Research Article

A Class of Three-Receiver Broadcast Channels with Degraded Message Sets and Side Information

Fangbiao Li and Zhi Xue

Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Correspondence should be addressed to Fangbiao Li; flyin2009@sjtu.edu.cn

Received 30 August 2013; Revised 17 October 2013; Accepted 4 November 2013

Academic Editor: Hector Puebla

Copyright © 2013 F. Li and Z. Xue. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We study a class of three-receiver discrete memoryless broadcast channel (DM-BC) with three degraded message sets and side information. We derive achievable rate region for this three-receive DM-BC with side information noncausally available at the transmitter. When the receivers follow a degradedness order, we determine the perfect secrecy capacity region of this class of three-receiver DM-BC with three degraded message sets and side information noncausally available at both the transmitter and the receiver. The achievable secrecy region of this paper subsumes Steinberg's rate region for two-receiver degraded BC with the sideinformation and the secrecy capacity region for one-receiver two-eavesdropper DM-BC with no side information as its special cases.

1. Introduction

Wyner introduced wiretap channel in his seminal paper [1]. In his communication model, a transmitter wishes to send confidential messages to a legitimate receiver while keeping the messages secret from the eavesdropper. He assumed that the channel to the eavesdropper is a physical degraded version of the channel to the legitimate receiver. He characterized the trade-off between the information rate to the receiver and the level of secrecy, as measured by equivocation. Furthermore, Wyner proposed a basic principle coding strategy to obtain secure communication for wiretap channels. Subsequently, Csiszár and Körner extended Wyner’s results to general broadcast channel with confidential messages in [2], where no degradation order exists between the legitimate receiver and the eavesdropper. They derived a capacity-equivocation region of this general, not necessarily degraded, wiretap channel.

Körner and Marton considered a general two-receiver DM-BC with degraded message sets in [3]. In their model, a common message \( M_0 \) is to be transmitted to all receivers; a private message \( M_1 \) is to be sent only to the first receiver. They determined the capacity region by using superposition coding. Information theoretic study of the \( k \)-receiver (\( k \geq 3 \)) discrete memoryless broadcast channel (DM-BC) was initiated by Borade et al. in [4]. They introduced multilevel broadcast channels, which combined some aspects of degraded message sets and established an achievable rate region (named BZT region [5]) for these channels. They simply surmised that the straightforward extension of the Körner-Marton region for two-receiver BC with degraded message sets to \( k \)-receiver BC is in general optimal. Nair and El Gamal [5] showed that the direct extension of the Körner-Marton region to more than two receivers is not optimal in general. They established the capacity region for the multilevel BC and then extended the results of the multilevel BC to determine inner and outer bounds on the capacity region of the general three-receiver BC with two-degraded message sets. They proved that the capacity region for a class of three-receiver BC with two-degraded message sets can be strictly larger than the straightforward extension of the Körner-Marton region. One of the contributions of [5] is that it introduces a new decoding scheme named indirect decoding. Chia and El Gamal [6] considered two scenarios of three-receiver BC with common and confidential messages, two-receiver one-eavesdropper BC and one-receiver two-eavesdropper BC. In the two-receiver one-eavesdropper BC model, the confidential message is to be sent to the first and the second receivers while kept secret from the third receiver. In the second paradigm, one-receiver two-eavesdropper BC, the confidential message is to be sent...
to one receiver and kept secret from the other two receivers. They established inner bounds on the secrecy capacity region for these two scenarios by using Wyner channel coding, Nair-Gamal *indirect decoding* and the new ideal of generating secrecy from a public available superposition codebook. They also showed that the inner bound was tight for several special cases. Recently, Salehkalaibar et al. [7] studied one-receiver two-eavesdropper BC with three degraded message sets and proposed a more general network compared to [6].

