Layered Decoding and Secrecy over Degraded Broadcast Channels

(Invited Paper)

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

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

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

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

***Abstract*—A K-receiver degraded broadcast channel with layered decoding and secrecy constraints is investigated, in which receivers are ordered by their channel quality. Each receiver is required to decode one more message compared to the receiver with one level worse channel quality, and this message should be kept secure from all receivers with worse channel quality. For both the discrete memoryless channel and the Gaussian channel, the secrecy capacity region is characterized. The achievability scheme is based on stochastic encoding and superposition coding schemes. Novel generalization of the analysis of leakage rates and of the proof of the converse is developed for the K-receiver scenario.**

I. Introduction

Physical layer security emerges as an attracting and promising new technique, which exploits physical channel randomness for achieving secure communication. The basic idea was proposed for the wiretap channel in the seminal paper [1] by Wyner, in which a secure scheme is designed to send messages reliably to a legitimate receiver and to keep transmitted messages secure from an eavesdropper. Csiszár and Körner further extended this approach to a more general broadcast model [2], in which the transmitter also wishes to send a common message to both the legitimate receiver and the "eavesdropper" (which is also a receiver in the system) in addition to the confidential message to the legitimate receiver. Among the communication models that have been studied with secrecy constraints (overviews of these studies can be found in [3] and [4]), broadcast networks with secrecy constraints have been studied intensively, e.g., [2], [5]–[7].

In this paper, we study a degraded broadcast channel model with layered decoding and secrecy constraints, in which one transmitter sends information to K receivers. The channel outputs at K receivers satisfy a Markov chain condition, which implies that receivers can be ordered such that the quality of their channels gets worse gradually, say from receiver K to receiver 1. There are K messages intended for these receivers. As the channel's quality gets one level better, the receiver is required to decode one more message, and this message should be kept secure from the receivers with worse outputs (see Fig. 1). Hence, receiver K is required to decode all messages. This model generalizes a few models studied previously to the general K-user scenario including the model studied in [2], an example studied in [8], and scenario 2 studied in [9] with all groups having a single node.

Our motivation to study such a degraded broadcast channel with layered decoding and secrecy constraints is due to its potential applications to the problem of secret sharing, in which a dealer distributes one or multiple secrets among a set of participants in such a manner that only qualified sets of users can recover the corresponding secrets by pooling their shares together while non-qualified sets of users obtain no information about the secrets even if they pool their shares together. It has been shown recently in [10] that secret sharing can be achieved via broadcast transmission of secret messages from the dealer to all participants, and requiring that the messages are decodable if any qualified set of participants share their channel outputs, and messages are kept secure from any other sets of participants even if they share their outputs. Suppose now one dealer wishes to establish K shared secrets among K nodes, and it is required that starting from node 1, whenever one node joins the group, one more secret should be recovered and this new secret should not be recovered by the previous group. This naturally leads to an equivalent degraded broadcast channel model with layered decoding and secrecy constraints. We note that in such a scenario, the original broadcast channel can be general and the degradedness of the equivalent model is due to the secret sharing requirements.

We also note that the model we study is different from some previously studied broadcast models as follows. One model (i.e., scenario 1) studied in [9] assumes that all broadcast messages should be kept secure from one eavesdropper, which does not expect any message from the transmitter, whereas here all eavesdroppers expect their own messages. A fading wiretap channel was studied in [11], in which the model is equivalent to the broadcast channel with multiple receivers and eavesdroppers. The difference also lies in that the eavesdroppers do not expect messages from the transmitter in [11], although layered decoding and secrecy appear in the work.

For the degraded broadcast channel with layered decoding and secrecy constraints, we study both the discrete memoryless channel (DMC) and the Gaussian channel, and obtain the secrecy capacity region for both cases. The secrecy scheme is based on the stochastic encoding (i.e., binning) and heterogeneous superposition. More specifically, for each message, we create a new layer superposed on the codeword of the lower-layer messages (intended for receivers with the worse channel quality), and the codewords for this layer are divided into a number of bins for stochastic encoding. The receivers with better channel quality can tell which bin the codeword is in,

i.e., they can decode the message with a small probability of error, while the receivers with the worse channel quality are kept ignorant of the message.

