2020 28th Iranian Conference on Electrical Engineering (ICEE)

Secrecy Capacity Outer Bound of Broadcast Channels with States Known at the Transmitter and Message Side Information at Receivers

Saeid Pakravan
Department of Electrical Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
Saeid.pakravan@mail.um.ac.ir

Ghosheh Abed Hodtani
Department of Electrical Engineering
Ferdowsi University of Mashhad
Mashhad, Iran
hodtani@um.ac.ir

Abstract— **In this article, a broadcast channel in the degraded state with two legitimate receivers in the attendance of an eavesdropper has been studied, where, the sender demands to forward two independent confidential messages that ought to be kept as secret as feasible of the eavesdropper to the legitimate receivers. In the studied system, it has been supposed that the non-causal channel state information has been considered at the transmitter side and every one of receivers has the message forwarded via source demanded via the further one. The model studied in this paper is further generalized into the formerly considered broadcast channel with confidential messages and considering side information in the receiver. It has been supplied an outer bound by considering confidentially conditions for proposed system.**

Keywords— Broadcast channel, Capacity outer bound, Secrecy capacity, Side information.

I. Introduction

Broadcast channel (BC) was firstly reported in [1]. Determining the capacity region of discrete memoryless BC (DM-BC) in general case is up to this time an irresolvable question, with the exception of few special cases in which one channel is superior to the other channel, including degraded, more capable, less noisy, deterministic and semi-deterministic channels. In general 2-receiver BC, the best-known capacity inner bound has been derived in [2]. It has been established an achievable rate region in [3] via superposition coding technique for 2-receiver BC that is degraded; in [4] it is demonstrated that this rate region is optimal.

Channels with considering side information (SI) was deliberated by Shannon for the first time. The capacity region for case of channel when SI is known at the transmitter causally has been derived in [5]. This scheme for the non-causally case was investigated in [6]. Cover and Chiang generalized the consequences from [6] to channels that SI is known at the transmitter and receiver side non-causally in [8]. The Gaussian versions of [5] was studied in [8]. BC with SI received considerable attention recently in different scenarios. Several works have been done upon this set of channels. BC with SI was firstly introduced in [9]. Steinberg and Shamai in [10] considered public BC in presence of SI non-causally available at the sender side, where Marton's achievability scheme has been extended to state-dependent channels. Later, SI known at

In [11], secure communication as an important issue was surveyed by Shannon. In [12] the degraded wiretap channel was studied. Wyner's outcome was extended to the public BC in the presence of confidential messages and also the secrecy capacity for this activity has been established in [12]. Liu in [13] studied the BC with 2-receivers that private messages are to be kept invisible of the inadvertent receiver. In [14], a BC with an external eavesdropper and two private messages was investigated. The authors in [15] studied BC cases with a common and a private message that common message has been conveyed to the whole of the receivers and the private message has been preserved of some of the receivers. The availability of message SI at the legitimate receivers is according to a case that each one of receiver knows the message forwarded via source demanded by the other one. It has been demonstrated to aid in modifying the secrecy rate region.

Despite that many work have been done on the secrecy capacity of BCs in presence of SI. The secrecy capacity for special cases of BCs when the CSI is available at sender and message side information (MSI) in destinations is still unknown. We focus on the secrecy capacity region of the BC with considering SI non-causally available at sender side and MSI at destinations. The availability of MSI has been demonstrated to aid in rectifying the secrecy rate region in our channels. This paper accurately focuses on a special case of an important problem to determine the secrecy capacity in communication. It is grounded on important work by Shannon, Cover, and Wyner, and it is an advancement over the most recent work cited in the aforementioned. The work may have broader application to cognitive radio.

This article has been established as follows: In Section II, the channel model has been characterized. Then, in Section III, an outer bound over the secrecy capacity region for presented scheme was devoted. Finally, the conclusion of paper was demonstrated in Section IV.

II. System Model

We explain the our scheme and also some basic definitions necessary for the continuation of the study in this section.

A. Channel model

The system model for the 2-receiver BC with non-causal CSIT and receiver SI in the attendance of one eavesdropper has been illustrated in below figure.

