ABSTRACT

Voice over Internet Protocol (VoIP) is technology that can pass voice, video, and data on packet format of IP-network . IP-network is communication network based on packet switch. The advantage of communication using VoIP is cheaper than conventional telephone.

VoIP use IP network for passing voice data. IP-network is public network. Characteristic of public network is easy to break by intruder. Security level of public network is lower than private network.

A method to secure VoIP network by encrypt commpresed voice-data in VoIP-server using stream-cipher cryptographic algorithm. In receiver end-VoIP-server, encrypted voice-data will decrypt to get original sound. Data that passed on IP-network is voice-data that has been encrypted, so attackers need decryption key and algorithm to break voice-data. Once stream cipher algorithm is SEAL.

VoIP network is very sensitive on delay. ITU-T recommended maximum delay end-to-end on VoIP-network is 150 ms. Adding cryptographic modul on VoIP server will increase delay end-to-end. Delay end-to-end after add cryptographic modul must low than maximum delay end-to-end that recommended by ITU-T.

The result from this research is with adding SEAL cryptographic modul on VoIP-network, delay end-to-end below maximum delay end-to-end that recommended by ITU-T. Encrypted voice-data will be not produce voice, so voice data packet which pass on IP network hard interupted.

Keywords : IP-network, cryptographic algorithm, delay end-to-end, encryption, decryption