CCIT Report #649 November 2007

IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security, submitted Nov. 2006, revised Oct. 2007

Secure Communication over Fading Channels [1] [2]

Yingbin Liang, H. Vincent Poor and Shlomo Shamai (Shitz) [3]

Abstract

The fading broadcast channel with confidential messages (BCC) is investigated, where a source node has common information for two receivers (receivers 1 and 2), and has confidential information intended only for receiver 1. The confidential information needs to be kept as secret as possible from receiver 2. The broadcast channel from the source node to receivers 1 and 2 is corrupted by multiplicative fading gain coefficients in addition to additive Gaussian noise terms. The channel state information (CSI) is assumed to be known at both the transmitter and the receivers. The parallel BCC with independent subchannels is first studied, which serves as an information-theoretic model for the fading BCC. The secrecy capacity region of the parallel BCC is established. This result is then specialized to give the secrecy capacity region of the parallel BCC with degraded subchannels. The secrecy capacity region is then established for the parallel Gaussian BCC, and the optimal source power allocations that achieve the boundary of the secrecy capacity region are derived. In particular, the secrecy capacity region is established for the basic Gaussian BCC. The secrecy capacity results are then applied to study the fading BCC. The ergodic performance is first studied. The ergodic secrecy capacity region and the optimal power allocations that achieve the boundary of this region are derived. The outage performance is then studied, where a long term power constraint is assumed. The power allocation is derived that minimizes the outage probability where either the target rate of the common message or the target rate of the confidential message is not achieved. The power allocation is also derived that minimizes the outage probability where the target rate of the confidential message is not achieved subject to the constraint that the target rate of the common message must be achieved for all channel states.

---

[1] The material in this paper was presented in part at the 44th Annual Allerton Conference on Communication, Control, and Computing, Monticello, IL, Sept. 2006.

[2] The research was supported by the National Science Foundation under Grants ANI-03-38807 and CNS-06-25637.

[3] Yingbin Liang and H. Vincent Poor are with the Department of Electrical Engineering, Princeton University, Engineering Quadrangle, Olden Street, Princeton, NJ 08544; e-mail: {yingbinl,poor}@princeton.edu; Shlomo Shamai (Shitz) is with the Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, Haifa 32000, Israel; email: sshlomo@ee.technion.ac.il