, m_2) with $m_1 = (m_{1k}, m_{1s})$, randomly choose $m_{2r} \in [1 : 2^{nR_{2r}}]$ and find $u^n(m_2, m_{1k}, m_{2r})$. Given $u^n(m_2, m_{1k}, m_{2r})$, randomly choose $m_{1r} \in [1 : 2^{nR_{1r}}]$, further find the corresponding $v^n(m_2, m_{1k}, m_{2r}, m_{1s}, m_{1r})$. Generate x^n according to $p(x|v)$, and transmit it to the channel.

Decoding: Receiver 2, upon receiving y_2^n, finds $u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_{2r})$ such that $(u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_{2r}), y_2^n)$ is jointly typical.

Receiver 1, upon receiving y_1^n, finds $u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r})$ such that $(u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r}), y_1^n)$ is jointly typical. Corresponding to $u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r})$, further find $v^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r}, \tilde{m}_{1s}, \tilde{m}_{1r})$ which is jointly typical with y_1^n. Finally, decode $\tilde{m}_1 = (\tilde{m}_{1k}, \tilde{m}_{1s})$.

Analysis of the error probability of decoding: Assume that $(M_1, M_2) = (m_1, m_2)$ with $m_1 = (m_{1k}, m_{1s})$ is sent.

First we consider $P_{e,2}$ at receiver 2. A decoding error happens iff one or both of the following events occur:

$$\begin{aligned} \mathcal{E}_{21} &= \{(u^n(m_2, m_{1k}, m_{2r}), y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \mathcal{E}_{22} &= \{(u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_{2r}), y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \hat{m}_2 \neq m_2\}. \end{aligned}$$

Thus, $P_{e,2}$ can be upper bounded as

$$P_{e,2} \leq \Pr(\mathcal{E}_{21}) + \Pr(\mathcal{E}_{22}).$$

By the LLN, $\Pr(\mathcal{E}_{21})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{22})$, since $u^n(\hat{m}_2, \hat{m}_{1k}, \hat{m}_{2r})$ is independent of $(u^n(m_2, m_{1k}, m_{2r}), y_2^n)$ for $\hat{m}_2 \neq m_2$, by the packing lemma [9], $\Pr(\mathcal{E}_{22})$ tends to zero as $n \to \infty$ if

$$R_2 + R_{1k} + R_{2r} < I(U;Y_2) - \delta(\epsilon). \tag{6}$$

At receiver 1, the decoder makes an error iff one or more of the following events occur:

$$\begin{aligned} \mathcal{E}_{11} &= \{(u^n(m_2, m_{1k}, m_{2r}), y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \mathcal{E}_{12} &= \{(u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r}), y_1^n) \in \mathcal{T}_\epsilon^{(n)} \\ &\qquad \text{for some } (\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r}) \neq (m_2, m_{1k}, m_{2r})\}, \\ \mathcal{E}_{13} &= \{(v^n(m_2, m_{1k}, m_{2r}, m_{1s}, m_{1r}), y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \mathcal{E}_{14} &= \{(v^n(m_2, m_{1k}, m_{2r}, \tilde{m}_{1s}, \tilde{m}_{1r}), y_1^n) \in \mathcal{T}_\epsilon^{(n)} \\ &\qquad \text{for some } \tilde{m}_{1s} \neq m_{1s}\}. \end{aligned}$$

So $P_{e,1}$ can be upper bounded by

$$P_{e,1} \leq \Pr(\mathcal{E}_{11}) + \Pr(\mathcal{E}_{12}) + \Pr(\mathcal{E}_{13}) + \Pr(\mathcal{E}_{14}).$$

By the LLN, $\Pr(\mathcal{E}_{11})$ and $\Pr(\mathcal{E}_{13})$ tends to zero as $n \to \infty$. For $\Pr(\mathcal{E}_{12})$, since $u^n(\tilde{m}_2, \tilde{m}_{1k}, \tilde{m}_{2r})$ is independent of $(u^n(m_2, m_{1k}, m_{2r}), y_1^n)$ for $(\tilde{m}_2, \tilde{m}_{1k}) \neq (m_2, m_{1k})$, by the packing lemma [9], $\Pr(\mathcal{E}_{12})$ tends to zero as $n \to \infty$ if

