Preventing TMTO attack in AES-CCMP in IEEE 802.11i

Abstract :

This study is conducted to establish an alternative, creative technique for the structure of Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP) key in IEEE 802.11i. the structure of proposed method increase the length of AES-CCMP key from 128 bits to 256 bits to eliminate Time-Memory Trade-Off (TMTO) attacks by using three proposed solutions including Random Nonce Key, Four Way Handshake alteration and Pseudo Random Function (PRF). Besides, two proposed and classic methods are compared in terms of TMTO attack probability, avalanche effect, changes in neighbor blocks, memory usage and execution time. According to the results, the proposed method is completely resistant to TMTO attack. In addition, avalanche effect and change in neighbor blocks of proposed method are so near to optimized state and also, two classic and proposed methods are approximately the same in case of memory usage and execution time.