CHAPTER 2

INTRODUCTION TO WIRELESS LAN

2.1 Introduction

Wired Local Area Networks [LAN] are used extensively as it makes the administration of systems easier. Here the location of system is fixed. When mobility of the system is considered as the next advancement in wireless communication, Wireless Local Area Networks [WLAN] came into the picture.

WLAN is flexible data communication system that can be used for applications where mobility is required. WLANs can provide data rate of 54 Mbps or higher.

2.2 Radio Frequency bands for WLAN

![Electromagnetic spectrum](image)

<table>
<thead>
<tr>
<th>Frequency (Hz)</th>
<th>Wavelength (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3 \times 10^5$</td>
<td>$3 \times 10^6$</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Long wave radio</td>
<td>AM broadcast</td>
</tr>
<tr>
<td>$10^{-1}$</td>
<td>$10^{-2}$</td>
</tr>
</tbody>
</table>

**Typical Frequencies**

- AM broadcast band: 535–1605 kHz
- Short wave radio band: 3–30 MHz
- FM broadcast band: 88–108 MHz
- VHF TV (2–4): 54–72 MHz
- VHF TV (5–6): 76–88 MHz
- UHF TV (7–13): 174–216 MHz
- UHF TV (14–83): 470–890 MHz
- US cellular telephone: 824–849 MHz
- European GSM cellular: 880–915 MHz
- GPS: 1575.42 MHz
- Microwave ovens: 2.45 GHz
- US DBS: 11.7–12.5 GHz
- US ISM bands: 902–928 MHz, 2.400–2.484 GHz, 5.725–5.850 GHz
- US UWB radio: 3.1–10.6 GHz

**Approximate Band Designations**

- Medium frequency: 300 kHz to 3 MHz
- High frequency (HF): 3 MHz to 30 MHz
- Very high frequency (VHF): 30 MHz to 300 MHz
- Ultra high frequency (UHF): 300 MHz to 3 GHz
- L band: 1–2 GHz
- S band: 2–4 GHz
- C band: 4–8 GHz
- X band: 8–12 GHz
- Ku band: 12–18 GHz
- K band: 18–26 GHz
- U band: 26–40 GHz
- V band: 40–60 GHz
- E band: 60–90 GHz
- W band: 75–110 GHz
- F band: 90–140 GHz

Fig 2.1 Electromagnetic spectrum
Figure 2.1 shows the Electromagnetic spectrum. This spectrum has wide range of frequencies from few KHz to more than 100 GHz. Out of the entire length of spectrum, WLAN is allowed to operate in few bands only.

WLAN uses Infrared light [IR] or radio frequencies [RF]. RF is widely used because of its longer range, higher bandwidth and wider coverage.

WLANs are designed to operate in Industrial, Scientific and Medical [ISM] radio bands and unlicensed-national information infrastructure [U-NII] bands.

<table>
<thead>
<tr>
<th>Band (GHz)</th>
<th>Bandwidth (MHz)</th>
<th>Power Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.902–0.928</td>
<td>26</td>
<td>1W</td>
</tr>
<tr>
<td>2.4–2.4835</td>
<td>83.5</td>
<td>1W</td>
</tr>
<tr>
<td>5.725–5.850</td>
<td>125</td>
<td>1W</td>
</tr>
<tr>
<td>24.0–24.5</td>
<td>250</td>
<td>50 mW/m @ 3 m</td>
</tr>
</tbody>
</table>

Fig 2.2 Industrial, Scientific and Medical radio bands

Fig 2.2 shows various bands of frequencies with which WLAN can operate. Their corresponding Bandwidth and Power level are also given.

WLAN uses 2.4 GHz and 5 GHz frequency bands which are reserved for unlicensed devices. Wireless networking provides the freedom and flexibility to operate within and between any buildings. There is no requirement of users to physically attach with the network. The User is expected to have a handheld device or a laptop at which RF interface card is installed. The user can get connected through a PC card slot of a laptop also. The connection from the wired backbone system to the users exists through Access Point [AP] which can connect multiple users simultaneously. AP is placed at any point of the wired network and it works as a gateway for the users who are connected wirelessly. The operating range of WLAN depends on usage and the environment of the entire system.
WLAN can also operate without backbone wired networks. They can be used to connect more than one computer together without a wired network. This is known as ad-hoc mode. A license-free part of Electromagnetic spectrum, 2.4 – 2.45 GHz is used for this purpose. International Telecommunication Union [ITU] announced the above said band as license-free so that multiple devices are operating in this band around the world.