978-1-7281-7296-5/20/$31.00 ©2020 IEEE

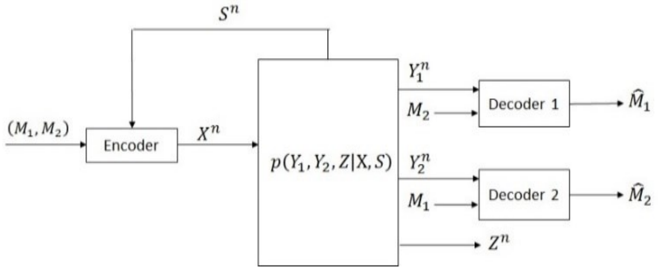

Fig. 1. The BC with 2-user and with 2-legitimate receivers and one eavesdropper in degraded version with considering SI.

Let $\mathcal{X}$ be the input set and $\mathcal{Y}_1$ and $\mathcal{Y}_2$ be the output sets related to the legal receivers and finally $\mathcal{Z}$ be the output set of eavesdropper; $\mathcal{S}$ be finite set that denotes CSI in the transmitter. Discrete random variables (RVs) have been signified with uppercase letters and their realizations have been signified with lowercase letters. We assume that X_i^n is the sequence of RV throughout. A DM-BC that considered degraded with 2-legal receivers, in attendance one eavesdropper and by expressions are determined via $(\mathcal{X}, \mathcal{S}, P(\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Z}|\mathcal{X}, \mathcal{S}), \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Z})$ which state $S_i \in \mathcal{S}$ are acquired i.i.d correspondent to $p(s)$, and $P(\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Z}|\mathcal{X}, \mathcal{S})$ are the channel transition probabilities. I Y_1 is a strong receiver than Y_2. Messages are also denoted by random variables M_1 and M_2. Consider the definitions below, used in the following sections in this paper.

B. Definitions

Definition 1: An $(n, 2^{nR_1}, 2^{nR_2}, \epsilon)$ code for DM 2-receiver BC with considering SI non-causally available at the sender side and MSI at receivers side contains 2-message sets; $\mathcal{M}_1 := \{1, \dots, 2^{nR_1}\}$ and $\mathcal{M}_2 := \{1, \dots, 2^{nR_2}\}$, contains from three maps: An encoder at the transmitter and a decoder at each legitimate receivers 1 and 2 consists of the following map:

$$enc.: \mathcal{M}_1 \times \mathcal{M}_2 \times S \to \mathcal{X}^n, \tag{1}$$

$$dec.(y_1): \mathcal{Y}_1^n \times \mathcal{M}_2 \to \widehat{\mathcal{M}}_1, \tag{2}$$

$$dec.(y_2): \mathcal{Y}_2^n \times \mathcal{M}_1 \to \widehat{\mathcal{M}}_2 \tag{3}$$

such that the $P_{Error}(avg)$ has been distinguished as below:

$$P_{Error}^{(n)} \triangleq P\{(\widehat{\mathcal{M}}_1, \widehat{\mathcal{M}}_2) \neq (\mathcal{M}_1, \mathcal{M}_2)\} \leq \epsilon. \tag{4}$$

where estimated messages are determined with $\widehat{\mathcal{M}}_1$ and $\widehat{\mathcal{M}}_2$ respectively at legitimate receivers 1 and 2.

Definition 2: When we have an integer n_0 for any $\mu > 0$ such that for all $n \geq n_0$ there exists an $(n, 2^{n(R_1-\mu)}, 2^{n(R_2-\mu)}, \epsilon)$ code; then, the rate pair (R_1, R_2) has been said achievable.

Definition 3: The capacity region has been distinguished as the set in the union from all ϵ-achievable rate (R_1, R_2).

