

Sphere Packing Bound for E -capacity of Secrecy Leakage of the Broadcast Channel With Confidential Messages

Nasrin Afshar

Institute for Informatics and Automation Problems of NAS of RA

Abstract

The discrete memoryless broadcast channel with confidential messages (BCC) involves two discrete memoryless channels with two sources and one encoder. A common message must be transmitted to two receivers and a private message to the intended receiver, while keeping the other receiver as ignorant of it as possible. Secrecy leakage rate is the rate of information available to the unintended receiver about the private message. Upper bound for E -capacity of secrecy leakage of the BCC is derived.

Key words: Broadcast channel with confidential messages, E -capacity, error probability exponent, method of types, secrecy leakage rate, sphere packing bound.

References

- [1] I. Csiszár and J. Körner, “Broadcast channel with confidential messages”, *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339-348, 1978.
- [2] 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.
- [3] 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. Inform. Theory, Tashkent, USSR*, vol. 1, pp. 19-21, 1984.
- [4] E. A. Haroutunian, “On Bounds for E-Capacity of DMC”, *IEEE Trans. Inform. Theory*, vol. IT-53, no. 11, pp. 4210-4220, 2007.
- [5] 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.
- [6] 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.

Գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու գաղտնիքի հոսակորուստի արագության գնդերի փաթեթավորման գնահատականը

Ն. Ավշար

Անփոփում

Գաղտնի հաղորդագրություններով լայնասփյուռ կապուղու ընդհանուր հաղորդագրությունը փոխանցվում է երկու հասցեատերերին, իսկ մասնավոր հաղորդագրությունը՝ միայն մեկին. այն պետք է հնարավորինս գաղտնի լինի մյուսի նկատմամբ: Կառուցվել է գաղտնիքի հոսակորուստի արագության E -ունակության վերին գնահատականը:

Граница сферической упаковки скорости утечки секрета в широкополосном канале с секретными сообщениями

Н.Афшар

Аннотация

Общее сообщение широкополосного канала с секретными сообщениями, передается двум адресатам, а частное сообщение только одному из них и должно быть насколько возможно секретным для второго. Построена верхняя граница E -пропускной способности скорости утечки секрета.