An Inner Bound for Secrecy E-capacity Region of the Multiple Access Channel with Confidential Messages

Nasrin Afshar
Islamic Azad University of Pardis
Tehran, Iran
e-mail:
afshar_nas@yahoo.com

Evgueni Haroutunian
Institute for Informatics and
Automation Problems of NAS RA
Yerevan, Armenia
e-mail: eghishe@sci.am

Mariam Haroutunian
Institute for Informatics and
Automation Problems of NAS RA
Yerevan, Armenia
e-mail: armar@ipia.sci.am

ABSTRACT

We study secrecy E-capacity region of a discrete memoryless multiple access channel with two confidential messages (DM-MACC). Two users transmit messages to a receiver while both users also receive the channel outputs but messages from each source must be in perfect secrecy with respect to the other source. The level of ignorance is measured by the equivocation rate. Secrecy E-capacity region is the set of rate pairs R_1, R_2 of codes with given error probability exponent (reliability) E at the receiver. The random coding bound for secrecy E-capacity region of the DM-MACC is determined.

Keywords

Error probability exponent, Multiple access channel, Secrecy E-capacity.

1. INTRODUCTION

In this paper, we study a two-user discrete memoryless multiple access channel with two confidential messages (DM-MACC). The system involves two sources, two encoders, one receiver. Two users transmit messages to a receiver while both users also receive the channel outputs. Hence, they may eavesdrop the transmitted messages from the other source. We assume that the transmitters are passive eavesdroppers (Fig. 1). The confidential message from every source must be transmitted through the channel while ensuring the eavesdropping user at another source to be kept in total ignorance of it. Shannon described the information-theoretic security approach in communications [1]. The wiretap channel was investigated by Wyner [2], where the channel from the transmitter to the legitimate receiver and the eavesdropper was a degraded broadcast channel. Csiszár and Körner [3] studied the security of communication for the broadcast channel considering confidential messages. We may refer the reader to [4] wherein various problems and results in secure communications for multi-user systems are discussed. Liang and Poor obtained the capacity bounds of the general multiple access channel where the users attempt to transmit common information to a destination and each user also has a confidential message [4].

Shannon proposed to study error probability exponent of code in [5] and introduced the concept of reliability-rate function $E(R)$, which defines the optimal exponent of the exponential decrease of the decoding error probability for the given rate R when the code length N increases. Bounds of average and maximal error probability exponent for discrete memoryless multiple access channel without secrecy constraint were studied in [6]. The rate-reliability function (E-capacity) $R(E)$ is inverse to the reliability-rate function $E(R)$ [7]. The E-capacity presents optimal dependence of the code rate R upon reliability E. It is also a generalization of Shannon's channel capacity. When $E \to 0$, the E-capacity tends to the channel capacity. Estimates of the E-capacity for different models of multiple access channel were studied in [8].

In this paper, we consider one exponent E for decoding error probability at the destination (the legitimate receiver) and determine an inner bound for secrecy E-capacity region of the DM-MACC, under the requirement that the eavesdropping user is kept in total ignorance of the confidential messages. The constructed region is on average error probability. The level of secrecy is measured by equivocation rate, which is the level of uncertainty of eavesdropping user.

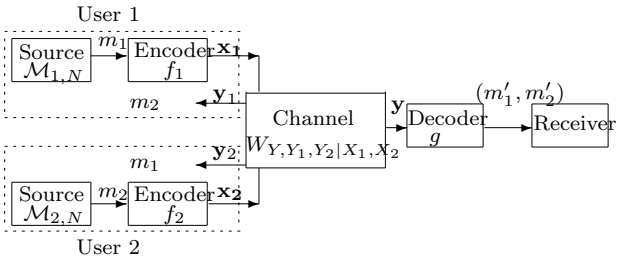

Figure 1: The model of discrete memoryless multiple access channel with two confidential messages

2. PRELIMINARIES

The DM-MACC is with input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, and output alphabets $\mathcal{Y}$, $\mathcal{Y}_1$, $\mathcal{Y}_2$ correspondingly, on the legitimate receiver and eavesdropping users. The vectors $\mathbf{x}_1 \in \mathcal{X}_1^N$ and $\mathbf{x}_2 \in \mathcal{X}_2^N$ are the inputs, $\mathbf{y} \in \mathcal{Y}^N$ is the output vector after N uses of channels. The vector $\mathbf{y}_i \in \mathcal{Y}_i^N$ is the channel output at the eavesdropping user, $i = 1, 2$. $\mathcal{M}_{1,N}$ and $\mathcal{M}_{2,N}$ are the message sets at the first and the second sources, respectively. We introduce some additional finite sets $\mathcal{U}_1$ and $\mathcal{U}_2$. The DM-MACC is characterized by the conditional PDs, $W_{Y|X_1,X_2}$, $W_{Y_1|X_1,X_2}$and $W_{Y_2|X_1,X_2}$ and by products for N uses of the channel

