Layered Secure Broadcasting over MIMO Channels and Application in Secret Sharing

Shaofeng Zou
Department of EECS
Syracuse University
Syracuse, NY
Email: szou02@syr.edu

Yingbin Liang
Department of EECS
Syracuse University
Syracuse, NY
Email: yliang06@syr.edu

Lifeng Lai
Department of ECE
Worcester Poly Insistitute
Worcester, MA
Email: llai@wpi.edu

Shlomo Shamai (Shitz)
Department of EE
Technion
Haifa, Israel
Email: sshlomo@ee.technion.ac.il

***Abstract*—In this paper, the degraded Gaussian Multiple-Input-Multiple-Output (MIMO) broadcast channel with layered decoding and secrecy constraints is investigated. In this model, there are in total K messages and K receivers that are ordered by the channel quality. Each receiver is required to decode one more message than the receiver with one level worse channel quality. Furthermore, this message should be kept secure from the receivers with worse channel qualities. The secrecy capacity region for this model is fully characterized. The converse proof relies on a novel construction of a series of covariance matrices. An application of this model to the problem of sharing multiple secrets, which is difficult to solve using number theoretic tools, is investigated. The secret sharing capacity region is characterized by reformulating the secret sharing problem as the secure communication problem over the K-receiver degraded Gaussian MIMO broadcast channel.**

I. Introduction

As a nature of wireless communications, broadcast causes significant challenges to achieve secure communication, because eavesdroppers in networks can easily receive information intended for other nodes. The basic physical layer communication model that includes secrecy constraints is the wiretap channel introduced by Wyner [1], in which a transmitter broadcasts to a legitimate receiver and an eavesdropper, and wishes to transmit a private message to the legitimate receiver and keep this message secure from the eavesdropper. This model was further generalized by Csiszár and Körner in [2], in which the transmitter further sends one common message to both the legitimate receiver and the eavesdropper. Recently, there have been extensive studies of broadcast channels with secrecy constraints, e.g., [3]–[6] (see [7] and [8] for more references of these studies).

More recently, a number of broadcast models with layered decoding and secrecy requirements have been proposed and studied. In particular, [9] studied a model (model 1) with two legitimate receivers and one eavesdropper. It is required that one message be decoded at both receivers and kept secure from the eavesdropper, and that the second message be decoded at one receiver and kept secure from the other receiver and the eavesdropper. [9] studied one more model (model 2), in which the second message does not need to be kept secure from the other receiver. Both models were further generalized in [10] in that each receiver and the eavesdropper in the above model was replaced by a group of nodes. In [9], [10], the secrecy capacity region was established for the multiple-input multiple-output (MIMO) Gaussian channels.

Furthermore, [11] generalized model 1 in [9] to K receivers (see Fig. 1). More specifically, the transmitter wishes to transmit K messages to K receivers. Due to the degradedness condition, from receiver K to receiver 1, the quality of their channels gets worse gradually. It is required that receiver k decodes one more message than receiver $k-1$ for $k = 2, \ldots, K$, and this additional message should be kept secure from all receivers with worse outputs, i.e., with lower indices. In [11], the secrecy capacity region was characterized for the discrete memoryless channel and the single-input single-output (SISO) Gaussian channel.

In this paper, we extend the study in [11] to the degraded MIMO Gaussian broadcast channel. Our main contribution lies in establishing the secrecy capacity region for the MIMO channel. Although an achievable region (i.e., an inner bound on the secrecy capacity region) follows from the result in [11] directly by properly choosing jointly Gaussian distributed input and auxiliary random variables, the converse proof is challenging. The techniques used for the converse proof in [11] for scalar Gaussian variables are not applicable to vector random variables. Furthermore, the layered secrecy constraints on more than two receivers require the converse proof to bound the secrecy rates in certain recursive structures for three or more consecutive receivers. Consequently, techniques used in [9], [10] for two receivers cannot be readily applied here, although some properties on matrix manipulations are useful in our proof. Our main technical development in the converse proof lies in the construction of a series of covariance matrices (representing input resources for messages) such that the secrecy rates can be upper bounded as the desired recursive forms in terms of these covariance matrices.

