The Secrecy Capacity Region of the Degraded Vector Gaussian Broadcast Channel

Ghadamali Bagherikaram, Abolfazl S. Motahari, Amir K. Khandani
Coding and Signal Transmission Laboratory,
Department of Electrical and Computer Engineering,
University of Waterloo, Waterloo, Ontario, N2L 3G1
Emails: {gbagheri,abolfazl,khandani}@cst.uwaterloo.ca

[1] ***Abstract*— In this paper, we consider a scenario where a source node wishes to broadcast two confidential messages for two respective receivers via a Gaussian MIMO broadcast channel. A wire-tapper also receives the transmitted signal via another MIMO channel. It is assumed that the channels are degraded and the wire-tapper has the worst channel. We establish the capacity region of this scenario. Our achievability scheme is a combination of the superposition of Gaussian codes and randomization within the layers which we will refer to as Secret Superposition Coding. For the outerbound, we use the notion of enhanced channel to show that the secret superposition of Gaussian codes is optimal. It is shown that we only need to enhance the channels of the legitimate receivers, and the channel of the eavesdropper remains unchanged.**

I. Introduction

Recently there has been significant research conducted in both theoretical and practical aspects of wireless communication systems with Multiple-Input Multiple-Output (MIMO) antennas. Most works have focused on the role of MIMO in enhancing the throughput and robustness. In this work, however, we focus on the role of such multiple antennas in enhancing wireless security.

The information-theoretic single user secure communication problem was first characterized by Wyner in [1]. Wyner considered a scenario in which a wire-tapper receives the transmitted signal over a degraded channel with respect to the legitimate receiver's channel. He measured the level of ignorance at the eavesdropper by its equivocation and characterized the capacity-equivocation region. Wyner's work was then extended to the general broadcast channel with confidential messages by Csiszar et al. [2]. They considered transmitting confidential information to the legitimate receiver while transmitting common information to both the legitimate receiver and the wire-tapper. They established a capacity-equivocation region of this channel. The secrecy capacity for the Gaussian wire-tap channel was characterized by Leung-Yan-Cheong in [3].

The Gaussian MIMO wire-tap channel has recently been considered by Khisti et al. in [4], [5]. Finding the optimal distribution, which maximizes the secrecy capacity for this channel is a nonconvex problem. Khisti et al., however, followed an indirect approach to evaluate the secrecy capacity of Csiszar et al. They used a genie-aided upper bound and characterized the secrecy capacity as the saddle-value of a min-max problem to show that Gaussian distribution is optimal. Motivated by the broadcast nature of the wireless communication systems, we considered the secure broadcast channel in [6]. In this work, we characterized the secrecy capacity region of the degraded broadcast channel and showed that the secret superposition coding is optimal.

The capacity region of the conventional Gaussian MIMO broadcast channel is studied in [7] by Weingarten et al. The notion of an enhanced broadcast channel is introduced in this work and is used jointly with entropy power inequality to characterize the capacity region of the degraded vector Gaussian broadcast channel. They showed that the superposition of Gaussian codes is optimal for the degraded vector Gaussian broadcast channel and that dirty-paper coding is optimal for the nondegraded case.

In this paper, we aim to characterize the secrecy capacity region of a secure degraded vector Gaussian MIMO broadcast channel. Our achievability scheme is a combination of the superposition of Gaussian codes and randomization within the layers. To prove the converse, we use the notion of enhanced channel and show that the secret superposition of Gaussian codes is optimal. We have extended the results of this paper to the general Gaussian MIMO broadcast channel in [8] and showed that secret dirty paper coding of Gaussian codes is optimal.

We acknowledge two other independent and concurrent works of [9], [10] where the authors considered the secrecy capacity region of the Gaussian MIMO broadcast channel.

The rest of the paper is organized as follows. In section II we introduce some preliminaries. In section III, we establish the secrecy capacity region of the Gaussian vector broadcast channel. In Section V, we conclude the paper.

II. Preliminaries

Consider a Secure Gaussian Multiple-Input Multiple-Output Broadcast Channel (SGMBC) as depicted in Fig. 1. In this

[1]Financial support provided by Nortel and the corresponding matching funds by the Natural Sciences and Engineering Research Council of Canada (NSERC), and Ontario Centers of Excellence (OCE) are gratefully acknowledged.