$$R_2 + R_{1k} + R_{2r} < I(U;Y_1) - \delta(\epsilon). \tag{7}$$

(Note that (7) holds once (6) is satisfied.) For $\Pr(\mathcal{E}_{14})$, note that if $(\tilde{m}_{1s}, \tilde{m}_{1r}) \neq (m_{1s}, m_{1r})$, then for a given $u^n(m_2, m_{1k}, m_{2r})$, $v^n(m_2, m_{1k}, m_{2r}, \tilde{m}_{1s}, \tilde{m}_{1r})$ is independent of $(v^n(m_2, m_{1k}, m_{2r}, m_{1s}, m_{1r}), y_1^n)$. By the packing lemma [9], $\Pr(\mathcal{E}_{14})$ tends to zero as $n \to \infty$ if

$$R_{1s} + R_{1r} < I(V;Y_1|U) - \delta(\epsilon). \tag{8}$$

Analysis of individual secrecy: First consider $H(M_2|Z^n)$.

$$\begin{aligned} &H(M_2|Z^n) = H(M_2, Z^n) - H(Z^n) \\ &= H(U^n, M_2, Z^n) - H(U^n|M_2, Z^n) - H(Z^n) \\ &= H(U^n) + H(Z^n|U^n) - H(U^n|M_2, Z^n) - H(Z^n) \\ &\overset{(a)}{\geq} H(U^n) + H(Z^n|U^n) \\ &\quad - n[R_{1k} + R_{2r} - I(U;Z)] - H(Z^n) - n\epsilon_1 \\ &\overset{(b)}{=} n[R_2 + R_{1k} + R_{2r}] \\ &\quad - n[R_{1k} + R_{2r} - I(U;Z)] - I(U^n; Z^n) - n\epsilon_1 \\ &= nR_2 + nI(U;Z) - I(U^n; Z^n) - n\epsilon_1 \\ &\overset{(c)}{\geq} nR_2 - n\delta_1(\epsilon), \end{aligned}$$

where (a) follows from [10, Lemma 1] that $H(U^n|M_2,Z^n)\le n[R_{1k}+R_{2r}-I(U;Z)]+n\epsilon_1$, if

$$R_{1k}+R_{2r}\ge I(U;Z)+\epsilon_1'; \tag{9}$$

(b) follows from the codebook construction that $H(U^n)=n[R_2+R_{1k}+R_{2r}]$; and (c) is by the fact that $I(U^n;Z^n)\le nI(U;Z)+n\epsilon_2$ and by taking $\delta_1(\epsilon)=\epsilon_1+\epsilon_2$. The proof of $I(U^n;Z^n)\le nI(U;Z)+n\epsilon_2$ is given as follows.

$$\begin{aligned}
I(U^n;Z^n)&=H(Z^n)-H(Z^n|U^n)\\
&=H(Z^n)-H(Z^n|U^n,V^n)-I(V^n;Z^n|U^n)\\
&\overset{(d)}{=}H(Z^n)-nH(Z|U,V)-H(V^n|U^n)+H(V^n|U^n,Z^n)\\
&\overset{(e)}{\le}H(Z^n)-nH(Z|U,V)-H(V^n|U^n)\\
&\quad+n[R_{1s}+R_{1r}-I(V;Z|U)]+n\epsilon_2\\
&\overset{(f)}{\le}nH(Z)-nH(Z|U,V)-n[R_{1s}+R_{1r}]\\
&\quad+n[R_{1s}+R_{1r}-I(V;Z|U)]+n\epsilon_2\\
&=nI(U;Z)+n\epsilon_2,
\end{aligned}$$

where (d) is due to the discrete memoryless channel; (e) follows from [10, Lemma 1] that $H(V^n|U^n,Z^n)\le n[R_{1s}+R_{1r}-I(V;Z|U)]+n\epsilon_2$, if

$$R_{1s}+R_{1r}\ge I(V;Z|U)+\epsilon_2'; \tag{10}$$

(Note that (10) holds if (12) holds.) (f) follows from the fact that $H(Z^n)=\sum_{i=1}^n H(Z_i|Z^{i-1})\le\sum_{i=1}^n H(Z_i)=nH(Z)$ and by the codebook construction $H(V^n|U^n)=n[R_{1s}+R_{1r}]$.