IEEE 802.11 Committee and ‘Wi-Fi’ alliance worked together to develop a standard for WLAN. With the introduction of these standards, wireless technology supports the data rate and interoperability necessary for WLAN operation. The first generation WLAN devices with their low speeds, high cost and lack of standards were not quite useful for many applications. With the introduction of new standards, data rate is increased and the cost is reduced.

### 2.3 Benefits of WLAN

The benefits offered by WLANs are given below:

i. Mobility

ii. Scalability

iii. Flexibility

iv. Short and Long term cost savings

v. Installation advantages

vi. Reliability in harsh environments

vii. Reduced Installation time.

viii. Mobility within Enterprise.

ix. Older buildings, Temporary sites.

x. Line of Sight [LOS], Building-to-Building Bridge.

The Internet Service Providers [ISP] are now getting connected through wireless service providers. These ISPs are called as Wireless Internet Service Providers [WISP]. WLANs do not replace the need for traditional wired routers, switches and servers in a wired LAN.
2.4 Evolution of WLAN

The first WLAN technologies are of low speed of 1 to 2 Mbps. But the freedom to roam and flexibility of wireless allowed these products to find a place in the market. Many of these early wireless technologies are still used because data collection devices do not require high data rates.

In 1997, IEEE released the 802.11 standard for Wireless Local Area Networking which allows transmission through air. The signaling technologies include the following:

i) IR Light

ii) Three types of radio transmissions within the Unlicensed 2.4 GHz frequency bands:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Orthogonal Frequency Division Multiplexing (OFDM)

iii) One type of radio transmission within the unlicensed 5 GHz Band:

- Orthogonal Frequency Division Multiplexing (OFDM)
  
  IEEE 802.11 a.

Spread Spectrum is a modulation technique which spreads its spectrum over wide range of frequencies so that it is less susceptible to noise and interference. This is considered as a feature to support the security mechanisms of the wireless networks.

There are several standards released by IEEE on Wireless Networks. The IEEE 802.11 is the first such standard released. It is the slowest standard based on RF and Light Technologies.
IEEE 802.11b uses 2.4 GHz as the transmission frequency. It has faster data rate and it is widely promoted as Wi-Fi by the ‘Wifi’ alliance. It is the modified version of IEEE 802.11 standard. The IEEE 802.11b standard provides new Physical layer known as Complementary Code Keying [CCK] to support data rates of 5.5 and 11 Mbps.

Texas Instruments developed IEEE 802.11b+ based on a modulation technique called Packet Binary Convolution Coe [PBCC]. The signaling rates are 22 and 33 Mbps.

IEEE 802.11a has faster data transfer compared with IEEE 802.11b. But it lacks backward compatibility. The IEEE 802.11a is based on OFDM transmission that operates at 5 GHz. The IEEE 802.11a and b MAC layer is the same as that of the other IEEE 802.11 standards.

IEEE 802.11g is the modified standard based on original IEEE 802.11 standard. The data rate is as faster as IEEE 802.11a but it is also backward compatible.

IEEE 802.11g+ is introduced by Texas Instruments. This standard interoperates fully with both IEEE 802.11a and IEEE 802.11g standards.

IEEE 802.11e is developed to support Quality of Service [QoS]. It improves the capability and efficiency for applications such as voice, video and audio transport over wireless networks

Interoperability between different vendor WLAN devices is possible with the IEEE 802.11f standard.

IEEE 802.11h adds indoor and outdoor channel selection for 5 GHz for bands. This enhances the channel energy measurement. This standard reduces interference using Dynamic Frequency Selection and power management is improved with Transmit Power Control.
IEEE 802.11i is the standard developed to provide network security. It uses Temporary Key Integrity Protocol [TKIP] encryption as the algorithm used to provide better network security. It has pre-authentication and encryption based on Advanced Encryption Standard [AES] algorithm.