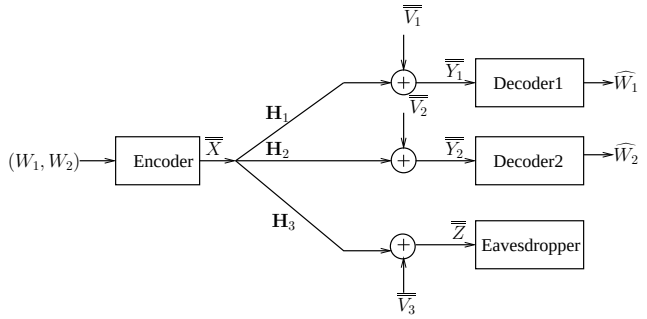

Fig. 1. Secure Gaussian MIMO Broadcast Channel

confidential setting, the transmitter wishes to send two independent messages (W_1, W_2) to the respective receivers in n uses of the channel and prevent the eavesdropper from having any information about the messages. At a specific time, the signals received by the destinations and the eavesdropper are given by

$$\begin{aligned} \mathbf{y_1} &= \mathbf{H}_1\mathbf{x} + \mathbf{n_1}, \\ \mathbf{y_2} &= \mathbf{H}_2\mathbf{x} + \mathbf{n_2}, \\ \mathbf{z} &= \mathbf{H}_3\mathbf{x} + \mathbf{n_3}, \end{aligned} \tag{1}$$

where

- $\mathbf{x}$ is a real input vector of size $t \times 1$ under an input covariance constraint. We require that $E[\mathbf{x}^T\mathbf{x}] \preceq \mathbf{S}$ for a positive semi-definite matrix $\mathbf{S} \succeq 0$. Here,$\prec, \preceq, \succ$, and $\succeq$ represent partial ordering between symmetric matrices where $\mathbf{B} \succeq \mathbf{A}$ means that $(\mathbf{B} - \mathbf{A})$ is a positive semi-definite matrix.
- $\mathbf{y_1}$, $\mathbf{y_2}$, and $\mathbf{z}$ are real output vectors which are received by the destinations and the eavesdropper respectively. These are vectors of size $r_1 \times 1$, $r_2 \times 1$, and $r_3 \times 1$, respectively.
- $\mathbf{H}_1$, $\mathbf{H}_2$, and $\mathbf{H}_3$ are fixed, real gain matrices which model the channel gains between the transmitter and the receivers. These are matrices of size $r_1 \times t$, $r_2 \times t$, and $r_3 \times t$ respectively. The channel state information is assumed to be known perfectly at the transmitter and at all receivers.
- $\mathbf{n_1}$, $\mathbf{n_2}$ and $\mathbf{n_3}$ are real Gaussian random vectors with zero means and covariance matrices $\mathbf{N_1} = E[\mathbf{n_1}\mathbf{n_1}^T] \succ 0$, $\mathbf{N_2} = E[\mathbf{n_2}\mathbf{n_2}^T] \succ 0$, and $\mathbf{N_3} = E[\mathbf{n_3}\mathbf{n_3}^T] \succ 0$ respectively.

Let W_1 and W_2 denote the the message indices of user 1 and user 2, respectively. Furthermore, let $\overline{\overline{X}}$, $\overline{\overline{Y}}_1$, $\overline{\overline{Y}}_2$, and $\overline{\overline{Z}}$ denote the random channel input and random channel outputs matrices over a block of n samples. Let $\overline{\overline{V}}_1$, $\overline{\overline{V}}_2$, and $\overline{\overline{V}}_3$ denote the additive noises of the channels. Thus,

$$\begin{aligned} \overline{\overline{Y}}_1 &= \mathbf{H}_1\overline{\overline{X}} + \overline{\overline{V}}_1, \\ \overline{\overline{Y}}_2 &= \mathbf{H}_2\overline{\overline{X}} + \overline{\overline{V}}_2, \\ \overline{\overline{Z}} &= \mathbf{H}_3\overline{\overline{X}} + \overline{\overline{V}}_3. \end{aligned} \tag{2}$$

Note that $\overline{\overline{V}}_i$ is an $r_i \times n$ random matrix and $\mathbf{H}_i$ is an $r_i \times t$ deterministic matrix where $i = 1, 2, 3$. The columns of $\overline{\overline{V}}_i$ are independent Gaussian random vectors with covariance matrices $\mathbf{N_i}$ for $i = 1, 2, 3$. In addition $\overline{\overline{V}}_i$ is independent of $\overline{\overline{X}}$, W_1 and W_2. A $((2^{nR_1}, 2^{nR_2}), n)$ code for the above channel consists of a stochastic encoder

$$f : (\{1, 2, ..., 2^{nR_1}\} \times \{1, 2, ..., 2^{nR_2}\}) \rightarrow \overline{\overline{\mathcal{X}}}, \tag{3}$$

and two decoders,

$$g_1 : \overline{\overline{\mathcal{Y}}}_1 \rightarrow \{1, 2, ..., 2^{nR_1}\}, \tag{4}$$

and

$$g_2 : \overline{\overline{\mathcal{Y}}}_2 \rightarrow \{1, 2, ..., 2^{nR_2}\}. \tag{5}$$

where a script letter with double overline denotes the finite alphabet of a random vector. The average probability of error is defined as the probability that the decoded messages are not equal to the transmitted messages; that is,

$$P_e^{(n)} = P(g_1(\overline{\overline{Y}}_1) \neq W_1 \cup g_2(\overline{\overline{Y}}_2) \neq W_2). \tag{6}$$

The secrecy levels of confidential messages W_1 and W_2 are measured at the eavesdropper in terms of equivocation rates, which are defined as follows.