For $H(M_1|Z^n)$, we have

$$\begin{aligned}
&H(M_1|Z^n)=H(M_{1k},M_{1s}|Z^n)\\
&=H(M_2,M_{1k},M_{2r},M_{1s}|Z^n)-H(M_2,M_{2r}|M_{1k},M_{1s},Z^n)\\
&=H(U^n,M_{1s}|Z^n)-H(U^n|M_{1k},M_{1s},Z^n)\\
&\overset{(g)}{\ge}H(U^n|Z^n)+H(M_{1s}|U^n,Z^n)-H(U^n|M_{1k},Z^n)\\
&=H(U^n|Z^n)+H(V^n|U^n,Z^n)-H(V^n|M_{1s},U^n,Z^n)\\
&\quad-H(U^n|M_{1k},Z^n)\\
&\overset{(h)}{\ge}H(U^n,V^n|Z^n)-n[R_{1r}-I(V;Z|U)]\\
&\quad-n[R_2+R_{2r}-I(U;Z)]-n\delta_2(\epsilon)\\
&=H(U^n,V^n)-I(U^n,V^n;Z^n)+nI(U,V;Z)\\
&\quad-n[R_{1r}+R_2+R_{2r}]-n\delta_2(\epsilon)\\
&\overset{(i)}{\ge}nR_1-n\delta_2(\epsilon),
\end{aligned}$$

where (g) is due to the fact that conditioning reduces entropy; (h) follows from [10, Lemma 1] that by taking

$$R_2+R_{2r}\ge I(U;Z)+\epsilon_3', \tag{11}$$

we have $H(U^n|M_{1k},Z^n)\le n[R_2+R_{2r}-I(U;Z)]+n\epsilon_3$; and by taking

$$R_{1r}\ge I(V;Z|U)+\epsilon_4', \tag{12}$$

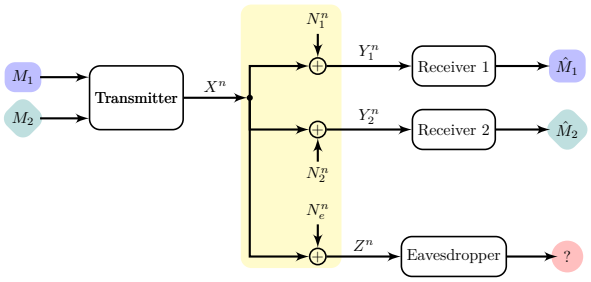

Fig. 2: Gaussian BC with an external eavesdropper.

we have $H(V^n|M_{1s},U^n,Z^n)\le n[R_{1r}-I(V;Z|U)]+n\epsilon_4$; and taking $\delta_2(\epsilon)=\epsilon_3+\epsilon_4$; (i) is by the codebook construction that $H(U^n,V^n)=n[R_2+R_{1k}+R_{2r}+R_{1s}+R_{1r}]$; and the fact that $I(U^n,V^n;Z^n)\le nI(U,V;Z)$, the proof of which is given as follows:

$$\begin{aligned}
I(U^n,V^n;Z^n)&=H(Z^n)-H(Z^n|U^n,V^n)\\
&\overset{(j)}{=}H(Z^n)-nH(Z|U,V)\\
&\overset{(k)}{\le}nH(Z)-nH(Z|U,V)\\
&=nI(U,V;Z),
\end{aligned}$$

where (j) is due to the discrete memoryless of the channel; and (k) follows from the fact that $H(Z^n)=\sum_{i=1}^n H(Z_i|Z^{i-1})\le\sum_{i=1}^n H(Z_i)=nH(Z)$.

Achievable rate region: Recall the non-negativity for rates; the rate relations as specified in (5); the conditions for reliable communication for both legitimate receivers, i.e., (6), (8), and individual secrecy at the eavesdropper, i.e., (9), (11), (12). Eliminating R_{1r},R_{2r},R_{1s} and R_{1k} by applying Fourier-Motzkin procedure [9], we get the desired rate region. □

IV. Gaussian BC with an external eavesdropper

The Gaussian broadcast channel with an external eavesdropper is shown in Fig. 2. Suppose X is the channel input with a power constraint P, and the signals received by both receivers and the eavesdropper are given by

$$\begin{aligned}
Y_1&=X+N_1;\\
Y_2&=X+N_2;\\
Z&=X+N_e,
\end{aligned}$$

where N_1,N_2 and N_e are additive white Gaussian noise (AWGN) independent of X, where $N_1\sim\mathcal{N}(0,\sigma_1^2)$, $N_2\sim\mathcal{N}(0,\sigma_2^2)$ and $N_e\sim\mathcal{N}(0,\sigma_e^2)$, respectively.