The ignorance of eavesdropper concerning the secret message $m_1$and $m_2$has been considered via the significance from ambiguity. Hitherward, the secrecy level of secret messages $\mathcal{M}_1$ and $\mathcal{M}_2$ have been demonstrated in conditions of equivocation rates which are defined according to below:

$$R_{e1} = \frac{1}{n} H(\mathcal{M}_1|Z^n), \tag{5}$$

$$R_{e2} = \frac{1}{n} H(\mathcal{M}_2|Z^n), \tag{6}$$

$$R_{e12} = \frac{1}{n} H(\mathcal{M}_1, \mathcal{M}_2|Z^n). \tag{7}$$

Definition 4: A secrecy rate pair $(R_1, R_2) \in R_+^2$ has been considered achievable for the BC alongside receiver SI whether for each $\delta > 0$ exist a $n(\delta) \in N$ and a sequence of $(n, M_1^{(n)}, M_2^{(n)})$-code such that for all $n \geq n(\delta)$ we have

$$R_1 \leq \delta + R_{e1}, \tag{8}$$

$$R_2 \leq \delta + R_{e2}, \tag{9}$$

and further

$$R_1 + R_2 \leq \delta + R_{e12} \tag{10}$$

while $P_{Error}^{(n)} \to 0$ as $n \to \infty$. The conditions (8), (9) and (10) assurance perfect secrecy to every message that is individual.

III. Capacity Results

Now, an outer bound has been presented over the secrecy capacity region for introduced channel scheme defined in previous section.

Theorem 1. An outer bound on the secrecy capacity region for a discrete memoryless 2-receiver BC with CSIT non-causally and MSI is specified via the whole $(R_1, R_2) \in R_+^2$ that satisfy below conditions

$$R_1 \leq I(V; Y_1) - \max\{I(V, S), I(V, Z)\} \tag{11}$$

$$R_2 \leq I(V; Y_2) - \max\{I(V, S), I(V, Z)\} \tag{12}$$

$$\begin{aligned} R_1 + R_2 \leq min\{&I(V; Y_1|U) + I(V; Y_2|U) - I(V; Z|U) \\ &, I(V; Y_1) + I(V; Y_2) - I(V; Z)\}. \end{aligned} \tag{13}$$

for RVs $U - VX - Y_1, Y_2 - Z$.

Proof. An interpretation from Fano's imparity for the BC with MSI in the receivers is necessary to gather the desired outer bound on the secrecy capacity region. Fano's lemma mentioned is specified via $H(\mathcal{M}_1|\mathcal{M}_2, Y_1^n) \leq n\epsilon_1^{(n)}$ and $H(\mathcal{M}_2|\mathcal{M}_1, Y_2^n) \leq n\epsilon_2^{(n)}$ with $\epsilon_1^{(n)}, \epsilon_2^{(n)} \to 0$ as $n \to \infty$. Authorized us to specify the auxiliary RVs as follows

$$U_i \triangleq (Y_1^{i-1}, Y_2^{i-1}, Z_{i-1}^n, S_{i+1}^n), \tag{14}$$

$$V_i \triangleq (M_1, M_2, U_i) \tag{15}$$

which satisfy the following Markov chain condition $U_i - V_i X_i - Y_{1i}, Y_{2i} - Z_i$. Let m_1 and m_2 be independent RVs showing our messages. R_1 can be bounded as follows:

$$nR_1 \leq H(M_1|Z^n) + n\delta \tag{16}$$

$$\leq H(M_1) + n\delta = H(M_1|M_2) + n\delta \tag{17}$$

$$= H(M_1|Y_1^n, M_2) + I(M_1; Y_1^n|M_2) + n\delta \tag{18}$$

$$\leq \sum_{i=1}^{n} I(M_1; Y_{1,i}|M_2, Y_1^{i-1}) + n\epsilon_1^{(n)} + n\delta \tag{19}$$

$$\leq \sum_{i=1}^{n} I(M_1, M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i-1}^n; Y_{1,i}) + n(\epsilon_1^{(n)} + \delta) \tag{20}$$

$$= \sum_{i=1}^{n} I(M_1, M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i-1}^n, S_{i+1}^n; Y_{1,i}) -$$

$$\sum_{i=1}^{n} I\left(S_{i+1}^{n};Y_{1,i}\middle|M_1,M_2,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n}\right)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (21)$$

$$=\sum_{i=1}^{n} I(M_1,M_2,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n},S_{i+1}^{n};Y_{1,i})-$$

