Mathematical Problems of Computer Science 38, 34-38, 2012.

On Random Coding Bound for E-capacity Region of the Broadcast Channel With Confidential Messages

Nasrin Afshar, Evgueni Haroutunian and Mariam Haroutunian

Institute for Informatics and Automation Problems of NAS of RA

The information theoretic security recently has attracted much attention [8]. One of the important objects in the secure communication is the broadcast channel with confidential messages (BCC) first investigated by Csiszár and Körner [1]. The model is depicted in Fig.1. The BCC involves two discrete memoryless channels with two sources, one encoder and two receivers. A common message must be transmitted at rate R_0 to both receivers and a private message to the intended receiver at rate R_1 while keeping the other receiver ignorant of it with equivocation rate R_e.

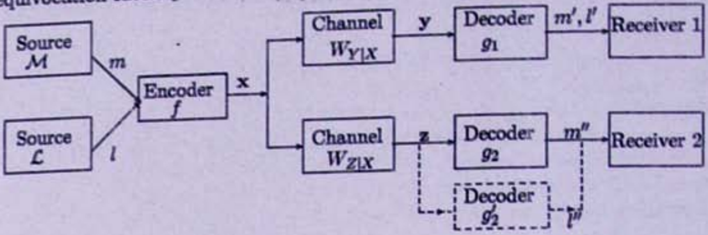

Figure 1. The discrete memoryless broadcast channel with confidential messages.

The E-capacity is an important concept in information theory [6]. The E-capacity (rate-reliability function) for a discrete memoryless channel (DMC) was introduced by E. Haroutunian in 1967 [3]. It presents dependence between rate R and reliability E (error probability exponent) of optimal codes. The function denoted by $R(E)$ (and also $C(E)$) [3] , [4] is inverse to the Shannon's reliability function $E(R)$. Furthermore, the concept of E-capacity can be considered as a generalization of the Shannon's channel capacity. When E goes to zero, the function $C(E)$ tends to the channel capacity C, and when E goes to infinity, the $C(E)$ goes to zero-error capacity C_0.

Csiszár and Körner found the capacity region of the BCC [1]. Liu et all proposed the capacity region of the BCC with two confidential messages [9]. Xu, Cao and Chen investigated an inner bound on the capacity region of the BCC with one common message and two confidential messages (BC-2CM) [11]. Random coding bound and sphere packing bound for E-capacity of DMC are studied in [5], [6]. Random coding bound for the E-capacity region of the broadcast channel with one common message and two private messages was found in [7].

In this paper, we investigate the BCC. We consider error probability exponents (relia-ilities): E_1, E_2, E_3, of exponentially decrease of error probability of, respectively, the first ecoder, the second decoder and of the decoder trying to find the confidential message. For $= (E_1, E_2, E_3)$ the E-capacity region is the set of all achievable rate triples R_0, R_1, R_e codes with given reliabilities E_1, E_2, E_3. We construct a random coding bound for E-acity region of the BCC. When error probability exponents are going to zero, the limit of s bound coincides with the capacity region of the BCC obtained by Csiszár and Körner. e notion of E-capacity region is used also for estimation of equivocation rate.

It should be noted, that the consideration of the E-capacity upper bound of secrecy kage, which is the rate of available information of unintended receiver with respect to the vate message, is a non-standard approach to lower bound construction of equivocation e in the BCC.

Result Formulation. Consider RVs X, Y, Z and auxiliary RVs U_0, U_1 with joint es:

$$Q \circ P_1 \circ V_{Y|X} = \{Q \circ P_1 \circ V_{Y|X}(u_0, u_1, x, y) = Q_0(u_0)Q_{1|0}(u_1|u_0)P_1(x|u_1)V_{Y|X}(y|x)\}, \quad (1)$$

$$Q \circ P_1 \circ V_{Z|X} = \{Q \circ P_1 \circ V_{Z|X}(u_0, u_1, x, z) = Q_0(u_0)Q_{1|0}(u_1|u_0)P_1(x|u_1)V_{Z|X}(z|x)\}. \quad (2)$$