Although the idea of the achievable scheme is simple, the analysis of leakage rates is more involved than the cases with two or three receivers. For the DMC, we develop a novel generation of the analysis of the leakage rate provided in [12] for one legitimate receiver to multiple receivers. For the Gaussian channel, we provide an alternative analysis for the leakage rate via an argument on the optimal input distribution for the Gaussian channel with a fixed codebook, and generalize such an argument to the K-receiver case. The two approaches carry complimentary insights for analyzing the leakage rate for scenarios with layered decoding and secrecy constraints. The converse proofs for the DMC and Gaussian channel require careful constructions of auxiliary random variables contained in recursive terms, which also generalize the existing techniques for two or three receivers.

This paper is organized as follows. In Section II, we introduce our system model for both the DMC and the Gaussian channel. In Sections III and IV, we present our main results for the DMC and the Gaussian channel, respectively. Finally, in Section V we conclude our paper.

II. Channel Model

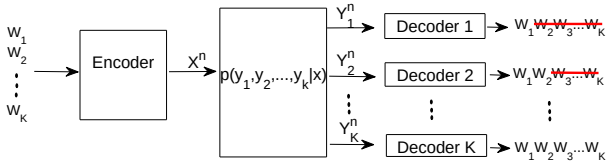

Fig. 1. System Model

In this paper, we study the model of the degraded broadcast channel with layered decoding and secrecy constraints (see Fig. 1), in which a transmitter transmits to K receivers. The channel transition probability function is given by $P_{Y_1\cdots Y_K|X}$, in which $X \in \mathcal{X}$ is the channel input and $Y_k \in \mathcal{Y}_k$ is the channel output of receiver k for $k = 1, \ldots, K$. It is assumed that the receivers have degraded outputs, i.e., $Y_1, \cdots, Y_K$ satisfy the following Markov chain condition:

$$X \to Y_K \to Y_{K-1} \to \ldots \to Y_2 \to Y_1. \tag{1}$$

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 $(2^{nR_1}, \cdots, 2^{nR_K}, n)$ code for the channel consists of

- K message sets: $W_k \in \mathcal{W}_k = \{1, \cdots, 2^{nR_k}\}$ for $k = 1, \cdots, K$, which are independent from each other and each message is uniformly distributed over the corresponding message set;
- An (possibly stochastic) encoder f^n: $\mathcal{W}_1 \times \cdots \times \mathcal{W}_K \to \mathcal{X}^n$;
- K decoders $g_k^n : \mathcal{Y}_k^n \to (\mathcal{W}_1, \cdots, \mathcal{W}_k)$ for $k = 1, \cdots, K$.

Hence, a secrecy rate tuple $(R_1, \cdots, R_K)$ is said to be *achievable*, if there exists a sequence of $(2^{nR_1}, \cdots, 2^{nR_K}, n)$ codes such that both the average error probability

$$P_e^n = \Pr\left(\cup_{k=1}^K \{(W_1, \cdots, W_k) \neq g_k^n(Y_k^n)\}\right) \tag{2}$$

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

$$\frac{1}{n} I(W_{k+1}, \cdots, W_K; Y_k^n | W_1, \cdots, W_k) \tag{3}$$

approach zero as n goes to infinity.

Here, condition (2) implies that each receiver k is able to decode messages $W_1, \ldots, W_k$, while (3) implies that receiver k is kept ignorant of messages $W_{k+1}, \ldots, W_K$. The secrecy capacity region is defined as the set of all achievable rate tuples.

We further consider the K-receiver degraded Gaussian broadcast channel, in which

$$Y_k = h_k X + Z_k, \ k = 1, \cdots, K, \tag{4}$$

where Z_k is a zero mean Gaussian noise variable with variance N at receiver k, and h_k is the real channel gain coefficient from the transmitter to receiver k. Without loss of generality, we assume that $h_1 < h_2 < \cdots < h_K$. The transmitter has an average power constraint P. We use $C(x) = \frac{1}{2}\log(1+x)$. The remainder of the model is the same as the DMC case discussed above.

III. The Discrete Memoryless Channel

For the discrete memoryless degraded broadcast channel with layered decoding and secrecy constraints, we characterize the secrecy region in the following theorem.

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

$$\begin{aligned} R_1 &\le I(U_1; Y_1), \\ R_k &\le I(U_k; Y_k|U_{k-1}) - I(U_k; Y_{k-1}|U_{k-1}), \\ &\qquad\qquad \text{for } k = 2, \ldots, K-1, \\ R_K &\le I(X; Y_K|U_{K-1}) - I(X; Y_{K-1}|U_{K-1}), \end{aligned} \tag{5}$$

for some $P_{U_1U_2\ldots U_{K-1}X}$ such that the following Markov chain holds

$$U_1 \to U_2 \to \ldots \to U_{K-1} \to X \to Y_K \to \ldots \to Y_1. \tag{6}$$

Remark 1. *By setting $R_1 = 0$ and $K = 3$, Theorem 1 reduces to the results for scenario 2 in [9] with each group having a single user for the model in [13], and for the example in [8].*

We next outline the proof of achievability and converse for Theorem 1. The detailed proof will be provided in a journal version of the work [14].