$$\sum_{i=1}^{n} I\left(Y_1^{i-1};S_i\middle|M_1,M_2,S_{i+1}^{n},Y_2^{i-1},Z_{i-1}^{n}\right)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (22)$$

$$=\sum_{i=1}^{n} I(M_1,M_2,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n},S_{i+1}^{n};Y_{1,i})-$$

$$\sum_{i=1}^{n} I\left(M_1,M_2,S_{i+1}^{n},Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n};S_i\right)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (23)$$

$$=\sum_{i=1}^{n} I(V_i;Y_{1,i})-\sum_{i=1}^{n} I(V_i;S_i)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (24)$$

where (16) in this proof follows from inequalities (5) and (8). (19) is due to Fano's imparity and (22) comprehend of sum Csiszar lemma. Finally, it has been consequence that equality (24) come from definition of the auxiliary RVs according to (15). Therefore, from inequality (6) and perfect secrecy condition (9), R_2 can be bounded as follows:

$$nR_2 \le \sum_{i=1}^{n} I\left(V_i;Y_{2,i}\right)-\sum_{i=1}^{n} I(V_i;S_i)+n\left(\epsilon_2^{(n)}+\delta\right). \quad (25)$$

Also we have

$$nR_1 \le H(M_1|Z^n)+n\delta \quad (26)$$

$$\le H(M_1)+n\delta = H(M_1|M_2)+n\delta \quad (27)$$

$$= H(M_1|Y_1^n,M_2)+I(M_1;Y_1^n|M_2)+n\delta \quad (28)$$

$$\le \sum_{i=1}^{n} I\left(M_1;Y_{1,i}\middle|M_2,Y_1^{i-1}\right)+n\epsilon_1^{(n)}+n\delta \quad (29)$$

$$\le \sum_{i=1}^{n} I(M_1,M_2,Y_1^{i-1},Y_2^{i-1},S_{i+1}^{n};Y_{1,i})+n(\epsilon_1^{(n)}+\delta) \quad (30)$$

$$=\sum_{i=1}^{n} I(M_1,M_2,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n},S_{i+1}^{n};Y_{1,i})-$$

$$\sum_{i=1}^{n} I\left(Z_{i-1}^{n};Y_{1,i}\middle|M_1,M_2,Y_1^{i-1},Y_2^{i-1},S_{i+1}^{n}\right)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (31)$$

$$=\sum_{i=1}^{n} I(M_1,M_2,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n},S_{i+1}^{n};Y_{1,i})-$$

$$\sum_{i=1}^{n} I\left(Y_1^{i-1};Z_i\middle|M_1,M_2,S_{i+1}^{n},Y_2^{i-1},Z_{i-1}^{n}\right)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (32)$$

$$=\sum_{i=1}^{n} I(M_1,M_2,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n},S_{i+1}^{n};Y_{1,i})-$$

$$\sum_{i=1}^{n} I\left(M_1,M_2,,Y_1^{i-1},Y_2^{i-1},Z_{i-1}^{n}S_{i+1}^{n};Z_i\right)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (33)$$

$$=\sum_{i=1}^{n} I(V_i;Y_{1,i})-\sum_{i=1}^{n} I(V_i;Z_i)+n\left(\epsilon_1^{(n)}+\delta\right) \quad (34)$$

the inequality (26) in this proof follows from inequalities (5) and (8); and (29) is due to Fano's imparity. (32) Comprehend of sum Csiszar lemma. Finally, the equality (34) has been concluded by definition of the auxiliary RVs according to (15). Therefore, from (6) and perfect secrecy condition (9), R_2 can be bounded as follows:

$$nR_2 \le \sum_{i=1}^{n} I\left(V_i;Y_{2,i}\right)-\sum_{i=1}^{n} I(V_i;Z_i)+n\left(\epsilon_2^{(n)}+\delta\right). \quad (35)$$