We further apply our result to studying a secret sharing problem, in which a dealer wishes to distribute K secrets to K participants by broadcasting over a wireless channel. It is required that participant 1 recover the first secret, and as one more participant joins the group to share its output, one more secret should be recovered by the group. Moreover, the new secret should be kept secure from any smaller groups. This problem involves sharing multiple secrets in a layered fashion, and can be very challenging to solve using the traditional number theoretic tools. In this paper, by designing virtual receivers for each sharing group of receivers, we show that this secret sharing problem is equivalent to the degraded Gaussian MIMO broadcast channel with layered decoding and secrecy constraints that we study. Moreover, the channel outputs at

those virtual receivers naturally satisfy the degradedness condition. We thus establish the secret sharing capacity region by applying the secrecy capacity region we obtain for the degraded Gaussian MIMO broadcast channel. Furthermore, the secure encoding scheme that achieves the secret capacity region provides an information theoretic scheme for sharing the secrets.

In this paper, we use $\mathbf{A} \prec \mathbf{B}$ and $\mathbf{A} \preceq \mathbf{B}$ to denote the fact that $\mathbf{B} - \mathbf{A}$ is positive definite and semi-positive definite, respectively. This paper is organized as follows. In Section II, we introduce the system model we study. In Section III, we present our characterization of the secrecy capacity region. In Section IV, we further apply our result to a secret sharing problem, and present the secret sharing capacity region. Finally, in Section V, we conclude our paper.

II. Channel Model

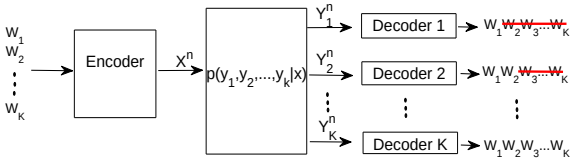

Fig. 1. The broadcast channel with layered decoding and secrecy.

In this paper, we study the degraded Gaussian MIMO broadcast channel with layered decoding and secrecy constraints (see Fig. 1). In this model, the received signal at receiver k for one channel use is given by

$$\mathbf{Y}_k = \mathbf{X} + \mathbf{N}_k, \ k = 1, \ldots, K, \tag{1}$$

where the channel input $\mathbf{X}$, the channel output $\mathbf{Y}_k$ and the noise $\mathbf{N}_k$ are r-dimensional vectors. Furthermore, the noise variables $\mathbf{N}_k$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_k$ for $k = 1, \ldots, K$ that satisfy the following order:

$$\mathbf{0} \prec \mathbf{\Sigma}_K \preceq \mathbf{\Sigma}_{K-1} \preceq \cdots \preceq \mathbf{\Sigma}_1. \tag{2}$$

The channel input $\mathbf{X}$ is subject to a covariance constraint

$$E[\mathbf{X}\mathbf{X}^\top] \preceq \mathbf{S} \tag{3}$$

where $\mathbf{S} \succ \mathbf{0}$. Since the secrecy capacity region does not depend on the correlation across the channel outputs, we can adjust the correlation between the noise vectors such that the channel inputs and channel outputs satisfy the following Markov chain:

$$\mathbf{X} \to \mathbf{Y}_K \to \mathbf{Y}_{K-1} \to \ldots \to \mathbf{Y}_2 \to \mathbf{Y}_1. \tag{4}$$

Hence, the quality of channels gradually degrades from receiver K to receiver 1.

The transmitter has K messages $W_1, \cdots, W_K$ intended for the K receivers. The system is required to satisfy the following layered decoding and secrecy constraints. For $k = 1, \ldots, K$, receiver k needs to decode the messages $W_1, \cdots, W_k$, and to be kept ignorant of messages $W_{k+1}, \cdots, W_K$ (see Fig. 1 for an illustration).

A secrecy rate tuple $(R_1, \cdots, R_K)$ is said to be *achievable*, if there exists a sequence of encoders at the transmitter and decoders at each receiver such that both the average error probability

$$P_e^n = \Pr\left(\cup_{k=1}^K \{(W_1, \cdots, W_k) \neq g_k^n(\mathbf{Y}_k^n)\}\right) \tag{5}$$

and the leakage rate at each receiver k for $k = 1, \ldots, K$

$$\frac{1}{n} I(W_{k+1}, \cdots, W_K; \mathbf{Y}_k^n | W_1, \cdots, W_k) \tag{6}$$

approach zero as n goes to infinity.

Here, the asymptotically small error probability as in (5) implies that each receiver k is able to decode messages $W_1, \ldots, W_k$, and asymptotically small leakage rate as in (6) for each receiver k implies that receiver k is kept ignorant of messages $W_{k+1}, \ldots, W_K$. Our goal is to characterize the secrecy capacity region that consists of all achievable rate tuples.