According to the noise level in the channels to both receivers and the eavesdropper, the overall channel can be regarded to be *stochastically* degraded. For simplicity, we only consider its corresponding *physically* degraded instances. The reason is that the same analysis can be easily extended to the stochastically degraded case. That is, the scenario: $\sigma_e^2\ge\sigma_2^2\ge\sigma_1^2$, as $X\to Y_1\to Y_2\to Z$ forms a Markov chain, is of our interest.

A. An outer bound

Proposition 2. *An outer bound to the individual secrecy capacity region for the Gaussian BC when $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain is given by the set of the rate pairs (R_1, R_2) satisfying*

$$R_1 \leq C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_1^2}\right) - C\left(\frac{\alpha(1-\gamma)P}{\gamma\alpha P+\sigma_e^2}\right) + \min\left\{R_2, C\left(\frac{(1-\gamma\alpha)P}{\gamma\alpha P+\sigma_e^2}\right)\right\}; \quad (13)$$

$$R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right), \quad (14)$$

for some $\alpha, \gamma \in [0,1]$, and $C(x) = 0.5\log_2(1+x)$, i.e., the Gaussian capacity function.

Proof: First let us consider R_2.

$$\begin{aligned} nR_2 = H(M_2) &\overset{(a)}{=} I(M_2; Y_2^n) + nO(\epsilon) \\ &\overset{(b)}{\leq} I(M_2; Y_2^n) - I(M_2; Z^n) + nO(\epsilon) \\ &= \underbrace{h(Y_2^n) - h(Z^n)}_{nR_2^1} - \underbrace{(h(Y_2^n|M_2) - h(Z^n|M_2))}_{nR_2^2} + nO(\epsilon), \end{aligned}$$

where (a) is due to the Fano's inequality; (b) is due to adding the non-negative term $-I(M_2; Z^n) + nO(\epsilon) \geq 0$, which is due to the individual secrecy constraint.

Note that, according to [11, Lemma 10 and equation (75)], nR_2^1 can be bounded by:

$$nR_2^1 = h(Y_2^n) - h(Z^n) \leq \frac{n}{2}\log\frac{P+\sigma_2^2}{P+\sigma_e^2}. \quad (15)$$

Further, due to the degradedness, we have for nR_2^2 :

$$nR_2^2 \geq h(Y_2^n|X^n) - h(Z^n|X^n) = \frac{n}{2}\log\frac{\sigma_2^2}{\sigma_e^2};$$

$$nR_2^2 \leq h(Y_2^n) - h(Z^n) \leq \frac{n}{2}\log\frac{P+\sigma_2^2}{P+\sigma_e^2}.$$

Hence, there exists $\alpha \in [0,1]$ such that

$$nR_2^2 = h(Y_2^n|M_2) - h(Z^n|M_2) = \frac{n}{2}\log\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_e^2}. \quad (16)$$

Combining (15) and (16), we have

$$\begin{aligned} nR_2 = nR_2^1 - nR_2^2 &\leq \frac{n}{2}\log\frac{P+\sigma_2^2}{P+\sigma_e^2} - \frac{n}{2}\log\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_e^2} \\ &= \frac{n}{2}\log\frac{(P+\sigma_2^2)(\alpha P+\sigma_e^2)}{(\alpha P+\sigma_2^2)(P+\sigma_e^2)}. \end{aligned}$$

Thus, we obtain (14).

Now we proceed to bound R_1.

$$\begin{aligned} nR_1 &= H(M_1) = H(M_1|M_2) = I(M_1; Y_1^n|M_2) + nO(\epsilon) \\ &= I(M_1; Y_1^n|M_2) - I(M_1; Z^n|M_2) + I(M_1; Z^n|M_2) + nO(\epsilon) \\ &= \underbrace{h(Y_1^n|M_2) - h(Z^n|M_2)}_{nR_1^1} + \underbrace{I(M_1; Z^n|M_2)}_{nR_1^3} \\ &\quad - \underbrace{(h(Y_1^n|M_1, M_2) - h(Z^n|M_1, M_2))}_{nR_1^2} + nO(\epsilon). \end{aligned} \quad (17)$$

Applying Costa's entropy-power inequality [12, Theorem 1] and using (16), we obtain

$$nR_1^1 = h(Y_1^n|M_2) - h(Z^n|M_2) \leq \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_e^2}; \quad (18)$$

For nR_1^2, due to the degradedness, we have

$$nR_1^2 \geq h(Y_1^n|X^n) - h(Z^n|X^n) = \frac{n}{2}\log\frac{\sigma_1^2}{\sigma_e^2};$$

$$nR_1^2 \leq h(Y_1^n|M_2) - h(Z^n|M_2) \leq \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_e^2}.$$

