K-User Degraded Broadcast Channel with Secrecy Outside a Bounded Range

Shaofeng Zou*, Yingbin Liang*, Lifeng Lai†, H. Vincent Poor‡ and Shlomo Shamai (Shitz)§
*Syracuse University, Email: szou02@syr.edu, yliang06@syr.edu
†Worcester Polytechnic Institute, Email: llai@wpi.edu
‡Princeton University, Email: poor@princeton.edu
§Technion, Email: sshlomo@ee.technion.ac.il

***Abstract*—A K-receiver degraded broadcast channel with secrecy outside a bounded range is studied, in which a transmitter sends K messages respectively to K receivers, and the channel quality gradually degrades from receiver K to receiver 1. Each receiver k is required to decode messages $W_1, \ldots, W_k$, for $1 \leq k \leq K$. Furthermore, each message W_k should be kept secure from receivers with two-level worse channel quality, i.e., receivers $1, \ldots, k-2$. The secrecy capacity region is fully characterized. The achievable scheme designates one superposition layer to each message with random binning employed for each layer for protecting all upper-layer messages from lower-layer receivers. Furthermore, the scheme allows adjacent layers to share rates so that part of the rate of each message can potentially be shared with its immediate upper-layer message to enlarge the rate region. More importantly, an induction approach is developed to perform Fourier-Motzkin elimination over $2K$ variables among $\Theta(K^2)$ bounds to obtain a close-form achievable rate region. A converse proof is developed that matches the achievable rate region, which involves recursive construction of the rate bounds.**

I. Introduction

The broadcast channel models scenarios in which one transmitter's signal can simultaneously reach multiple receivers, and it has been used widely to model wireless transmissions due to the open nature of wireless environments. Often in broadcast situations, among the receivers within communication range of the transmitter, some are intended receivers while others are unintended receivers or even eavesdroppers from which the messages should be kept secure. Various broadcast channel models with both transmission reliability constraints (i.e., legitimate receivers should decode messages destined for them) and secrecy constraints (i.e., eavesdroppers should be kept ignorant of messages) have been intensively studied, especially in recent years. An overview of these studies can be found in [1] and [2].

The basic model with one legitimate receiver and one eavesdropper, i.e., the wiretap channel, was initiated by Wyner in [3]. A more general model with an additional common message intended for both the legitimate receiver and the eavesdropper was studied by Csiszár and Körner in [4]. The broadcast channel with multiple legitimate receivers respectively decoding individual messages and with one eavesdropper being kept ignorant of all messages was studied in [5] and [6]. Furthermore, the broadcast channel with layered decoding and layered secrecy requirements was studied in [6]–[8], in which as the channel quality of a receiver gets one level better, one more message is required to be decoded, and this message is required to be secured from all receivers with worse channel quality.

Differently from the above model where the messages are kept secure from receivers with immediate next-level worse channel quality, a new broadcast channel model with secrecy outside a bounded range was studied in [9] and [10], in which each message is required to be kept secure from the receivers with two-level worse channel quality. Such a model is particularly useful to describe scenarios in which the receivers' channel quality varies continuously. The secrecy capacity was characterized in this setting for the three-receiver model in [9] and four-receiver model in [10]. It turns out that a natural generalization of the three-receiver model does not provide the capacity region for the four-receiver model. A novel rate splitting and sharing scheme was proposed in [10], which is shown to be critical to further enlarge the achievable region and establish the secrecy capacity region for the four-receiver model. The idea is to first use lower-layer messages to serve as random sources to protect high-layer messages, and if the lower-layer messages are more than enough to protect high-layers messages, then further share the remaining rate of lower-layer messages with upper-layer messages, as such parts of lower layer messages can satisfy the same secrecy constraints as high-layer messages.

Further generalization of the capacity characterization for the above four-receiver model to the arbitrary K-user case becomes very challenging due to the following reasons. First, based on the understanding in the four-receiver model, each message as well as the random bin number at each layer can potentially serve as a random source to protect all higher-layer messages (from lower layer receivers). The design of joint embedded coding and random binning is very complicated to handle. For example, consideration of whether to adopt random binning at layer k depends on whether embedded coding of layer $k-1$ is sufficient to protect W_k from receiver $k-2$, and whether embedded coding of layer $k-2$ and (possible) random binning in layer $k-1$ are sufficient to protect W_{k-1} and W_k, and so on. Incorporating all these considerations into the design of an achievable scheme is not feasible for an arbitrary K-user model. Secondly, due to rate splitting and sharing across adjacent layers, the rate region is expressed in terms of individual rate components. A typical technique to convert the rate region in terms of the (total) rate for each message is Fourier-Motzkin elimination. However, for the arbitrary K-user model, a large number $2K$ of rate variables should be eliminated from $\Theta(K^2)$ rate bounds. Such a procedure is not

analytically tractable in general.