Proof of Achievability*:* In the following, we provide the major steps in the proof and omit some detailed computations

in the analysis of error probability and leakage rates due to the space limitations. The achievability proof is based on stochastic encoding and superposition coding. We use random codes and fix a joint probability distribution $P_{U_1\cdots U_{K-1}X}$ satisfying the Markov chain in (6). Let $T_\epsilon^n(P_{U_1\ldots U_{K-1}XY_1\ldots Y_K})$ denote the strongly jointly ϵ-typical set based on the fixed distribution.

Random codebook generation: In the following achievability proof, for notational convenience, we write X as U_K, i.e., $P_{U_1\cdots U_{K-1}X} = P_{U_1\cdots U_K}$.

- Generate 2^{nR_1} independent identically distributed (i.i.d.) u_1^n with distribution $\prod_{i=1}^n p(u_{1,i})$. Index these codewords as $u_1^n(w_1)$, $w_1 \in [1, 2^{n\widetilde{R}_1}]$.
- For each $u_{k-1}^n(w_1, w_2, l_2, \cdots, w_{k-1}, l_{k-1})$, $k = 2, \cdots, K$, generate $2^{n\widetilde{R}_k}$ i.i.d. sequences u_k^n with distribution $\prod_{i=1}^n p(u_{k,i}|u_{k-1,i})$. Partition these sequences into 2^{nR_k} bins, each with $2^{n(\widetilde{R}_k - R_k)}$ sequences. We use $w_k \in [1 : 2^{nR_k}]$ to denote the bin index, and $l_k \in [1 : 2^{n(\widetilde{R}_k - R_k)}]$ to denote the index within each bin. Hence each u_k^n is indexed by $(w_1, w_2, l_2, \cdots, w_k, l_k)$.

The chosen codebook is revealed to the transmitter and all receivers.

Encoding: To send a message tuple $(w_1, w_2, \ldots, w_K)$, for each $2 \le k \le K$, the encoder randomly generate $l_k \in [1 : 2^{n(\widetilde{R}_k - R_k)}]$ based on a uniform distribution. The transmitter then sends $u_K^n(w_1, w_2, l_2, \cdots, w_K, l_K)$.

Decoding: For $k = 1, \ldots, K$, receiver k claims that $(\hat{w}_1, \cdots, \hat{w}_k)$ is sent, if there exists a unique tuple $(\hat{w}_1, \hat{w}_2, \hat{l}_2, \cdots, \hat{w}_k, \hat{l}_k)$ such that

$$\begin{aligned}&(u_1^n(\hat{w}_1), u_2^n(\hat{w}_1, \hat{w}_2, \hat{l}_2), \ldots, u_k^n(\hat{w}_1, \hat{w}_2, \hat{l}_2, \cdots, \hat{w}_k, \hat{l}_k), y_k^n)\\ &\in T_\epsilon^n(P_{U_1\ldots U_k Y_k}).\end{aligned} \tag{7}$$

Otherwise, it declares an error.

Analysis of error probability: By the law of large numbers and the packing lemma, it can be shown that if the following inequalities are satisfied, receiver k (for $k = 1, \ldots, K$) can decode messages $w_1, w_2, \ldots, w_k$ with a vanishing error probability:

$$\begin{aligned}&R_1 \le I(U_1; Y_1),\\ &\widetilde{R}_k \le I(U_k; Y_k|U_{k-1}), \text{for } 2 \le k \le K.\end{aligned} \tag{8}$$

Analysis of leakage rate: We first compute an average of the leakage rate over the random codebook ensemble as follows. For convenience, we let $W^k = (W_1, \ldots, W_k)$, $W_{k+1}^K = (W_{k+1}, \ldots, W_K)$.

