Jordan University of Science and Technology

Alleviating the Effect of the Strict Avalanche Criterion (SAC) of Symmetric-Key Encryption in Wireless Communication Channels

Authors: Mustafa M. Matalgah, Walid Y. Zabdeh, and Amer M. Magableh

Abstract: The strict avalanche criterion (SAC) is a desirable property of traditional symmetric-key cryptographic algorithms. The SAC is said to be satisfied if, whenever a single input bit is complemented, each of the output bits changes with a probability of one half. In terms of the block ciphers context, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. Consequently catastrophic error results when decrypting the ciphertext. Although this criterion is desirable to assure security, these algorithms do not take into account the bit error characteristics of the wireless channel. If an error occurs in the encrypted data over the channel, which is highly likely in wireless channels, the decryption process at the receiver results in half the original bits to be in error due to the SAC effect. Therefore, the need for new secure encryption algorithm that takes into account the bit error characteristics of the wireless channel becomes necessary. In this paper, we present two methods to tackle this effect while at the same time not tolerating security. We first present a modification to the way the traditional Data Encryption Standard (DES) itself is performed to make it prone to errors caused by the wireless channel. Secondly, we present a modification to the way encrypted data is transmitted over the channel. The two proposed methods are shown to achieve less SAC effect and hence improved error performance, higher data rates, and at at least as secure as traditional encryption algorithms. We assume the additive white Gaussian noise (AWGN) channel model in our analysis