International Journal of Hybrid Information Technology
Vol.7, No.3 (2014), pp.121-132
http://dx.doi.org/10.14257/ijhit.2014.7.3.13

Research on an Outer Bound of Achievable Secrecy Rate Region for BCE

Yan Zhu, Xiao Chen, Yongkai Zhou, Fangbiao Li and Zhi Xue

School of Electronic, Information and Electrical Engineering
Shanghai Jiaotong University
Shanghai, China
E-mail: {topbestzy1983, chenxiao, ssmailzyk, flyin2009, zxue}@sjtu.edu.cn

Abstract

The security performance problems of broadcast channel with an eavesdropper (BCE) have been studied for many years in the field of communication. Many articles have given the meaningful results. However, almost no consequent of an outer bound on BCE has been given by previous work, especially, no significant results has been given. So this paper proposes and proves an outer bound of BCE by using information entropy, and further proves this outer bound is tight in the cut-set bound by max-flow min-cut theorem. It illustrates the outer bound is meaningful. Finally, by contrasting a variety of existing results, we can get that the outer bound in this paper include (tight) in the existing outer bound of BCE in the case of not considering the eavesdropper.

Keywords: *Broadcast channel; eavesdropper; outer bound; max-flow min-cut theorem.*

1. Introduction

Due to the broadcast characteristics of wireless network, the wireless communication security can't be guaranteed in effect. Traditional methods of communication security are mostly encryption technology which based on application layer. However, such technologies which have been widely used can't achieve perfect secrecy, because they are all assumed that the computing capability of eavesdropper is limited.

The information theory security is different from traditional secure communication methods. It belongs to physical layer security and can be effective against the eavesdropper. Therefore, it is widely considered to be the most stringent secrecy concept.

The concept of information theory security was first proposed by Shannon in [1], and the condition of perfect secrecy had been given by Shannon: the mutual information between the information received by eavesdropper and sent by transmitter is equal to 0. After that Wyner introduced the concept of wire-tap channel in [2], he proved that the perfect secrecy can be achieved between the legitimate communication parties only if the eavesdropper's channel is a degraded version but not key-dependent. Then, Csiszar and Korner extended Wyner's work in [3], and they proved that if the legitimate transceiver channel is better than the eavesdropper's channel, the perfect secrecy can be achieved rather than having to ensure that the eavesdropper's channel is a degraded one. Here after Leung-Yan –Cheong and Hellman researched the Gaussian wire-tap channel with eavesdropper and proved the secrecy capacity of communication system is equal to the difference of channel capacity between the main channel and the eavesdropper's channel in [4].

ISSN: 1738-9968 IJHIT

This paper considers the broadcast channel with eavesdropper (BCE). The achievable security rate region of BCE was first proposed by Ghadamali Bagherikaram *et al.* in [5] and [6]. We focus on proving the achievable security rate region which has been proposed in the following part of this paper.

The remaining paper is organized as follows. System model will be described in Section 2. Section 3 will then focus on the proposal and certification for an outer bound of achievable security rate region of BCE. Through comparing the cut-set bound by max-flow min-cut theorem, we will elaborate and prove the significance of the outer bound in section 4. Section 5 will give the consequence analysis of contrasting the existing outer bound of BCE in the case of not considering the eavesdropper. The conclusion will be given in Section 6. Concrete proof will be completed in the appendix.

2. Preliminaries

The system model of BCE is shown as Fig.1. M_0, M_1 and M_2 indicate the message variables which have been sent by the transmitter. χ is the finite input alphabet of channel. y_1, y_2 and z are the finite output alphabets of receiver 1, receiver 2 and the eavesdropper's channel respectively. $p(y_1, y_2, z \mid x)$ is the transition probability function of the channel. Suppose that $\omega_0 = \{1, 2, \ldots W_0\}$ is a public message set, $\omega_1 = \{1, 2, \ldots W_1\}$ and $\omega_2 = \{1, 2, \ldots W_2\}$ are private message set of user 1 and user 2 respectively. M_0, M_1, M_2 are the message variables which corresponding to the message sets ω_0 , ω_1 , ω_2 . That is $M_i \subseteq \omega_i, i = 0, 1, 2$ ·

