Research on the Secrecy Achievable Rate Region for the Broadcast channel with eavesdropper

Yan Zhu ,Xiao Chen, Yongkai Zhou, Fangbiao Li, Liang Pang, Xinxing Yin, Zhi Xue,
School of Electronic, Information and Electrical Engineering, Shanghai Jiaotong University, Shanghai, China
E-mail: { topbestzy1983, chenxiao, ssmailzyk, flyin2009, cyclone0000, yinxinxing, zxue, } @sjtu.edu.cn

***Abstract*—This paper considers the problems of the achievable rate regions on broadcast channel with the eavesdropper. Many articles have given the meaningful results, like the inner bound of this model. However, the specific analysis processes for this model have not been given by previous work. So we focus on the study of the secrecy achievable rate regions on broadcast channel with eavesdropper and get a detailed analysis of the inner bounder.**

Keywords-Broadcast channel; eavesdropper; inner bounder; secrecy achievable rate region.

I. 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].

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 analyzing the achievable security rate region which has been obtained in the following part of this paper.

The remaining paper is organized as follows. System model will be described in section II. Section III and IV will then focus on the analysis of achievable security rate region (inner bound), and the conclusion will be given in section V.

II. SYSTEM MODEL

The system model of BCE is shown as follow. 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 $\omega_0 = \{1, 2, ...W_0\}$ is a public message set, $\omega_1 = \{1, 2, ...W_1\}$ and $\omega_2 = \{1, 2, ...W_2\}$ 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 $((2^{nR_0}, 2^{nR_1}, 2^{nR_2}), n)$ of discrete memoryless broadcast channel with eavesdropper is composed by following elements:

An encoder:

$$f : (\{1, 2, ..., 2^{nR_0}\} \times \{1, 2, ..., 2^{nR_1}\} \times \{1, 2, ..., 2^{nR_2}\}) \to \chi^n$$

Two decoders:

$$g_1 : y_1^n \to \{1, 2, ..., 2^{nR_0}\} \times \{1, 2, ..., 2^{nR_1}\}$$

$$g_2 : y_2^n \to \{1, 2, ..., 2^{nR_0}\} \times \{1, 2, ..., 2^{nR_2}\}$$

The average error probability is defined as:

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

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:

$$I(Z^n, M_1) = 0 \Leftrightarrow H(M_1) = H(M_1 \mid Z^n)$$
$$I(Z^n, M_2) = 0 \Leftrightarrow H(M_2) = H(M_2 \mid Z^n)$$
$$I(Z^n, (M_1 M_2)) = 0 \Leftrightarrow H(M_1, M_2) = H(M_1, M_2 \mid Z^n)$$
$$n \to \infty$$

III. THE INNER BOUND OF BCE

We will analyze achievable secrecy rate region of BCE in this section. The related coding scheme in the process of proof the inner bound of BCE is based on the combination of random differentiate, superimposed code, rate divided and Gelfand-Pinsker divided.

Theorem 1:

Let $\Re_K$ represent the region constituted by all of non-negative rate triples (R_0, R_1, R_2) which satisfy the following conditions,

$$\begin{aligned}
&R_0 \le \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
&R_0 + R_1 \le I(U_1;Y_1 \mid V) - I(U_1;Z \mid V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
&R_0 + R_2 \le I(U_2;Y_2 \mid V) - I(U_2;Z \mid V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z) \\
&R_0 + R_1 + R_2 \le I(U_1;Y_1 \mid V) + I(U_2;Y_2 \mid V) - I(U_1,U_2;Z \mid V) \\
&\quad - I(U_1;U_2 \mid V) + \min\{I(V;Y_1), I(V;Y_2)\} - I(V;Z)
\end{aligned} \tag{1}$$

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,

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

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

From theorem 1, we can know that arbitrary rate triples $(R_0, R_1, R_2) \in \Re_K$ are achievable for BCE.

IV. ANALYSIS AND PROOF OF THEOREM 1

Divide the confidential messages M_1 and M_2 into two parts:

Divide $M_1 \in \{1, 2, ..., 2^{nR_1}\}$ into $M_{11} \in \{1, 2, ..., 2^{nR_{11}}\}$ and $M_{10} \in \{1, 2, ..., 2^{nR_{10}}\}$

Divide $M_2 \in \{1, 2, ..., 2^{nR_2}\}$ into $M_{22} \in \{1, 2, ..., 2^{nR_{22}}\}$ and $M_{20} \in \{1, 2, ..., 2^{nR_{20}}\}$, M_{11} and M_{22} can only be decoded by the corresponding destination receiver, while M_{10} and M_{20} can be decoded by both the destination receivers. We use auxiliary random variable V represent (W_{10}, W_{20}, W_0), while auxiliary random variable U_1 and U_2 represent the message M_{11} and M_{22} respectively. We can know that,

$$R_{11} + R_{10} = R_1$$
$$R_{22} + R_{20} = R_2$$

A. Auxiliary codebook generation

The structure of the encoder is shown in Fig 2. Fix $p(v)$, $p(u_1 \mid v)$, $p(u_2 \mid v)$ and $p(x \mid u_1 u_2)$.