Definition 1 *The equivocation rates R_{e1}, R_{e2} and R_{e12} for the secure broadcast channel are:*

$$\begin{aligned} R_{e1} &= \frac{1}{n}H(W_1|\overline{\overline{Z}}), \\ R_{e2} &= \frac{1}{n}H(W_2|\overline{\overline{Z}}), \\ R_{e12} &= \frac{1}{n}H(W_1, W_2|\overline{\overline{Z}}). \end{aligned} \tag{7}$$

The perfect secrecy rates R_1 and R_2 are the amount of information that can be sent to the legitimate receivers both reliably *and* confidentially.

Definition 2 *A secrecy rate pair (R_1, R_2) is said to be achievable if for any $\epsilon > 0, \epsilon_1 > 0, \epsilon_2 > 0, \epsilon_3 > 0$, there exists a sequence of $((2^{nR_1}, 2^{nR_2}), n)$ codes, such that for sufficiently large n,*

$$P_e^{(n)} \leq \epsilon, \tag{8}$$

$$R_{e1} \geq R_1 - \epsilon_1, \tag{9}$$

$$R_{e2} \geq R_2 - \epsilon_2, \tag{10}$$

$$R_{e12} \geq R_1 + R_2 - \epsilon_3. \tag{11}$$

In the above definition, the first condition concerns the reliability, while the other conditions guarantee perfect secrecy for each individual message and both messages as well. The model presented in (1) is SGMBC. For lack of space, the SGMBC cannot be discussed within this paper, and we will only consider a subclass of this channel here. The special subclass that we will consider is the Secure Aligned Degraded MIMO Broadcast Channel (SADBC). The MIMO broadcast channel of (1) is said to be aligned if the number of transmit

antennas is equal to the number of receive antennas at each of the users and the eavesdropper ($t = r_1 = r_2 = r_3$) and the gain matrices are all identity matrices ($\mathbf{H}_1 = \mathbf{H}_2 = \mathbf{H}_3 = \mathbf{I}$). Furthermore, if the additive noise vectors' covariance matrices are ordered such that $0 \prec \mathbf{N_1} \preceq \mathbf{N_2} \preceq \mathbf{N_3}$, then the channel is SADBC.

III. The Capacity Region of The SADBC

In this section, we characterize the capacity region of the SADBC. In [6], we considered the degraded broadcast channel with confidential messages and establish its secrecy capacity region.

Theorem 1 *The capacity region for transmitting independent secret messages over the degraded broadcast channel is the convex hull of the closure of all (R_1, R_2) satisfying*

$$R_1 \leq I(X;Y_1|U) - I(X;Z|U), \quad (12)$$
$$R_2 \leq I(U;Y_2) - I(U;Z). \quad (13)$$

for some joint distribution $P(u)P(x|u)P(y_1, y_2, z|x)$.

Proof: Our achievable coding scheme is based on Cover's superposition scheme and random binning. We refer to this scheme as the Secret Superposition Scheme. In this scheme, randomization in the first layer increases the secrecy rate of the second layer. Our converse proof is based on a combination of the converse proof of the conventional degraded broadcast channel and Csiszar Lemma. Please see [6] for details. ■

Note that finding optimal distribution which characterizes the boundary points of (12) and for the Gaussian channels involves solving a functional, nonconvex optimization problem. Usually nontrivial techniques and strong inequalities are used to solve optimization problems of this type. Indeed, for the single antenna case, we successfully evaluated the capacity expression of this scheme in [11]. Liu et al. in [12] evaluated the capacity expression of MIMO wire-tap channel by using the channel enhancement method. In the following section, we state and prove our result for the capacity region of SADBC.

First, we define the achievable rate region due to Gaussian codebook under a covariance matrix constraint $\mathbf{S} \succeq 0$. The achievability scheme of Theorem 1 is the secret superposition of Gaussian codes and successive decoding at the first receiver. According to the above theorem, for any covariance matrix input constraint $\mathbf{S}$ and two semi-definite matrices $\mathbf{B_1} \succeq 0$ and $\mathbf{B_2} \succeq 0$ such that $\mathbf{B_1} + \mathbf{B_2} \preceq \mathbf{S}$, it is possible to achieve the following rates,

$$R_1^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}}) = \frac{1}{2}\log|\mathbf{N_1^{-1}}(\mathbf{B_1} + \mathbf{N_1})| - \frac{1}{2}\log|\mathbf{N_3^{-1}}(\mathbf{B_1} + \mathbf{N_3})|,$$
$$R_2^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}}) = \frac{1}{2}\log\frac{|\mathbf{B_1} + \mathbf{B_2} + \mathbf{N_2}|}{|\mathbf{B_1} + \mathbf{N_2}|} - \frac{1}{2}\log\frac{|\mathbf{B_1} + \mathbf{B_2} + \mathbf{N_3}|}{|\mathbf{B_1} + \mathbf{N_3}|}.$$