A codeword $((2^{nR_a}, 2^{nR_b}, 2^{nR_c}), n)$ of discrete memoryless broadcast channel with eavesdropper is composed by following elements:

An encoder:

$f : (\{1, 2, \ldots, 2^{nR_a}\} \times \{1, 2, \ldots, 2^{nR_b}\} \times \{1, 2, \ldots, 2^{nR_c}\}) \rightarrow \chi^n$

Two decoders:

$g_1 : y_1^n \rightarrow \{1, 2, \ldots, 2^{nR_a}\} \times \{1, 2, \ldots, 2^{nR_b}\}$

$g_2 : y_2^n \rightarrow \{1, 2, \ldots, 2^{nR_a}\} \times \{1, 2, \ldots, 2^{nR_c}\}$

The average error probability is defined as:

$$\tilde{P}_e^n \; \square \; P(g_1(Y_1^n) \neq (M_0, M_1) \cup g_2(Y_2^n) \neq (M_0, M_2))$$

It should be noted that Wyner introduced the concept of perfect secrecy in [2]. It is that the eavesdropper can't receive any confidential messages which have been transmitted. Therefore, the perfect secrecy means:

$$\begin{aligned} I(Z^n, M_1) = 0 &\Leftrightarrow H(M_1) = H(M_1 \mid Z^n) \\ I(Z^n, M_2) = 0 &\Leftrightarrow H(M_2) = H(M_2 \mid Z^n) \\ I(Z^n, (M_1 M_2)) = 0 &\Leftrightarrow H(M_1, M_2) = H(M_1, M_2 \mid Z^n) \\ n \rightarrow \infty & \end{aligned}$$

3. The Outer Bound of BCE

We will propose the outer bound of achievable secrecy rate region of BCE in this section. It is as following,

Theorem 1:

Let $\Re_a$ represent the region constituted by all of non-negative rate triples (R_a, R_b, R_c) which satisfy the following conditions,

$$\begin{gathered}
R_a \leq \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
R_a + R_b \leq I(U_1;Y_1|V) - I(U_1;Z|V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
R_a + R_c \leq I(U_2;Y_2|V) - I(U_2;Z|V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
R_a + R_b + R_c \leq I(U_1;Y_1|VU_2) + I(U_2;Y_2|V) - I(U_1,U_2;Z|V) \\
-I(U_1;U_2|V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
R_a + R_b + R_c \leq I(U_2;Y_2|VU_1) + I(U_1;Y_1|V) - I(U_1,U_2;Z|V) \\
-I(U_1;U_2|V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z)
\end{gathered} \tag{1}$$

In (1), V, U_1, U_2 are auxiliary random variable, random variable group $(V, U_1, U_2, X, Y_1, Y_2, Z)$ obey,

$$p(v,u_1,u_2,x,y_1,y_2,z) = p(v)p(u_1,u_2|v)p(x|u_1,u_2)p(y_1,y_2,z|x)$$

That is $(V, U_1, U_2, X, Y_1, Y_2, Z)$ which satisfies the Markov condition $V \to U_1U_2 \to X \to Y_1Y_2Z$.

From theorem 1, we can know that $\Re_a$ is the outer bound on the secrecy achievable rate regions of BCE.

Definition 1:

Define the following equation,

$$\begin{aligned}
X^i &\square (X_1, X_2, \ldots, X_i); \\
\tilde{X}^i &\square (X_{i+1}, X_{i+2}, \ldots, X_n); \\
\Sigma_1 &\square \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1}; Y_{1i} | M_0 Y_1^{i-1} Z_i); \\
\Sigma_1^* &\square \sum_{i=1}^{n} I(Y_1^{i-1}; Y_{2i} | M_0 \tilde{Y}_2^{i+1} Z_i);
\end{aligned}$$

(2)

The lengths of all vectors are assumed to be n in (2). Similar to the above defined type, we use M_0M_1, M_0M_2 and $M_0M_1M_2$ replace M_0 in (Σ_1, Σ_1^*) respectively, then we can get a corresponding expression of $(\Sigma_2, \Sigma_2^*), (\Sigma_3, \Sigma_3^*)$ and (Σ_4, Σ_4^*) .