Although all the aforementioned papers discussed the class of three-receiver BC with or without secrecy constraints, they did not consider the case where there is side information available at the transmitter or at both the transmitter and the receiver. Shannon first studied the channels with side information causally available at the transmitter in [8], where he determined the capacity region of the SISO channel. Following Shannon’s research, Gel’fand-Pinsker investigated the single-user channel with side information noncausally available at the transmitter and determined its capacity in [9]. Cover and Chiang [10] extended Gel’fand and Pinsker’s result to the case where the side information was available at both the transmitter and the receiver. After that, Steinberg [11] studied two paradigms where side information on the random parameter was provided to the transmitter in a noncausal or causal manner. He derived the inner and outer bounds on the capacity region with noncausal coding. For causal coding, he derived a single-letter characterization of the capacity region. Chia and El Gamal [12] established a lower bound on the secrecy capacity of the wiretap channel with state information available causally at both the encoder and the decoder. They showed that the lower bound is strictly larger than that for the noncausal case by Liu and Chen [13]. Recently, Hajizadeh and Hodtani [14] investigated two classes of three-receiver BC with side information available at the transmitter or at both ends, multilevel BC and three-receiver less noisy BC. For the multilevel BC with side information, they assumed that two degraded message sets are to be sent to three receivers, one for all receivers, the other only for the first receiver. They found the achievable rate region of multilevel BC with side information noncausally available at the transmitter. For the three-receiver less noisy BC with side information available at the transmitter, they assumed that three degraded message sets are to be sent to three receivers, respectively, and that the first receiver is less noisy than the second one and the second receiver is less noisy than the third one. When the side information is available at both the transmitter and the receiver, they established the capacity region of the three-receiver less noisy BC.

Different from [14], our paper considers another class of three-receiver, which is called one-receive two-eavesdropper, DM-BC with three degraded message sets and noncausally side information (see Figure 1). In this class of three-receiver BC, a common message $M_0$ is to be sent to three receivers $(Y_1, Z_2, Z_3)$, a private message $M_1$ is to be sent to the first and the second receiver $(Y_1, Z_2)$, and meanwhile unrevealed to the third receiver $(Z_3$, viewed as one eavesdropper$)$; then a second private message $M_2$ is to be sent to the first receiver $(Y_1)$ while kept secret from the second and the third receiver $(Z_2, Z_3$, viewed as two eavesdroppers$)$. The objective of this paper is to study this class of three-receiver BC with side information and three degraded message sets with secrecy constraints. When the side information is noncausally available only at the transmitter, we establish the achievable rates by using a combination of superposition coding, Gel’fand-Pinsker coding scheme, and Nair-El Gamal indirect decoding. The achievable secrecy region of this paper subsumes Steinberg’s rate region for two-receiver degraded BC with the side information and the secrecy capacity region for one-receiver two-eavesdropper DM-BC with no side information as its special cases. When the side information is noncausally available at both the transmitter and the three receivers, we determine the perfect secrecy capacity region of the one-receiver two-eavesdropper BC with three degraded message sets and side information when the receivers follow a degradedness order.

The rest of this paper is organized as follows. In Section 2, we describe the channel model and present some basic definitions. In Section 3, we will divide it into two subsections. In the first subsection, we derive achievable rate region for three-receiver DM-BC when the side information is noncausally available at the transmitter. In the second subsection, we determine the perfect secrecy capacity region of three-receiver degraded DM-BC when the side information is noncausally available at both the transmitter and the receiver. Conclusions and further discussions are given in Section 4.

2. Channel Model and Definitions

We denote discrete random variables and their realizations with uppercase and lowercase letters, respectively; for example, $x$ and $y$ are, respectively, the realization of $X$ and $Y$. The random variables $X, Y_1, Z_2, Z_3$, and $S$ take values from finite sets $\mathcal{X}, \mathcal{Y}_1, \mathcal{Z}_2, \mathcal{Z}_3$, and $\mathcal{S}$. $X^n$ denotes the $n$-sequence random variable, where the superscript is omitted when the choice is clear. The entropy of a discrete random variable is denoted by $H(\cdot)$ and the mutual information between two random variables is denoted by $I(\cdot;\cdot)$. We denote by $\mathcal{Y}^n_0(X, Y)$ the set of $\epsilon$-strongly joint typical sequence of length $n$, and we assume that $X^n_0$ is the sequence of random variables $(X_1, X_{i+1}, \ldots, X_n)$ throughout. Furthermore, $p(x)$ indicates the probability mass function of $X$ over $\mathcal{X}$ and $p(x | y)$ indicates the conditional probability mass function of $X$ given $Y$.

We consider a class of three-receiver discrete memoryless broadcast channels (DM-BC) with input alphabet $\mathcal{X}$, three
output alphabets $\mathcal{Y}_1, \mathcal{X}_2, \mathcal{X}_3$, set of states $S_i$, each of them is finite, and a collection of conditional probability mass functions (pmfs) $p(y_1, z_2, z_3 | x, s)$ on $\mathcal{Y}_1 \times \mathcal{X}_2 \times \mathcal{X}_3, S_i$ are independently and identically distributed (i.i.d.) $p(s)$.

