CHAPTER 4

METHODS TO IMPROVE SECURITY IN WLAN

4.1 Introduction

In the previous chapter, various security vulnerabilities of WLAN are presented briefly. The broadcast nature of WLAN makes it very much susceptible to intentional or unintentional interference by unauthorized persons. As per the data available in 2006, 48% of U.S. enterprises with more than 200 employees have installed WLAN. 75% of educational institutes, 68% of Retail shops, 68% of Manufacturing Units and 65% of Government offices in U.S. use WLAN in 2006 [70].

Some people use Firewalls and Virtual Private Networks [VPN] to protect from WLAN threats. As WLAN signals can bypass all wired-side security, they are not useful. As the wireless networks run on risk, one way is to stop working with Wireless Networks. From corporate executives to students use laptops and they are badly in need of wireless networks to quick transfer of data wherever they are. So, Wireless Networks are very much required for people in business and education.

To ascertain security for WLAN, few techniques and methods are being implemented. In this chapter, such techniques are to be explained in detail.

4.2 Password Protection

The first and simple method of improving security to a network is providing password for the users. It is possible to crack the passwords by brute force method or by analyzing the signals [5]. People used to write the password in books to remember it. The information in the book may be accidentally or intentionally viewed by another person. He can login with the known password into the network. It has been proved the password protection
cannot provide the required security. It may be one of the security levels in Wireless Networks but it is not providing complete security for WLAN.

4.3 ‘SSID’ and ‘MAC’

There is a requirement to find some techniques which can provide security to Wireless Networks to the level of satisfaction. There are some simple methods which are given as ‘Advices’ to the WLAN users [71]. The first of this kind is to change the default Extendable Service Set Identifier [ESSID]. The default setting can be changed into a combination which cannot be easily guessed or identified by malicious user. Then the AP is to be configured in such a way that it should not broadcast ESSID. In this method, only authorized persons can connect with the AP. The second level of security is the Medium Access Control [MAC] address filter. A MAC Address is unique identity of any network adapter when it is manufactured. AP maintains a list of MAC addresses which can be permitted to connect with it. When the WLAN network is set, all eligible MAC addresses are to be entered in the list of AP. When there is a change in the network adapter, the modified data is to be entered in the list.

4.4 Encryption Standards

Even if hackers cannot go past the AP, they can get data when it is transmitted. To protect data in transit, the encryption techniques are being used. IEEE 802.11a and IEEE 802.11b worked with Data Encryption Standard [DES] algorithm. Wireless Equivalent Privacy [WEP] is the initial security standard proposed by IEEE for the Wireless Networks. This algorithm was broken easily within few minutes. IEEE proposed Wireless Protected Access [WPA] as their next security standard and then WPA-2 or IEEE 802.11i was proposed. Advanced Encryption Standard [AES] based on Rijndael algorithm was adapted as the new security standard for WLAN.

Generally, by passively analyzing the pattern or by capturing the data for a brief period, it is possible for the intruder to find the password used. It is also possible to find the keys of
the encryption used. So even the encryption can be easily broken if we leave enough signal for the intruder to capture and analyze. For example in WEP, all encrypted packets use the first 24 bits for initialization and the remaining as data. So for 64 bit encryption provides approximately one trillion combinations. This can be easily broken with the help of modern computers within few minutes. If the encryption key is doubled, approximately 20 trillion combinations are available which can be broken with relatively longer time [7].

Key size can be increased further. With the powerful computers and versatile software available today, these encryption keys can be broken easily. The only issue here is with the increase in the key size, there is a need of more packets to be passively monitored to break the key. It also requires more time.

With encryption turned ‘ON’, the transmission data rate of WLAN is reduced. This is considered as the price to be offered to enhance security of the wireless network. Few companies are not willing to switch ‘ON’ encryption to have better throughput. So, they switch ‘OFF’ encryption. The security of those networks is at stake in this scenario. If outsiders receive these signals, they can monitor and retrieve data without any difficulty.