Lemma 1:

For any $i = 1, 2, 3, 4$, there is Σ_i, Σ_i^*.

Please refer to Appendix for the proof.

4. The Significance of Outer Bound on BCE

We know that the obtained outer bound may be different by using different methods. Therefore, the given mode of outer bound is also a variety of way. As a result of giving an outer bound, we must determine whether it makes sense. While the minimum standards of measuring whether the outer bound meaningful is that it at least be included in (tight in) the cut-set bound which is obtained by using max-flow min-cut theorem. The following theorem guarantees the outer bound (given by Theorem 1) meaningful.

Theorem 2:

The outer bound which is given by Theorem 1 tight in the cut-set bound which is given by max-flow min-cut theorem.

According to max-flow min-cut theorem we can obtain its corresponding outer bounder for the joint distribution of $p(x)p(y_1, y_2, z|x)$ as follow,

$$\begin{aligned} R_a + R_b &\le I(X;Y_1) - I(X;Z) \\ R_a + R_c &\le I(X;Y_2) - I(X;Z) \\ R_a + R_b + R_c &\le I(X;Y_1Y_2) - I(X;Z) \end{aligned}$$

(3)

Please refer to Appendix for the proof.

5. Consequence Analysis

Currently, the representative outer bound of discrete memoryless broadcast channel is proposed in the literature [8], [9] and [10] respectively. These conclusions have summarized the outer bound which has been proposed earlier in [3] and [7]. From the following remarks we can get that the outer bound in theorem 1 include (tight) in the existing outer bound of BCE in the case of not considering the eavesdropper.

Remark 1:

If removed the eavesdropper in the model of literature [8], according to the characteristic of mutual information, we can easily prove that the outer bound in theorem 1 include (tight) in the outer bound of BCE which has proposed in [8].

Remark 2:

It has been proved that the outer bound in [9] is strictly tight in the outer bound which has been proposed earlier in [3] and [7]. If removed the eavesdropper in the model of literature [9], we can get that the outer bound in theorem 1 include (tight) in the outer bound of BCE which has proposed in [9] just by simple proof.

Remark 3:

It has been proved that the outer bound in [10] is strictly tight in the outer bound which has been proposed earlier in [3] and [7]. If removed the eavesdropper in the model of literature [10], the outer bound in theorem 1is consistent with the results given by [10].

6. Conclusions

This paper focuses on the communication system of broadcast channel with an eavesdropper, and then according to the definitions of achievable secrecy rate and equivocation rate, we proposed and proved an outer bound on achievable secrecy rate region of BCE by using information entropy theory and we compared it with previous results to determine its meaning.

Since we proved the outer bound of BCE in theory, so the experimental procedure does not exist, Section 5 gives a comparison with other outer bounds, which illustrates the validity of our results.

In the future work, we will study the outer bounds on different communication models.

7. Appendix

7.1. Proof of Lemma 1

Similar to the proof of lemma 7 in [3], we get,

$$\begin{aligned} \Sigma_1 &= \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1};Y_{1i} \mid M_0Y_1^{i-1}Z_i) = \sum_{i=1}^{n}\sum_{j=i+1}^{n} I(Y_{2j};Y_{1i} \mid M_0Y_1^{i-1}\tilde{Y}_2^{j+1}Z_i) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{i-1} I(Y_{1j};Y_{2i} \mid M_0Y_1^{j-1}\tilde{Y}_2^{i+1}Z_i) = \sum_{i=1}^{n} I(Y_1^{i-1};Y_{2i} \mid M_0\tilde{Y}_2^{i+1}Z_i) = \Sigma_1^* \end{aligned}$$

(4)

Using the same method we can get,

$$\Sigma_i = \Sigma_i^*, i = 2,3,4.$$

According to Fano inequality, we can obtain,

$$\begin{aligned} &H(M_0, M_1 \mid Y_1^n) \le n\varepsilon_n / 2, \\ &H(M_0, M_2 \mid Y_2^n) \le n\varepsilon_n / 2. \end{aligned} \tag{5}$$