$$\begin{aligned}&I(W_{k+1}^K; Y_k^n|W^k, \mathcal{C})\\ &= I(W^K, L^K; Y_k^n|\mathcal{C}) - I(W^k, L^K; Y_k^n|W_{k+1}^K, \mathcal{C})\\ &\le I(U_K^n; Y_k^n|\mathcal{C}) - I(W^k, L^K; Y_k^n|W_{k+1}^K, \mathcal{C})\\ &= I(U_K^n; Y_k^n|\mathcal{C}) - H(W^k, L^K|W_{k+1}^K, \mathcal{C})\\ &\quad + H(W^k, L^K|Y_k^n, W_{k+1}^K, \mathcal{C}).\end{aligned} \tag{9}$$

We bound the above three terms one by one. For the first term, we have

$$\begin{aligned}&I(U_K^n; Y_k^n|\mathcal{C})\\ &= I(U_k^n, U_K^n; Y_k^n|\mathcal{C})\\ &= I(U_k^n; Y_k^n|\mathcal{C}) + I(U_K^n; Y_k^n|U_k^n, \mathcal{C})\\ &\le H(U_k^n|\mathcal{C}) + I(U_K^n; Y_k^n|U_k^n, \mathcal{C})\\ &\le n\sum_{j=1}^k \widetilde{R}_j + nH(Y_k|U_k) - nH(Y_k|U_K)\\ &= n\sum_{j=1}^k \widetilde{R}_j + nI(U_K; Y_k|U_k).\end{aligned} \tag{10}$$

For the second term, due to the independence of $W_1, \cdots, W_K$ and $L_1, \cdots, L_K$, we have

$$\begin{aligned}&H(W^k, L^K|W_{k+1}^K, \mathcal{C})\\ &= \sum_{j=1}^k n\widetilde{R}_j + \sum_{j=k+1}^K n(\widetilde{R}_j - R_j).\end{aligned} \tag{11}$$

We bound the last term as follows

$$\begin{aligned}&H(W^k, L^K|Y_k^n, W_{k+1}^K, \mathcal{C})\\ &\le H(L_{k+1}^K|Y_k^n, W^K, L^k, \mathcal{C}) + n\epsilon_n\\ &= \sum_{j=k+1}^K H(L_j|Y_k^n, W^K, L^{j-1}, \mathcal{C}) + n\epsilon_n\\ &\le \sum_{j=k+1}^K H(L_j|Y_k^n, U_{j-1}^n, W_j) + n\epsilon_n.\end{aligned} \tag{12}$$

It can be shown that if $\tilde{R}_j - R_j \ge I(U_j; Y_k|U_{j-1})$ for $k+1 \le j \le K$, then

$$\frac{1}{n}H(L_j|Y_k^n, U_{j-1}^n, W_j) \le \widetilde{R}_j - R_j - I(U_j; Y_k|U_{j-1}) + \epsilon_n'.$$

Combining the analysis of the three terms together, we have that $\frac{1}{n}I(W_{k+1}, \ldots, W_K; Y_k^n|W_1, \ldots, W_k, \mathcal{C}) \to 0$ as $n \to \infty$ for $1 \le k \le K-1$, if the following inequalities are satisfied:

$$\widetilde{R}_k - R_k \ge I(U_k; Y_{k-1}|U_{k-1}), \quad \text{for } 2 \le k \le K. \tag{13}$$

Combining the bounds in (8) and (13), we obtain that the rate tuple $(R_1, \cdots, R_K)$ is achievable if

$$\begin{aligned}&R_1 \le I(U_1; Y_1),\\ &R_k \le I(U_k; Y_k|U_{k-1}) - I(U_k; Y_{k-1}|U_{k-1}),\\ &\qquad\qquad \text{for } 2 \le k \le K.\end{aligned} \tag{14}$$

We note that the above statement also involves an argument that there exists the same codebook such that both the error probability and secrecy constraints are satisfied. ■

Proof of Converse*:* By Fano's inequality and the secrecy requirements, we have the following inequalities

$$\begin{aligned}&H(W_k|Y_k^n) \le n\epsilon_n, \text{ for } 1 \le k \le K\\ &\frac{1}{n}I(W_{k+1}, \ldots, W_K; Y_k^n|W_1, \ldots, W_k) \le \epsilon_n\\ &\qquad\qquad \text{for } 1 \le k \le K-1.\end{aligned} \tag{15}$$