III. Main Result

We first note that the corresponding discrete memoryless model has been studied in [11], which characterizes the secrecy capacity region as follows:

Lemma 1. *[11, Theorem 1] The secrecy capacity region of the discrete memoryless degraded broadcast channel with layered decoding and secrecy constraints as described in Section II contains rate tuples $(R_1, \cdots, R_K)$ satisfying*

$$\begin{aligned} R_1 &\leq I(U_1; Y_1), \\ R_k &\leq I(U_k; Y_k | U_{k-1}) - I(U_k; Y_{k-1} | U_{k-1}), \\ &\qquad \text{for } k = 2, \ldots, K-1, \\ R_K &\leq I(X; Y_K | U_{K-1}) - I(X; Y_{K-1} | U_{K-1}), \end{aligned} \tag{7}$$

for some $P_{U_1 U_2 \ldots U_{K-1} X}$ such that the following Markov chain holds

$$U_1 \to U_2 \to \ldots \to U_{K-1} \to X \to Y_K \to \ldots \to Y_1. \tag{8}$$

In this paper, we characterize the secrecy capacity region for the degraded Gaussian MIMO channel with layered decoding and secrecy constraints in the following theorem.

Theorem 1. *The secrecy capacity region of the degraded Gaussian MIMO broadcast channel with layered decoding and secrecy constraints as described in Section II contains all rate tuples $(R_1, \ldots, R_K)$ that satisfy the following inequalities:*

$$\begin{aligned} R_1 &\leq \frac{1}{2} \log \frac{|\mathbf{\Sigma}_1 + \mathbf{S}|}{|\mathbf{\Sigma}_1 + \mathbf{S}_1|} \\ R_k &\leq \frac{1}{2} \log \frac{|\mathbf{\Sigma}_k + \mathbf{S}_{k-1}|}{|\mathbf{\Sigma}_k + \mathbf{S}_k|} - \frac{1}{2} \log \frac{|\mathbf{\Sigma}_{k-1} + \mathbf{S}_{k-1}|}{|\mathbf{\Sigma}_{k-1} + \mathbf{S}_k|}, \\ &\qquad \text{for } 2 \leq k \leq K-1, \\ R_K &\leq \frac{1}{2} \log \frac{|\mathbf{\Sigma}_K + \mathbf{S}_{K-1}|}{|\mathbf{\Sigma}_K|} - \frac{1}{2} \log \frac{|\mathbf{\Sigma}_{K-1} + \mathbf{S}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|}, \end{aligned} \tag{9}$$

for some $\mathbf{0} \preceq \mathbf{S}_{K-1} \preceq \mathbf{S}_{K-2} \preceq \ldots \preceq \mathbf{S}_2 \preceq \mathbf{S}_1 \preceq \mathbf{S}$.

Proof of Achievability*:* The achievability of region (9) follows by choosing the auxiliary random variables

$\mathbf{U}_1, \ldots, \mathbf{U}_{K-1}, \mathbf{X}$ to be jointly Gaussian distributed and satisfy the following Markov chain condition:

$$\mathbf{U}_1 \to \mathbf{U}_2 \to \ldots \to \mathbf{U}_{K-1} \to \mathbf{X}, \tag{10}$$

where the covariance of $\mathbf{U}_k$ is set to be $\mathbf{S} - \mathbf{S}_k$ for $k = 1, \ldots, K-1$, and the covariance of $\mathbf{X}$ is set to be $\mathbf{S}$. ■

Proof of Converse (Outline): Due to the space limitations, we provide only an outline of key steps of the converse proof. The reader can refer to [12] for the full proof. We note that the proof applied some techniques in the converse proof in [13] with new developments for our problem.

Following the converse proof of Lemma 1 for the discrete memoryless channel in [11], we have the inequalities as follows.

$$\begin{aligned} &R_1 \le I(\mathbf{U}_1; \mathbf{Y}_1), \\ &R_k \le I(\mathbf{U}_k; \mathbf{Y}_k | \mathbf{U}_{k-1}) - I(\mathbf{U}_k; \mathbf{Y}_{k-1} | \mathbf{U}_{k-1}), \\ &\qquad\qquad \text{for } 2 \le k \le K, \end{aligned} \tag{11}$$

where the random variables satisfy the following Markov chain condition:

$$\mathbf{U}_1 \to \ldots \to \mathbf{U}_{K-1} \to \mathbf{X} \to \mathbf{Y}_K \to \ldots \to \mathbf{Y}_1. \tag{12}$$

We first derive the bounds on R_2 and R_3 in (9) in order to show that the bounding techniques can be extended to prove the bounds on $R_4, \ldots, R_K$. We then derive the bound on R_1.