Definition 3 *Let $\mathbf{S}$ be a positive semi-definite matrix. Then, the Gaussian rate region of SADBC under a covariance matrix constraint $\mathbf{S}$ is given by*

$$\mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}}) = \left\{ \begin{array}{l} \left(R_1^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}}), R_2^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}})\right) | \\ s.t \;\; \mathbf{S} - (\mathbf{B_1} + \mathbf{B_2}) \succeq 0, \;\; \mathbf{B_k} \succeq 0, \;\; k = 1, 2 \end{array} \right\}. \quad (14)$$

We will show that $\mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}})$ is the capacity region of the SADBC. Before that, certain preliminaries need to be addressed.

Definition 4 *The rate vector $R^* = (R_1, R_2)$ is said to be an optimal Gaussian rate vector under the covariance matrix $\mathbf{S}$, if $R^* \in \mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}})$ and if there is no other rate vector $R'^* = (R_1', R_2') \in \mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}})$ such that $R_1' \geq R_1$ and $R_2' \geq R_2$ where at least one the inequalities is strict. The set of positive semi-definite matrices $(\mathbf{B_1^*}, \mathbf{B_2^*})$ such that $\mathbf{B_1^*} + \mathbf{B_2^*} \preceq \mathbf{S}$ is said to be realizing matrices of an optimal Gaussian rate vector if the rate vector $\left(R_1^G(\mathbf{B_{1,2}^*}, \mathbf{N_{1,2,3}}), R_2^G(\mathbf{B_{1,2}^*}, \mathbf{N_{1,2,3}})\right)$ is an optimal Gaussian rate vector.*

Definition 5 *A SADBC with noise covariance matrices of $(\mathbf{N_1'}, \mathbf{N_2'}, \mathbf{N_3'})$ is an enhanced version of another SADBC with noise covariance matrices $(\mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3})$ if*

$$\mathbf{N_1'} \preceq \mathbf{N_1}, \quad \mathbf{N_2'} \preceq \mathbf{N_2}, \quad \mathbf{N_3'} = \mathbf{N_3}, \quad \mathbf{N_1'} \preceq \mathbf{N_2'}. \quad (15)$$

Obviously, the capacity region of the enhanced version contains the capacity region of the original channel. Note that in characterizing the capacity region of the conventional Gaussian MIMO broadcast channel, all channels must be enhanced by reducing the noise covariance matrices. In our scheme, however, we only enhance the channels for the legitimate receivers and the channel of the eavesdropper remains unchanged. This is due to the fact that the capacity region of the enhanced channel must contain the original capacity region. Reducing the noise covariance matrix of the eavesdropper's channel, however, may reduce the secrecy capacity region. The following theorem connects the definitions of the optimal Gaussian rate vector and the enhanced channel.

Theorem 2 *Consider a SADBC with positive definite noise covariance matrices $(\mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3})$. Let $\mathbf{B_1^*}$ and $\mathbf{B_2^*}$ be realizing matrices of an optimal Gaussian rate vector under a transmit covariance matrix constraint $\mathbf{S} \succ 0$. There then exists an enhanced SADBC with noise covariance matrices $(\mathbf{N_1'}, \mathbf{N_2'}, \mathbf{N_3'})$ that the following properties hold.*

1) *Enhancement:* $\mathbf{N_1'} \preceq \mathbf{N_1}, \quad \mathbf{N_2'} \preceq \mathbf{N_2}, \quad \mathbf{N_3'} = \mathbf{N_3}, \quad \mathbf{N_1'} \preceq \mathbf{N_2'}$,
2) *Proportionality:* *There exists an $\alpha \geq 0$ and a matrix $\mathbf{A}$ such that* $(\mathbf{I} - \mathbf{A})(\mathbf{B_1^*} + \mathbf{N_1'}) = \alpha\mathbf{A}(\mathbf{B_1^*} + \mathbf{N_3'})$,
3) *Rate and optimality preservation:* $R_k^G(\mathbf{B_{1,2}^*}, \mathbf{N_{1,2,3}}) = R_k^G(\mathbf{B_{1,2}^*}, \mathbf{N_{1,2,3}'}) \quad \forall k = 1, 2$, *furthermore, $\mathbf{B_1^*}$ and $\mathbf{B_2^*}$ are realizing matrices of an optimal Gaussian rate vector in the enhanced channel.*

Theorem 2 states that if there exists the realizing matrices of the boundary of $\mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}})$, then the secret superposition coding with Gaussian codebook is the optimal choice for the capacity region of a SADBC. Note that this Theorem provides a sufficient condition to evaluate the capacity region of SADBC.

