Mathematical Problems of Computer Science 36, 79–90, 2012.

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

Nasrin Afshar, Evgueni Haroutunian and Mariam Haroutunian

Institute for Informatics and Automation Problems of NAS of RA
e-mail: evhar@ipia.sci.am

Abstract

We study secrecy E-capacity region of the discrete memoryless broadcast channel with two independent confidential messages sent to two receivers (BC-2CM). The system involves two sources, one encoder, two discrete memoryless channels and two receivers. Each private message is sent to the corresponding receiver while keeping the other receiver in total ignorance of it. The level of ignorance is measured by the equivocation rate. E-capacity region is the set of rate pairs R_1, R_2 of codes with given error probability exponents (reliabilities) E_1, E_2 at respective receivers. We derived a random coding bound for secrecy E-capacity region of the BC-2CM. When error probability exponents are going to zero, this bound coincides with the inner bound of secrecy capacity region of the BC-2CM obtained by R. Liu, I. Maric, P. Spasojevic and R. Yates.

Key words: Broadcast channel with confidential messages, secrecy E-capacity, equivocation rate, error probability exponent, method of types, random coding bound.

References

[1] T. M. Cover, "Broadcast channels", *IEEE Trans. Inf. Theory,* vol. IT-18, no. 1, pp. 2-14, 1972.

[2] T. M. Cover and J. A. Thomas, "*Elements of Information Theory*", 2nd edition, A Wiley-Interscience Publication, 2006.

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

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

[5] S. I. Gelfand and M. S. Pinsker, "Capacity of broadcast channel with one deterministic component", *Probl. Pered. Inf.,* vol. 16, no. 1, pp. 17-25, 1980.

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

[7] 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", (in Russian), *Abstracts of Papers of 6th Int. Symp. Inf. Theory, Tashkent, USSR,* vol. 1, pp. 19-21, 1984.
[8] E. A. Haroutunian, "On Bounds for E-Capacity of DMC", *IEEE Trans. Inf. Theory,* vol. IT-53, no. 11, pp. 4210-4220, 2007.
[9] 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.
[10] E. A. Haroutunian, M. E. Haroutunian and N. Afshar, "Random Coding Bound for E-capacity Region of the Wiretap Channel", *8th International Conference of Computer Science and Information Technologies, Yerevan,* pp. 121-124, 2011.
[11] 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.
[12] M. Hayashi , R. Matsumoto, "Universally attainable error and information exponents for the broadcast channels with confidential messages", *Arxiv:1104.4285v2 [cs.IT]*, 24 April 2011.
[13] 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.
[14] 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.
[15] K. Marton, "A coding theorem for the discrete memoryless broadcast channel", *IEEE Trans. Inf. Theory,* vol. IT-25, no. 3, pp. 306-311, 1979.
[16] C. E. Shannon, "A mathematical theory of communication", *Bell Syst. Tech. J.,*— vol. 27, no. 3, pp. 379-423, 1948. 38, no. 5, pp. 611-659, 1959.
[17] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.,* vol. 54, no. 8, pp. 1355-1387, 1975.
[18] 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.

Երկու գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու գաղտնիության E-ունակության տիրույթի պատահական կոդավորման գնահատականը

Ն. Ավշար, Ե. Հարությունյան և Մ. Հարությունյան

Ամփոփում

Մ՚՚նք հետազոտում ենք երկու անկախ գաղտնի հաղորդագրություններով ընդհատ առանց հիշողության լայնասփյուռ կապուղու գաղտնիության E-ունակության տիրույթը: աղտնիության մակարդակը չափվում է անորոշության արագությամբ: Կառուցված է գաղտնիության E-ունակության տիրույթի պատահական կոդավորման գնահատականը:

Граница случайного кодирования области E-пропускной способности секретности широковещательного канала с двумя секретными сообщениями

Н.Афшар, Е.Арутюнян и М. Арутюнян

Аннотация

Мы изучаем область секретной -пропускной способности дискретного широковещательного канала без памяти с двумя независимыми секретными сообщениями, посылаемыми двум адресатам. Уровень секретности измеряется скоростью неопределенности. Мы строим границу случайного кодирования для области секретной E-пропускной способности широковещательного канала с двумя секретными сообщениями.