To bound R_2, we start with (11), and we have,

$$R_2 \le (h(\mathbf{Y}_2|\mathbf{U}_1) - h(\mathbf{Y}_1|\mathbf{U}_1)) - (h(\mathbf{Y}_2|\mathbf{U}_2) - h(\mathbf{Y}_1|\mathbf{U}_2)), \tag{13}$$

where we use the Markov chain condition (12).

Using techniques in [13], we have the following upper and lower bounds on $h(\mathbf{Y}_2|\mathbf{U}_1) - h(\mathbf{Y}_1|\mathbf{U}_1)$,

$$-r(0) \le h(\mathbf{Y}_2|\mathbf{U}_1) - h(\mathbf{Y}_1|\mathbf{U}_1) \le -r(1), \tag{14}$$

where

$$r(t) = \frac{1}{2} \log \frac{|\mathbf{A} + \mathbf{B} + t\mathbf{\Delta}|}{|\mathbf{A} + t\mathbf{\Delta}|}. \tag{15}$$

In above equation (15),

$$\begin{aligned} &\mathbf{A} = \mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_1)^{-1} \\ &\mathbf{B} = \mathbf{\Sigma}_1 - \mathbf{\Sigma}_2 \\ &\mathbf{\Delta} = \mathbf{J}(\mathbf{X} + \mathbf{N}_1|\mathbf{U}_1)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_1 - \mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_1)^{-1}. \end{aligned}$$

More specifically, $\mathbf{J}(\mathbf{X}|\mathbf{U})$ is the conditional Fisher information matrix of $\mathbf{X}$ given $\mathbf{U}$ for an arbitrarily correlated random vector pair with well defined densities, and is defined as

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) = E[\rho(\mathbf{X}|\mathbf{U})\rho(\mathbf{X}|\mathbf{U})^T], \tag{16}$$

where the expectation is taken over the joint density $f(\mathbf{u}, \mathbf{x})$, and the conditional score function $\rho(\mathbf{x}|\mathbf{u})$ is given by

$$\begin{aligned} \rho(\mathbf{x}|\mathbf{u}) &= \nabla \log f(\mathbf{x}|\mathbf{u}) \\ &= \left[\frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_1} \cdots \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_n} \right]^T. \end{aligned} \tag{17}$$

It can be verified that $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}$, $\mathbf{\Delta} \succeq \mathbf{0}$, and $r(t)$ is a continuous and monotonically decreasing function of t. Hence, there must exist $0 \le t_1 \le 1$ such that

$$h(\mathbf{Y}_2|\mathbf{U}_1) - h(\mathbf{Y}_1|\mathbf{U}_1) = -r(t_1). \tag{18}$$

We define $\mathbf{S}_1 := A + t_1\mathbf{\Delta} - \mathbf{\Sigma}_2$. Therefore,

$$h(\mathbf{Y}_2|\mathbf{U}_1) - h(\mathbf{Y}_1|\mathbf{U}_1) = -r(t_1) = \frac{1}{2} \log \frac{|\mathbf{S}_1 + \mathbf{\Sigma}_2|}{|\mathbf{S}_1 + \mathbf{\Sigma}_1|}. \tag{19}$$

It can be seen that, $\mathbf{S}_1$ satisfies $\mathbf{A} - \mathbf{\Sigma}_2 \preceq \mathbf{S}_1 \preceq \mathbf{A} + \mathbf{\Delta} - \mathbf{\Sigma}_2$, and can be shown that

$$\mathbf{0} \preceq \mathbf{S}_1 \preceq \mathbf{S}. \tag{20}$$

We can also show that

$$\begin{aligned} &\frac{1}{2} \log \frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_2)^{-1}|}{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_2)^{-1} + \mathbf{\Sigma}_1 - \mathbf{\Sigma}_2|} \\ &\le h(\mathbf{Y}_2|\mathbf{U}_2) - h(Y_1|\mathbf{U}_2) \le \frac{1}{2} \log \frac{|\mathbf{S}_1 + \mathbf{\Sigma}_2|}{|\mathbf{S}_1 + \mathbf{\Sigma}_1|}. \end{aligned} \tag{21}$$

