Data Modeling and Predictive Analytics on Neural Cryptography for Wireless Communication

J K Mandal
Department of Computer Science & Engineering
University of Kalyani
Kalyani, Nadia, West Bengal 741235, India

The objectives of the Neural Cryptography is to enhance the security of the wireless communication system in such a way that the instead of exchanging the whole session key, soft computing based synchronization technique is used to construct a cryptographic key exchange protocol for generating the identical session key at sender and receiver. Here the partners benefit from mutual interaction, so that a passive attacker is usually unable to learn the generated key in time. This synchronized network can be used for message communication by encrypting the plaintext using any light weight encryption/decryption technique with the help of synchronized session key at both ends. Also grouped synchronization can be used to synchronize group of n party to form a synchronized grouped session key. Both the communicating networks receive an indistinguishable input vector, produce an output bit and are trained based on the output bit. The dynamics of the two networks and their weight vector are found to a novel experience, where the demonstrate networks synchronize to an identical time dependent weight vector. For the predictive analysis on the neural cryptography total fifteen statistical tests of the NIST test suite has been considered to evaluate randomness of the synchronized session key. These tests focused on a variety of different types of non-randomness that could exist in a sequence. Some tests are decomposable into a variety of subtests. The purpose of these tests is to determine whether that number of ones and zeros in a session key are approximately the same as would be expected for a truly random session key.