7.2. Proof of Theorem 1

1) We analyze R_a firstly, as the security condition $R_{ea} \ge R_a - \varepsilon_n / 2,$ so that,

$$\begin{aligned} nR_a &\le nR_{ea} + n\varepsilon_n / 2 = H(M_0 \mid Z^n) + n\varepsilon_n / 2 \\ &= I(M_0; Y_1^n \mid Z^n) + H(M_0 \mid Y_1^n Z^n) + n\varepsilon_n / 2 \\ &\overset{(a)}{\le} \sum_{i=1}^{n} I(M_0; Y_{1i} \mid Y_1^{i-1} Z_i) + n\varepsilon_n \\ &= \sum_{i=1}^{n} [I(M_0 Y_1^{i-1}; Y_{1i} \mid Z_i) - I(Y_1^{i-1}; Y_{1i} \mid Z_i)] + n\varepsilon_n \\ &\overset{(b)}{\le} \sum_{i=1}^{n} [I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i} \mid Z_i) - I(\tilde{Y}_2^{i+1}; Y_{1i} \mid M_0 Y_1^{i-1} Z_i)] + n\varepsilon_n \\ &= \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i} \mid Z_i) - \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1}; Y_{1i} \mid M_0 Y_1^{i-1} Z_i) + n\varepsilon_n \\ &\overset{(c)}{=} \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i} \mid Z_i) - \Sigma_1 + n\varepsilon_n \\ &\overset{(d)}{\le} \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i} \mid Z_i) + n\varepsilon_n \\ &= \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}) - \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i) + \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{1i}) + n\varepsilon_n \end{aligned} \tag{6}$$

In (6), (a) holds because the chain rule $I(M_0; Y_1^n \mid Z^n) = \sum_{i=1}^{n} I(M_0; Y_{1i} \mid Y_1^{i-1} Z_i)$ and Fano inequality $H(M_0 \mid Y_1^n Z^n) \le n\varepsilon_n / 2$; (b) holds because it enlarge the inequality by removing $-\sum_{i=1}^{n} I(Y_1^{i-1}; Y_{1i} \mid Z_i)$; (c) holds because the definition $\Sigma_1 \square \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1}; Y_{1i} \mid M_0 Y_1^{i-1} Z_i)$; (d) holds because it enlarge the inequality by removing $-\Sigma_1$. In the same way we can get,

$$\begin{aligned} nR_a \le& \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i}) - \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i) \\ &+ \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{2i}) + n\varepsilon_n \end{aligned} \tag{7}$$

$$\begin{aligned} nR_a \le & \min\{\sum_{i=1}^{n} I(M_0 Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1}\tilde{Y}_2^{i+1};Y_{2i})\} \\ & -\sum_{i=1}^{n} I(M_0 Y_1^{i-1}\tilde{Y}_2^{i+1};Z_i) \\ & +\min\{\sum_{i=1}^{n} I(M_0 Y_1^{i-1}\tilde{Y}_2^{i+1};Z_i \mid Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1}\tilde{Y}_2^{i+1};Z_i \mid Y_{2i})\} \\ & +n\varepsilon_n \end{aligned} \tag{8}$$

2) Analysis $R_a + R_b$, due to the security conditions $R_{eba} \ge R_a + R_b - \varepsilon_n / 2$, so that,

$$\begin{aligned} n(R_a + R_b) \le nR_{eba} + n\varepsilon_n/2 &= H(M_0, M_1 \mid Z^n) + n\varepsilon_n/2 \\ &= H(M_0 \mid Z^n) + H(M_1 \mid M_0 Z^n) + n\varepsilon_n/2 \\ &= H(M_0 \mid Z^n) + I(M_1;Y_1^n \mid M_0 Z^n) + H(M_1 \mid M_0 Y_1^n Z^n) \\ & \quad + n\varepsilon_n/2 \\ & \overset{(a)}{\le} \underbrace{H(M_0 \mid Z^n)}_{(i)} + \underbrace{I(M_1;Y_1^n \mid M_0 Z^n)}_{(j)} + n\varepsilon_n \end{aligned} \tag{9}$$

In (9), (a) holds because Fano inequality, it has $H(M_1 \mid M_0 Y_1^n Z^n) \le n\varepsilon_n/2$.

