Implementation of Station-to-Station Protocol for Prevention Man-In-The-Middle Attack

Si Thu Min Thein, Khin Than Mya

University of Computer Studies, Yangon

minsithu.85@gmail.com, *kinthanmya@gmail.com*

Abstract

Computer security is very important role for information and data. Data communication is the most important in the world. Communication technology is increased as well as an authorized person can intercept the security of the system and can get the data. So, computer security is the most important and must secure our data in communication. In this system, man-in-the-middle attack, in which the adversary inserts, deletes, or arbitrarily modifies messages sent from one user to another by using Diffie-Hellman key exchange algorithm. To prevent this man-in-the-middle attack, station-to-station protocol can be used. STS protocol is a cryptographic key agreement scheme based on classic Diffie-Hellman.