CHAPTER 6

CONCLUSION AND SCOPE FOR FUTURE RESEARCH

6.1 INTRODUCTION

This chapter presents the overall view of this study. It includes conclusions by describing the progress made towards this goal in terms of development of three party key exchange protocol before discussing opportunities for further investigation.

6.2 CONCLUSIONS

The aim of this thesis is to develop a framework for attack resistant key exchange protocol. In chapter 1, the concepts of cryptography and security services have been discussed. The analysis of key exchange protocol, attacks and types of attacks and are explained in detail. The motivation behind the proposed system, research aims and objectives and the organization of the thesis has been explained.

In Chapter 2, literature survey of various techniques for the key exchange has been reviewed. Most of the protocols had been developed for classifying the key exchange protocol into classes such as symmetric and asymmetric cases. Various encryption techniques such as Data Encryption Standard(DES), RSA and hash functions such as Secure Hash Function
(SHA), one way trapdoor hash function, pseudorandom hash function had been used to classify the encrypted key exchange protocol.

In Chapter 3, the procedure for the encrypted key exchange protocol is been explained. The mathematical notation for generation of the session key is described. Undetectable online password guessing attack on the encrypted key exchange protocol is explained with a simple example. The mathematical background of impersonation attack is also explained. The calculation of one way trapdoor hash function, pseudorandom hash function and symmetric encryption with formulae is been discussed.

In Chapter 4, the parallel message transmission technique, Flow chart and the procedure for the proposed protocol are presented. The proposed method is based on the encrypted key exchange technique and is capable of resisting to Undetectable online password guessing attack and impersonation attack. This method is successful in exchanging the session key securely between the communicating parties. Security and efficiency analysis on the proposed protocol is made based on the security requirements such as mutual authentication, resistance to password guessing attack, transmission round and computational complexity and practicality. The experimental results indicate that the hybridized approach can efficiently exchange the key maintaining secrecy and also achieve high performance accuracy.

Finally in Chapter 5, the outputs of the proposed methods are clearly shown with figures and graphs. The performance metric used in the proposed methods is percentage of efficiency rate. The performance measure is calculated by using the formulae given in Chapter 4 and tabulated. From the experimental results, it is observed that the proposed protocol based on
parallel message transmission technique gives the better performance rate and accuracy compare to other methods.

The performance of the three party key exchange protocol in the proposed method is tested with three different metrics namely the one-way trapdoor hash function, pseudorandom hash function and the symmetric encryption. From the tables and curves in chapter 5, it is observed that the proposed protocol gives better results while using the parallel messaging technique. In the 1\textsuperscript{st} stage for the computation of trapdoor hash function of 128 it takes 1031 microseconds and for 2048 bits it takes 350950 microseconds and in the 2\textsuperscript{nd} stage the computation of pseudorandom hash function of a chosen prime number it takes 16641 microseconds for $N_A$ and for the same prime it takes 276.3 microseconds for the computation of $K_{AS}$ respectively. In the 3\textsuperscript{rd} stage the computational time for symmetric encryption is calculated for minimum and maximum number of bits such as, for 64 bits it takes 351.4 microseconds and for 2048 bits it takes 4778.5 microseconds. The proposed system is quite effective with performance comparable to that of previous methods such as Chang and Chang and Lo Yeh protocols.

6.3 SUGGESTIONS FOR FUTURE WORK

As not only the field of interest, but also the results of this study turned out to be rich and broad, there are several ways to extend too many directions. Some of the possible ways are discussed below to investigate this work in near future.
In three party Encrypted key exchange protocol for symmetric encryption process, random numbers are being generated along with the generation of large prime numbers which is then computed using the one-way trapdoor hash function and pseudorandom hash function respectively. As the size of the random number of large prime number increases the computation time will also increase. The computational time and cost can be reduced by using the overlapping technique. However if the prime chosen or the random number chosen are of smaller size then there is a chance for the attackers to guess the small value of prime using brute force attack. In future, by carefully choosing the smaller prime number and random number, the computational time may be still reduced to achieve same/better performance rate with reduced computational cost and time. In the proposed protocol, parallel message transmission technique is been used to reduce the transmission time of multiple messages. Currently, the two communicating parties can simultaneously send request to the server, and the server in turn after processing simultaneously send response to both the clients. The response time to each client depends on the processing time taken by the server to decrypt each request and generate the response. The response time can be reduced by increasing the computation time at the server.

The experimental results were considered for three communicating parties which can in future be tested for more number of communicating parties. When the same methodology is attempted for multiple communicating parties, a much better performance could be achieved in terms of the computation time, cost and efficiency.