$$W^N_{Y|X_1,X_2}(\mathbf{y}|\mathbf{x}_1,\mathbf{x}_2) = \prod_{n=1}^{N} W_{Y|X_1,X_2}(y_n|x_{1,n},x_{2,n})),$$

$$W^N_{Y_i|X_1,X_2}(\mathbf{y}_i|\mathbf{x}_1,\mathbf{x}_2)=\prod_{n=1}^{N}W_{Y_i|X_1,X_2}(y_{i,n}|x_{1,n},x_{2,n})),$$

$$i=1,\,2.$$

Messages $m_1\in\mathcal{M}_{1,N},\ m_2\in\mathcal{M}_{2,N}$ should be transmitted to the receiver while ensuring the message m_i to be kept secret from the user $3-i,\ i=1,\,2$. The level of secrecy is measured by the equivocation rate at the eavesdropping user.

A *stochastic encoder* f_i is specified by conditional probabilities $f_i(\mathbf{x}_i|m_i)$, where $\mathbf{x}_i\in\mathcal{X}_i^N$, $m_i\in\mathcal{M}_{i,N}$ and $\sum\limits_{\mathbf{x}_i}f_i(\mathbf{x}_i|m_i)=1,\ i=1,\,2$.

A *code* is a triple $(f_1,\,f_2,\,g)$, where f_1 and f_2 are stochastic encoders and $g:\mathcal{Y}^N\to\mathcal{M}_{1,N}\times\mathcal{M}_{2,N}$ is a deterministic decoder for legitimate receiver. A code $(f_1,\,f_2,\,g)$ is characterized also by coding rates $(R_1,\,R_2)$. The level of ignorance of eavesdropper at user i rather than the confidential message m_{3-i} is measured by equivocation rate $\frac{1}{N}H(M_{3-i,N}|\mathbf{Y}_i,\mathbf{X}_i)$.

The average probability of error of the code $(f_1,\,f_2,\,g)$ is

$$e(f_1,\,f_2,\,g,\,W_{Y|X_1,X_2})\triangleq(|\mathcal{M}_1|\times|\mathcal{M}_2|)^{-1}$$
$$\sum_{m_1\in\mathcal{M}_{1,N},\,m_2\in\mathcal{M}_{2,N}}\Pr\big\{(g^{-1}(m_1,m_2))^c\big|m_1,\,m_2\big\}. \qquad (1)$$

A rate pair $(R_1,\,R_2)$ is called *E-achievable* for the DM-MACC if there exists a sequence of codes such that the following conditions are valid:

$$\lim_{N\to\infty}\frac{1}{N}\log|\mathcal{M}_{i,N}|=R_i,\ i=1,\,2, \qquad (2)$$

the reliability requirement

$$e(f_1,f_2,\,g,\,W_{Y|X_1,X_2})\le\exp\{-NE\}, \qquad (3)$$

and the secrecy constrains

$$\liminf_{N\to\infty}\frac{1}{N}H(M_{i,N}|\mathbf{Y}_{3-i},\mathbf{X}_{3-i})\ge R_i,\ i=1,\,2. \qquad (4)$$

Secrecy E-capacity region $\mathcal{R}_s(E)$ for average error probability is defined as the set of all E-achievable rates $(R_1,\,R_2)$. In the next section, we construct a random coding bound $\mathcal{R}_s^r(E)$ for secrecy E-capacity $\mathcal{R}_s(E)$. To this end, we apply the method of types [9]. For the definitions and properties of type and conditional type and definitions of mutual information and Kullback-Leibler's divergence we refer to [8], [9].

3. MAIN RESULT

Let $U_0\to(X_1,\,X_2)\to Y$ be a Markov chain. We consider the following distributions

$$P_{U_0}=\{P_{U_0}(u_0),\ u_0\in\mathcal{U}_0\},$$
$$P=\{P(u_0,x_1,x_2)=P_{U_0}(u_0)P_{X_1,X_2|U_0}(x_1,x_2|u_0),$$
$$u_0\in\mathcal{U}_0,x_1\in\mathcal{X}_1,x_2\in\mathcal{X}_2\},$$

$$V=\{V_{Y|X_1,X_2}(y|x_1,x_2),x_1\in\mathcal{X}_1,x_2\in\mathcal{X}_2,y\in\mathcal{Y}\},$$
$$P\circ V=\{P_{U_0}(u_0)P_{X_1,X_2|U_0}(x_1,x_2|u_0)V_{Y|X_1,X_2}(y|x_1,x_2),$$
$$u_0\in\mathcal{U}_0,x_1\in\mathcal{X}_1,x_2\in\mathcal{X}_2,y\in\mathcal{Y}\}.$$

The marginal distributions are defined as follows:

$$P_i^*(x_i|u_0)=\sum_{x_{3-i}}P_{X_1,X_2|U_0}(x_1,x_2|u_0),$$

$$P_i^*=\{P_i^*(x_i|u_0),x_i\in\mathcal{X}_i\},i=1,\,2,$$

and

$$P^*=\{P_{U_0}(u_0)P_1^*(x_1|u_0)P_2^*(x_2|u_0),$$
$$u_0\in\mathcal{U}_0,\ x_1\in\mathcal{X}_1,\ x_2\in\mathcal{X}_2\}.$$