We let $Y_k^{i-1} = (Y_{k,1}, \ldots, Y_{k,i-1})$, $Y_{k-1,i+1}^n = (Y_{k-1,i+1}, \ldots, Y_{k-1,n})$, $Y_{k-1}^{i-1} = (Y_{k-1,1}, \ldots, Y_{k-1,i-1})$, $Y_{k-2,i+1}^n = (Y_{k-2,i+1}, \ldots, Y_{k-2,n})$. We set $U_{k,i} := \{W_1, \ldots, W_k, Y_k^{i-1}, Y_{k-1,i+1}^n\}$ for $k = 1, \ldots, K$ where $Y_0^n = \phi$. It is easy to verify that $(U_{1,i}, \ldots, U_{K-1,i}, X_i)$ satisfy the Markov chain condition

$$U_1 \to U_2 \to \ldots \to U_{K-1} \to X \to Y_K \to \ldots \to Y_1. \quad (16)$$

We first bound the rate for the first message W_1. Since all receivers can decode message W_1, i.e. there is no secrecy constraint for W_1, following the standard steps, we obtain the following bound:

$$\begin{aligned} nR_1 = H(W_1) &\le \sum_{i=1}^n I(W_1, Y_1^{i-1}; Y_{1i}) + n\epsilon_n \\ &\le \sum_{i=1}^n I(U_{1i}; Y_{1i}) + n\epsilon_n. \end{aligned} \quad (17)$$

For the message W_k, $2 \le k \le K$, we derive the following bound:

$$\begin{aligned} nR_k &= H(W_k|W^{k-1}) \\ &\le I(W_k; Y_k^n|W^{k-1}) + n\epsilon_n \\ &\le I(W_k; Y_k^n|W^{k-1}) + 2n\epsilon_n - I(W_k; Y_{k-1}^n|W^{k-1}) \\ &= \sum_{i=1}^n I(W_k; Y_{k,i}|W^{k-1}, Y_k^{i-1}) + 2n\epsilon_n \\ &\quad - \sum_{i=1}^n I(W_k; Y_{k-1,i}|W^{k-1}, Y_{k-1,i+1}^n) \\ &= \sum_{i=1}^n I(W_k, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}, Y_k^{i-1}) \\ &\quad - I(W_k, Y_k^{i-1}; Y_{k-1,i}|W^{k-1}, Y_{k-1,i+1}^n) \\ &\quad - I(Y_{k-1,i+1}^n; Y_{k,i}|W^k, Y_k^{i-1}) \\ &\quad + I(Y_k^{i-1}; Y_{k-1,i}|W^k, Y_{k-1,i+1}^n) + 2n\epsilon_n \\ &\overset{(a)}{=} \sum_{i=1}^n I(Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}, Y_k^{i-1}) \\ &\quad + I(W_k; Y_{k,i}|W^{k-1}, Y_k^{i-1}, Y_{k-1,i+1}^n) \\ &\quad - I(Y_k^{i-1}; Y_{k-1,i}|W^{k-1}, Y_{k-1,i+1}^n) \\ &\quad - I(W_k; Y_{k-1,i}|W^{k-1}, Y_k^{i-1}, Y_{k-1,i+1}^n) + 2n\epsilon_n \\ &\overset{(b)}{=} \sum_{i=1}^n I(W_k; Y_{k,i}|W^{k-1}, Y_k^{i-1}, Y_{k-1,i+1}^n) \\ &\quad - I(W_k; Y_{k-1,i}|W^{k-1}, Y_k^{i-1}, Y_{k-1,i+1}^n) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}) \\ &\quad - I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}) \\ &\quad - I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}) \\ &\quad + I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n; Y_{k,i}|W^{k-1}) \\ &\quad - I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n; Y_{k-1,i}|W^{k-1}) \\ &\quad - I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}) \\ &\quad + I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}) + 2n\epsilon_n \end{aligned}$$

$$\begin{aligned} &= \sum_{i=1}^n I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad - I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad + I(Y_{k-1}^{i-1}, Y_{k-2,i+1}^n; Y_{k,i}|W^{k-1}) \\ &\quad - I(Y_{k-1}^{i-1}, Y_{k-2,i+1}^n; Y_{k-1,i}|W^{k-1}) \\ &\quad - I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}) \\ &\quad + I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad - I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad - I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad + I(Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) + 2n\epsilon_n \\ &\le \sum_{i=1}^n I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad - I(W_k, Y_k^{i-1}, Y_{k-1,i+1}^n; Y_{k-1,i}|W^{k-1}, Y_{k-1}^{i-1}, Y_{k-2,i+1}^n) \\ &\quad + 2n\epsilon_n \\ &\le \sum_{i=1}^n I(U_{k,i}; Y_{k,i}|U_{k-1,i}) - I(U_{k,i}; Y_{k-1,i}|U_{k-1,i}) + 2n\epsilon_n \end{aligned} \quad (18)$$