In this paper, despite the challenges mentioned above, we fully characterize the secrecy capacity region for the K-receiver model with secrecy outside a bounded range. Our solution of the problem includes the following new ingredients. First, our achievable scheme employs random binning in each layer, which avoids the complex consideration of whether or not it is necessary to employ random binning for each layer. Our observation of rate sharing only between adjacent layers without loss of generality is critical to keep the obtained rate region simple enough for further manipulation. Secondly, we design an induction algorithm to perform Fourier-Motzkin elimination. Instead of directly eliminating $2K$ variables among $\Theta(K^2)$ bounds, we eliminate a pair of variables at a time. We then further show that the region after each elimination step possesses a common structure by induction. Finally, the converse proof is developed to match the achievable rate region, which involves careful recursive construction of rate upper bounds.

The remainder of this paper is organized as follows. In Section II, we introduce our system model. In Section III, we present our main results and describe the main idea of the achievable scheme. In Section IV, we provide outlines of the proofs of achievability and converse. Finally, in Section V, we conclude our paper.

II. Channel Model

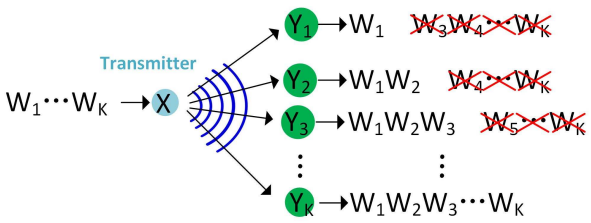

Fig. 1. The broadcast channel with secrecy outside a bounded range

In this paper, we consider the K-receiver degraded broadcast channel with secrecy outside a bounded range (see Fig. 1). A transmitter sends information to K receivers over a discrete memoryless channel. The channel transition probability function is given by $P_{Y_1\cdots Y_K|X}$, where $X \in \mathcal{X}$ denotes the channel input, and $Y_k \in \mathcal{Y}_k$ denotes the channel output at receiver k, for $1 \le k \le K$. The channel is assumed to be degraded, i.e., the following Markov chain condition holds:

$$X \to Y_K \to Y_{K-1} \to \cdots \to Y_1.$$

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

There are in total K messages $W_1, W_2, \ldots, W_K$ intended for K receivers with the following decoding and secrecy requirements. Receiver k is required to decode messages $W_1, W_2, \ldots, W_k$, for $k = 1, 2, \ldots, K$. Furthermore, message W_k needs to be kept secure from receivers $1, \ldots, k-2$ for $k = 3, \ldots, K$. Thus, each message is required to be kept secure from receivers with two-level worse channel quality.

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

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

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

and the leakage rate at each receiver k for $k = 3, \ldots, K$,

$$\frac{1}{n} I(W_k, \cdots, W_K; Y_{k-2}^n) \tag{2}$$

approach zero as n goes to infinity.

Here, the asymptotically small error probability as in (1) implies that each receiver k is able to decode messages $W_1, \ldots, W_k$, and the asymptotically small leakage rate as in (2) for each receiver $k-2$ implies that receiver $k-2$ is kept ignorant of messages $W_k, \ldots, W_K$. Our goal is to characterize the secrecy capacity region that consists of all achievable rate tuples.

III. Main Results

Our main result is the following characterization of the secrecy capacity region for the K-user model with secrecy outside a bounded range. For simplicity of notation, we let $U_K = X$.

