Encrypted Voice Over TCP/IP by Using Neural Encryption Algorithm (NEA)

By

Tubtim Sanguanwongthong

Abstract

This thesis proposes a new encryption, Neural Encryption Algorithm (NEA), designs and develops a software of voice/text chat over TCP/IP with NEA including Data Encryption Standard (DES), Triple DES, Secure And Fast Encryption Routine with a Key of length 64 bits (SAFER K-64), Rivest Shamir and Adleman (RSA) and no encryption for comparison in secure voice/data communication over TCP/IP under Windows operating system.

Since there are a lot of well-known cryptographies with both symmetric-key and public-key encryptions, the NEA, a symmetric-key encryption is proposed to provide the new alternative way for secure communication. This proposed encryption has been applied in the proposed software for voice and text chat.

The software development testing process is divided into 3 steps.

1. Study how to transmit/receive voice/text with no encryption in LAN.
2. Design server as the authentication center of user-and-password login.
3. Design client for voice and text chat with applying DES, Triple DES, SAFER K-64, RSA, NEA and none of encryption.

In the proposed software, PCM is being applied for digitizing voice with 8 kHz sampling rate and 512-byte buffer size. In testing security, the packet sniffer is applied to detect the packet segment and read data message in network.