CHAPTER 6
CONCLUSION

6.1. Introduction

Cryptographic security services are necessary in WLAN and also in data link layer, which has been accepted as an International standard in software industries, research organizations etc. Due to intensive research and development the reputation of WLAN can be really improved as advanced mechanism for entity authentication, key management, Data authentication and confidentiality.

The problems of security issues of bluetooth using elliptic curve cryptography are addressed in this chapter. The new techniques of security issues of bluetooth using elliptic curve are also proposed as follows.

i. Research study on different performance issues of bluetooth using elliptic curve cryptography.

ii. Bluetooth security features.

iii. Elliptic curve cryptography and its algorithms.

The proposed representations are clarified to be effective in analyzing the performance issues of security issues of bluetooth using elliptic curve cryptography. Further in this dissertation novel techniques for bluetooth security issues using elliptic curve cryptography are innovated. In this chapter, the summary of all the proposed methodologies are shown. In sequence the major contributions of the research work are listed. Subsequently the scope for further innovative research based on the work presented in this thesis is envisaged.

6.2. Summary

The First chapter is the Introduction. It introduces a detailed survey on existing approaches covering different security issues of bluetooth using elliptic curve cryptography, preamble, inherent risks with bluetooth devices, bluetooth security architecture, security issues of bluetooth, Introduction to cryptography, cryptographic algorithms in bluetooth security, applications of security issues of bluetooth using elliptic curve cryptography, research contributions, outline of the Thesis.
The second chapter explains the literature survey. This chapter mainly discusses and introduces the review of literature pertaining to the subject is undertaken to understand the better prevailing aspects in the field of security issues of bluetooth using elliptic curve cryptography and the contributions from various researchers and scientists in the field of bluetooth security issues using elliptic curve cryptography.

The third chapter deals with the security issues of bluetooth. It discusses about various algorithms for security issues of bluetooth using elliptic curve cryptography. It explain elliptic curve groups, choice of parameters, elliptic curve algorithms, simple binary algorithms, simple NAF algorithms, classical m-ary algorithms, window NAF algorithms, Implementation of security issues of bluetooth using Elliptic Curve Cryptography (ECC), Implementation of Man in the Middle Attack (MITM) (Woman in the Middle attack) (WITM) (Bucket Brigade Attack (BBA), performance evaluation of bluetooth security issues using elliptic curve cryptography.

The Fourth Chapter is an Elliptic Curve Cryptography. It briefly explains an introduction to elliptic curve cryptography, history of elliptic curve cryptography, study of an elliptic curve cryptography for the security issues of bluetooth, mathematical model and implementation of security issues of bluetooth using an elliptic curve cryptography, Security issues of Bluetooth based on Digital Signature Algorithm using Elliptic Curve Cryptography(SBECDSA).

The fifth chapter is Wireless LAN and Its Security Algorithms. It explores an introduction to WLAN, performance issues of wireless networks, network performance issues, The WLAN performance issues. We have also implemented the security issues of WLAN’s using space time processing especially using alamouti code.

6.3. Contributions

i. Introduction of a new technique such as security issues of bluetooth using an elliptic curve cryptography.

ii. Our great achievement also comes in calculating the best, average and worst Case time complexities of elliptic curve cryptography.
iii. We put a dedicated effort to compute the various Best case, Average case and worst case time complexities for the newly proposed digital signature algorithm.

iv. This research work also explores very briefly how to implement security issues of bluetooth using man in the middle attack (woman in the middle attack).

v. Security issues of bluetooth using an elliptic curve cryptography is also explained using RSA and Diffie Hellman Key swapping algorithm.

vi. Successful exploration of threat issues and strategies for security issues of bluetooth and WLAN using an elliptic curve cryptography.

vii. Proposing mathematical model to the technique of WLAN and security issues of Bluetooth using an elliptic curve cryptography.

viii. Implementation of security issues of WLAN’s using elliptic curve cryptography. We have simulated the security issues of WLAN’s using space time processing especially using Alamouti code.

ix. The WLAN’s security standards are implemented by using RC4.

6.4. Scope for Future Work

The research work presented in this thesis could be extended in many folds. Indeed to the best of my knowledge, this is the first attempt towards the representation of security issues of bluetooth using an elliptic curve cryptography by the use of:

i. Digital Signature Algorithm (DSA),

ii. Man in the middle attack (woman in the middle attack),

iii. Mathematical model using diffie hellman and RSA algorithm.

and thus, the presented research work is expected to open up a new avenue for exploiting the applicability of AES, DES, linked lists, sorting algorithms, primitive and non primitive data structures etc., for the better design, performance, evaluation as well as Security scenarios in Bluetooth.

The first goal was to study the history of bluetooth, security issues of bluetooth, threats concerned to the idea of bluetooth etc. The second goal was to
identify the implementation of security issues of bluetooth using a mathematical model, DSA algorithm.

There is still a task for future research which needs to be undertaken regarding performance, design, implementation issues of bluetooth. Current study focused on some of the bluetooth security mechanisms, however there are more security issues of bluetooth which can be studied further.

**Few features for future studies are covered below:**

i. This research work is biased on security issues of WLAN and bluetooth using an elliptic curve cryptography could also extended to other divide and conquer techniques, back tracking, branch and bound, greedy technique, back tracking idea.

ii. Computing performance issues of security issues of bluetooth using an Elliptic Curve Cryptography and WLAN could be measure Throughput, End-to-End Delay, Packet Loss Rate (PLR) (Packet Drop Rate) and CPU utilization time.

iii. Another area of study would be to implement security issues of bluetooth using bubble sort, selection sort, merge sort, heap sort, quick sort, radix sort and also try to calculate best case, average case and worst case time complexities.

iv. Security issues of bluetooth are calculated by Advanced Encryption Scheme (AES) and Data Encryption Standard (DES) algorithms.

v. It also possible to implement security issues of WLAN and bluetooth algorithms using non primitive data structures such as stack, queue, double ended queue (Deque), priority queue and various linked lists such as single linked lists, double linked lists, circular linked lists, reversing a linked lists concepts.

vi. We can also extended how to compute the various security issues of bluetooth using various kinds of pointers such as near, far and huge pointers in C and C++ languages.

vii. The interesting topic such as security issues of bluetooth also supports how to measure security of various WLAN components using IPSec (Internet Protocol Security).
While pursuing our research study various goals were identified and presented. The main focus of this study was to identify and calculate the security and performance issues of bluetooth using an elliptic curve cryptography.

Finally we can conclude numerous methodologies to propose security issues of bluetooth using elliptic curve cryptography. However it is a daunting responsibility to bring it all together into a comprehensive implementation of the security issues of bluetooth using elliptic curve cryptography for our research work.

A comprehensive study has been carried on diverse security issues of bluetooth. Investigation reveals that no unique solution exists for security issues problem in a WLAN. The applicability of solutions for security ideas of bluetooth varies according to the different types threat’s occurs due to network or system. Different security issues will be appropriate for different requirements of a system in different networks at different points. The critical analysis carried out here along with the advantages and disadvantages of each security mechanism provided in this research work can form the basis for the choice of security methodology. Discussed parameters such as encryption/decryption/man in the middle attack /women in the middle attack, advanced encryption scheme/data encryption Scheme needs to be carefully weighed in the final selection of the best security scheme for bluetooth using an elliptic curve cryptography.