Jordan University of Science and Technology

Simple Encryption Algorithm with Improved Performance in Wireless Communications

Authors: M. M. Matalgah and Amer M. Magableh

Abstract: In this paper, inspired by network coding theory we propose an efficient hybrid encryption-coding algorithm that requires using traditional encryption only for the first small amount of data. This amount of data, which we refer to as the first block, is determined by the traditional encryption algorithm to be applied on this first block. In our proposed algorithm, all the rest of the information will then be transmitted securely over the wireless channel, using network coding, without a need for using traditional encryption. Unlike the traditional and opportunistic encryption algorithms, the proposed algorithm achieves higher data rates and less avalanche error effect and at the same time it is as secure as traditional encryption algorithms. Assuming the additive white Gaussian noise (AWGN) channel model employing our proposed algorithm we analyze its performance in terms of throughput and security level. Numerical results of different case studies are provided.