ABSTRACT

The objectives of the proposed thesis 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 has been proposed to synchronize group of \( n \) party to form a synchronized grouped session key. The candidate searched some of such techniques which are simple and easy to understand, and also to trade-off between security and performance of light weight devices as well as energy awareness during the course of research.

The thesis considered synchronization of sender and receiver using soft computing tool for generating identical session key and light weight soft computing based encryption/decryption technique as an example corresponding to each technique. Here five such techniques based on soft computing based synchronization have been designed, implemented and tested through High Level Languages. These techniques have been discussed with their merits and demerits. Identical soft computing based network has been considered at sender and receiver. 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. This observable fact has been used to form a secured variable length secret session key using a public channel. Any light weight message encryption technique is used to encrypt the plaintext. In this thesis as an example light weight soft computing based message encryption technique is used to illustrate the cryptographic technique. Encrypted text get further encrypted using synchronized session key and transmitted to the receiver. During decryption receiver has the same synchronized session key which is used to perform first round of decryption operation and outcomes of this further decrypted by message decryption technique (exactly reverse process of message encryption) are performed and plaintext is regenerated.

Comparison of all proposed techniques with each other and also with Tree Parity Machine (TPM) and Permutation Parity Machine (PPM), RSA, Triple-DES (168 bits), AES (128 bits),
RC4 and Vernam Cipher has been done with respect to the parameters like fifteen statistical tests of the NIST test suite, analysis of the average time (in cycle) needed for generating 128/192/256 bit session key by synchronization between two party and group of party, memory heap used during synchronization, relative time spent in GC and thread required in synchronization phase, encryption and decryption time, character frequencies, Avalanche and strict Avalanche effects, Bit Independence effects, Chi-Square values, character frequency test, entropy test, floating frequency test and autocorrelation test.

A model of session key generation through synchronization and encryption through cascaded implementation embodied with proposed algorithms has been introduced. The approach of cascaded implementation is an attempt to integrate the five proposed techniques. The proposed model may introduce new dimension to ensure security at maximum possible level. The model is very much suitable for the security of the system where unify computing is an essential component and it is idle to trade-off between security and performance of light weight devices having very low processing capabilities or limited computing power in wireless communication.