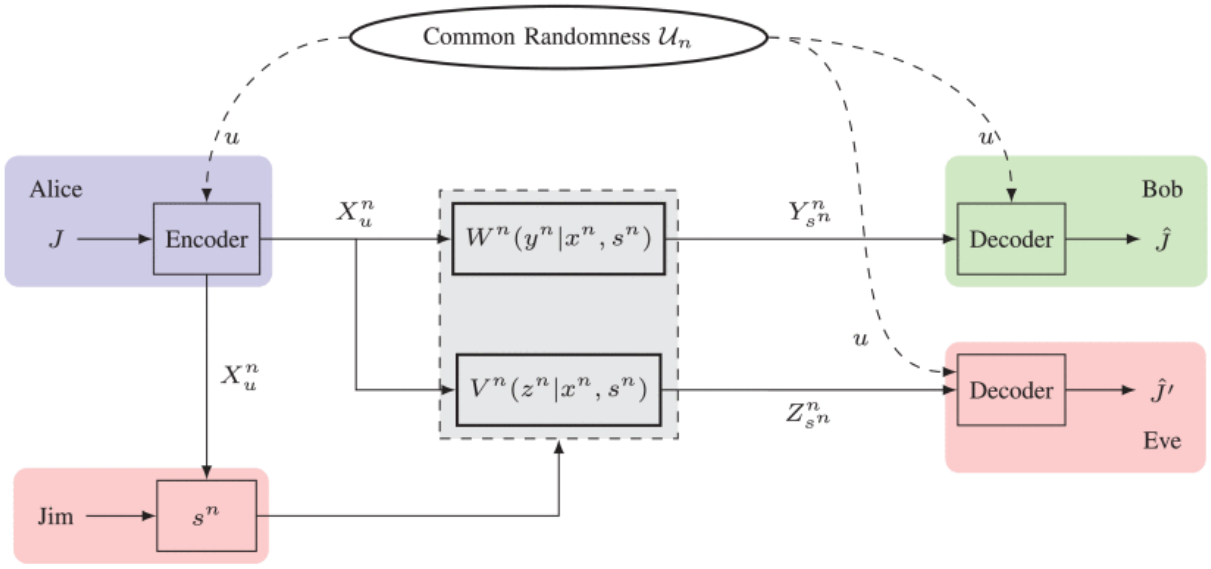
GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Arbitrarily Varying Wiretap Channels With Non-Causal Side Information at the Jammer

CARSTEN RUDOLF JANDA, MORITZ WIESE, EDUARD JORSWIECK, HOLGER BOCHE

What are the fundamental limits of confidential communications with passive and active adversaries if the active adversary has side information about the message and channel input?



(a)

Confidential communication model comprises the passive eavesdropper Eve, the two legitimate nodes Alice and Bob, and the active attacker Jim. The channel is modelled by an arbitrarily varying channel whose channel state is controlled by the jammer Jim who has non-causal access to the channel input. Common randomness is available at Alice and Bob, but overheard at Eve. Attacker is very strong and still positive secrecy rates are achievable because Alice encodes the confidential data by stochastic encoder preparing for the worst-case channel state to Bob and the worst information leakage to Eve.

KEY FINDINGS

Secure communication in a potentially hostile environment is becoming more and more critical. The Arbitrarily Varying Wiretap Channel (AVWC) provides information-theoretical bounds on how much information can be exchanged even in the presence of an active attacker. If the active attacker has non-causal side information, situations in which a legitimate communication system has been hacked can be modeled. We investigate the AVWC with non-causal side information at the jammer for the case that there exists a best channel to the eavesdropper. Non-causal side information means that the transmitted codeword is known to an active adversary before it is transmitted. A single-letter formula for the Common Randomness (CR)-assisted secrecy capacity is derived. We provide a formula for the CR-assisted secrecy capacity for when the channel to the eavesdropper is strongly degraded with respect to the main channel. We compare our results to the CR-assisted secrecy capacity for the cases of maximum error criterion but without non-causal side information (blind adversary), maximum error criterion with non-causal side information of the messages (semi-blind adversary), and the case of average error criterion without non-causal side information (blind adversary).

C. R. Janda, M. Wiese, E. A. Jorswieck and H. Boche, "Arbitrarily Varying Wiretap Channels With Non-Causal Side Information at the Jammer," in IEEE Transactions on Information Theory, vol. 69, no. 4, pp. 2635-2663, April 2023, doi: 10.1109/TIT.2023.3245722.