$\forall \varepsilon > 0$, define that,

$$\begin{aligned}
Q_{11} &= I(U_1;Y_1 \mid V) - I(U_1;Z, U_2 \mid V), \\
Q_{12} &= I(U_1;Z \mid V, U_2), \\
Q_{21} &= I(U_2;Z \mid V, U_1), \\
Q_{22} &= I(U_2;Y_2 \mid V) - I(U_2;Z, U_1 \mid V), \\
Q_3 &= I(U_1;U_2 \mid V) - \varepsilon.
\end{aligned} \tag{2}$$

From (2), we can get,

$$\begin{aligned}
Q_{11} + Q_{12} + Q_3 &= I(U_1;Y_1 \mid V) - \varepsilon, \\
Q_{21} + Q_{22} + Q_3 &= I(U_2;Y_2 \mid V) - \varepsilon.
\end{aligned} \tag{3}$$

First, generate $2^{n(R_0 + R_{10} + R_{20})}$ independent and identically distributed (i.i.d) codeword sequence $v^n(k), k \in \{1, 2, ..., 2^{n(R_0 + R_{10} + R_{20})}\}$ according to the distribution $p(v^n) = \prod_{i=1}^{n} p(v_i)$. For each codeword $v^n(k)$, generate $2^{n(Q_{11} + Q_{12} + Q_3)}$ independent and identically distributed (i.i.d) codeword sequence $u_1^n(i, i', i'')$ according to the distribution $p(u_1^n \mid v^n) = \prod_{i=1}^{n} p(u_{1i} \mid v_i)$, $i \in \{1, 2, ..., 2^{nQ_{11}}\}$, $i' \in \{1, 2, ..., 2^{nQ_{12}}\}$ and $i'' \in \{1, 2, ..., 2^{nQ3}\}$.

Now, we explain the subscript that is involved in the above. First, let the codeword vector u_1^n divide into $2^{nQ_{11}}$ bins randomly, mark this bin as subscript i. Then, let each bin be divided into $2^{nQ_{12}}$ sub bins, mark this sub bin as subscript i'. Finally, mark the codeword which corresponding to each sub bin as subscript i''. The purpose of doing this is to facilitate the selection of codeword during the process of encoding. Analogously, for each codeword $v^n(k)$ generate $2^{n(Q_{21} + Q_{22} + Q_3)}$ i.i.d codeword sequence $u_2^n(j, j', j'')$ according to the distribution $p(u_2^n \mid v^n) = \prod_{i=1}^{n} p(u_{2i} \mid v_i)$, $j \in \{1, 2, ..., 2^{nQ_{21}}\}$, $j' \in \{1, 2, ..., 2^{nQ_{22}}\}$ and $j'' \in \{1, 2, ..., 2^{nQ_3}\}$.

B. Encode

In order to send the message (M_{10}, M_{20}, M_0), we first need to know the subscript k of the message, then, select codeword $v^n(k)$ which is corresponding to it. After the codeword $v^n(k)$ had been selected, we have $2^{n(Q_{11}+Q_{12}+Q_3)}$ codeword $u_1^n(i,i',i'')$ can be chosen to represent M_{11}. In order to determine the codeword, we will map $2^{nR_{11}}$ message M_{11} into $2^{nQ_{11}}$ division units (bins). Give $R_{11} \geq Q_{11} \geq 0$, so that each division unit at least corresponding to one message M_{11}. Therefore, the subscript i of division unit is determined, if the message M_{11} is given.

Discussion of following two cases:

- If $R_{11} \leq Q_{11} + Q_{12}$, then each division unit (bin) will correspond to $2^{n(R_{11}-Q_{11})}$ numbers of message M_{11}. We randomly divide $2^{nQ_{12}}$ numbers of sub bins into $2^{n(R_{11}-Q_{11})}$ numbers of cells. Thus, when message M_{11} has been given, we can find the corresponding cell, and select a sub bin from the cell randomly, after that, the subscript i' of sub bin is determined, and then we can randomly select a codeword $u_1^n(i,i',i'')$ from the sub bin to represent the corresponding message M_{11}.
- If $Q_{11} + Q_{12} \leq R_{11} \leq Q_{11} + Q_{12} + Q_3$, then each division unit (bin) will at least correspond to one message M_{11}. Thus, when message M_{11} has been given, each subscript i' of sub bin is determined. There are $2^{n(R_{11}-Q_{11}-Q_{12})}$ numbers of message M_{11} in each sub bin. Thus, we randomly divide 2^{nQ_3} numbers of codeword into $2^{n(R_{11}-Q_{11}-Q_{12})}$ numbers of cells. So that, we can find the corresponding cell when message M_{11} has been given, and then, we can randomly select a codeword $u_1^n(i,i',i'')$ to represent the corresponding message M_{11}.