Combining (21) with the fact that $\mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_2)^{-1} - \mathbf{\Sigma}_2 \preceq \mathbf{S}_1$, we have

$$-r(0) \le h(\mathbf{Y}_2|\mathbf{U}_2) - h(\mathbf{Y}_1|\mathbf{U}_2) \le -r(1), \tag{22}$$

where $r(t)$ is given in (15) with $\mathbf{A}$, $\mathbf{B}$ and $\mathbf{\Delta}$ being defined as,

$$\begin{aligned} &\mathbf{A} = \mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_2)^{-1}, \\ &\mathbf{B} = \mathbf{\Sigma}_1 - \mathbf{\Sigma}_2, \\ &\mathbf{\Delta} = \mathbf{S}_1 + \mathbf{\Sigma}_2 - \mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_2)^{-1}, \end{aligned}$$

which satisfy $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}$, and $\mathbf{\Delta} \succeq \mathbf{0}$. Since $r(t)$ is monotone and continuous, there exists $0 \le t_2 \le 1$ such that

$$h(\mathbf{Y}_2|\mathbf{U}_2) - h(\mathbf{Y}_1|\mathbf{U}_2) = -r(t_2).$$

Let $\mathbf{S}_2 = \mathbf{A} + t_2\mathbf{\Delta} - \mathbf{\Sigma}_2$. Hence,

$$h(\mathbf{Y}_2|\mathbf{U}_2) - h(\mathbf{Y}_1|\mathbf{U}_2) = -r(t_2) = \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{\Sigma}_2|}{|\mathbf{S}_2 + \mathbf{\Sigma}_1|} \tag{23}$$

and

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_2|\mathbf{U}_2)^{-1} - \mathbf{\Sigma}_2 \preceq \mathbf{S}_2 \preceq \mathbf{S}_1. \tag{24}$$

Therefore, substituting (19) and (23) into (13), we have

$$R_2 \le \frac{1}{2} \log \frac{|\mathbf{S}_1 + \mathbf{\Sigma}_2|}{|\mathbf{S}_2 + \mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{S}_1 + \mathbf{\Sigma}_1|}{|\mathbf{S}_2 + \mathbf{\Sigma}_1|}. \tag{25}$$

We next derive an upper bound on R_3, which is a necessary step to show that the proof techniques can be iteratively extended to bound $R_4, \ldots, R_K$. Following from (11), we have

$$R_3 \le h(\mathbf{Y}_3|\mathbf{U}_2) - h(\mathbf{Y}_2|\mathbf{U}_2) - (h(\mathbf{Y}_3|\mathbf{U}_3) - h(\mathbf{Y}_2|\mathbf{U}_3)). \tag{26}$$

Then using [10, Theorem 11] and (23), we have

$$h(\mathbf{Y}_3|\mathbf{U}_2) - h(\mathbf{Y}_2|\mathbf{U}_2) \le \frac{1}{2} \log \frac{|\mathbf{S}_2 + \mathbf{\Sigma}_3|}{|\mathbf{S}_2 + \mathbf{\Sigma}_2|}. \tag{27}$$

Following from the arguments similar to those for deriving (23) and (24), we can show that there exists $\mathbf{S}_3$ such that $\mathbf{0} \preceq \mathbf{S}_3 \preceq \mathbf{S}_2 \preceq \mathbf{S}_1 \preceq \mathbf{S}$ and

$$h(\mathbf{Y}_3|\mathbf{U}_3) - h(\mathbf{Y}_2|\mathbf{U}_3) = \frac{1}{2}\log\frac{|\mathbf{S}_3+\mathbf{\Sigma}_3|}{|\mathbf{S}_3+\mathbf{\Sigma}_2|}. \quad (28)$$

Therefore, substituting (27) and (28) to (26), we have

$$R_3 \le \frac{1}{2}\log\frac{|\mathbf{S}_2+\mathbf{\Sigma}_3|}{|\mathbf{S}_3+\mathbf{\Sigma}_3|} - \frac{1}{2}\log\frac{|\mathbf{S}_2+\mathbf{\Sigma}_2|}{|\mathbf{S}_3+\mathbf{\Sigma}_2|}. \quad (29)$$

Using techniques similar to those for bounding R_2 and R_3, we can derive the desired bounds on $R_4, \ldots, R_K$ iteratively.