Proof: The realizing matrices $\mathbf{B_1^*}$ and $\mathbf{B_2^*}$ are the solution of the following optimization problem:

$$\max_{(\mathbf{B_1},\mathbf{B_2})} R_1^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}}) + \mu R_2^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}}) \quad (16)$$
$$\text{s.t } \mathbf{B_1} \succeq 0, \quad \mathbf{B_2} \succeq 0, \quad \mathbf{B_1} + \mathbf{B_2} \preceq \mathbf{S},$$

where $\mu \geq 1$. Using the Lagrange Multiplier method, the above constraint optimization problem is equivalent to the following unconditional optimization problem:

$$\max_{(\mathbf{B_1},\mathbf{B_2})} R_1^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}}) + \mu R_2^G(\mathbf{B_{1,2}}, \mathbf{N_{1,2,3}})$$
$$+Tr\{\mathbf{B_1 O_1}\} + Tr\{\mathbf{B_2 O_2}\} + Tr\{(\mathbf{S} - \mathbf{B_1} - \mathbf{B_2})\mathbf{O_3}\},$$

where $\mathbf{O_1}$, $\mathbf{O_2}$, and $\mathbf{O_3}$ are positive semi-definite $t \times t$ matrices such that $Tr\{\mathbf{B_1^* O_1}\} = 0$, $Tr\{\mathbf{B_2^* O_2}\} = 0$, and $Tr\{(\mathbf{S} - \mathbf{B_1^*} - \mathbf{B_2^*})\mathbf{O_3}\} = 0$. As all $\mathbf{B_k^*}$, $k = 1, 2$, $\mathbf{O_i}$, $i = 1, 2, 3$, and $\mathbf{S} - \mathbf{B_1^*} - \mathbf{B_2^*}$ are positive semi-definite matrices, then we must have $\mathbf{B_k^* O_k} = 0$, $k = 1, 2$ and $(\mathbf{S} - \mathbf{B_1^*} - \mathbf{B_2^*})\mathbf{O_3} = 0$. According to the necessary KKT conditions, and after some manipulations we have:

$$(\mathbf{B_1^*} + \mathbf{N_1})^{-1} + (\mu - 1)(\mathbf{B_1^*} + \mathbf{N_3})^{-1} + \mathbf{O_1} = \mu(\mathbf{B_1^*} + \mathbf{N_2})^{-1} + \mathbf{O_2}, \quad (17)$$

$$\mu(\mathbf{B_1^*} + \mathbf{B_2^*} + \mathbf{N_2})^{-1} + \mathbf{O_2} = \mu(\mathbf{B_1^*} + \mathbf{B_2^*} + \mathbf{N_3})^{-1} + \mathbf{O_3}. \quad (18)$$

We choose the noise covariance matrices of the enhanced SADBC as the following:

$$\mathbf{N_1^{'}} = \left(\mathbf{N_1}^{-1} + \mathbf{O_1}\right)^{-1}, \quad (19)$$
$$\mathbf{N_2^{'}} = \left((\mathbf{B_1^*} + \mathbf{N_2})^{-1} + \frac{1}{\mu}\mathbf{O_2}\right)^{-1} - \mathbf{B_1^*},$$
$$\mathbf{N_3^{'}} = \mathbf{N_3}.$$

As $\mathbf{O_1} \succeq 0$ and $\mathbf{O_2} \succeq 0$, then the above choice has the enhancement property. The expression $\left((\mathbf{B_1^*} + \mathbf{N_1})^{-1} + \mathbf{O_1}\right)^{-1}$ can be written as:

$$\begin{aligned}
\left((\mathbf{B_1^*} + \mathbf{N_1})^{-1} + \mathbf{O_1}\right)^{-1} &= \left((\mathbf{B_1^*} + \mathbf{N_1})^{-1}\right. \\
&\quad \left.(\mathbf{I} + (\mathbf{B_1^*} + \mathbf{N_1})\mathbf{O_1})\right)^{-1} \\
&\overset{(a)}{=} (\mathbf{I} + \mathbf{N_1 O_1})^{-1}(\mathbf{B_1^*} + \mathbf{N_1}) \\
&\quad -\mathbf{B_1^*} + \mathbf{B_1^*} \\
&= (\mathbf{I} + \mathbf{N_1 O_1})^{-1}\left((\mathbf{B_1^*} + \mathbf{N_1})\right. \\
&\quad \left. - (\mathbf{I} + \mathbf{N_1 O_1})\mathbf{B_1^*}\right) + \mathbf{B_1^*} \\
&\overset{(b)}{=} (\mathbf{I} + \mathbf{N_1 O_1})^{-1}\mathbf{N_1} + \mathbf{B_1^*} \\
&= \left(\mathbf{N_1}\left(\mathbf{N_1^{-1}} + \mathbf{O_1}\right)\right)^{-1}\mathbf{N_1} + \mathbf{B_1^*} \\
&= \left(\mathbf{N_1^{-1}} + \mathbf{O_1}\right)^{-1} + \mathbf{B_1^*} \\
&= \mathbf{B_1^*} + \mathbf{N_1^{'}},
\end{aligned}$$