The channel and state sequence are memoryless, for example,

$$p(y_1^n, z_2^n, z_3^n | x^n, s^n) = \prod_{i=1}^{n} p(y_{1,i}, z_{2,i}, z_{3,i} | x_i, s_i),$$

$$p_3(s^n) = \prod_{i=1}^{n} p_3(s_i). \quad (1)$$

Denote the marginals of the channel by $p_{Y|I,X}(y_1 | s, x)$ and $p_{Z_1|I,X}(z_2 | s, x), p_{Z_2|I,X}(z_3 | s, x).

The states $S$ are known to be noncausally at the transmitter, or at both the transmitter and the receiver as side information. The transmitter wishes to send a common message $M_0$ to three receivers, $M_1$ to the first and the second receiver which needs to be kept secret from the third receiver and to send $M_2$ only to the first receiver which needs to be kept secret from the second and the third receiver (viewed as two eavesdroppers) in $n$ uses of the channel.

A broadcast channel $p(y_1, z_2, z_3 | s, x)$ is said to be physically degraded if

$$p(y_1, z_2, z_3 | s, x) = p_{Y|I,X}(y_1 | s, x) p_{Z_1|Y_1}(z_2 | y_1) p_{Z_2|Z_2}(z_3 | z_2) \quad (2)$$

in which case $Z_1$ is a degraded version of $Y_1$, and $Z_2$ is a degraded version of $Z_2$. According to this definition, we note that the side information parameter $s$ controls only the nondegraded channel, whereas $p_{Z_2|Y_1}(z_2 | y_1), p_{Z_2|Z_2}(z_3 | z_2)$ is independent of the $s$.

**Definition 1.** A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$-code for the one-receiver two-eavesdropper DM-BC with three degraded message sets and side information available at the transmitter, as depicted in Figure 1, consists of an encoder map

$$f : \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \times \mathcal{S} \rightarrow \mathcal{X}^n,$$

$$\mathcal{M}_0 = \{1, \ldots, 2^{nR_0}\}, \text{ (common message set for } Y_1, Z_2, Z_3\),$$

$$\mathcal{M}_1 = \{1, \ldots, 2^{nR_1}\}, \text{ (private message set for } Y_1 \text{ and } Z_2\),$$

$$\mathcal{M}_2 = \{1, \ldots, 2^{nR_2}\}, \text{ (private message set for } Y_1\),$$

and a tuple of decoding maps

$$g_1 : \mathcal{Y}_1 \rightarrow \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2,$$

$$g_2 : \mathcal{Z}_2 \rightarrow \mathcal{M}_0 \times \mathcal{M}_1,$$

$$g_3 : \mathcal{Z}_3 \rightarrow \mathcal{M}_0.$$

Applying the encoder to $M_0, M_1, M_2$, which are uniformly distributed over the message sets, yields channel input $X = X^n$, and the corresponding channel outputs are $Y_1 = Y^n_1$, $Z_2 = Z^n_2$, $Z_3 = Z^n_3$. In particular, we have $g_1(Y_1) = (\tilde{M}_0, \tilde{M}_1, \tilde{M}_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$, $g_2(Z_2) = (\tilde{M}_0, \tilde{M}_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$, $g_3(Z_3) = (\tilde{M}_0) \in [1 : 2^{nR_0}]$, where the notation (,) highlights that the decoded messages are estimate. The probability of error is defined as

$$P_e = \Pr \left( \tilde{M}_0 \neq M_0, i = 1:3 \text{ or } \tilde{M}_1 \neq M_1, j = 1:2 \text{ or } \tilde{M}_2 \neq M_2 \right). \quad (3)$$

The rate tuples of the code are defined as follows:

$$(R_0, R_1, R_2) = \frac{1}{n} (\log M_0, \log M_1, \log M_2). \quad (4)$$

**Definition 2.** A rate tuple $(R_0, R_1, R_2)$ with perfect secrecy is achievable if there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes as previously mentioned with

$$\lim_{n \to \infty} P_e = 0,$$

$$\lim_{n \to \infty} \sup_n \frac{1}{n} I(M_2; Z^n_2) = 0,$$

$$\lim_{n \to \infty} \sup_n \frac{1}{n} I(M_1, M_2; Z^n_2) = 0,$$

where sup denotes the supremum of an expression. The capacity region with secrecy is the closure of the set of all achievable rate tuples $(R_0, R_1, R_2)$ with secrecy.

### 3. One-Receiver Two-Eavesdropper BC with Side Information

In this section, we first consider the scenario that the side information is noncausally available at the transmitter. We derive achievable rate region for this three receive DM-BC with side information noncausally available at the transmitter. The achievable secrecy region is established by using a combination of Gelfand-Pinsker binning scheme and rate splitting technique. In the achievability proof scheme, superposition coding scheme will be used to divide the available randomness into different levels so as to mislead the eavesdroppers. Achievability in this case also follows from the new idea of Nair-El Gamal indirect decoding. Subsequently, we consider the scenario that the side information is noncausally available at both the transmitter and the receiver. When the side information is available at both the transmitter and the receiver, we determine the perfect secrecy capacity region of this one-receive two-eavesdropper BC with three degraded message sets with secrecy constraints as the receivers form a degradedness order. Converse proof of Theorem 6 is provided in detail.