Finally, we bound the rate R_1. We introduce a virtual receiver $\mathbf{Y}_0 = \mathbf{X} + \mathbf{N}_0$, where the covariance matrix of $\mathbf{N}_0$ is given by $\mathbf{\Sigma}_0 = t\mathbf{\Sigma}_1$, with $t \ge 1$. Hence, $\mathbf{\Sigma}_0 \succeq \mathbf{\Sigma}_1$. Following [10, Theorem 1] and (19), we have

$$h(\mathbf{Y}_0|\mathbf{U}_1) - h(\mathbf{Y}_1|U_1) \le \frac{1}{2}\log\frac{|\mathbf{S}_1+\mathbf{\Sigma}_0|}{|\mathbf{S}_1+\mathbf{\Sigma}_1|}, \quad (30)$$

for any $t \ge 1$. On the other hand, we have

$$\frac{1}{2}\log|\mathbf{\Sigma}_0| = h(\mathbf{N}_0) \le h(\mathbf{Y}_0|\mathbf{U}_1) \le h(\mathbf{Y}_0) \le \frac{1}{2}\log|\mathbf{S}+\mathbf{\Sigma}_0|, \quad (31)$$

which implies

$$\begin{aligned}\frac{1}{2}\log\frac{|\mathbf{\Sigma}_0|}{|\mathbf{S}_1+\mathbf{\Sigma}_0|} &\le h(\mathbf{Y}_0|\mathbf{U}_1) - \frac{1}{2}\log|\mathbf{S}_1+\mathbf{\Sigma}_0| \\ &\le \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_0|}{|\mathbf{S}_1+\mathbf{\Sigma}_0|}. \end{aligned} \quad (32)$$

If $t \to \infty$, $\frac{1}{2}\log\frac{|\mathbf{\Sigma}_0|}{|\mathbf{S}_1+\mathbf{\Sigma}_0|} \to 0$ and $\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_0|}{|\mathbf{S}_1+\mathbf{\Sigma}_0|} \to 0$. Hence, $h(\mathbf{Y}_0|\mathbf{U}_1) - \frac{1}{2}\log|\mathbf{S}_1+\mathbf{\Sigma}_0| \to 0$ as $t \to \infty$. Since (30) holds for any $t \ge 1$, we have $h(\mathbf{Y}_1|\mathbf{U}_1) \ge \frac{1}{2}\log|\mathbf{S}_1+\mathbf{\Sigma}_1|$.

Following from (11), we have

$$\begin{aligned} R_1 &\le I(\mathbf{U}_1;\mathbf{Y}_1) = h(\mathbf{Y}_1) - h(\mathbf{Y}_1|\mathbf{U}_1) \\ &\le \frac{1}{2}\log|\mathbf{S}+\mathbf{N}_1| - \frac{1}{2}\log|\mathbf{S}_1+\mathbf{\Sigma}_1| = \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_1|}{|\mathbf{S}_1+\mathbf{\Sigma}_1|}, \end{aligned} \quad (33)$$

which completes the converse proof. ■

IV. Application to Secret Sharing

In this section, we apply our result obtained in Section III to study a secret sharing problem, in which a dealer wishes to share K secrets $W_1, W_2, \ldots, W_K$ with K participants via a broadcast channel (see Fig. 2). The channel input sent by the dealer is denoted by $\mathbf{X}$ and the channel output received at participant k is denoted by Y_k for $k = 1, \ldots, K$. It is required that participant 1 decodes W_1, and participant 1 and 2 decode W_1 and W_2 by sharing their outputs (Y_1, Y_2), but W_2 should be kept secure from participant 1. Such requirements extend to k participants for $k = 1, \ldots, K$ in the sense that participants 1 to k can recover the first k messages $W_1, \ldots, W_k$ by sharing their outputs $(Y_1, \ldots, Y_k)$, but the new message W_k should be secure from the first $k-1$ participants. Hence, as one more participant joins the group, one more secret can be recovered, and this new secret is secure from (and hence cannot be recovered by) a smaller group. The goal is to characterize the secret sharing capacity region, which contains all possible achievable rate tuples $(R_1, R_2, \ldots, R_K)$ for K secrets.

This secret sharing problem involves sharing multiple secrets in a layered fashion, and is challenging to solve using the classical approach based on number theory. Here, we solve this problem by constructing an equivalent broadcast model described in Section II.

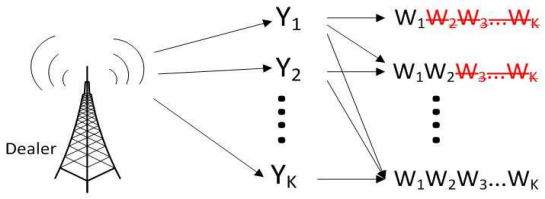

Fig. 2. The model of secret sharing via a broadcast channel.