To the right side in (8), the calculation of (i) item can be obtained in the proof from 1), then we calculate (j) term as following,

$$\begin{aligned} I(M_1;Y_1^n \mid M_0 Z^n) &\overset{(a)}{=} \sum_{i=1}^{n} I(M_1;Y_{1i} \mid M_0 Y_1^{i-1} Z_i) \\ &= \sum_{i=1}^{n} [I(M_1\tilde{Y}_2^{i+1};Y_{1i} \mid M_0 Y_1^{i-1} Z_i) - I(\tilde{Y}_2^{i+1};Y_{1i} \mid M_0 M_1 Y_1^{i-1} Z_i)] \\ &= \sum_{i=1}^{n} I(M_1;Y_{1i} \mid M_0 Y_1^{i-1}\tilde{Y}_2^{i+1} Z_i) - \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1};Y_{1i} \mid M_0 M_1 Y_1^{i-1} Z_i) \\ & \quad +\sum_{i=1}^{n} I(\tilde{Y}_2^{i+1};Y_{1i} \mid M_0 Y_1^{i-1} Z_i) \\ &\overset{(b)}{=} \sum_{i=1}^{n} I(M_1;Y_{1i} \mid M_0 Y_1^{i-1}\tilde{Y}_2^{i+1} Z_i) + \Sigma_1 - \Sigma_2 \\ &= \sum_{i=1}^{n} I(M_1;Y_{1i} \mid M_0 Y_1^{i-1}\tilde{Y}_2^{i+1}) - \sum_{i=1}^{n} I(M_1;Z_i \mid M_0 Y_1^{i-1}\tilde{Y}_2^{i+1}) \\ & \quad +\sum_{i=1}^{n} I(M_1;Z_i \mid M_0 Y_1^{i-1}\tilde{Y}_2^{i+1}) + \Sigma_1 - \Sigma_2 \end{aligned} \tag{10}$$

In (10), (a) holds because the chain rule; (b) holds because the definition $\Sigma_1 \triangleq \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1};Y_{1i} \mid M_0 Y_1^{i-1} Z_i), \Sigma_2 \triangleq \sum_{i=1}^{n} I(\tilde{Y}_2^{i+1};Y_{1i} \mid M_0 M_1 Y_1^{i-1} Z_i)$. Combine (i) and (j) terms in (9), and put the result into (10), we can get,

$$\begin{aligned} n(R_a + R_b) \le \min\{ & \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i})\} \\ & - \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i) \\ & + \min\{\sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{2i})\} \\ & + \sum_{i=1}^{n} I(M_1; Y_{1i} \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) - \sum_{i=1}^{n} I(M_1; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) \\ & + \sum_{i=1}^{n} I(M_1; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) + n\varepsilon_n \end{aligned} \tag{11}$$

Similarly, we can obtain,

$$\begin{aligned} n(R_a + R_c) \le \min\{ & \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i})\} \\ & - \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i) \\ & + \min\{\sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{2i})\} \\ & + \sum_{i=1}^{n} I(M_2; Y_{2i} \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) - \sum_{i=1}^{n} I(M_2; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) \\ & + \sum_{i=1}^{n} I(M_2; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) + n\varepsilon_n \end{aligned} \tag{12}$$