where (a) and (b) follows from the fact that $\mathbf{B_1^* O_1} = 0$. Similarly, it can be shown that

$$\mu(\mathbf{B_1^*} + \mathbf{N_2})^{-1} + \mathbf{O_2} = \mu(\mathbf{B_1^*} + \mathbf{N_2^{'}})^{-1},$$

Therefore, according to (17) the following property holds for the enhanced channel.

$$(\mathbf{B_1^*} + \mathbf{N_1^{'}})^{-1} + (\mu - 1)(\mathbf{B_1^*} + \mathbf{N_3^{'}})^{-1} = \mu(\mathbf{B_1^*} + \mathbf{N_2^{'}})^{-1}.$$

Since $\mathbf{N_1^{'}} \preceq \mathbf{N_2^{'}} \preceq \mathbf{N_3^{'}}$ then, there exists a matrix $\mathbf{A}$ such that $\mathbf{N_2^{'}} = (\mathbf{I} - \mathbf{A})\mathbf{N_1^{'}} + \mathbf{A}\mathbf{N_3^{'}}$ where $\mathbf{A} = (\mathbf{N_2^{'}} - \mathbf{N_1^{'}})(\mathbf{N_3^{'}} - \mathbf{N_1^{'}})^{-1}$. Therefore, the above equation can be written as.

$$(\mathbf{B_1^*} + \mathbf{N_1^{'}})^{-1} + (\mu - 1)(\mathbf{B_1^*} + \mathbf{N_3^{'}})^{-1} = \mu\left[(\mathbf{I} - \mathbf{A})(\mathbf{B_1^*} + \mathbf{N_1^{'}}) + \mathbf{A}(\mathbf{B_1^*} + \mathbf{N_3^{'}})\right]^{-1}.$$

Let $(\mathbf{I} - \mathbf{A})(\mathbf{B_1^*} + \mathbf{N_1^{'}}) = \alpha\mathbf{A}(\mathbf{B_1^*} + \mathbf{N_3^{'}})$ then after some manipulations, the above equation becomes

$$\frac{1}{\alpha}\mathbf{I} + (\mu - 1 - \frac{1}{\alpha})\mathbf{A} = \frac{\mu}{\alpha + 1}\mathbf{I}. \quad (20)$$

The above equation is satisfied by $\alpha = \frac{1}{\mu - 1}$ which completes the proportionality property.

We can now prove the rate conservation property. The expression $\frac{|\mathbf{B_1^*} + \mathbf{N_1^{'}}|}{|\mathbf{N_1^{'}}|}$ can be written as follow.

$$\begin{aligned}
\frac{|\mathbf{B_1^*} + \mathbf{N_1^{'}}|}{|\mathbf{N_1^{'}}|} &= \frac{|\mathbf{I}|}{|\mathbf{N_1^{'}}\left(\mathbf{B_1^*} + \mathbf{N_1^{'}}\right)^{-1}|} \\
&= \frac{|\mathbf{I}|}{|\left(\mathbf{B_1^*} + \mathbf{N_1^{'}} - \mathbf{B_1^*}\right)\left(\mathbf{B_1^*} + \mathbf{N_1^{'}}\right)^{-1}|} \\
&= \frac{|\mathbf{I}|}{|\mathbf{I} - \mathbf{B_1^*}\left(\mathbf{B_1^*} + \mathbf{N_1^{'}}\right)^{-1}|} \\
&= \frac{|\mathbf{I}|}{|\mathbf{I} - \mathbf{B_1^*}\left((\mathbf{B_1^*} + \mathbf{N_1})^{-1} + \mathbf{O_1}\right)|} \\
&\overset{(a)}{=} \frac{|\mathbf{I}|}{|\mathbf{I} - \mathbf{B_1^*}\left(\mathbf{B_1^*} + \mathbf{N_1}\right)^{-1}|} \\
&= \frac{|\mathbf{B_1^*} + \mathbf{N_1}|}{|\mathbf{N_1}|},
\end{aligned} \quad (21)$$

where (a) once again follows from the fact that $\mathbf{B_1^* O_1} = 0$. To complete the proof of rate conservation, consider the following equalities.