When message M_{22} has been given, the selection method of codeword $u_2^n(j,j',j'')$ is totally similar to codeword $u_1^n(i,i',i'')$, so description will not be repeated here.

The encoder selects codeword pair $(u_1^n(i,i',i''), u_2^n(j,j',j''))$ according to the rules of jointly typical, that is,

$$(u_1^n(i,i',i''), u_2^n(j,j',j''), v^n(k)) \in A_\varepsilon^n(U_1,U_2,V) \quad (4)$$

In (4), $A_\varepsilon^n(U_1,U_2,V)$ represents the jointly typical set constitute by sequence u_1^n, u_2^n, v^n.

If the above codeword pairs exist, but not unique, then we will randomly select one pair from them; if the above codeword does not exist, then we will declare an error.

After getting codeword $u_1^n(i,i',i'')$ and $u_2^n(j,j',j'')$, we can obtain channel input x^n according to the distribution $p(x^n \mid u_1^n, u_2^n) = \prod_{i=1}^{n} p(x_i \mid u_{1i}, u_{2i})$.

C. Decode

The signals which are received by the legitimate receivers Y_1 and Y_2 is obtained according to the channel output distribution $p(y_1^n \mid x^n) = \prod_{i=1}^{n} p(y_{1i} \mid x_i)$ and $p(y_2^n \mid x^n) = \prod_{i=1}^{n} p(y_{2i} \mid x_i)$.

For the first legitimate receiver, we should find the sequence $v^n(k)$ which satisfies the condition of jointly typical sequence $(y_1^n, v^n(k)) \in A_\varepsilon^n(Y_1,V)$. When such a $v^n(k)$ exists and is unique, let $\hat{k} = k$; otherwise, declare an error. After Y_1 decodes k, and then codeword $u_1^n(i,i',i'')$ will be decoded, the specific process is as follows,

- Receiver Y_1 looks for the codeword sequence $u_1^n(i,i',i'')$ which satisfies the condition of jointly typical $(u_1^n(i,i',i''), y_1^n, v^n(k)) \in A_\varepsilon^n(U_1,Y_1,V)$. If such a $u_1^n(i,i',i'')$ exists and is unique, let $\hat{i} = i, \hat{i}' = i', \hat{i}'' = i''$; otherwise, declare an error.
- Using $\hat{k}$, $\hat{i}$, $\hat{i}'$ and $\hat{i}''$, Y_1 can decode the corresponding message $(\tilde{M}_0, \tilde{M}_{10}, \tilde{M}_{11})$.
- The decoding process of decoder Y_2 is totally similar to decoder Y_1.

D. Error probability analysis

The error probability analysis of theorem 1 here is similar to the error probability analysis process in Marton's classic paper[7], so the discussion will not be repeated here.

E. Equivocation Calculate

In order to satisfy the channel secrecy requirements, we just ensure the security of public message M_0, joint message $(M_0, M_1), (M_0, M_2)$ and (M_0, M_1, M_2)

First, analyze the security constraints of public message M_0, we have,

$$\begin{aligned}
R_{e0} &= H(M_0 \mid Z^n)/n \\
&= (H(M_0, Z^n) - H(Z^n))/n \\
&= (H(M_0, V^n, Z^n) - H(V^n \mid M_0, Z^n) - H(Z^n))/n \\
&= (H(M_0, V^n) + H(Z^n \mid M_0, V^n) - H(V^n \mid M_0, Z^n) - H(Z^n))/n \\
&\geq (H(M_0, V^n) + H(Z^n \mid M_0, V^n) - n\varepsilon_n - H(Z^n))/n \\
&\geq (H(V^n) + H(Z^n \mid V^n) - n\varepsilon_n - H(Z^n))/n \\
&= (H(V^n) - I(Z^n; V^n) - n\varepsilon_n)/n \\
&\geq (\min\{I(Y_1^n; V^n), I(Y_2^n; V^n)\} - I(Z^n; V^n) - n\varepsilon_n)/n \\
&\geq R_0 - \varepsilon_n
\end{aligned} \tag{5}$$

In (5), the first inequality holds because Fano inequality, for sufficiently large n, we have,

$$H(V^n \mid M_0, Z^n) \leq H(P_{me0}^{(n)}) + nP_{me0}^{(n)} R_{m0} \leq n\varepsilon_n$$