3) $R_a + R_b + R_c$ situation, the derivation is similar to 2), so the details are omitted here, we can obtain,

$$\begin{aligned} n(R_a + R_b + R_c) \le \min\{ & \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i})\} \\ & - \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i) \\ & + \min\{\sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{2i})\} \\ & + \sum_{i=1}^{n} I(M_1; Y_{1i} \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) - \sum_{i=1}^{n} I(M_1; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) \\ & + \sum_{i=1}^{n} I(M_1; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) + \sum_{i=1}^{n} I(M_2; Y_{2i} \mid M_0 M_1 Y_1^{i-1} \tilde{Y}_2^{i+1}) \\ & - \sum_{i=1}^{n} I(M_2; Z_i \mid M_0 M_1 Y_1^{i-1} \tilde{Y}_2^{i+1}) + \sum_{i=1}^{n} I(M_2; Z_i \mid M_0 M_1 Y_1^{i-1} \tilde{Y}_2^{i+1}) + n\varepsilon_n \end{aligned} \tag{13}$$

and

$$\begin{aligned} n(R_a + R_b + R_c) \le \min\{ & \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Y_{2i})\} \\ & - \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i) \\ & + \min\{\sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{1i}), \sum_{i=1}^{n} I(M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}; Z_i \mid Y_{2i})\} \\ & + \sum_{i=1}^{n} I(M_2; Y_{2i} \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) - \sum_{i=1}^{n} I(M_2; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) \\ & + \sum_{i=1}^{n} I(M_2; Z_i \mid M_0 Y_1^{i-1} \tilde{Y}_2^{i+1}) + \sum_{i=1}^{n} I(M_1; Y_{1i} \mid M_0 M_2 Y_1^{i-1} \tilde{Y}_2^{i+1}) \\ & - \sum_{i=1}^{n} I(M_1; Z_i \mid M_0 M_2 Y_1^{i-1} \tilde{Y}_2^{i+1}) + \sum_{i=1}^{n} I(M_1; Z_i \mid M_0 M_2 Y_1^{i-1} \tilde{Y}_2^{i+1}) + n\varepsilon_n \end{aligned} \tag{14}$$

We introduce random variable K , K independent from $M_0 M_1 M_2 X^n Y_1^n Y_2^n Z^n$, and subject to the uniform distribution of $\{1, 2, \ldots, n\}$. Let,

$$\begin{gathered} V \square M_0 Y_1^{K-1} \tilde{Y}_2^{K+1} K, U_1 \square M_1 V, U_2 \square M_2 V, \\ X \square X_K, Y_1 \square Y_{1K}, Y_1 \square Y_{2K}, Z \square Z_K, \end{gathered} \tag{15}$$

Obviously, the above-defined variables satisfy the Markov conditions,

$$V \to U_1 U_2 \to X \to Y_1 Y_2 Z$$

Put (15) into (8), (11), (12), (13) and (14), we can get the result (1) which have been given in Theorem 1. This completes the proof.

7.3. Proof of Theorem 2

First we consider,

$$\begin{aligned} R_a + R_b & \le I(U_1; Y_1 \mid V) - I(U_1; Z \mid V) \\ & \quad + \min\{I(V; Y_1), I(V; Y_2)\} - I(V; Z) \\ & \le I(U_1; Y_1 \mid V) - I(U_1; Z \mid V) \\ & \quad + I(V; Y_1) - I(V; Z) \\ & \le I(VU_1; Y_1) - I(VU_1; Z) \end{aligned} \tag{16}$$

Note that,

$$\begin{aligned} I(VU_1X; Y_1) &= I(VU_1; Y_1) + I(X; Y_1 \mid VU_1), \\ I(VU_1X; Z) &= I(VU_1; Z) + I(X; Z \mid VU_1), \end{aligned} \tag{17}$$

Thus we substitute (17) into formula (16),

$$\begin{aligned} R_a + R_b & \le I(VU_1; Y_1) - I(VU_1; Z) \\ & = I(VU_1X; Y_1) - I(VU_1X; Z) - I(X; Y_1 \mid VU_1) + I(X; Z \mid VU_1) \\ & = I(X; Y_1) - I(X; Z) - I(X; Y_1 \mid VU_1) + I(X; Z \mid VU_1) \\ & \overset{(a)}{\le} I(X; Y_1) - I(X; Z) \end{aligned} \tag{18}$$

