NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Computer Engineering

Theory and Application of Wireless LANs

GRADUATION PROJECT
COM 400

Student: Hamzeh Ahmad. (20032653)

Supervisor: Prof.Dr.Doğan Ibrahim.

Nicosia-2005

ACKNOWLEDGMENTS

Foremost and More over I want to pay special regards to my family who are enduring these all expenses and supporting me in all events. I am nothing without their prayers. They also encouraged me in crises. I shall never forget their sacrifices for my education so that I can enjoy my successful life as they are expecting, I will never forget my father, my mother, my brother and my sisters. They may get peaceful life in Heaven.

I also would like to express sincere gratitude to my project advisor Prof. Dr. Doğan Ibrahim for his invaluable advice and for the generosity he exhibited with his time and effort over this project.

I would like to publicly thank all the individuals who contributed to this project. Certainly, the successful completion of this document would not have been possible without the valuable input and review feedback from all of the N.E.U staff especially Prof. Doğan Ibrahim. Several individuals provided extra effort.

Thank you all for your special effort.

I hope this project proves worthy of your trust and hope that it can be useful for other student to have information they need from it.

ABSTRACT

Wireless Communication is an application of science and technology that has come to be vital for modern progress. From the early radio and telephone to current devices such as mobile phones and laptops, accessing the global network has become the most essential and indispensable part of our lifestyle. Wireless communication is an ever-developing field, and the future holds many possibilities in this area. One expectation for the future in this field is that, the devices can be developed to support communication with higher data rates and more security. Research in this area suggests that a dominant means of supporting such communication capabilities will be through the use of Wireless LANs. As the deployment of Wireless LAN increases well around the globe, it is increasingly important for us to understand different technologies and select the most appropriate one.

This project provides a detailed study of the wireless LAN.

TABLE OF CONTENETS

ACKNOWLEDGMENT.....I
ABSTRACT.....II
TABLE OF CONTENETS.....III
INTRODUCTION.....VI
Chapter 1.....1
Introduction to Wireless Local Area Network.....1
1.1 Introduction.....1
1.2 What is a WLAN?.....2
1.3 WHY A WIRELESS LAN?.....3
1.4 How WLANs Work?.....3
1.5 Using of WLANs.....4
1.6 Advantages OF Wireless LANs:.....4
1.7 Disadvantages OF Wireless LANs:.....5
1.8 Components OF Wireless LANs:.....7
1.9 Topology of Wireless LANs:.....8
1.10 Types of Wireless LANs:.....9
1.10.1 An ad-hoc or peer-to-peer wireless network:.....9
1.10.2 Infrastructure wireless network:.....9
1.10.3 Independent WLAN Using Access Point as Repeater:.....11
1.11 Applications of WLAN:.....11
1.12 Security.....12
1.13 The standards relating to Wireless LANs.....13
1.14 Which standard to choose.....13
1.15 WLAN Issues.....15
1.15.1 Security.....15
1.15.2 Performance.....18
1.16 Implementing a WLAN.....19
1.16.1 Planning.....19
1.16.2 Site survey.....20
1.16.3 Positioning APs.....20
1.16.4 Power over Ethernet (PoE).....21
1.17 Network Management.....21
Chapter 2.....23
Technology and implementations of Wireless (LANS).....23
2.1 INTRODUCTION.....23
2.2 Wireless LAN Technology's.....24
2.2.1 Radio Technologies.....24
2.2.2 Infrared Data Association (IrDA) Technology.....27
2.3 Wireless LAN Technologies Difficulties.....31
2.4 The standards relating to Wireless LANs.....32
2.4.1 Current standards.....33
2.4.2 Future standards.....36
2.5 Roaming.....38

2.6 Types of (APs) access points: 40
2.6.1 Dedicated hardware access points (HAP): 40
2.6.2 Software Access Points: 40
2.7 Implementation and Configuration of Wireless LAN 41
2.7.1 A wireless peer-to-peer network 41
2.7.2 Client and Access Point 42
2.7.3 Multiple Access Points. 42
2.7.4 Extension Point. 43
2.7.5 LAN to LAN Wireless Communications 44
2.7.6 The use of directional antennas 45
2.8 Customer Considerations 45
2.8.1 Range and coverage 45
2.8.2 Throughput 46
2.8.3 Integrity and Reliability 46
2.8.4 Compatibility with the Existing Network 47
2.8.5 Interoperability of Wireless Device 47
2.8.6 Interference and Coexistent 47
2.9 Licensing Issues 48
2.9.1 Simplicity/Ease of Use 48
2.9.2 Security 49
2.9.3 Cost 49
2.9.4 Scalability 49
2.9.5 Battery Life for Mobile Platforms 49
2.9.6 Safety 50
2.10 Summary 50
Chapter 3 51
Security of Wireless Local Area Networks 51
3.1 Introduction 51
3.2 Why secure the WLAN? 52
3.3 How much security is enough? 52
3.4 Security Threats and Types of Attacks 53
3.4.1 Active Attacks: 54
3.4.2 Passive Attacks: 55
3.5 Security Standards 56
3.5.1 HIPERLAN 56
3.5.2 IEEE 802.11 58
3.6 Security Mechanisms 61
3.6.1 Built in 802.11b mechanisms 61
3.6.2 Non 802.11b built-in security 63
3.6.3 How it works 64
3.7 Emerging 802.11 security standards. 64
3.7.1 IEEE 802.11i Enhanced Wireless Security standard. 64
3.7.2 Wi-Fi Protected Access (WPA). 65
3.8 Vulnerabilities of standard 802.11 security 66
3.9 Security solutions for today's 802.11 WLAN 67
3.9.1 IEEE 802.1X Port Based Network Access Control 67