IEEE 802.11k defines radio resource measurements for WLAN. Both the terminal and the access points can make requests for information from their peers and make decision on their status.

IEEE 802.11n defines standardized modifications to both 802.11 Physical Layers [PHY] and the Medium Access Control Layers [MAC]. This standard is capable of providing throughput of 100 Mbps. It maintains interoperability with 802.11a and/or 802.11g devices.

IEEE 802.11r standard targets to minimize terminal transfer from one access point to another. It is desirable to achieve faster Basic Service Set [BSS] transition time which is compatible with applications such as Voice over Internet Protocol [VoIP]. The security features are not to be affected in this standard.

The above said standards are being followed world wide to have uniformity among the products of WLAN by various vendors.
2.5 Architecture for WLAN

2.5.1. Reference Architecture

Fig. 2.3 shows the Infrastructure and Ad-hoc topologies which are different types of configurations of IEEE 802.11 standard. In the Infrastructure configuration, wireless terminals are connected to a backbone network through AP. In the Ad-hoc configuration, terminals communicate in a peer-to-peer basis.

AP provides access through the wireless medium. The basic service area is the coverage area of one AP. The Basic Service Set [BSS] is a set of stations controlled by one AP. The distribution system is the wired infrastructure used to connect a set of BSS to create an extended service set [ESS].
A number of wireless communication devices such as laptops are connected through WLAN to a backbone wired LAN. Each laptop carries an interface card which helps to connect with AP. Laptops connect to the wired LAN through AP and it can communicate with other devices through the server.

A Peer-to-Peer (Ad-Hoc) Topology is a wireless set which contains two or more Computers, each with a wireless cord. This configuration is not having an access point. It is known as Independent basic service set (IBSS). A laptop can be connected to a main computer or with many computers to share information. Coverage limitations are the drawback of this topology as everyone must be able to hear everyone else.

2.5.2 Layered Protocol Architecture

<table>
<thead>
<tr>
<th>Layer</th>
<th>Entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Link Layer</td>
<td>LLC</td>
</tr>
<tr>
<td></td>
<td>MAC</td>
</tr>
<tr>
<td></td>
<td>MAC Management</td>
</tr>
<tr>
<td></td>
<td>Station</td>
</tr>
<tr>
<td>Physical Layer</td>
<td>PLCP</td>
</tr>
<tr>
<td></td>
<td>PHY Management</td>
</tr>
<tr>
<td></td>
<td>Management</td>
</tr>
<tr>
<td></td>
<td>PMD</td>
</tr>
</tbody>
</table>

Fig 2.4 shows the entities in the protocol stack of the IEEE 802.11 standard. The Physical [PHY] and Medium Access Control [MAC] layers are broken into their sub layers. The MAC layer is divided into MAC sub layer and MAC management sub layer entities. The MAC sub layer is responsible for access mechanism, fragmentation & reassembly of packets. The MAC layer management sub layer is responsible for roaming in ESS, power management and association, dissociation & re-association processes for registration and connection management. The PHY layer is divided into three sub layers: PHY layer...
convergence protocol [PLCP], PHY medium dependent protocol [PMD] and the PHY layer management sub layer. The PLCP is responsible for carrier sensing assessment and forming packets for different PHY layers. The PMD sub layer specifies the modulation coding technique for signaling with the medium and PHY layer management decides on channel tuning to different options for each PHY layer. The station management sub layer is responsible for coordination of the interactions between MAC and PHY layers.