Hence, there exists a $\gamma \in [0,1]$ such that

$$nR_1^2 = h(Y_1^n|M_1, M_2) - h(Z^n|M_1, M_2) = \frac{n}{2}\log\frac{\gamma\alpha P+\sigma_1^2}{\gamma\alpha P+\sigma_e^2}.$$

Further, applying the entropy power inequality (EPI) [13], we can bound $h(Z^n|M_1, M_2)$ by

$$h(Z^n|M_1, M_2) \geq \frac{n}{2}\log 2\pi e(\gamma\alpha P+\sigma_e^2). \quad (19)$$

For nR_1^3, we observe that

$$\begin{aligned} nR_1^3 = I(M_1; Z^n|M_2) &= I(M_1, M_2; Z^n) - I(M_2; Z^n) \\ &= I(M_2; Z^n|M_1) + I(M_1; Z^n) - I(M_2; Z^n) \\ &\leq nR_2 + nO(\epsilon). \end{aligned}$$

Moreover, we can bound nR_1^3 as follows

$$\begin{aligned} nR_1^3 = I(M_1; Z^n|M_2) &= h(Z^n|M_2) - h(Z^n|M_1, M_2) \\ &\leq h(Z^n) - h(Z^n|M_1, M_2) \\ &\leq \frac{n}{2}\log\frac{P+\sigma_e^2}{\gamma\alpha P+\sigma_e^2}. \end{aligned}$$

Therefore, we have so far

$$\begin{aligned} nR_1 &= nR_1^1 - nR_1^2 + nR_1^3 + nO(\epsilon) \\ &\leq \frac{n}{2}\log\frac{\alpha P+\sigma_1^2}{\alpha P+\sigma_e^2} - \frac{n}{2}\log\frac{\gamma\alpha P+\sigma_1^2}{\gamma\alpha P+\sigma_e^2} \\ &\quad + \min\left\{nR_2, \frac{n}{2}\log\frac{P+\sigma_e^2}{\gamma\alpha P+\sigma_e^2}\right\} + nO(\epsilon). \end{aligned}$$

Letting $\epsilon \to 0$, we obtain (13) that concludes our proof. ■

From Proposition 2, we obtain a looser outer bound as described in the following corollary.

Corollary 3. *An outer bound to the individual secrecy capacity region for the Gaussian BC when $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain is given by the set of the rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right); \\ R_2 &\leq C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_e^2}\right); \quad (20) \\ R_1 + R_2 &\leq C\left(\frac{\alpha P}{\sigma_1^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P+\sigma_2^2}\right), \end{aligned}$$

for some $\alpha \in [0,1]$.

B. An inner bound

Proposition 4. *An inner bound of the individual secrecy capacity region for the Gaussian BC when $X \to Y_1 \to Y_2 \to Z$ forms a Markov chain is given by the set of the rate pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 \leq & C\left(\frac{\alpha P}{\sigma_1^2}\right) - C\left(\frac{\alpha P}{\sigma_e^2}\right) + C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) \\ & - \max\left\{R_2, C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right)\right\}; \qquad (21) \\ R_2 \leq & C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right), \end{aligned}$$

where $\alpha \in [0,1]$.

Proof: The region is obtained from Theorem 1 by using jointly Gaussian (U,V) with $U \sim \mathcal{N}(0,(1-\alpha)P)$, $V \sim \mathcal{N}(0,\alpha P)$, $X = U + V$, where U and V are independent and $\alpha \in [0,1]$. ∎

C. A constant gap within 0.5 bits

Proposition 5. *The achievable individual secrecy rate region given in Proposition 4, i.e., the set of (R_1, R_2) satisfying (21) for some $\alpha \in [0,1]$, approaches the individual secrecy capacity region of the Gaussian BC within 0.5 bits.*

Proof: Consider the gap between the inner and outer bounds as specified in (21) and (20), respectively. Taking the same choice of α in both bounds, the gap may occur only in the $R_1 + R_2$ term. More specifically, we consider their subregions in the following two cases for comparison.
Case 1: $R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right)$. In this case, the corresponding subregions of (R_1, R_2) in the inner and outer bound are the same.
Case 2: $C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) < R_2 \leq C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right)$. Note that this case is possible only if

$$C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right) < C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_2^2}\right) - C\left(\frac{(1-\alpha)P}{\alpha P + \sigma_e^2}\right).$$