We use the fact that m_1 and m_2 are independent messages to established the upper bound over R_1+R_2. So, this bound can be bounded as follows:

$$n(R_1+R_2) \le H(M_1,M_2|Z^n)+n\delta \quad (36)$$

$$= H(M_1,M_2|Z^n)-H(M_1|Y_1^n,M_2)+H(M_1|Y_1^n,M_2)$$

$$-H(M_2|Y_2^n,M_1)+H(M_2|Y_2^n,M_1)+n\delta \quad (37)$$

$$\le H(M_1,M_2|Z^n)-H(M_1|Y_1^n,M_2)$$

$$-H(M_2|Y_2^n,M_1)+n\left(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta\right) \quad (38)$$

$$= H(M_1|M_2)+H(M_2|M_1)-H(M_1,M_2)$$

$$+H(M_1,M_2|Z^n)-H(M_1|Y_1^n,M_2)$$

$$-H(M_2|Y_2^n,M_1)+n\left(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta\right) \quad (39)$$

$$= I(M_1;Y_1^n|M_2)+I(M_2;Y_2^n|M_1)$$

$$-I(M_1,M_2;Z^n)+n\left(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta\right) \quad (40)$$

$$\le I(M_1,M_2;Y_1^n)+I(M_1,M_2;Y_2^n)$$

$$-I(M_1,M_2;Z^n)+n\left(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta\right) \quad (41)$$

$$=\sum_{i=1}^{n} I\left(M_1,M_2;Y_{1,i}\middle|Y_1^{i-1}\right)+\sum_{i=1}^{n} I\left(M_1,M_2;Y_{2,i}\middle|Y_2^{i-1}\right)$$

$$-\sum_{i=1}^{n} I\left(M_1,M_2;Z_{1,i}\middle|Z_{i+1}^{n}\right)+n\left(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta\right) \quad (42)$$

$$=\sum_{i=1}^{n} I\left(M_1,M_2,Y_2^{i-1},Z_{i+1}^{n},S_{i+1}^{n};Y_{1,i}\middle|Y_1^{i-1}\right)$$

$$-\sum_{i=1}^{n} I\left(Y_2^{i-1},Z_{i+1}^{n},S_{i+1}^{n};Y_{1,i}\middle|M_1,M_2,Y_1^{i-1}\right)$$

$$+\sum_{i=1}^{n} I\left(M_1,M_2,Y_1^{i-1},Z_{i+1}^{n},S_{i+1}^{n};Y_{2,i}\middle|Y_2^{i-1}\right)$$

$$-\sum_{i=1}^{n} I\left(Y_1^{i-1},Z_{i+1}^{n},S_{i+1}^{n};Y_{2,i}\middle|M_1,M_2,Y_2^{i-1}\right)$$

$$-\sum_{i=1}^{n} I\left(M_1,M_2,Y_1^{i-1},Y_2^{i-1},S_{i+1}^{n};Z_i\middle|Z_{i+1}^{n}\right)$$

$$+\sum_{i=1}^{n} I\left(Y_1^{i-1},Y_2^{i-1},S_{i+1}^{n};Z_i\middle|M_1,M_2,Z_{i+1}^{n}\right)$$

$$+n\left(\epsilon_1^{(n)}+\epsilon_2^{(n)}+\delta\right) \quad (43)$$

$$=\sum_{i=1}^{n} I\left(M_1,M_2;Y_{1,i}\middle|Y_1^{i-1},Y_2^{i-1},Z_{i+1}^{n},S_{i+1}^{n}\right)$$

$$\begin{aligned}
&+\sum_{i=1}^{n} I\big(Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{1,i}\big|Y_1^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{1,i}\big|M_1, M_2, Y_1^{i-1}\big)\\
&+\sum_{i=1}^{n} I\big(M_1, M_2; Y_{2,i}\big|Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n\big)\\
&+\sum_{i=1}^{n} I\big(Y_1^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{2,i}\big|Y_2^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(Y_1^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{2,i}\big|M_1, M_2, Y_2^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(M_1, M_2; Z_i\big|Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n, Z_{i+1}^n\big)\\
&-\sum_{i=1}^{n} I\big(Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n; Z_i\big|Z_{i+1}^n\big)\\
&+\sum_{i=1}^{n} I\big(Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n; Z_i\big|M_1, M_2, Z_{i+1}^n\big)\\
&+n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{44}$$