Theorem 1. *Consider the K-receiver degraded broadcast channel with secrecy outside a bounded range as described in Section II. The secrecy capacity region consists of rate tuples $(R_1, R_2, \ldots, R_K)$ satisfying*

$$R_1 \le I(U_1; Y_1), \tag{3a}$$

$$\sum_{i=2}^{k} R_i \le \sum_{i=2}^{k} I(U_i; Y_i|U_{i-1}), \text{ for } 2 \le k \le K, \tag{3b}$$

$$\sum_{i=l}^{j} R_i \le \left(\sum_{i=l-1}^{j} I(U_i; Y_i|U_{i-1})\right) - I(U_j; Y_{l-2}|U_{l-2}), \text{ for } 3 \le l \le j \le K, \tag{3c}$$

for some $P_{U_1U_2\ldots U_K}$ such that the following Markov chain condition holds:

$$U_1 \to U_2 \to \cdots \to U_K \to Y_K \to \cdots \to Y_2 \to Y_1. \tag{4}$$

In the above capacity region, the bounds (3a) and (3b) are due to the decoding requirements, i.e., receiver k should decode messages $W_1, \ldots, W_k$, for $1 \le k \le K$. The sum rate bounds are due to the rate sharing scheme we design. The bounds (3c) are due to the secrecy requirements, i.e., messages $W_l, \ldots, W_j$ need to be kept secure from receiver $l-2$ for $3 \le l \le j \le K$. Furthermore, the bounds (3c) can be further written as

$$\sum_{i=l}^{j} R_i \le \sum_{i=l-1}^{j} \Big(I(U_i; Y_i|U_{i-1}) - I(U_i; Y_{l-2}|U_{i-1})\Big),$$

which has a clear intuitive interpretation.

The converse proof of Theorem 1 is mainly based on recursive construction of rate upper bounds and intensive manipulations of mutual information terms. An outline of the proof is provided in Section V. We next explain our design of an achievable scheme and derivation of the achievable region in more detail as follows.

We adopt the following techniques to design our achievable scheme: 1) superposition coding; 2) joint embedded coding and random binning; and 3) rate splitting and sharing. Due to the requirement of layered decoding, we design one layer of superposition coding for each message, i.e., layer k corresponds to W_k, for $1 \leq k \leq K$. We then design random binning for each layer. We use joint embedded coding and random binning to provide randomness for secrecy. We further apply rate splitting and sharing to enlarge the achievable region.

Since the messages do not need to be kept secure from their immediate downstream receivers, such a receiver's message can serve as embedded coding to provide additional randomness. More specifically, within the k-th layer, we split the message W_k into two parts $W_{k,1}$ and $W_{k,2}$. The message $W_{k,1}$ serves as embedded coding which is an additional random source in addition to the random binning to protect $W_{k,2}$ and the higher layer messages from receiver Y_{k-1}, i.e., we require that $(W_{k,2}, W_{k+1,1}, W_{k+1,2}, \ldots, W_{K,1}, W_{K,2})$ are secured from Y_{k-1}, for $2 \leq k \leq K-1$. On the other hand, the upstream receiver Y_{k+1} can also decode $W_{k,2}$ because Y_{k+1} has a better channel quality than Y_k. The message $W_{k,2}$ satisfies both the decoding and secrecy requirements for message W_{k+1}. Therefore, the rate of $W_{k,2}$ can be counted towards the rate of either W_k or W_{k+1}. By such a rate sharing strategy, the achievable region may be enlarged.

We note that the rate can only be shared between adjacent receivers, which is an important observation of the problem, and is critical to reducing the complexity of the design of the achievable scheme. More specifically, the rate of $W_{k,2}$ cannot be counted towards the rates of $W_{k+2}, \ldots, W_K$, because $W_{k+2}, \ldots, W_K$ are required to be secured not only from receiver Y_{k-1} but also from receiver Y_k both of which are required to decode $W_{k,2}$.

Based on the achievable scheme, we obtain the following achievable region:

$$\begin{aligned}
R_1 &\leq I(U_1; Y_1), \\
R_{k,1} + R_{k,2} &\leq I(U_k; Y_k|U_{k-1}), \text{ for } 2 \leq k \leq K, \\
R_{l-1,2} + \sum_{i=l}^{j}(R_{i,1} + R_{i,2}) &\leq \sum_{i=l-1}^{j} I(U_i; Y_i|U_{i-1}) \\
&\quad - I(U_j; Y_{l-2}|U_{l-2}), \\
&\text{for } 3 \leq l \leq K, l-1 \leq j \leq K. \qquad (5)
\end{aligned}$$

The above region is expressed in terms of component rates due to rate splitting. In order to express the above region in terms of total rate for each message, we define $R_k = R_{k-1,2} + R_{k,1}$ for $3 \leq k \leq K-1$, $R_2 = R_{2,1}$ and $R_K = R_{K-1,2} + R_{K,1} + R_{K,2}$. We then wish to project the region (5) onto the rate space $(R_1, \ldots, R_K)$. This can be done by adding the above rate definitions to the achievable region (5) and then performing the Fourier-Motzkin elimination to eliminate $R_{k,1}$ and $R_{k,2}$ for $2 \leq k \leq K$.