The above inequality holds for

$$\begin{aligned} & 0 \leq \alpha < 1 && \text{as} \quad \sigma_e^2 \geq P + 2\sigma_2^2; \\ \text{or} \quad & 0 \leq \alpha < \tfrac{(\sigma_e^2 - \sigma_2^2)^2}{P(P+\sigma_2^2)} - \tfrac{\sigma_2^2}{P} && \text{as} \quad \sigma_e^2 \leq P + 2\sigma_2^2 \quad \text{and} \\ & && \quad \sigma_e^2 > \sigma_2^2 + \sqrt{\sigma_2^2(P+\sigma_2^2)}. \end{aligned}$$

The gap between the subregions of (R_1, R_2) the inner and upper bound, occurs only in the $R_1 + R_2$ term that is upper bounded by $C\left(\frac{\alpha P}{\sigma_e^2}\right)$. We note that

- If $\sigma_e^2 \geq P + 2\sigma_2^2$, we have for $0 \leq \alpha < 1$,

$$C\left(\frac{\alpha P}{\sigma_e^2}\right) \overset{(a)}{<} C\left(\frac{P}{\sigma_e^2}\right) \overset{(b)}{\leq} C\left(\frac{P}{P + 2\sigma_2^2}\right) \leq C(1) = 0.5$$

where (a) is by the fact that $C(x)$ is an increasing function with respect to x and α is upper bounded by 1; (b) is due to the fact that $\sigma_e^2 \geq P + 2\sigma_2^2$.

- If $\sigma_e^2 \leq P + 2\sigma_2^2$ and $\sigma_e^2 > \sigma_2^2 + \sqrt{\sigma_2^2(P+\sigma_2^2)}$, we have for $0 \leq \alpha < \frac{(\sigma_e^2 - \sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P}$,

$$C\left(\frac{\alpha P}{\sigma_e^2}\right) \overset{(c)}{<} C\left(\frac{\sigma_e^2 - \sigma_2^2}{P + \sigma_2^2} - \frac{\sigma_2^2(P+\sigma_e^2)}{\sigma_e^2(P+\sigma_2^2)}\right) \overset{(d)}{\leq} C(1) = 0.5$$

where (c) is due to the fact that $C(x)$ is an increasing function with respect to x and α is upper bounded by $\frac{(\sigma_e^2 - \sigma_2^2)^2}{P(P+\sigma_2^2)} - \frac{\sigma_2^2}{P}$; (d) is due to the fact that $(\sigma_e^2 - \sigma_2^2)/(P + \sigma_2^2) \leq 1$ since $\sigma_e^2 \leq P + 2\sigma_2^2$. ∎

V. Conclusion

In this paper, we studied the problem of secure communication over broadcast channels under the individual secrecy constraint. Especially, we utilized the message for the weaker receiver to secure partial message to the stronger receiver, which improves the transmission efficiency while guaranteeing an acceptable secrecy level from the end user's perspective. As a general result, we proposed an achievable rate region for the discrete memoryless broadcast channel under this notion of secrecy. We also looked into the corresponding Gaussian scenario. Both inner bound and upper bounds are derived, and a constant gap result (i.e., 0.5 bits within the individual secrecy capacity region) is obtained.

References

[1] T. Cover, "Broadcast channels," *IEEE Transactions on Information Theory*, vol. 18, no. 1, pp. 2–14, Jan 1972.

[2] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 197–207, Mar 1973.

[3] R. G. Gallager, "Coding and capacity for degraded broadcast channels," *Problemy Peridachi Informatsi*, vol. 10, no. 3, pp. 3–14, 1974.

[4] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, 2009.

[5] G. Bagherikaram, A. S. Motahari, and A. K. Khandani, "Secrecy rate region of the broadcast channel with an eavesdropper," *CoRR*, vol. abs/0910.3658, 2009.

[6] Y. Chen, O. O. Koyluoglu, and A. Sezgin, "On the achievable individual-secrecy rate region for broadcast channels with receiver side information," in *Proc. 2014 IEEE International Symposium on Information Theory (ISIT)*, June 2014, pp. 26–30.

[7] A. Carleial and M. Hellman, "A note on wyner's wiretap channel (corresp.)," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[8] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[9] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.

[10] Y.-K. Chia and A. El Gamal, "Three-receiver broadcast channels with common and confidential messages," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2748–2765, May 2012.

[11] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[12] M. Costa, "A new entropy power inequality," *IEEE Transactions on Information Theory*, vol. 31, no. 6, pp. 751–760, Nov 1985.

[13] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.