$$\begin{aligned}
&=\sum_{i=1}^{n} I\big(M_1, M_2; Y_{1,i}\big|Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n\big)\\
&+\sum_{i=1}^{n} I\big(M_1, M_2; Y_{2,i}\big|Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n\big)\\
&-\sum_{i=1}^{n} I\big(M_1, M_2; Z_i\big|Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n, Z_{i+1}^n\big)\\
&+n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{45}$$

$$\begin{aligned}
&\le\sum_{i=1}^{n} I\big(M_1, M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{1,i}\big|Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n\big)\\
&+\sum_{i=1}^{n} I\big(M_1, M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{2,i}\big|Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n\big)\\
&-\sum_{i=1}^{n} I\big(M_1, M_2, Y_1^{i-1}, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Z_i\big|Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n, Z_{i+1}^n\big)\\
&+n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{46}$$

$$\begin{aligned}
&=\sum_{i=1}^{n} I\big(V_i; Y_{1,i}\big|U_i\big) + \sum_{i=1}^{n} I\big(V_i; Y_{2,i}\big|U_i\big) - \sum_{i=1}^{n} I\big(V_i; Z_i\big|U_i\big)\\
&+n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{47}$$

where (36) in this proof follows from inequalities (7) and (10); and (38) is because of Fano's imparity. In (45) we use a interpretation of Csiszar Korner's sum identity modified for our scenarios. Finally, we have equality (47) by definition of the auxiliary RVs according to equalities (14) and (15). Sum rate $R_1 + R_2$ also can be bounded as follows:

$$n(R_1 + R_2) \le H(M_1, M_2|Z^n) + n\delta \tag{48}$$

$$\begin{aligned}
&= H(M_1, M_2|Z^n) - H(M_1|Y_1^n, M_2) + H(M_1|Y_1^n, M_2)\\
&\quad -H(M_2|Y_2^n, M_1) + H(M_2|Y_2^n, M_1) + n\delta
\end{aligned} \tag{49}$$

$$\begin{aligned}
&\le H(M_1, M_2|Z^n) - H(M_1|Y_1^n, M_2)\\
&\quad -H(M_2|Y_2^n, M_1) + n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big) =
\end{aligned} \tag{50}$$

$$\begin{aligned}
&H(M_1|M_2) + H(M_2|M_1) - H(M_1, M_2) + H(M_1, M_2|Z^n) -\\
&H(M_1|Y_1^n, M_2) - H(M_2|Y_2^n, M_1) + n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{51}$$

$$\begin{aligned}
&\le I(M_1; Y_1^n|M_2) + I(M_2; Y_2^n|M_1)\\
&\quad -I(M_1, M_2; Z^n) + n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{52}$$

$$\begin{aligned}
&\le I(M_1, M_2; Y_1^n) + I(M_1, M_2; Y_2^n)\\
&\quad -I(M_1, M_2; Z^n) + n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{53}$$

$$\begin{aligned}
&=\sum_{i=1}^{n} I\big(M_1, M_2; Y_{1,i}\big|Y_1^{i-1}\big) + \sum_{i=1}^{n} I\big(M_1, M_2; Y_{2,i}\big|Y_2^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(M_1, M_2; Z_{1,i}\big|Z_{i+1}^n\big) + n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{54}$$

$$\begin{aligned}
&=\sum_{i=1}^{n} I\big(M_1, M_2, Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{1,i}\big|Y_1^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(Y_2^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{1,i}\big|M_1, M_2, Y_1^{i-1}\big)\\
&+\sum_{i=1}^{n} I\big(M_1, M_2, Y_1^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{2,i}\big|Y_2^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(Y_1^{i-1}, Z_{i+1}^n, S_{i+1}^n; Y_{2,i}\big|M_1, M_2, Y_2^{i-1}\big)\\
&-\sum_{i=1}^{n} I\big(M_1, M_2, Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n; Z_i\big|Z_{i+1}^n\big)\\
&+\sum_{i=1}^{n} I\big(Y_1^{i-1}, Y_2^{i-1}, S_{i+1}^n; Z_i\big|M_1, M_2, Z_{i+1}^n\big)\\
&+n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{55}$$