However, the total number of bounds in the achievable region (5) is $\Theta(K^2)$ with $2K$ variables to be eliminated. Directly applying Fourier-Motzkin elimination is not analytically tractable. In order to solve such a problem, we design an induction algorithm to perform Fourier Motzkin elimination. We eliminate the rate pairs $R_{k-1,2}$ and $R_{k,1}$ for $3 \leq k \leq K$, one at each step. We wish to show that the region $\mathcal{R}_k$ after eliminating $R_{k-1,2}$ and $R_{k,1}$ takes the following structure:

$$\begin{aligned}
R_1 &\leq I(U_1; Y_1), \\
\sum_{i=2}^{j} R_i &\leq \sum_{i=2}^{j} I(U_i; Y_i|U_{i-1}), \text{ for } 2 \leq j \leq k-1, \\
\sum_{i=2}^{k} R_i + R_{k,2} &\leq \sum_{i=2}^{k} I(U_i; Y_i|U_{i-1}), \\
\sum_{i=l}^{j} R_i &\leq \sum_{i=l-1}^{j} I(U_i; Y_i|U_{i-1}) - I(U_j; Y_{l-2}|U_{l-2}), \\
&\text{for } 3 \leq l \leq j \leq k-1, \\
\sum_{i=l}^{k} R_i + R_{k,2} &\leq \sum_{i=l-1}^{k} I(U_i; Y_i|U_{i-1}) - I(U_k; Y_{l-2}|U_{l-2}), \\
&\text{for } 3 \leq l \leq k. \qquad (6)
\end{aligned}$$

Such a claim can be easily verified for the case when $k = 3, 4, 5$. If such a claim holds for $\mathcal{R}_k$, we are then able to show that the region $\mathcal{R}_{k+1}$ after eliminating $R_{k,2}$ and $R_{k+1,1}$ has the same structure given by

$$\begin{aligned}
R_1 &\leq I(U_1; Y_1), \\
\sum_{i=2}^{j} R_i &\leq \sum_{i=2}^{j} I(U_i; Y_i|U_{i-1}), \text{ for } 2 \leq j \leq k, \\
\sum_{i=2}^{k+1} R_i + R_{k+1,2} &\leq \sum_{i=2}^{k+1} I(U_i; Y_i|U_{i-1}), \\
\sum_{i=l}^{j} R_i &\leq \sum_{i=l-1}^{j} I(U_i; Y_i|U_{i-1}) - I(U_j; Y_{l-2}|U_{l-2}), \\
&\text{for } 3 \leq l \leq j \leq k, \\
\sum_{i=l}^{k+1} R_i + R_{k+1,2} &\leq \sum_{i=l-1}^{k+1} I(U_i; Y_i|U_{i-1}) - I(U_{k+1}; Y_{l-2}|U_{l-2}), \\
&\text{for } 3 \leq l \leq k+1.
\end{aligned}$$

Thus, the above induction argument yields the achievable region in Theorem 1.

IV. Outline of Proof

In this section, we outline the achievability and converse proofs of Theorem 1.

A. Proof of Achievability (Outline)

Fix a distribution $P_{U_1 U_2 \ldots, U_{K-1} X} P_{Y_1 \ldots Y_K|X}$ satisfying the Markov chain condition in (4). For simplicity, we define $U_K = X$ in the following proof. We design the achievable scheme as follows:

Random codebook generation:

- Generate 2^{nR_1} independent and identically distributed (i.i.d.) u_1^n with distribution $\prod_{i=1}^n p(u_{1,i})$. Index these codewords as $u_1^n(w_1)$, $w_1 \in [1, 2^{nR_1}]$.
- For each $u_1^n(w_1)$, generate $2^{nR_{2,1}+R_{2,2}}$ i.i.d. u_2^n with distribution $\prod_{i=1}^n p(u_{2,i}|u_{1,i})$. Partition these codewords into $2^{nR_{2,2}}$ bins. Index these codewords as $u_2^n(w_1, w_{2,1}, w_{2,2})$, $w_{2,1} \in [1, 2^{nR_{2,1}}]$, $w_{2,2} \in [1, 2^{nR_{2,2}}]$.
- For each $u_2^n(w_1, w_{2,1}, w_{2,2})$, generate $2^{n\widetilde{R}_3}$ i.i.d. u_3^n with distribution $\prod_{i=1}^n p(u_{3,i}|u_{2,i})$. Partition these codewords into $2^{nR_{3,1}}$ bins. We further partition each bin into $2^{nR_{3,2}}$ sub-bins. Hence, there are $2^{n(\widetilde{R}_3 - R_{3,1} - R_{3,2})}$ u_k^n in each sub-bin. We use $w_{3,1} \in [1 : 2^{nR_{3,1}}]$ to denote the bin number, $w_{3,2} \in [1 : 2^{nR_{3,2}}]$ to denote the sub-bin number, and $l_3 \in [1 : 2^{n(\widetilde{R}_3 - R_{3,1} - R_{3,2})}]$ to denote the index within the bin. Hence, each u_3^n is indexed by $(w_1, w_{2,1}, w_{2,2}, w_{3,1}, w_{3,2}, l_3)$.
- For each $u_{k-1}^n(w_1, \ldots, w_{k-1,1}, w_{k-1,2}, l_{k-1})$, generate $2^{n\widetilde{R}_k}$ i.i.d. u_k^n with distribution $\prod_{i=1}^n p(u_{k,i}|u_{k-1,i})$. Partition these codewords into $2^{nR_{k,1}}$ bins. We further partition each bin into $2^{nR_{k,2}}$ sub-bins. Hence, there are $2^{n(\widetilde{R}_k - R_{k,1} - R_{k,2})}$ u_k^n in each sub-bin. We use $w_{k,1} \in [1 : 2^{nR_{k,1}}]$ to denote the bin number, $w_{k,2} \in [1 : 2^{nR_{k,2}}]$ to denote the sub-bin number, and $l_k \in [1 : 2^{n(\widetilde{R}_k - R_{k,1} - R_{k,2})}]$ to denote the index within the bin. Hence, each u_k^n is indexed by $(w_1, \ldots, w_{k-1,1}, w_{k-1,2}, l_{k-1}, w_{k,1}, w_{k,2}, l_k)$.

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

Encoding:

To send a message tuple $(w_1, w_{2,1}, w_{2,2}, \ldots, w_{K,1}, w_{K,2})$, the transmitter randomly and uniformly generates $l_k \in [1 : 2^{n(\widetilde{R}_k - R_{k,1} - R_{k,2})}]$ for $3 \le k \le K$, and sends $x^n(w_1, \ldots, w_{K,1}, w_{K,2}, l_3, \ldots, l_K)$.

Decoding:

- Receiver 1 claims that $\widehat{w}_1$ is sent, if there exists a unique $\widehat{w}_1$ such that
$$\left(u_1^n(\widehat{w}_1), y_1^n\right) \in T_\epsilon^n(P_{U_1Y_1}).$$
Otherwise, it declares an error.
- Receiver 2 claims that $(\widehat{w}_1, \widehat{w}_{2,1}, \widehat{w}_{2,2})$ is sent, if there exists a unique tuple $(\widehat{w}_1, \widehat{w}_{2,1}, \widehat{w}_{2,2})$ such that
$$\left(u_1^n(\widehat{w}_1), u_2^n(\widehat{w}_1, \widehat{w}_{2,1}, \widehat{w}_{2,2}), y_2^n\right) \in T_\epsilon^n(P_{U_1U_2Y_2}).$$
Otherwise, it declares an error.
- For $3 \le k \le K$, receiver k claims that $(\widehat{w}_1, \ldots, \widehat{w}_{k,1}, \widehat{w}_{k,2})$ is sent, if there exists a unique tuple $(\widehat{w}_1, \ldots, \widehat{w}_{k,1}, \widehat{w}_{k,2}, \widehat{l}_3, \ldots, \widehat{l}_k)$ such that
$$\left(u_1^n(\widehat{w}_1), \ldots, u_k^n(\widehat{w}_1, \ldots, \widehat{w}_{k,1}, \widehat{w}_{k,2}, \widehat{l}_3, \ldots, \widehat{l}_k), y_k^n\right) \in T_\epsilon^n(P_{U_1 \cdots U_k Y_k}).$$
Otherwise, it declares an error.