We assume that the dealer communicates to the participants via a Gaussian multiple input single output (MISO) broadcast channel corrupted by additive Gaussian noise variables. The dealer has K antennas and each receiver has one antenna. The relationship of the channel input from the dealer and the channel outputs at all participants is characterized as

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_K \end{pmatrix} = \mathbf{H}\begin{pmatrix} X_1 \\ \vdots \\ X_K \end{pmatrix} + \begin{pmatrix} Z_1 \\ \vdots \\ Z_K \end{pmatrix} \quad (34)$$

where $\mathbf{H}$ is the $K \times K$ channel matrix, which is assumed to be invertible, $(Y_1, \ldots, Y_K)$ are channel outputs at the K participants, $(X_1, \ldots X_K)$ are the channel inputs from the K antennas of the dealer, and $(Z_1, \ldots, Z_K)$ is a random Gaussian vector with the covariance matrix $\mathbf{\Sigma}$ with each entry $\mathbf{\Sigma}_{ij} = E[Z_iZ_j] = \sigma_{ij}^2$. We assume that the dealer's input is subject to a resource constraint, $E[\mathbf{X}\mathbf{X}^T] \preceq \mathbf{S}$.

We note that it is reasonable to assume that $\mathbf{H}$ is invertible in order to guarantee that each participant's output contains new information compared to other participants so that new secret can be recovered when this participant joins a group.

We reformulate the above secret sharing model into a degraded MIMO broadcast communication system by designing a virtual receiver for each sharing group of participants. More specifically, we design a virtual receiver $\mathbf{V}_k$ for the group of the first k participants, i.e., $\mathbf{V}_k = (Y_1, \ldots, Y_k)$, for $1 \le k \le K$. For technical convenience, we add $K-k$ outputs $\widetilde{Y}_{k+1}, \ldots, \widetilde{Y}_K$ to $\mathbf{V}_k$ so that it contains K components, i.e., the virtual receiver $\mathbf{V}_k$ has K antennas. The channel outputs at those K antennas are given by,

$$\mathbf{V}_k = \begin{pmatrix} Y_1 \\ \vdots \\ Y_k \\ \widetilde{Y}_{k+1} \\ \vdots \\ \widetilde{Y}_K \end{pmatrix} = \mathbf{H}\begin{pmatrix} X_1 \\ \vdots \\ X_K \end{pmatrix} + \begin{pmatrix} Z_1 \\ \vdots \\ Z_k \\ Z_{k+1} + t\widetilde{Z}_{k+1} \\ \vdots \\ Z_K + t\widetilde{Z}_K \end{pmatrix} \quad (35)$$

where $\widetilde{Z}_k$, $2 \leq k \leq K$, is random Gaussian noise variables with mean zero and variance $\tilde{\sigma}_{kk}^2 > 0$, and $\widetilde{Z}_k$ is independent from all other random variables. Here, t is a large enough constant (i.e., $t \to \infty$), so that $\widetilde{Y}_{k+1}, \ldots, \widetilde{Y}_K$ are fully corrupted by the noise. We define a new random Gaussian vector $\mathbf{Z}_V(k) = (Z_1, \ldots, Z_k, Z_{k+1}+t\widetilde{Z}_{k+1}, \ldots, Z_K+t\widetilde{Z}_K)^T$ and rewrite (35) as

$$\mathbf{V}_k = \mathbf{H}\mathbf{X} + \mathbf{Z}_V(k), \text{ for } k = 1, \ldots, K. \tag{36}$$

Since the channel matrix $\mathbf{H}$ is invertible, we have

$$\mathbf{H}^{-1}\mathbf{V}_k = \mathbf{X} + \mathbf{H}^{-1}\mathbf{Z}_V(k). \tag{37}$$

By treating $\mathbf{H}^{-1}\mathbf{V}_k$ as the new channel output $\mathbf{V}'_k$ at virtual receiver $\mathbf{V}_k$, and define a new random Gaussian noise vector $\mathbf{Z}'_V(k) = \mathbf{H}^{-1}\mathbf{Z}_V(k)$, we have

$$\mathbf{V}'_k = \mathbf{X} + \mathbf{Z}'_V(k), \tag{38}$$

which is equivalent to the model in (36).

We now state a lemma that provides the order of the covariance matrices of $\mathbf{Z}'_V(k)$, denoted by $\mathbf{\Sigma}'_V(k)$, for $1 \leq k \leq K$.

Lemma 2. *Let $\mathbf{Z}'_V(k)$, $1 \leq k \leq K$, be random Gaussian vectors defined as above. The covariance matrices of $\mathbf{Z}'_V(k)$ satisfy the following ordering property:*

$$\mathbf{\Sigma}'_V(1) \succeq \mathbf{\Sigma}'_V(2) \succeq \ldots \succeq \mathbf{\Sigma}'_V(K). \tag{39}$$

The proof of Lemma 2 is omitted due to the space limitations.