The following notations of mutual information and divergence are adopted from [8]

$$I_{P,V}(X_1\wedge X_2\wedge Y|U_0)=H_{P_1^*}(X_1|U_0)+H_{P_2^*}(X_2|U_0)$$
$$+H_{P,V}(Y|U_0)-H_{P,V}(Y,X_1,X_2|U_0)=$$
$$=I_{P,V}(X_1,X_2\wedge Y|U_0)+I_P(X_1\wedge X_2|U_0),$$

and

$$D(P\circ V\|P^*\circ W)=D(P\|P^*)+D(V\|W|P).$$

Let us define the following region of rates $R_1,\,R_2$:

$$0\le R_1\le\min_{P,V:D(P\circ V\|P^*\circ W)\le E}|I_{P,V}(X_1\wedge X_2,Y|U_0)$$
$$+D(P\circ V\|P^*\circ W)-E|^+-I_{P,W_{Y_2|X_1,X_2}}(X_1\wedge Y_2|X_2,U_0), \qquad (5)$$
$$0\le R_2\le\min_{P,V:D(P\circ V\|P^*\circ W)\le E}|I_{P,V}(X_2\wedge X_1,Y|U_0)$$
$$+D(P\circ V\|P^*\circ W)-E|^+-I_{P,W_{Y_1|X_1,X_2}}(X_2\wedge Y_1|X_1,U_0), \qquad (6)$$
$$R_1+R_2\le\min_{P,V:D(P\circ V\|P^*\circ W)\le E}|I_{P,V}(X_1\wedge X_2\wedge Y|U_0)$$
$$+D(P\circ V\|P^*\circ W)-E|^+-I_{P,W_{Y_2|X_1,X_2}}(X_1\wedge Y_2|X_2,U_0)$$
$$-I_{P,W_{Y_1|X_1,X_2}}(X_2\wedge Y_1|X_1,U_0), \qquad (7)$$

and the inner bound $\mathcal{R}_s^r(E)$ of secrecy E-capacity region $\mathcal{R}_s(E)$ as follows

$$\mathcal{R}_s^r(E)=\bigcup_{P^*}\{(R_1,R_2):\ (5)\text{ - }(7)\text{ take place for joint PD}$$
$$P_{U_0}\circ P_{X_1,X_2|U_0}\circ V_{Y|X_1,X_2}\}. \qquad (8)$$

Theorem 1. *For all* $E>0$,

$$\mathcal{R}_s^r(E)\subseteq\mathcal{R}_s(E).$$

To prove the theorem we must show that there exists a code $\mathcal{C}$ such that for each $\delta>0$ and N large enough with

$$|\mathcal{M}_{i,N}|=$$
$$\exp\{N[I_{P,V}(X_1\wedge X_2,Y|U_0)+D(P\circ V\|P^*\circ W)$$
$$-E-I_{P,W_{Y_i|X_1,X_2}}(X_1\wedge Y_2|X_2,U_0)-\delta/2]\},$$
$$i=1,\,2,$$

condition (3) holds and equivocation rates satisfy (4). The analysis of error probability is similar to that of MAC without secrecy constraint in [8] and the estimation of the equivocation rate is similar to that of [4].

Remark. Let $E \to 0$ in (8). If we set $U_i = X_i$, $i = 1, 2$, and $M_0 = 1$ in the generalized multiple access channel with confidential messages in [4], the random coding bound for secrecy E-capacity region $\mathcal{R}_s^r(E)$ (8) converges to the secrecy rate region in [4, Corollary 6.3].

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[2] A. D. Wyner, "The wire-tap channel", *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339-348, 1978.

[4] Y. Liang, H. V. Poor and S. Shamai, "Information theoretic security", *Foundations and Trends in Communications and Information Theory*, vol. 5, nos. 4-5, 2009.

[5] C. E. Shannon, "Probability of error for optimal codes in Gaussian channels", *Bell System Technical Journal*, vol. 38, no. 5, pp. 611-659, 1959.

[6] A. Nazari, "Error exponent for discrete memoryless multiple-access channel", *Ph.D dissertation, Dept. Elect. Eng., University of Michigan*, 2011.

[7] E. A. Haroutunian, "Upper estimate of transmission rate for memoryless channel with countable number of output signals under given error probability exponent", *3rd All Union Conference on Theory of Information Transmission and Coding, Uzhgorod, Publishing House of the Uzbek Academy of Sciences*, pp. 83-86, 1967.

[8] E. A. Haroutunian, M. E. Haroutunian and A. N. Harutyunyan, "Reliability criteria in information theory and in statistical hypothesis testing", *Foundations and Trends in Communications and Information Theory*, vol. 4, nos. 2-3, 2008.

[9] I. Csiszár and J. Körner, "Information Theory: Coding Theorems for Discrete Memoryless Systems", *2nd edition. New York, Wiley*, 2011.