$$\begin{aligned}
\frac{|\mathbf{B_1^*} + \mathbf{B_2^*} + \mathbf{N_2^{'}}|}{|\mathbf{B_1^*} + \mathbf{N_2^{'}}|} &= \frac{|\mathbf{B_2^*}\left(\mathbf{B_1^*} + \mathbf{N_2^{'}}\right)^{-1} + \mathbf{I}|}{|\mathbf{I}|} \\
&= \frac{|\mathbf{B_2^*}\left((\mathbf{B_1^*} + \mathbf{N_2})^{-1} + \frac{1}{\mu}\mathbf{O_2}\right) + \mathbf{I}|}{|\mathbf{I}|} \\
&\overset{(a)}{=} \frac{|\mathbf{B_1^*} + \mathbf{B_2^*} + \mathbf{N_2}|}{|\mathbf{B_1^*} + \mathbf{N_2}|},
\end{aligned} \quad (22)$$

where (a) follows from the fact $\mathbf{B_2^* O_2} = 0$. Therefore, according to (21), (22), and the fact that $\mathbf{N_3^{'}} = \mathbf{N_3}$, the rate preservation property holds for the enhanced channel. To prove the optimality preservation, we need to show that $(\mathbf{B_1^*}, \mathbf{B_2^*})$ are

also realizing matrices of an optimal Gaussian rate vector in the enhanced channel. For that purpose, note that the necessary KKT conditions for the enhanced channel coincides with the KKT conditions of the original channel. ■

We can now use Theorem 2 to prove that $\mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}})$ is the capacity region of the SADBC. We follow Bergmans' approach [13] to prove a contradiction. Note that since the original channel is not proportional, we cannot apply Bergmans' proof on the original channel directly. Here we apply his proof on the enhanced channel instead.

Theorem 3 *Consider a SADBC with positive definite noise covariance matrices* $(\mathbf{N_1}, \mathbf{N_2}, \mathbf{N_3})$. *Let* $\mathcal{C}(\mathbf{S}, \mathbf{N_{1,2,3}})$ *denote the capacity region of the SADBC under a covariance matrix constraint* $\mathbf{S} \succ 0$. *Then,* $\mathcal{C}(\mathbf{S}, \mathbf{N_{1,2,3}}) = \mathcal{R}^G(\mathbf{S}, \mathbf{N_{1,2,3}})$.

Proof: The achievability scheme is secret superposition coding with Gaussian codebook. For the converse proof, we use a contradiction argument and assume that there exists an achievable rate vector(R_1, R_2) which is not in the Gaussian region. We can apply the steps of Bergmans' proof of [10] on the enhanced channel to show that this assumption is impossible. According to the Theorem 1, R_1 is bounded as follows.

$$\begin{aligned} R_1 &\leq h(\mathbf{y_1}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}) - (h(\mathbf{y_1}|\mathbf{x}, \mathbf{u}) - h(\mathbf{z}|\mathbf{x}, \mathbf{u})) \\ &= h(\mathbf{y_1}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}) - \frac{1}{2}\left(\log|\mathbf{N_1'}| - \log|\mathbf{N_3'}|\right) \end{aligned}$$

Since $R_1 > R_1^G(\mathbf{B_{1,2}}, \mathbf{N'_{1,2,3}})$, the above inequality means that

$$h(\mathbf{y_1}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}) > \frac{1}{2}\left(\log|\mathbf{B_1^*} + \mathbf{N_1'}| - \log|\mathbf{B_1^*} + \mathbf{N_3'}|)\right)$$

By the definition of matrix $\mathbf{A}$ and since $\mathbf{y_1} \rightarrow \mathbf{y_2} \rightarrow \mathbf{z}$ forms a Morkov chain, the received signals $\mathbf{z}$ and $\mathbf{y_2}$ can be written as $\mathbf{z} = \mathbf{y_1} + \widetilde{\mathbf{n}}$ and $\mathbf{y_2} = \mathbf{y_1} + \mathbf{A}^{\frac{1}{2}}\widetilde{\mathbf{n}}$ where $\widetilde{\mathbf{n}}$ is an independent Gaussian noise with covariance matrix $\widetilde{\mathbf{N}} = \mathbf{N_3'} - \mathbf{N_1'}$. According to Costa's Entropy Power Inequality and the previous inequality, we have

$$\begin{aligned} &h(\mathbf{y_2}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}) \\ &\quad\geq \frac{t}{2}\log\left(|\mathbf{I} - \mathbf{A}|^{\frac{1}{t}} 2^{\frac{2}{t}(h(\mathbf{y_1}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}))} + |\mathbf{A}|^{\frac{1}{t}}\right) \\ &\quad> \frac{t}{2}\log\left(\frac{|\mathbf{I} - \mathbf{A}|^{\frac{1}{t}}|\mathbf{B_1^*} + \mathbf{N_1'}|^{\frac{1}{t}}}{|\mathbf{B_1^*} + \mathbf{N_3'}|^{\frac{1}{t}}} + |\mathbf{A}|^{\frac{1}{t}})\right) \\ &\quad\stackrel{(a)}{=} \frac{1}{2}\log(\mathbf{B_1^*} + \mathbf{N_2'}) - \frac{1}{2}\log(\mathbf{B_1^*} + \mathbf{N_3'}) \qquad (23) \end{aligned}$$

where (a) is due to the proportionality property. The rate R_2 is bounded as follows

$$R_2 \leq h(\mathbf{y_2}) - h(\mathbf{z}) - (h(\mathbf{y_2}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}))$$