In (18), (a) holds because according to the security conditions, there is,

$$I(X;Y_1|VU_1) \geq I(X;Z|VU_1)$$

The same way, we have,

$$R_a + R_c \leq I(X;Y_2) - I(X;Z) \tag{19}$$

Finally, we prove,

$$\begin{aligned} R_a + R_b + R_c &\leq I(U_2;Y_2|VU_1) + I(U_1;Y_1|V) - I(U_1,U_2;Z|V) - I(U_1;U_2|V) \\ &\quad + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\ &\leq I(U_2;Y_2|VU_1) + I(U_1;Y_1|V) - I(U_1,U_2;Z|V) - I(U_1;U_2|V) \\ &\quad - I(V;Z) + I(V;Y_1) \\ &= I(U_2;Y_2|VU_1) + I(VU_1;Y_1) - I\ VU_1U_2\ Z\ V\ - I\ U_1\ U_2\ V \\ &\leq I(U_2;Y_1Y_2|VU_1) + I(VU_1;Y_1Y_2) - I\ VU(_1U_2\ Z;V| -)I\ U_1(U_2;\ V| \\ &\leq I(VU_1U_2;Y_1Y_2) - I\ VU_1U_2\ Z\ V\ - I\ U_1\ U_2\ V \end{aligned} \tag{20}$$

Note that,

$$\begin{aligned} I(VU_1U_2X;Y_1Y_2) &= I(VU_1U_2;Y_1Y_2) + I(X;Y_1Y_2|VU_1U_2), \\ I(VU_1U_2X;Z) &= I(VU_1U_2;Z) + I(X;Z|VU_1U_2), \end{aligned} \tag{21}$$

Thus we substitute (21) into formula (20),

$$\begin{aligned} R_a + R_b + R_c &\leq I(VU_1U_2;Y_1Y_2) - I\ VU_1U_2\ Z\ V\ - I\ U_1\ U_2\ V \\ &= I(X;Z|VU_1U_2) - I(X;Y_1Y_2|VU_1U_2) - I(U_1;U_2|V) \\ &\quad - I(VU_1U_2X;Z) + I(VU_1U_2X;Y_1Y_2) \\ &= I(X;Z|VU_1U_2) - I(X;Y_1Y_2|VU_1U_2) - I(U_1;U_2|V) \\ &\quad + I(X;Y_1Y_2) - I(X;Z) \\ &\leq I(X;Y_1Y_2) - I(X;Z) - I(U_1;U_2|V) \\ &\leq I(X;Y_1Y_2) - I(X;Z) \end{aligned} \tag{22}$$

In (22), the last two inequalities hold because base on the perfect security, there is $I(X;Y_1Y_2|VU_1U_2) \geq I(X;Z|VU_1U_2)$, and during the proof procedure we repeatedly used the Markov properties $V \to U_1U_2 \to X \to Y_1Y_2Z$ of random variable group $(V, U_1, U_2, X, Y_1, Y_2, Z)$.

So far, this completes the proof that the outer bound in theorem 1 include (tight) in the cut-set bound which is obtained by using max-flow min-cut theorem.

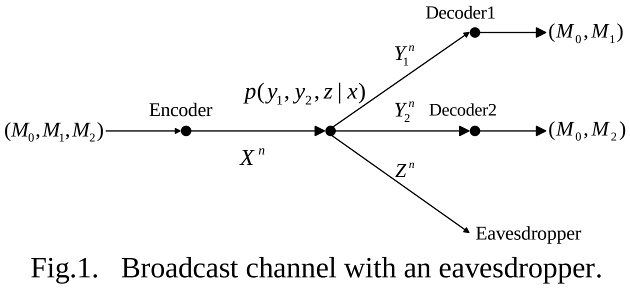

Fig.1. Broadcast channel with an eavesdropper.

Acknowledgements

Yan Zhu and Xiao Chen contributed equally to this work and share first authorship. Thank Liang Pang and Xinxing Yin for their helpful discussion and contribution on this paper. This work was supported in part by the Natural Science Foundation of China under Grant No. 60932003, No. 61271220 and No. 61171173.

References

[1] C. E.Shannon, “Communication theory of secrecy systems,” Bell Systems Technical Journal, vol. 28, (**1948**), pp. 656–715.

[2] A. D. Wyner, “The Wire-tap Channel,” Bell Systems Technical Journal, vol. 54, (**1975**), pp. 1355–1367.