Analysis of the error probability: By the law of large numbers and the packing lemma, we can show that receiver k decodes the message $(w_1, \ldots, w_{k,1}, w_{k,2})$ for $2 \le k \le K$ and receiver 1 decodes the message w_1 with asymptotically small probability of error if the following inequalities are satisfied:

$$\begin{aligned} R_1 &\le I(U_1; Y_1), \\ R_{2,1} + R_{2,2} &\le I(U_2; Y_2|U_1), \\ \widetilde{R}_k &\le I(U_k; Y_k|U_{k-1}), \text{ for } 3 \le k \le K. \end{aligned} \tag{7}$$

Analysis of the leakage rate: We require $W_{k-1,2}, W_{k,1}, W_{k,2}, \ldots, W_{K,1}, W_{K,2}$ to be secured from receiver Y_{k-2} for $3 \le k \le K$. Therefore, it suffices to show

$$\frac{1}{n} I\Big(W_{k-1,2}, W_{k,1}, W_{k,2}, \ldots, W_{K,1}, W_{K,2}; Y_{k-2}^n \Big| W_1, \ldots, W_{k-2,1}, W_{k-2,2}\Big) \to 0, \text{ as } n \to \infty, \tag{8}$$

for $3 \le k \le K$. It can be shown that if

$$\widetilde{R}_{l-1} - R_{l-1,2} + \sum_{i=l}^{j} (\widetilde{R}_i - R_{i,1} - R_{i,2}) \ge I(U_j; Y_{l-2}|U_{l-2}) \tag{9}$$

for $3 \le l \le K-1$ and $l-1 \le j \le K$, then the condition (8) is satisfied.

Combining the conditions (7) and (9), we have the achievable region as in (5).

Rate sharing: We note that the message $W_{k-1,2}$ satisfies the decoding and secrecy requirement for W_{k-1} but also for W_k. Hence, its rate can be counted towards either R_{k-1} or R_k. Thus, we design a rate sharing scheme by defining $R_2 = R_{2,1}$, $R_K = R_{K-1,2} + R_{K,1} + R_{K,2}$ and $R_k = R_{k-1,2} + R_{k,1}$, for $3 \le k \le K-1$. After adding these equations and performing Fourier-Motzkin elimination to eliminate $R_{k,1}$ and $R_{k,2}$ for $2 \le k \le K$, we obtain the achievable region as in (3).

B. Proof of Converse (Outline)

To prove the converse, we construct the auxiliary random variables as follows:

$$\begin{aligned} U_{1,i} &= (W_1, Y_1^{i-1}), \\ U_{2,i} &= (W_1, W_2, Y_2^{i-1}), \\ U_{k,i} &= (W_1, \ldots, W_k, Y_k^{i-1}, Y_{k-2,i+1}^n), \text{ for } 3 \le k \le K, \end{aligned} \tag{10}$$

which satisfy the following Markov chain condition:

$$U_{1,i} \to \ldots \to U_{K,i} \to X_i \to Y_{K,i} \to \ldots \to Y_{1,i}, \tag{11}$$

for $i = 1, \ldots, n$.

The bounds (3a) and (3b) corresponding to the decoding requirements can be derived following similar techniques as those used to derive the sum rate bound $R_3 + R_4$ as in [10]. However, the proof for the bounds (3c) is more involved and requires careful recursive construction of the terms. In the following, we only outline the key steps due to space limitations.

By Fano's inequality and the secrecy requirements, we have

$$\begin{aligned} H(W_k|Y_k^n) &\le n\epsilon_n, \text{ for } 1 \le k \le K, \\ I(W_k, \ldots, W_K; Y_{k-2}^n | W_1, \ldots, W_{k-2}) &\le n\epsilon_n, \text{ for } 3 \le k \le K. \end{aligned}$$

For any $3 \leq l \leq j \leq K$, we can bound $\sum_{i=l}^{j} R_i$ as follows:

$$\sum_{m=l}^{j} nR_m = H(W_l, \ldots, W_j) + H(W_{l-1}) - H(W_{l-1})$$
$$\leq \sum_{m=l-1}^{j} H(W_m) - I(W_{l-1}, \ldots, W_j; Y_{l-2}^n | W_1, \ldots, W_{l-2}) + n\epsilon_n.$$