4.5 Wi-Fi Firewall

Implementation of VPN or encryption technologies such as WEP, WPA and VPA2 cannot counteract the effects of rogue APs, mis-configured APs and soft APs. Conventional security systems cannot detect MAC spoofing, Honeypots and Denial of Service. A new security solution called Wi-Fi Firewall which comprises of wireless sensor devices is required. Wi-Fi Firewall can monitor the wireless activity in the vicinity of the company premises, identify harmful WLAN transmissions, prevent transmission that cause security concern and locate devices. Wi-Fi firewall has five key features:

- Planning WLAN RF Coverage
- Detecting WLAN Transmissions
iii. Classifying WLAN Transmissions
iv. Protecting against intrusion
v. Locating WLAN Devices

4.6 Intrusion Prevention

An Intrusion Prevention system monitors the activity and the happenings in the related free space. It ensures that security policies are followed by the communication within the WLAN. It informs the administrator when a security violation exists. This system detects the rogue AP in the vicinity and locates it using ‘Triangulation’ method. Once detected, the rogue AP is isolated and then it is physically removed from the system.

The intrusion prevention system should provide flexibility to the network administrator. For example, the ‘permission to access’ given to an executive should be allowed even he is working from home. When the network is expanded, the intrusion prevention system should also be expanded to the desired extent.

Intrusion prevention is enhanced if the system has mobile detection ability. In WLAN environment, users move around from one location to another. Users can get dead spots without realizing it. So, on the spot readings and analysis should be done by intrusion prevention systems.

4.7 ‘No’ Signal to Intruders

Most of the hacking can be avoided if the signal which is wirelessly propagating from an AP is not available to the intruders. In this proposed work, an effort is being made to keep the signal confined to the intended region so that it is not available to the intruders. This may be considered as the first level of security for WLAN. This can also be considered as the security at the physical layer level for WLAN. Generally, the hacking of wireless networks is done for fun with available resources and these people are known as passive eavesdroppers who are large in numbers. It is possible to avoid this type of
incursions to wireless networks with the restriction of transmitted signal within the required region. This can be accomplished with the help of directional antennas which are also playing the role of sector antennas so that more security can be achieved by limiting the transmitted wave within the required region [2]. With the advent of modern antenna fabrication techniques, smart antennas are also used for providing security to WLAN as it shapes the radiation beam to the desired direction and avoids transmission in other direction [10]. If the direction of the major beam is to be changed, it can be changed easily by programming rather than by physical modifications [8].

4.8 Biometrics

To work along with the above said method, more security features can be added to WLAN. The concept of implementing biometric features along with the encryption techniques can be used to provide better security to WLAN. The biometric features such as fingerprint, face and iris are unique to a person. They have been used for identification purposes. Thumb impressions of the culprits are used by police for long. With any of the biometric feature, the identification of the person can be carried out by server [50].

Unique keys can also be extracted from the biometrics features. These keys can be used as key for encryption algorithm which is used for WLAN. As these keys are unique, unless this uniqueness is known, it is impossible for intruders to intervene the network [49]. There are several algorithms used to derive key from corresponding biometric features such as face [52] [57], Iris [53], hand [54], voice [55], keystrokes [60], handwritten signatures [56] and fingerprints [65] [66]. The encryption done with any one the above specified methods can give better security for WLAN.

4.9 Conclusion

WLAN is essential for modern business. Each and every company which employs WLAN is aware of its problems also. More than anything, security of WLAN is greatly at
stake. If WLAN is not dependable, it is difficult to make use of it for sensitive information transfer.

There is a requirement to improve security of WLAN. The encryption standards which are adopted by IEEE are trying to provide security as much as possible. But still there are few persons trying to overcome these standards.

In this fourth chapter, few methods which are being used to improve security of WLAN such as Password protection, MAC filter, SSID information and Firewalls are discussed.

The concept of providing ‘No’ signal to the intruders staying outside the region of intended coverage is discussed in section 4.7. This is an area where much concentration is required. The design of antennas which works as AP of WLAN is important issue to address this problem.

Generally WLAN operates with omni-directional antennas which radiate in all directions. So, transmitted signal can travel in unwanted direction also which may help intruders. This antenna is to be replaced by directional antenna which transmit signal only in the intended direction. As the signal is not traveling at all directions, unauthorized persons can not access the signal.

In this proposed work, design of a directional antenna which can work as AP of WLAN is to be discussed. To begin with various antennas and their parameters are presented in the next chapter.