[3] I. Csiszar and J. Korner, “Broadcast Channels with Confidential Messages,” IEEE Trans. Info. Theory, May (**1978),** pp. 339-348,

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian Wire-tap Channel,” IEEE Trans. Inf. Theory, vol. 24, (**1978**), pp. 351-456.

[5] G. Bagherikaram, A. S. Motahari and A. K. Khandani, “The Secrecy Rate Region of Broadcast Channel” eprint arXiv, 0806, 4200, (**2008**).

[6] G. Bagherikaram, A. S. Motahari and A. K. Khandani, “The Secrecy Rate Region of Broadcast Channel” available at http://arxiv.org/PS_cache/arxiv/pdf/0910/0910.3658vl.pdf.

[7] K. Marton, “A coding theorem for the discrete memory-less broadcast channel”, IEEE Trans. Inf. Theory, vol. 25, (**1979**), pp. 306-311.

[8] Y. Liang and G. Kramer, “Capacity theorems for cooperative relay broadcast channels”, Information Sciences and Systems, 2006 40th Annual Conference on IEEE, (**2006**), pp. 1719-1724.

[9] C. Nair and A. El Gamal, “An Outer Bound to the Capacity Region of the Broadcast Channel”, Information Theory, IEEE Transactions on, vol. 53, no. 1, (**2007**), pp. 350-355.

[10] J. Xu, Y. Cao and B. Chen “Capacity bounds for broadcast channels with confidential messages”, Information Theory, IEEE Transactions on, vol. 55, no. 10, (**2009**), pp. 4529-4542.

[11] Y. Zhu, “Artificial Noise Generated in MIMO Scenario: Optimal Power Design”, IEEE Signal Processing Letters, vol. 20, October (**2013**), pp. 964-967.

[12] Y. Zhu, “Research on the Multiple-inputs Single-output Channel Under Attack,” ICCIS, Aug 17-19, China, (**2012**), pp. 973-976.

[13] X. Chen, Y. Zhu, Z. Xue, F. B. Li and J. Gu, “Security in Single-Input Single-Output Multiple-helpers Wireless Channel,” ICCIS, August 17-19, China, (**2012**), pp. 969-972.

[14] Y. Zhu, “Research on Secrecy Communication via Bilateral Artifical Noise Transmitting” ICCIS , June 21-23, China, (**2013**), pp. 218-220,

[15] Y. Liang and H. V. Poor, “Secure communication over fading channels,” IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2470-2492, June (**2008**).

[16] A. E. Hero, “Secure Space-Time Communication,” IEEE Trans. Info. Theory, December (**2003**), pp. 3235-3249.

[17] X. Chen, “Research on the Security of MISO Wireless Channel with Artificial Noise” ICCIS , June 21-23, China, (**2013).**

Authors

Yan Zhu, he is a Ph.D. student in the Electronic, Information and Electrical Engineering School at Shanghai Jiaotong University. His research interests include information theory, coding for communications systems, physical layer security and wireless communication security.

Xiao Chen, he is a Ph.D. student in the Electronic, Information and Electrical Engineering School at Shanghai Jiaotong University. His research interests include information theory, coding for communications systems, physical layer security and wireless communication security.

Yongkai Zhou, he is a Ph.D. student in the Electronic, Information and Electrical Engineering School at Shanghai Jiaotong University. His research interests include information theory, coding for communications systems, physical layer security and wireless communication security.

Fangbiao Li, he is a Ph.D. student in the Electronic, Information and Electrical Engineering School at Shanghai Jiaotong University. His research interests include information theory, coding for communications systems, physical layer security and wireless communication security.

Zhi Xue, he received the B.Tech. Degree from Shanghai Jiaotong University. He went to the United States for cooperation in scientific research at Bell Labs as a visiting scholar in 1997. Then he received Ph.D. degree from Shanghai Jiaotong University where he is a Professor and Doctoral Tutor. Currently, he is the vice president of Information Security Engineering School in Shanghai Jiaotong University. His research interests include information theory, coding for communications systems, physical layer security and wireless communication security.