ABSTRACT

In this thesis, the authors address the problem of Algorithms for Wireless LAN for Secured Transmission. In the last few years communication technology has been growing quickly. The focus was on how to connect communicating devices in a flexible, secure, reliable, cheap, and simple way. The ordinary solution was to connect devices with cables to make data exchange and devices synchronization is possible. But the cable solution often is complicated and reduces the flexibility of communication, so that wireless technologies become the finest solution for the cable replacement problem. To reach this objective there are some other objectives to be achieved in terms of how to compare the basic features like Security, Data Throughput and Computation time with well known and commonly used algorithms. Here, concentration is done on the Bluetooth Security. This thesis mainly considers the security of short range Wireless communication equipments. As discussed above one more important aspect of security development specifically in Bluetooth is to design an efficient implementation of opted procedures consisting of their basic elements and interaction. There are so many similarities between WLAN and WPAN therefore they can merge into an individual technology known as WLANs. The main focus of this research work is on the security of WLAN’s provided through Bluetooth security and Elliptic Curve Cryptography. In this research work we are designing and implementing efficient algorithms for Bluetooth Security using Elliptic Curve Cryptography (ECC). The term efficient specifies to design or an implementation which results in a good balance between cost, power consumption and performance. Performance is one which indicates time necessary for performing the task in question. A Cryptography is a case in which it has assumed secure by using a set of procedures or cryptography is generally believed to be secure against computationally bounded adversaries or beneficial attacks against the procedures are not known.

The research work also proposes an overview of some of the major attacks that Bluetooth has faced over the years along with some possible solutions. The main aim of this research work also investigates security features of Bluetooth using Elliptic Curve Cryptography (ECC). The ECC is the latest and fastest encryption method which offers stronger security. As the authors know that although a vast majority of devices already currently now communicates using Bluetooth methodology. The Bluetooth Security experts provide automatic updates to its
security protocol and user privacy protection technique for every security breach so that protection of the device user’s personal information becomes the primary aim. The research work also explores the Bucket brigade attack on Bluetooth security using Elliptic Curve Cryptography (ECC). As the authors know that Bucket Brigade Attack (BBA) is one of the amazing solutions to the problem of key agreement or key swapping. The beauty of this scheme is when two parties who like to communicate using symmetric key and an elliptic Curve Cryptography an Intruder (Hacker) enters in between a Sender and Receiver.

The research work mainly focuses on the security issues of Bluetooth using elliptic curve Cryptography.

**The research work super scribes the following issues:**

i. The first aim of this research work is to evaluate security threats in Bluetooth enabled security devices. This research work mainly shows keen concentration on practical aspects of Bluetooth. The authors have roughly sliced security issues of Bluetooth into this section.

ii. In the first section we are concentrating on the weaknesses of Bluetooth security based on literature review and a Bluetooth Security Laboratory situation for implementing Bluetooth Security attacks in practice has been originate.

iii. A comparative analysis of the existing Man (Woman) in the Middle Attack on Bluetooth is presented an innovative system for determining and preventing intrusions in Bluetooth networks is proposed and further classification of Bluetooth enabled ad-hoc network is provided.

iv. Different types of attacks against Bluetooth Security are investigated and the feasibility of the some of them is demonstrated in the research lab.

v. The objective of this research work has been to develop designs and implementations for efficiently realizing and maintaining Study of Algorithms for Wireless LAN’s using Bluetooth Security and an Elliptic Curve Cryptography (ECC).

vi. This research work also implemented Security issues of Bluetooth based on Digital Signature using Elliptic Curve Cryptography (SBECDSA) using Mat lab.
vii. The authors have also implemented Security issues of Bluetooth based on Digital Signature Authentication using Elliptic Curve Cryptography (SBECDSA) and compare the encryption and decryption time required to convert any fixed length character and variable length character using different key sizes.

viii. Implementation of Security issues of WLAN’s using Space Time Processing in Digital Signal Processing (DSP). Research work has simulated the security issues of WLAN’s especially using Alamouti code.

ix. Research work has implemented the Security of WLAN’s using WLAN standards such as RC4.