Therefore, by designing virtual receivers, we reformulate the problem of secret sharing via the MISO broadcast channel into the problem of secure communication over the degraded MIMO broadcast channel described in Section II. It can also be seen that the requirements of the secret sharing problem is equivalent to the layered decoding and secrecy requirements for the communication problem. Thus, the secret sharing capacity region equals the secrecy capacity region of the degraded MIMO broadcast channel. Thus applying Theorem 1 we obtain the following secret sharing capacity region.

Corollary 1. *The capacity region for the secret sharing problem described above contains rate tuples $(R_1, R_2, \ldots, R_K)$ satisfying*

$$\begin{aligned}
R_1 &\leq \frac{1}{2}\log\frac{|\mathbf{\Sigma}'_V(1)+\mathbf{S}|}{|\mathbf{\Sigma}'_V(1)+\mathbf{S}_1|} \\
R_k &\leq \lim_{t\to\infty}\frac{1}{2}\log\frac{|\mathbf{\Sigma}'_V(k)+\mathbf{S}_{k-1}|}{|\mathbf{\Sigma}'_V(k)+\mathbf{S}_k|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}'_V(k-1)+\mathbf{S}_{k-1}|}{|\mathbf{\Sigma}'_V(k-1)+\mathbf{S}_k|}, \\
&\qquad \textit{for } 2 \leq k \leq K-1, \\
R_K &\leq \lim_{t\to\infty}\frac{1}{2}\log\frac{|\mathbf{\Sigma}'_V(K)+\mathbf{S}_{K-1}|}{|\mathbf{\Sigma}'_V(K)|} - \frac{1}{2}\log\frac{|\mathbf{\Sigma}'_V(K-1)+\mathbf{S}_{K-1}|}{|\mathbf{\Sigma}'_V(K-1)|},
\end{aligned} \tag{40}$$

for some $\mathbf{0} \preceq \mathbf{S}_{K-1} \preceq \mathbf{S}_{K-2} \preceq \ldots \preceq \mathbf{S}_2 \preceq \mathbf{S}_1 \preceq \mathbf{S}$.

V. Conclusion

In this paper, we have studied the K-receiver degraded Gaussian MIMO broadcast channel with layered decoding and secrecy constraints. For this problem, for $k = 1, \ldots, K$, receiver k needs to decode messages $W_1, W_2, \ldots, W_k$, while messages $W_{k+1}, \ldots, W_K$ need to be kept secured from receiver k. We have fully characterized the secrecy capacity region of this channel. We have also introduced an application of this model to a secret sharing problem, which is difficult to solve using number theoretic tools. We have characterized the secret sharing capacity region by reformulating the secret sharing problem into the problem of the degraded Gaussian MIMO broadcast channel. It is also of great interest to study the general (non-degraded) MIMO broadcast channel in the future.

Acknowledgment

The work of S. Zou and Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565 and by the National Science Foundation under Grants CCF-10-26566 and CNS-11-16932. L. Lai was supported by a National Science Foundation CAREER Award under Grant CCF-13-18980 and by the National Science Foundation under Grant CNS-13-21223. The work of S. Shamai (Shitz) was supported by the Israel Science Foundation (ISF), and the European Commission in the framework of the Network of Excellence in Wireless COMmunications NEWCOM#.

References

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

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

[3] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[4] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2493–2507, Jun. 2008.

[5] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.

[6] Y. Liang, L. Lai, H. V. Poor, and S. Shamai (Shitz), "A broadcast approach for fading wiretap channels," to appear in *IEEE Transactions on Information Theory*.

[7] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5, pp. 355–580, Now Publishers, Hanover, MA, USA, 2008.

[8] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[9] R. Liu, T. Liu, H. V. Poor, and S. Shamai, "A vector generalization of costa's entropy-power inequality with applications," *IEEE Transactions on Information Theory*, vol. 56, no. 4, pp. 1865 –1879, April 2010.

[10] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 5681–5698, 2012.

[11] S. Zou, Y. Liang, L. Lai, and S. Shamai, "Layered decoding and secrecy over degraded broadcast channels," in *IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Darmstadt, Germany, Jun. 2013.

[12] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "An information theoretic approach to secret sharing," *Submitted to IEEE Transactions on Information Theory*, March 2014, Available at http://arxiv.org/abs/1404.6474.

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