Using (23) and the fact that $R_2 > R_2^G(\mathbf{B_{1,2}}, \mathbf{N'_{1,2,3}})$, the above inequality means that

$$\begin{aligned} &h(\mathbf{y_2}) - h(\mathbf{z}) \geq R_2 + h(\mathbf{y_2}|\mathbf{u}) - h(\mathbf{z}|\mathbf{u}) > \\ &\frac{1}{2}\log(\mathbf{B_1^*} + \mathbf{B_2^*} + \mathbf{N_2'}) - \frac{1}{2}\log(\mathbf{B_1^*} + \mathbf{B_2^*} + \mathbf{N_3'}) \end{aligned}$$

which is a contradiction with the fact that Gaussian distribution maximizes $h(\mathbf{x} + \mathbf{n_2}) - h(\mathbf{x} + \mathbf{n_3})$ [14]. ■

IV. Conclusion

A scenario where a source node wishes to broadcast two confidential messages for two respective receivers via a Gaussian MIMO broadcast channel, while a wire-tapper also receives the transmitted signal via another MIMO channel is considered. We considered the secure vector Gaussian degraded broadcast channel and established its capacity region. Our achievability scheme is the secret superposition of Gaussian codes. Instead of solving a nonconvex problem, we used the notion of an enhanced channel to show that secret superposition of Gaussian codes is optimal. To characterize the secrecy capacity region of the vector Gaussian degraded broadcast channel, we only enhanced the channels for the legitimate receivers, and the channel of the eavesdropper remains unchanged.

References

[1] A. Wyner, "The Wire-tap Channel", *Bell System Technical Journal*, vol. 54, pp. 1355-1387, 1975

[2] I. Csiszar and J. Korner, "Broadcast Channels with Confidential Messages", *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339-348, May 1978.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian Wiretap Channel", *IEEE Trans. Inform. Theory*, vol. 24, no. 4, pp. 451-456, July 1978.

[4] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO Wiretap Channel", *in Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, Jun. 2007.

[5] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas: The MISOME Wiretap Channel", available at `http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.4219v1.pdf`.

[6] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "Secure Broadcasting: The Secrecy Rate Region", *Allerton Conference on Communications, Control and Computing,*, September 2008.

[7] H. Weingarten, Y. Steinberg, S. Shamai(Shitz), "The Capacity Region of the Gaussian Multiple-Input Multiple-Output Broadcast Channel", *IEEE Trans. Inform. Theory*, vol. 52, no. 9, pp. 3936-3964, September 2006.

[8] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "The Secrecy Capacity Region of the Gaussian MIMO Broadcast Channel", Submitted to *IEEE Trans. Inform. Theory*, March 2009, available at `http://arxiv.org/PS_cache/arxiv/pdf/0903/0903.3261v1.pdf`.

[9] E. Ekrem and S.Ulukus, "The Secrecy Capacity Region of the Gaussian MIMO Multi-Receiver Wiretap Channel", Submitted to *IEEE Trans. Inform. Theory*, March 2009, available at `http://arxiv.org/PS_cache/arxiv/pdf/0903/0903.3096v1.pdf`.

[10] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz),"Multiple Input Multiple Output Gaussian Broadcast Channels with Confidential Messages", Submitted to *IEEE Trans. Inform. Theory*, March 2009, available at `http://arxiv.org/PS_cache/arxiv/pdf/0903/0903.3786v1.pdf`.

[11] G. Bagherikaram, A. S. Motahari and A. K. Khandani, "Secrecy Capacity Region of Gaussian Broadcast Channel", presented at the *43rd annual Conference on Information Sciences and Systems (CISS 2009),*, March 2009.

[12] T. Liu, S. Shamai(Shitz), "A Note on the Secrecy Capacity of the Multi-antenna Wiretap Channel", February 2008. available at `http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.4105v1.pdf`..

[13] P. P. Bergmans, "A Simple Converse for Broadcast Channels with Additive White Gaussian Noise", *IEEE Trans. Inform. Theory*, vol. IT-20, no. 2, pp. 279-280, March 1974.

[14] T. Liu, P. Viswanath, "An Extremal Inequality Motivated by Multiterminal Information Theoretic Problems", *IEEE Trans. on Inf. Theory*, vol. 53, no. 5, pp. 1839-1851, May 2007.