We define the following functions appearing in our inner estimates of E-capacity region:

$R_0^*(Q, P_1, E_1, E_2) \triangleq$

$$\min\Big\{\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\leq E_1}\Big|I_{Q,P_1,V_{Y|X}}(U_0 \wedge Y) + D(V_{Y|X}\|W_{Y|X}|Q_1, P_1) - E_1\Big|^+,$$

$$\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)\leq E_2}\Big|I_{Q,P_1,V_{Z|X}}(U_0 \wedge Z) + D(V_{Z|X}\|W_{Z|X}|Q_1, P_1) - E_2\Big|^+\Big\}, \quad (3)$$

$R_1^*(Q, P_1, E_1) \triangleq$

$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\leq E_1}\Big|I_{Q,P_1,V_{Y|X}}(U_1 \wedge Y|U_0) + D(V_{Y|X}\|W_{Y|X}|Q_1, P_1) - E_1\Big|^+, \quad (4)$$

$R_e^*(Q, P_1, E_1, E_3) \triangleq$

$$\min_{V_{Y|X}:D(V_{Y|X}\|W_{Y|X}|Q_1,P_1)\leq E_1}\Big|I_{Q,P_1,V_{Y|X}}(U_1 \wedge Y|U_0) + D(V_{Y|X}\|W_{Y|X}|Q_1, P_1) - E_1\Big|^+ -$$

$$\min_{V_{Z|X}:D(V_{Z|X}\|W_{Z|X}|Q_1,P_1)\leq E_3} I_{Q,P_1,V_{Z|X}}(U_1 \wedge Z|U_0). \quad (5)$$

us consider the following bounds of rates R_0, R_1, R_e:

$$0 \leq R_0 + R_1 \leq R_0^*(Q, P_1, E_1, E_2) + R_1^*(Q, P_1, E_1), \quad (6)$$

$$0 \leq R_0 \leq R_0^*(Q, P_1, E_1, E_2), \quad (7)$$

$$0 \leq R_e \leq R_e^*(Q, P_1, E_1, E_3), \quad R_e \leq R_1. \quad (8)$$

e result of the paper is formulated in the following

THEOREM 1. *For* $E_1 > 0, E_2 > 0, E_3 > 0,$ *the region*

$$\mathcal{R}^*(E) \triangleq \bigcup_{Q,P_1} \{(R_0,\ R_1,\ R_e) : (6-8)\ \textit{take place for}\ \ U_0 \to U_1 \to X \to (Y,\ Z)\} \quad (9)$$

n inner bound for E-capacity region $\mathcal{C}(E)$ of the BCC:

$$\mathcal{R}^*(E) \subseteq \mathcal{C}(E) \subseteq \overline{\mathcal{C}}(E).$$

References

[1] I. Csiszár and J. Körner, "Broadcast channel with confidential messages", *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, 1978.

[2] I. Csiszár and J. Körner, "*Information Theory: Coding Theorems for Discrete Memoryless Systems*", New York, Wiley, 1981.

[3] 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.

[4] E. A. Haroutunian, B. Belbashir, "Lower bound of the optimal transmission rate depending on given error probability exponent for discrete memoryless channel and for asymmetric broadcast channel", *Abstracts of Papers of 6th Int. Symp. Inf. Theory, Tashkent, USSR*, vol. 1, pp. 19-21, 1984.

[5] E. A. Haroutunian, "On Bounds for E-Capacity of DMC", *IEEE Trans. Inf. Theory*, vol. IT-53, no. 11, pp. 4210-4220, 2007.

[6] 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.

[7] M. E. Haroutunian, "Random coding bound for E-capacity region of the broadcast channel", *Mathematical Problems of Computer Science*, no. 21, pp. 50-60, 2000.

[8] 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.

[9] R. Liu, I. Maric, P. Spasojevic and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions", *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493-2507, 2008.

[10] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, 1975.

[11] J. Xu, Y. Cao and B. Chen, "Capacity bound for broadcast channels with confidential messages", *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4529-4542, 2009.