#### 3.1. Side Information Noncausally Available at the Transmitter

**Theorem 3.** Rate tuples $(R_0, R_1, R_2)$ are achievable with perfect secrecy for one-receiver two-eavesdropper DM-BC with three degraded message sets and side information noncausally available at the transmitter when $Z_2$ is a degraded version of $Y_1$. 

Mathematical Problems in Engineering 3
and $Z_3$ is a degraded version of $Z_2$; that is, $Y_1 \rightarrow Z_2 \rightarrow Z_3$ forms a Markov chain, provided that

$$R_0 \leq I(W;Z_3) - I(W;S),$$
$$R_1 \leq I(V;Z_2 | W) - I(V;Z_3 | W) - I(V;S | W),$$
$$R_2 \leq I(X;Y_1 | U) - I(X;Z_2 | U) - I(X;S | U)$$

for some distributions $p(w,u,v | s)$ and functions $x(w,u,v,s)$. 

**Corollary 4.** Setting $S = \emptyset$, $U = V$ in achievable rates of Theorem 3, our achievable rate region with secrecy is reduced to the capacity region of the one-receiver two-eavesdropper DM-BC with three degraded message sets when $Y_1, Z_2, Z_3$ forms a degradedness order as given in [7].

**Corollary 5.** Setting $Z_3 = Y_1, U = V = W$ in achievable rates of Theorem 3, the achievable rate region with secrecy is reduced to the capacity region of Steinberg’s rate region for two-receiver degraded DM-BC with noncausally side information [11].

**Proof.** The most important part of the proof of the achievable rate is the code generation. We use superposition technique and Wyner’s wiretap coding [1] as the secrecy achievability method. We also employ indirect decoding scheme [5] where the first decoder finds $M_1$ from the satellite codewords instead of cloud centers and use superposition coding scheme to divide the available randomness into different levels, which are used to mislead the eavesdroppers.

Consider a DM-BC with $(X \times \mathcal{D}, p(y_1,z_2,z_3 | x,s)p(s), \mathcal{Y}_1, \mathcal{Z}_2, \mathcal{Z}_3)$. Fix $n$ and a joint distribution on $\mathcal{D}$. The side information alphabet set $\mathcal{D}$ is distributed i.i.d according to

$$p_{\mathcal{D}}(s^n) = \prod_{i=1}^{n} p(s_i).$$

(1) **Code Generation.** Randomly and independently generate $2^{n(R_0+R_1^0)}$ sequences $u^n(m_0,m_0',m_0'',m_0''',m_0''''',m_0''''''')$, each one i.i.d according to $\prod_{i=1}^{n} p_U(u_i)$ and randomly throw them into $2^{nR_0}$ bins. For each $u^n(m_0,m_0')$, randomly and independently generate $2^{n(R_1^0+R_2^0)}$ sequences $u^n(m_0,m_0',m_1,m_1',s_1,s_2)$, each one i.i.d according to $\prod_{i=1}^{n} p_U(u_i | w_2(m_0,m_0'))$, and randomly throw them into $2^{nR_1}$ bins. For each $u^n(m_0,m_0',m_1,m_1',s_1)$, randomly and independently generate $2^{nR_2^0}$ sequences $u^n(m_0,m_0',m_1',s_1,s_2)$, each one i.i.d according to $\prod_{i=1}^{n} p_U(u_i | w_1(m_0,m_0'))$, and randomly throw them into $2^{nR_2^0}$ bins. For each $u^n(m_0,m_0',m_1,m_1',s_1,s_2)$, randomly and independently generate $2^{n(R_3^0+R_4^0)}$ sequences $x^n(m_0,m_0',m_1,m_1',s_1,s_2)\rightarrow s_3, s_2, s_1, s_0 \rightarrow \tilde{R}_3 = R_{11} + R_{12}$. The randomness variables $s_1, s_2,$ and $s_3$ are used to mislead the eavesdroppers.