$$\begin{aligned}
&=\sum_{i=1}^{n} I(V_i, Y_{1,i}) + \sum_{i=1}^{n} I(V_i, Y_{2,i}) - \sum_{i=1}^{n} I(V_i, Z_i)\\
&+n\big(\epsilon_1^{(n)} + \epsilon_2^{(n)} + \delta\big)
\end{aligned} \tag{56}$$

where (36) in this proof follows from inequalities (7) and (10); and (50) is because of Fano's imparity. In the end, we have equality (56) by definition of the auxiliary RVs according to (15).

In above inequalities $\epsilon_1^{(n)}, \epsilon_2^{(n)}$ and δ tend to zero as $n \to \infty$. Using the time-sharing scheme, inequalities (24), (25), (34), (35), (47) and (56) establishes inequalities in Theorem 1. ■

IV. Conclusion

In this study, for the degraded BC with 2-legitimate receivers an outer bound in attendance of an eavesdropper has been derived. It has been supposed that the non-causal CSI has been recognized at sender side and any one of receiver knows the message forwarded via source demanded with another one, referential to as MSI at receiver. The scheme studied in this article is further universal than the formerly considered BC with confidential messages and receiver side information because circumstances on the receivers are comprehensive and also channel state has been supposed is existent at the sender in this paper.

REFERENCES

[1] Cover, Thomas. "Broadcast channels." *IEEE Transactions on Information Theory* 18, no. 1 (1972): 2-14.

[2] Marton, Katalin. "A coding theorem for the discrete memoryless broadcast channel." *IEEE Transactions on Information Theory* 25, no. 3 (1979): 306-311.

[3] Bergmans, P. "Random coding theorem for broadcast channels with degraded components." *IEEE Transactions on Information Theory* 19, no. 2 (1973): 197-207.

[4] Gallager, Robert G. "Capacity and coding for degraded broadcast channels." *Problemy Peredachi Informatsii* 10, no. 3 (1974): 3-14.

[5] Shannon, Claude E. "Channels with side information at the transmitter." *IBM journal of Research and Development* 2, no. 4 (1958): 289-293.

[6] Gelfand, S. I. "Coding for channel with random parameters." *Probl. Contr. and Inf. Theory* 9, no. 1 (1980): 19-31.

[7] Cover, Thomas M., and Mung Chiang. "Duality between channel capacity and rate distortion with two-sided state information." *IEEE Transactions on Information Theory* 48, no. 6 (2002): 1629-1638.

[8] Anzabi-Nezhad, Nima S., Ghosheh Abed Hodtani, and Mohammad Molavi Kakhki. "Information theoretic exemplification of the receiver re-cognition and a more general version for the costa theorem." *IEEE Communications letters*17, no. 1 (2012): 107-110.

[9] Steinberg, Yossef. "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information." *IEEE Transactions on Information Theory*51, no. 8 (2005): 2867-2877.

[10] Steinberg, Yossef, and Shlomo Shamai. "Achievable rates for the broadcast channel with states known at the transmitter." In *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, pp. 2184-2188. IEEE, 2005.

[11] Shannon, Claude E. "Communication theory of secrecy systems." *Bell system technical journal* 28, no. 4 (1949): 656-715.

[12] Wyner, Aaron D. "The wire-tap channel." *Bell system technical journal* 54, no. 8 (1975): 1355-1387.

[13] Liu, Ruoheng, Ivana Maric, Predrag Spasojevic, and Roy D. Yates. "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions." *IEEE Transactions on Information Theory* 54, no. 6 (2008): 2493-2507.

[14] Bagherikaram, Ghadamali, Abolfazl S. Motahari, and Amir K. Khandani. "Secure broadcasting: The secrecy rate region." In *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pp. 834-841. IEEE, 2008.

[15] Mansour, Ahmed S., Rafael F. Schaefer, and Holger Boche. "Secrecy measures for broadcast channels with receiver side information: Joint vs individual." In *Information Theory Workshop (ITW), 2014 IEEE*, pp. 426-430. IEEE, 2014.