2.6 Applications for WLAN

The development of Wireless technology helps in the following sectors:

i) Manufacturing
ii) Healthcare
iii) Retail
iv) Education
v) Banking and Financial
vi) Military

2.7 WLAN Challenges and issues

Some of the challenges and issues involved with WLAN are given below:

2.7.1. Radio signal Interference and degradation

An important challenge in WLANs is the radio signal interference. Number of wireless devices is operating in the unlicensed band. Changing channels is the best possible way to avoid interference. Other electronic devices such as portable phones, Microwave Owens, Wireless Speakers and security devices are operating in the unlicensed band of 2.4 GHz. As this band is more crowded with availability of the above mentioned devices, interference caused in this band is also more. Physical objects and building structures are also causing various levels of interference.
It is possible for the Electromagnetic Interference [EMI] generated by non-radio equipments which are placed vary close to the wireless devices cause interference in them. The EMI signal affects the components of the transmitter. To minimize the effects of EMI, radio equipments should be isolated from the potential EMI sources.

2.7.2 Power Management

Power consumption is an important issue with wireless devices such as laptops and Personal Digital Assistants [PDA] as the power and battery have limited life period. There are three power saving modes available with the PC cards of few commercial vendors:

1) Constant Awake mode [CAM]
2) Power Save mode [PSP]
3) Fast Power save mode [FastPSP]

2.7.3 Interoperability

Most vendors are interested in having only their APs and Network Interface Cards [NIC] to be used by the customers. They do not want their products to match with other brands. In a closed network such as corporate network, single vendor system has an edge. In an open environment such as University system, single vendor operation is not feasible. In this situation, there is a requirement for the products from various vendors should be operated with proper interconnection.

2.7.4 Network Security

Network security is the prime concern for wireless networks. Researchers had already exposed several limitations of wireless networks such as authentication, data privacy and message integrity mechanisms. The threat of Intruders from outside or inside the
organization is getting increased. Attackers called “war drivers” drive around the streets continuously to look out for insecure WLANs and hack their networks and data.

IEEE introduced Wired Equivalent Privacy [WEP] as the first security standard. But it is having its own limitations and it was proved it can be broken in a quick time by capturing the packets for a short duration. IEEE then introduced Wireless Protected Access [WPA] and later on WPA2 or IEEE 802.11i. This standard uses Advanced Encryption Standard [AES] algorithm with Temporal Key Integrity Protocol [TKIP] and Message Integrity Code [MIC] protocols. But still the wireless networks are vulnerable and more sophisticated security mechanisms are badly required.

2.7.5 Reliability and Connectivity

WLAN improves the reliability of the packet transmission to be at the same level as that of wired Ethernet. Transmission Control Protocol / Internet Protocol [TCP/IP] protects the network against the loss of data over air.

Wireless networks are having limitations against connection issues in changing environments such as obstacles, reflection and scattering of signals. The choice of the antenna and the mounting locations are to be selected carefully to avoid interference. Lack of guaranteed bandwidth is causing problem for certain nodes in Wireless networks.

2.7.6 Installation and Site Design Issues

Before installing wireless devices, a proper survey of the site is to be carried out. The parameters which are to be considered for the survey are component configuration, placement and physical environment. In a point to point bridging scenario, mountains, curvature of the earth, buildings and other man-made objects, trees are the obstructions which are considered a force to reckon with.
Data rates, Antenna type, Placement of antenna, Physical environments, obstructions, Building materials and line of sight are few of the operating and environmental conditions that are needed to identify with.

2.7.7 Health Issues

The exposure of humans to RF radiation is a serious health issue. Non-ionizing radiation of radio emissions cause some health problems to the humans. As most of the antennas are directional, the hazardous emission levels are only at the front part of the antenna. High gain, wall-mount antennas are designed and installed at the locations at a minimum distance of 30 cm from everyone.

Mobile phones are considered as a radiation source which is close to the human. Research is going on world wide to find the extent of health problems related with usage of mobile phones. Though, it is not yet proved that mobile phones can cause cancer and related diseases, the amount of heat generated can definitely a major concern to people who are using it for long hours.

2.8 Conclusion

Wireless LAN is widely used throughout the world because of its easiness. The WLAN products are manufactured by various vendors across the globe and it is readily available at a moderate cost. From high profile corporate offices to university buildings, WLAN is in use. In this chapter, various types of WLAN standards are discussed. The types of architectures of WLAN are also explained. The applications of WLAN are given.

The challenges and issues of WLAN are also discussed in this chapter. The most important issue is security of WLAN. This is to be covered extensively in the next chapter.