The second inequality holds because,

$$\begin{aligned}
H(M_0, V^n, Z^n) &= H(M_0, V^n) + H(Z^n \mid M_0, V^n) \\
&\geq H(V^n, Z^n) \\
&= H(V^n) + H(Z^n \mid V^n)
\end{aligned}$$

The third inequality holds because,

$$H(V^n) \geq \min\{I(Y_1^n; V^n), I(Y_2^n; V^n)\};$$

Secondly, we analyze the security constraints of joint message (M_0, M_1), similar to the above proof, we have

$$\begin{aligned}
R_{e10} &= H(M_0, M_1 \mid Z^n)/n \\
&= (H(M_0, M_1, Z^n) - H(Z^n))/n \\
&= (H(M_0, M_1, V^n, U_1^n, Z^n) - H(V^n, U_1^n \mid M_0, M_1, Z^n) - H(Z^n))/n \\
&= (H(M_0, M_1, V^n, U_1^n) + H(Z^n \mid M_0, M_1, V^n, U_1^n) - H(V^n \mid M_0, M_1, Z^n) - H(U_1^n \mid M_0, M_1, V^n, Z^n) - H(Z^n))/n \\
&\geq (H(M_0, M_1, V^n, U_1^n) + H(Z^n \mid M_0, M_1, V^n, U_1^n) - n\varepsilon_n - H(Z^n))/n \\
&= (H(M_0, M_1, V^n, U_1^n) + H(Z^n \mid V^n, U_1^n) - n\varepsilon_n - H(Z^n))/n \\
&\geq (H(V^n, U_1^n) + H(Z^n \mid V^n, U_1^n) - n\varepsilon_n - H(Z^n))/n \\
&= (H(V^n) + H(U_1^n \mid V^n) - n\varepsilon_n - I(V^n, U_1^n; Z^n))/n \\
&\geq (\min\{I(Y_1^n; V^n), I(Y_2^n; V^n)\} + I(U_1^n; Y_1^n \mid V^n) - I(U_1^n; Z^n \mid V^n) - I(Z^n; V^n) - n\varepsilon_n)/n \\
&\geq R_0 + R_1 - \varepsilon_n
\end{aligned} \tag{6}$$

In (6), the first inequality holds because Fano inequality, for sufficiently large n, we have,

$$H(V^n \mid M_0, M_1, Z^n) \leq H(P_{me0}^{(n)}) + nP_{me0}^{(n)} R_{m0} \leq n\varepsilon_n / 2$$

$$H(U_1^n \mid M_0, M_1, V^n, Z^n) \leq H(P_{me1}^{(n)}) + nP_{me1}^{(n)} R_{m1} \leq n\varepsilon_n / 2$$

The following equation holds because $(M_0, M_1) \to V^n \to U_1^n \to Z^n$ constitutes a Markov chain, so we have,

$I(M_0, M_1; Z^n \mid V^n, U_1^n) = 0$, so

$$H(Z^n \mid M_0, M_1, V^n, U_1^n) = H(Z^n \mid V^n, U_1^n)$$

As proof method is similar and the space limit, we will not derivate the security constraints of joint message (M_0, M_1, M_2) here.

V. CONCLUSION

This paper focuses on the communication system of broadcast channel with an eavesdropper, and then introduces the concept of equivocation and secrecy achievable rate region. We also analyze the inner bound of BCE model. It plays a very important role in researching the out bound of BCE model in the future work.

ACKNOWLEDGMENT

This work was supported in part by the Natural Science Foundation of China under Grant No. 60932003 and No. 61271220

REFERENCES

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

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

[3] I.Csiszar, J. Korner, "Broadcast Channels with Confidential Messages," IEEE Trans. Info. Theory, pp. 339-348, May 1978.

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

[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, pp.306-311. 1979.:

[8] Y. Zhu,et.al. "Research on the Multiple-inputs Single-output Channel Under Attack," ICCIS, Aug 17-19, China, pp. 973-976, 2012.

[9] X. Chen, Y. Zhu, Z. Xue, F. B. Li, J. Gu, "Security in Single-Input Single-Output Multiple-helpers Wireless Channel," ICCIS, Aug 17-19, China, pp. 969-972, 2012

[10] Y. Zhu, et.al. "Research on Secrecy Communication via Bilateral Artifical Noise Transmitting" ICCIS , June 21-23, China, pp. 218-220, 2013

[11] Y. Liang and H. V. Poor, "Secure communication over fading channels," IEEE Trans. Inf. Theory, vol. 52, no. 6, pp. 2470-2492, June 2008.

[12] A. E. Hero, "Secure Space-Time Communication," IEEE Trans. Info. Theory, pp. 3235-3249, December 2003.

[13] X. Chen, et.al. "Research on the Security of MISO Wireless Channel with Artificial Noise" ICCIS , June 21-23, China, 2013.