(2) **Encoding.** Given the message $(m_0,m_1,m_2)$ and side information $s_0$, the encoder finds $(m_0, m_1, m_1')$ according to the bin indices since the messages are in the indices. Then, encoder looks for a $m_1'$ in the bin $m_1'$ of $a_k^n$ sequences such that $(a_k^n(m_0, m_1', m_1', s_1, s_2, s_3)) = \mathcal{F}^{(n)}_{s_0}$. Then, the encoder finds $m_1'$ such that $(a_k^n(m_0, m_1', m_1', s_1, s_2, s_3)) = \mathcal{F}^{(n)}_{s_0}$. Then, the encoder finds $m_1'$ in the $x^n$ sequences such that $(a_k^n(m_0, m_1', m_1', s_1, s_2, s_3)) = \mathcal{F}^{(n)}_{s_0}$. Finally, the encoder finds $m_1'$ in the $x^n$ sequences such that $(a_k^n(m_0, m_1', m_1', s_1, s_2, s_3)) = \mathcal{F}^{(n)}_{s_0}$. We assume that the correct indices are found through the encoding procedure; that is, $m_0'= m_0', m_1' = m_1', m_2' = m_2', s_0 = s_0'n$. We send the found $x^n$ sequence.

(3) **Decoding and Analysis of the Probability of Error.** Receiver $Z_3$ finds $m_1$ by decoding $W$, $Z_2$ finds $m_1$ by decoding $V$ and finds $m_0$ by decoding $V$, and $Y_1$ finds $m_0$ by decoding $W$, and $Y_1$ finds $m_0$ by decoding $W$. This results in loss of generality, we assume that the tuple $(m_0, m_1, m_2) = (1, 1, 1)$ is sent.

At receiver $Z_3$, the decoder finds the unique $m_0$ such that $(u^n(m_0, m_1', m_2'), Z_3^n) \in \mathcal{F}^{(n)}_{s_0}$; otherwise, it declares an error. Thus, the possible error events are as the follows:

$$E_{31} = \{W^n \in (1, M_0'), Z_3^n \not\in \mathcal{F}^{(n)}_{s_0}\},$$
$$E_{32} = \{W^n \in (m_0', M_0'), Z_3^n \in \mathcal{F}^{(n)}_{s_0}\},$$
for some $m_0' \neq 1, m_0' \neq M_0'$. Thus, the probability of error for decoder $Z_3$ is upper bounded as

$$P(E_{31}) \leq P(E_{31}) + P(E_{32}).$$

We now bound each term. By the law of large numbers (LLN) [15], $P(E_{31})$ tends to zero as $n \rightarrow \infty$:

$$P(E_{32}) = \sum_{m_0', m_0''} P(u^n) P(z_0^n) \leq 2^{n(R_0+R_0')} \cdot 2^{-n(H(W;Z_3)+\epsilon)} \cdot 2^{-n(H(Z_0)+\epsilon)} \cdot 2^{-n(H(Z_3)+\epsilon)} = 2^{n(R_0+R_0'-I(W;Z_3)+3\epsilon)}.$$
At receive $Z_2$, we can similarly bound the probability of error for $Z_2$. For $Z_2$, we define the error events

$E_{21} = \{ W^n (M_0', 1), V^n (M'_0, 1, M'_1, m'_1, s_{12}), Z_2 \} \notin \mathcal{E}^n_c$,

$E_{22} = \{ W^n (M_0', 1), V^n (M'_0, 1, m'_1, m_{12}', s_{12}), Z_2 \} \in \mathcal{E}^n_c$

for some $m_1 \neq 1, m_{12}' \neq M_{12}', s_{12} \neq S_{12}$,

$E_{23} = \{ W^n (m_0', m_0), V^n (m_0', m_0, m_1, m_{12}', s_{12}), Z_2 \}
\in \mathcal{E}^n_c$ for some $m_0 \neq 1, m'_1 \neq M'_0, m_1 \neq 1,$

$m_{12}' \neq M_{12}', s_{12} \neq S_{12}$. \hfill (12)

The probability of error for $Z_2$ is then upper bounded by

$$P(E_2) \leq P(E_{21}) + P(E_{22}) + P(E_{23}). \hfill (13)$$

By the LLN, $P(E_{21})$ tends to zero as $n \to \infty$. Next, we consider the event $E_{22}$. For $m_1 \neq 1, V^n(M'_0, 1, m_1, m_{12}')$ is conditionally independent of $(V^n(M'_0, 1, m_{12}', Z_2))$ given $W^n(M_0', 1)$ and is distributed according to $\prod_{i=1}^n P_{Y_{1i}}(v_i \mid u_i)$. Thus, by the packing lemma [16], $P(E_{22}) \to 0$ as $n \to \infty$ if

$$R_1 + R'_1 + \tilde{R}_2 \leq I (V; Z_2 | W) - 6\varepsilon. \hfill (14)$$

Similarly, for event $E_{23}, P(E_{23}) \to 0$ as $n \to \infty$ if

$$R_0 + R'_0 + R_1 + R'_1 + \tilde{R}_1 \leq I (WV; Z_2) - 5\varepsilon. \hfill (15)$$