We further bound $H(W_m)$ for each $l-1 \leq m \leq j$ as follows:

$$\begin{aligned} H(W_m) \leq & \sum_{i=1}^{n} I(U_{m,i}; Y_{m,i} | U_{m-1,i}) \\ & - I(Y_m^{i-1}; Y_{m,i} | W_1, \ldots, W_{m-1} Y_{m-1}^{i-1} Y_{m-3,i+1}^n) \\ & + I(Y_{m-3,i+1}^n; Y_{m,i} | W_1, \ldots, W_{m-1} Y_m^{i-1}) \\ & - I(Y_{m-2,i+1}^n; Y_{m,i} | W_1, \ldots, W_m Y_m^{i-1}). \end{aligned} \quad (12)$$

We also bound $-I(W_{l-1}, \ldots, W_j; Y_{l-2}^n | W_1, \ldots, W_{l-2})$ as follows:

$$\begin{aligned} & -I(W_{l-1}, \ldots, W_j; Y_{l-2}^n | W_1, \ldots, W_{l-2}) \\ & \quad \leq \sum_{i=1}^{n} -I(U_{j,i}; Y_{l-2,i} | U_{l-2,i}) \\ & \quad - I(Y_{l-2}^{i-1}; Y_{l-2,i} | W_1, \ldots, W_{l-2} Y_{l-4,i+1}^n) \\ & \quad + I(Y_{j-2,i+1}^n; Y_{l-2,i} | W_1, \ldots, W_j Y_j^{i-1} Y_{l-2,i+1}^n) \\ & \quad + I(Y_j^{i-1}; Y_{l-2,i} | W_1, \ldots, W_j Y_{l-2,i+1}^n) \\ & \quad + I(Y_{l-2,i+1}^n; Y_{l-2,i} | W_1, \ldots, W_{l-2} Y_{l-4,i+1}^n). \end{aligned} \quad (13)$$

Summing up (12) for each $l - 1 \leq m \leq j$ and (13), and applying Csiszár's sum identity, we can show that those redundant terms either cancel each other or are less than zero. Therefore, the converse proof for (3c) is completed.

V. Conclusion

In this paper, we have studied a K-receiver discrete memoryless degraded broadcast channel with secrecy outside a bounded range. We have characterized the secrecy capacity region for this model by designing an achievable scheme based on superposition coding, joint embedded coding and random binning and rate splitting and sharing. To design an achievable scheme that loses no optimality but yields a tractable achievable rate region, we have employed random binning in each layer to avoid the complex decision of whether or not to use random binning as in the achievable scheme for the four-receiver model [10]. Moreover, we have exploited a critical property of the problem so that the design of rate sharing is only between adjacent receivers, which significantly reduces the complexity of designing the achievable scheme. We have further proposed a novel induction algorithm to perform Fourier-Motzkin elimination on the achievable region with $2K$ variables to be eliminated among $\Theta(K^2)$ bounds. We have also constructed a converse proof, which involves careful recursive construction of the terms in the bounds. We anticipate that our induction algorithm to implement Fourier-Motzkin elimination can be useful to study other network models with rate sharing among a large number of users.

Acknowledgment

The work of S. Zou and Y. Liang was supported by a National Science Foundation CAREER Award under Grant CCF-10-26565. The work of L. Lai was supported by a National Science Foundation CAREER Award under Grant CCF-13-18980 and the National Science Foundation under Grant ECCS-14-08114. The work of H. V. Poor was supported by the National Science Foundation under Grant CMMI-1435778. The work of S. Shamai (Shitz) was supported by the Israel Science Foundation (ISF).

References

[1] 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, 2009.

[2] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai (Shitz), "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1841–1856, Sept 2015.

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

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

[5] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," *EURASIP J. Wirel. Commun. Netw.*, vol. 2009, pp. 1:1–1:29, Mar. 2009.

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

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

[8] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "An information theoretic approach to secret sharing," *IEEE Trans. Inform. Theory*, vol. 61, no. 6, pp. 3121–3136, 2015.

[9] ——, "Degraded broadcast channel: Secrecy outside of a bounded range," in *Proc. IEEE Information Theory Workshop (ITW)*, Jerusalem, Israel, Apr 2015, pp. 1–5.

[10] ——, "Rate splitting and sharing for degraded broadcast channel with secrecy outside a bounded range," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Hong Kong, China, June 2015, pp. 1357–1361.