Chair of Communications Engineering
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Securing OFDM Against Jamming Attacks

In wireless systems, a jammer may send interfering signals to disrupt legitimate communication. Orthogonal frequency-domain multiplexing (OFDM) is especially vulnerable to jamming attacks [1]. Liang, Ren and Li [1] proposed a modified OFDM scheme which is secured against jamming attacks by introducing randomized phase shifts that are coordinated between sender and receiver. It is known in general [2] that randomized protocols can mitigate even adversarial jamming. True randomness is difficult to get, but a very small amount is sufficient to achieve full channel capacity [3].

The task of the student is to understand the vulnerability of OFDM and to review the secured OFDM scheme by Liang, Ren and Li [1]. If possible, the student should consider whether the amount of randomness used there can be reduced.

[1] Y. Liang, J. Ren, and T. Li, “Secure OFDM System Design and Capacity Analysis Under Disguised Jamming,” 2020. doi: 10.1109/TIFS.2019.2929449.
[2] D. Blackwell, L. Breiman, and A. J. Thomasian, “The Capacities of Certain Channel Classes Under Random Coding,” 1960. doi: 10.1214/aoms/1177705783.
[3] R. Ahlswede, “Elimination of correlation in random codes for arbitrarily varying channels,” 1978. doi: 10.1007/BF00533053.

Prerequisites

Information Theory

Advisors

Johannes Rosenberger