We can see that this is a redundant inequality. At receive $Y_1$, we define the error events as

$E_{11} = \{ W^n (M_0', 1), U^n (M'_0, 1, M'_1, 1, s_{12}, s_{11}) \},$

$X^n (M'_0, 1, M'_1, 1, s_{12}, s_{11}, M'_0, 1, s_2, Y_1^n) \notin \mathcal{E}^n_c \}$,

$E_{12} = \{ W^n (M_0', 1), U^n (M'_0, 1, M'_1, 1, s_{12}, s_{11}) \},$

$X^n (M'_0, 1, M'_1, 1, s_{12}, s_{11}, M'_0, m'_1, m_2, s_2, Y_1^n)
\in \mathcal{E}^n_c$ for some $m_2 \neq 1, m'_2 \neq M'_2, s_2 \neq S_2$

$E_{13} = \{ W^n (M_0', 1), U^n (M'_0, 1, m_1, m_1, m_2, s_{11}) \},$

$X^n (M'_0, 1, m'_1, m_2, m_2, s_2, Y_1^n) \in \mathcal{E}^n_c$

for some $m_1 \neq 1, m'_1 \neq M'_1, m_2 \neq 1,$

$m'_2 \neq M'_2, s_{12} \neq S_{12}, s_{11} \neq S_{11}$

$E_{14} = \{ W^n (m_0', m_0), U^n (m_0', m_0, m'_1, m_1),
X^n (m_0', m_0, m_0, m_0, m_1, m_2, s_{11}, Y_1^n)
\in \mathcal{E}^n_c$

for some $m_0 \neq 1, m'_0 \neq M'_0, m_1 \neq 1, m'_1 \neq M'_1,$

$m_2 \neq 1, m'_2 \neq M'_2, s_{12} \neq S_{12}, s_{11} \neq S_{11} \}$. \hfill (16)

Therefore, the probability of error of the receiver $Y_1$ can be made arbitrarily small if

$$R_2 + R'_2 + \tilde{R}_2 \leq I (X, Y_1 | U) - 6\varepsilon,$$

$$R_1 + R'_1 + \tilde{R}_1 + R_2 + R'_2 + \tilde{R}_2 \leq I (X, Y_1 | W) - 6\varepsilon,$$

$$R_0 + R'_0 + R_1 + R'_1 + \tilde{R}_1 + R_2 + R'_2 + \tilde{R}_2 \leq I (X, Y_1) - 5\varepsilon. \hfill (17)$$

Using a similar argument on analysis of information leakage rate as in [7], we have $I(M_1, M_2; Z_0^n | C) \leq \kappa e$, if $\tilde{R}_2 \geq I(X; Z_2 | W)$, also have $I(M_2; Z_0^n | C) \leq \kappa e$ if $\tilde{R}_2 \geq I(X; Z_2 | U)$, and have $I(M_1; Z_0^n | C) \leq \kappa e$ if $\tilde{R}_2 \geq I(V; Z_3 | W)$.

Subsequently, we use Gel’fand-Pinsker coding scheme and determine that the encoder can choose the proper $m'_0,$ $m'_1, m'_2$ indices to make the probability of error tend to zero proving that for every $\varepsilon > 0$ and $n \to \infty$:

$$R'_0 > I (W; S),$$

$$R'_1 > I (V; S | W),$$

$$R'_2 > I (X; S | U). \hfill (19)$$

Finally, combining all the terms and using Fourier-Motzkin Elimination, we obtain the expressions in Theorem 3 and complete the proof of achievability. \hfill (20)

3.2. Side Information Noncausally Available at Both the Transmitter and the Receivers

**Theorem 6.** The secrecy capacity region of one-receiver two- eavesdropper DM-BC with three degraded message sets and side information noncausally available both at the transmitter and at the receiver when $Z_3$ is a degraded version of $Y_1$ and $Z_3$ is a degraded version $Z_2$, that is, $Y_1 \rightarrow Z_2 \rightarrow Z_3$ forms a Markov chain, is given by the union rate tuples $(R_0, R_1, R_2)$ such that

$$R_0 \leq I (W; Z_3 | S),$$

$$R_1 \leq I (V; Z_2 | W, S) - I (V; Z_3 | W, S),$$

$$R_2 \leq I (X; Y_1 | V, S) - I (X; Z_2 | V, S). \hfill (21)$$

**Proof.**

(1) Achievability. Setting $\tilde{Y}_1 = (Y_1, S), \tilde{Z}_k = (Z_k, S), k = 2, 3, U = V,$ and substituting it into (6), we can achieve the direct part of the proof.