Where steps (a) and (b) follow from the sum identity property in [2, Lemma 7]. For $k = K$, we further derive (18),

$$\begin{aligned} &nR_K \\ &\le \sum_{i=1}^n I(U_{K,i}; Y_{K,i}|U_{K-1,i}) - I(U_{K,i}; Y_{K-1,i}|U_{K-1,i}) + 2n\epsilon_n \\ &= \sum_{i=1}^n I(U_{K,i}, X_i; Y_{K,i}|U_{K-1,i}) - I(U_{K,i}, X_i; Y_{K-1,i}|U_{K-1,i}) \\ &\quad - I(X_i; Y_{K,i}|U_{K,i}) + I(X_i; Y_{K-1,i}|U_{K,i}) + 2n\epsilon_n \\ &\le \sum_{i=1}^n I(X_i; Y_{K,i}|U_{K-1,i}) - I(X_i; Y_{K-1,i}|U_{K-1,i}) + 2n\epsilon_n \end{aligned} \quad (19)$$

The proof of the converse is completed by defining a uniformly distributed random variable $Q \in \{1, \cdots, n\}$, and setting $U_k \triangleq (Q, U_{k,Q})$, $Y_k \triangleq Y_{k,Q}$ for $k \in [1:K]$ and $X \triangleq (Q, X_Q)$. ■

Remark 2. *In the proof of achievability, we use the heterogeneous superposition scheme [15] which is optimal in the sense of achieving the secrecy capacity region.*

IV. The Gaussian Channel

In this section, we consider the Gaussian broadcast channel with K degraded receivers specified by (4).

Theorem 2. *The secrecy capacity region of a K-user Gaussian broadcast channel with layered decoding and secrecy constraints as described in Section II contains rate tuples*

$(R_1, R_2, \ldots, R_K)$ *satisfying*

$$R_1 \leq C\left(\frac{h_1^2 P_1}{N+h_1^2\sum_{j=2}^{K} P_j}\right)$$
$$R_k \leq C\left(\frac{h_k^2 P_k}{N+h_k^2\sum_{j=k+1}^{K} P_j}\right) - C\left(\frac{h_{k-1}^2 P_k}{N+h_{k-1}^2\sum_{j=k+1}^{K} P_j}\right) \quad \text{for } 2 \leq k \leq K, \tag{20}$$

where the union is taken over all nonnegative variables $P_1, P_2, \ldots, P_K$*, such that* $\sum_{k=1}^{K} P_k \leq P$*.*

Remark 3. *For the Gaussian channel, heterogeneous superposition [15] and homogeneous superposition [16] are equivalent in achieving the secrecy capacity region. We note that the equivalence of the two types of superposition schemes may not always hold [17].*

Outline of the Proof: The proof of achievability can be based on Theorem 1 by setting $(U_1, \ldots, U_K, X)$ to be jointly Gaussian distributed random variables. Alternatively, the coding scheme can be developed as follows based on stochastic encoding and superposition coding. Due to the space limitations, we omit the details and the converse proof.

■

V. Conclusion

In this paper, we have studied the secrecy capacity region for $K-$receiver degraded broadcast channel with layered secrecy for both the DMC and the Gaussian channel. For the problem considered, messages $W_1, \ldots, W_k$ needs to be decoded by user k, while messages $W_{k+1}, \ldots, W_K$ need to be kept secured from receiver k, for $k = 1, \ldots, K$. For both the DMC and the Gaussian channels, we have characterized the secrecy capacity region. Our next step is to apply the results here to study the problem of secret sharing as we mention in the introduction.

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), "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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] L. Lai, Y. Liang, W. Du, and S. Shlomo (Shitz), "Secret sharing via noisy broadcast channels," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Saint-Petersburg, Russia, July-August 2011.

[11] Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcasting over fading wiretap channels," in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*, July 2012, pp. 234–238.

[12] A. El Gamal and Y.-H. Kim, *Network Information Theory*. New York: Cambridge University Press, 2012.

[13] G. Bagherikaram, A. Motahari, and A. Khandani, "The secrecy rate region of the broadcast channel," *arXiv preprint*, 2008.

[14] S. Zou, L. Lai, Y. Liang, and S. Shamai (Shitz), "Secrecy over broadcast networks and applications in secret sharing," in preparation, 2013.

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

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

[17] L. Wang, E. Sasoglu, B. Bandemer, and Y.-H. Kim, "A comparison of superposition coding schemes," 2013.