(2) Converse. We define

$$W'_i := (M_0, S_i, S_{i+1}, Z_3^n),$$

$$V_i := (M_0, M_1, S_i, S_{i+1}, Z_2^n, Z_3^n). \hfill (22)$$
First, we consider the rate $R_0$

\[ nR_0 = H(M_0) \]

(a) \[ \leq I(M_0; Z_3 | S^n) + n \epsilon_n \]

\[ = \sum_{i=1}^{n} I(M_0; Z_{3j} | S^n, Z_{3j+1}^n) + n \epsilon_n \]

\[ = \sum_{i=1}^{n} I(M_0, Z_{3j+1}^n; Z_{3j} | S^n) \]

\[ - \sum_{i=1}^{n} I(Z_{3j+1}^n; Z_{3j} | S^n) + n \epsilon_n \]

\[ \leq \sum_{i=1}^{n} I(M_0, Z_{3j+1}^n, S_i^{i-1}, S_{i+1}; Z_{3j} | S^n) + n \epsilon_n \]

\[ = \sum_{i=1}^{n} I(W_i, Z_{3j} | S_i) + n \epsilon_n \]

(23)

where (a) follows from Fano's inequality.

Next, we consider the rate $R_1$

\[ nR_1 = H(M_1) \]

(b) \[ \leq I(M_1; Z_2^n | M_0, S^n) + 2n \epsilon_n \]

\[ = I(M_1; Z_2^n | M_0, S^n) - I(M_1; Z_2^n | M_0) + 2n \epsilon_n \]

\[ = I(M_1; Z_2^n | M_0, S^n) - I(M_1; Z_3^n | M_0, S^n) \]

\[ + I(M_1; M_0 | Z_2^n, S^n) + 2n \epsilon_n \]

\[ = I(M_1; Z_2^n | M_0, S^n) - I(M_1; Z_3^n | M_0, S^n) \]

\[ + I(M_1; M_0 | Z_2^n, S^n) + 2n \epsilon_n \]

\[ = I(M_1; Z_2^n | M_0, S^n) - I(M_1; Z_3^n | M_0, S^n) \]

\[ + H(M_0 | Z_3^n, S^n) - H(M_0 | Z_3^n, S^n, M_1) + 2n \epsilon_n \]

\[ \leq I(M_1; Z_2^n | M_0, S^n) - I(M_1; Z_3^n | M_0, S^n) \]

\[ + H(M_0 | Z_3^n, S^n) + 2n \epsilon_n \]
\[
\begin{align*}
&\leq \sum_{i=1}^{n} I \left( M_1, Z_{2j}^n \mid M_0, S^n, Z_{3j+1}^n \right) \\
&\quad - \sum_{i=1}^{n} I \left( M_1, Z_{2j}^n \mid M_0, S^n, Z_{3j+1}^n \right) + 3n\epsilon_n \\
&= \sum_{i=1}^{n} I \left( M_1, Z_{2j}^n \mid M_0, S^n, Z_{3j+1}^n \right) \\
&\quad - \sum_{i=1}^{n} I \left( M_1, Z_{2j}^n \mid M_0, S^n, Z_{3j+1}^n \right) + 3n\epsilon_n \\
&= \sum_{i=1}^{n} \left( V_i ; Z_{2j}^n \mid W_i, S_i \right) - \sum_{i=1}^{n} \left( V_i ; Z_{2j}^n \mid W_i, S_i \right) + 3n\epsilon_n,
\end{align*}
\]
where (a) and (c) follow from Fano's inequality, (b) follows from the secrecy condition, and (d) and (e) follow from the Csiszár sum identity; thus, we have
\[
\begin{align*}
&\sum_{i=1}^{n} I \left( Z_{3j+1}^n \mid M_0, M_1, Z_{2j}^n, S^n \right) \\
&= \sum_{i=1}^{n} I \left( Z_{2j}^n \mid M_0, M_1, Z_{3j+1}^n \right),
\end{align*}
\]
(f) follows the fact
\[
\sum_{i=1}^{n} I \left( Z_{2j}^n \mid M_0, S^n, Z_{3j+1}^n \right) \\
\leq \sum_{i=1}^{n} I \left( Z_{2j}^n \mid M_0, S^n, Z_{3j+1}^n \right)
\]
which is due to the fact that $Z_3$ is a degraded version of $Z_2$.

Finally, we consider the $R_2$
\[
n R_2 = H ( M_2 ) = \sum_{i=1}^{n} I \left( M_2 ; Y_1^n \mid M_0, M_1, S^n \right) + H ( M_2 \mid M_0, M_1, S^n )
\]
\[
\begin{align*}
&\leq I \left( M_2 ; Y_1^n \mid M_0, M_1, S^n \right) + n\epsilon_n \\
&\leq I \left( M_2 ; Y_1^n \mid M_0, M_1, S^n \right) - I \left( M_2 ; Z_{2i}^n \mid S^n \right) + 2n\epsilon_n \\
&= I \left( M_2 ; Y_1^n \mid M_0, M_1, S^n \right) - I \left( M_2 ; Z_{2i}^n \mid M_1, S^n \right) \\
&\quad + I \left( M_2 ; M_0 ; M_1, Z_{2i}^n, S^n \right) + 2n\epsilon_n \\
&= I \left( M_2 ; Y_1^n \mid M_0, M_1, S^n \right) - I \left( M_2 ; Z_{2i}^n \mid M_1, S^n \right) \\
&\quad - I \left( M_2 ; Z_{2i}^n \mid M_0, M_1, S^n \right) + I \left( M_2 ; M_0 ; M_1, Z_{2i}^n, S^n \right) + 2n\epsilon_n \\
&= I \left( M_2 ; Y_1^n \mid M_0, M_1, S^n \right) - I \left( M_2 ; Z_{2i}^n \mid M_0, M_1, S^n \right) \\
&\quad + I \left( M_2 ; M_0 ; M_1, Z_{2i}^n, S^n \right) + 2n\epsilon_n.
\end{align*}
\]
where (a) and (c) follow Fano’s inequality, (b) follows from the secrecy condition, (d) follows the fact that
\[
\sum_{i=1}^{n} I \left( X_i ; Z_{2j} \mid M_0, M_1, S^n, Z_{2j}^{i-1}, Z_{3j+1}^{n}, Y_{1m+1}, M_2 \right)
\]
\[
\leq \sum_{i=1}^{n} I \left( X_i ; Y_{1j} \mid M_0, M_1, S^n, Z_{2j}^{i-1}, Z_{3j+1}^{n}, Y_{1m+1}, M_2 \right)
\]
which is due to the degradation condition, and (e) is due to the following Markov Chain:
\[
(M_2, Y_{1j+1}, M_0, M_1, Z_{2j}^{i-1}, Z_{3j+1}^{n}) \rightarrow (X_i, M_0, M_1, S^n, Z_{2j}^{i-1}, Z_{3j+1}^{n}) \rightarrow (Y_{1j}, Z_{2j}).
\]

Finally, let \( Q \in \{1,2,\ldots,n\} \) be a uniformly distributed random variable independent of all other random variables and define \( W = (W_Q, Q), V = (V_Q, Q), X = X_Q, Y_1 = Y_{1Q}, Z_2 = Z_{2Q}, Z_3 = Z_{3Q} \) that completes the converse proof in the standard way [15].

\[ \blacksquare \]

4. Conclusion

A class of three-receiver, one-receiver two-eavesdropper, discrete memoryless broadcast channel (DM-BC) with three degraded message sets and noncausally side information is considered in this paper. We study this class of three-receiver BC with three degraded message sets and side information with secrecy constraints. We establish the achievable rates using a combination of superposition coding, Gelfand-Pinsker binning scheme, and Nair-El Gamal indirect decoding when the side information is noncausally available at the transmitter. The achievable secrecy region of this paper subsumes Steinberg’s rate region for two-receiver degraded BC with the noncausally side information and the secrecy capacity region for one-receiver two-eavesdropper DM-BC with no side information as its special cases. As the side information is noncausally available at both the transmitter and the three receivers, we determine the perfect secrecy capacity region of the one-receiver two-eavesdropper BC with three degraded message sets when the receivers follow a degradedness order; that is, \( Y_1 \rightarrow Z_2 \rightarrow Z_3 \) forms a Markov chain. In our future work, we will consider more general three-receiver BC with two or three degraded message sets and side information causally or noncausally available at the transmitter and the receiver (the receivers without following the degradedness order).

Conflict of Interests

The authors declare that they have no financial and personal relationships with other people or organizations that can inappropriately influence their work, and there is no professional or personal interest of any nature or kind in any product, service, and/or company that could be construed as influencing the position presented in, or the review of this paper.

Acknowledgment

This work was supported in part by the National Science Foundation of China under Grants no. 60932003 and no. 61271220.

References