3.9.2 LEAP....71
3.9.3 AirFortress....73
3.10 The Future of wireless security: 802.1x....75
3.11 Summary....75
Chapter 4....76
Applications of Wireless Local Area Networks....77
4.1 INTRODUCTION....77
4.2 How Wireless LANs Are Used in the Real World....78
4.3 Applications of WLAN in Government Organization....79
4.3.1 Traveling Workers:-....79
4.3.2 State and Local e-Government:-....79
4.3.3 Extending Availability:-....79
4.3.4 Designing and Planning for Rapid Growth....80
4.3.5 Financial Services:-....81
4.3.6 Working toward the Bottom Line....81
4.4 Application of WLAN in Manufacturing....82
4.4.1 Wi-Fi the Easiest to Install....83
4.4.2 Flexible Access Makes Life Easier....83
4.4.3 Internet Connection Sharing....84
4.4.4 Printer Sharing Increases Usability....85
4.4.5 Terminal Emulation....86
4.4.6 Direct Database Connectivity....86
4.4.7 Wireless Middleware....87
4.5 Applications of WLAN in Health Care Organization....88
4.6 Applications of WLAN in Education and Research Organization....89
4.7 SUMMARY....91
CONCLUSIONS....92
REFERENCES....93
Glossary....95
LIST OF ABRIVIATIONS....99

INTRODUCTION

Wireless LANs use electromagnetic airwaves (radio and infrared) to communicate Information from one point to another without relying on any physical connection. The Data being transmitted is superimposed (modulated) onto the electromagnetic airwaves and delivered to the receiving end. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. The Radio signal occupies more than a single frequency, since the frequency or bit rate of the Modulating information adds to the carrier. To extract data, a radio receiver tunes in one Radio frequency while ignoring all other frequencies. In a typical WLAN configuration an access point, this is outfitted with a transceiver Device connects to the wired network at a fixed location. At a minimum, the access point Receives, buffers and transmits data between the WLAN and the wired network Infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The access point (or the Antenna attached to the access point) is usually mounted high but may be mounted

While wireless networking has several advantages over a traditional wired LAN, it introduces security risks that a wired LAN is not susceptible to. Without a robust wireless security solution, organizations leave themselves vulnerable to attack through their WLAN. Although malicious attacks are a non-controllable reality, companies can take action to integrate a solid wireless security solution that prevents unauthorized users from accessing confidential company information.

This project is about Wireless LANs. The project investigates the Wireless LAN theory, the standards associated with Wireless LAN systems, the security of Wireless LANs, and the typical applications of Wireless LANs.

Chapter 1 is an introduction to Wireless LANs. The theory and the standards of Wireless LAN systems have been investigated in this chapter.

Chapter 2 is about the technology and the implementation of the Wireless LAN systems. The components of a typical Wireless LAN system have been described in this chapter and examples of typical implementations are given.

Chapter 3 investigates the important issue of the security in Wireless LAN systems. The chapter describes how security can be implemented in such a system and recommendations have been made to secure a Wireless LAN system.

Chapter 4 is about the applications of Wireless LAN systems. A variety of application areas are given in this chapter and it is shown that currently Wireless LAN systems are used in most LAN based computer applications.

Chapter 1

Introduction to Wireless Local Area Network

1.1 Introduction

A wireless local area network (WLAN) is an adaptable data communications system Implemented as an extension to or as an alternative for a wired local area network.WLANs act as reduce the need for wired connections and makes new applications Possible by combining data connectivity with user mobility and adding new flexibility to Networking. Using radio frequency (RF) or infrared (IR) technology, wireless LAN Transmit and receive data over the air, minimizing the need for wired connections.

Today, wireless LAN technology is relatively mature. A variety of applications have been identified and addressed and technologies that enable these applications are well understood. Chip sets (a key enabling technology) aimed at WLAN implementations and Applications are emerging in the market.1 Mobile WLAN users are able to access Information and network resources from remote locations as they attend meetings, Collaborate with other users, or move to other campus/office locations. However, the benefits of WLANs extend beyond user mobility and productivity. With WLANs, the network itself is movable. Temporary networks can be set-up when anywhere they are required and dismantled just as conveniently.

WLANs have proven their effectiveness in vertical markets and are now experiencing Broader applicability in a wide range of business settings, including the health-care, retail, Manufacturing, warehousing, and academic communities. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to Transmit real-time information to centralized hosts for processing. Today wireless LANs Are becoming more widely recognized as a general-purpose connectivity alternative for a Broad range of business customers. The key marketing challenge remains the education of potential customers in the effective use of wireless LANs as a vehicle to enhance the Capabilities of their networks.

1.2 What is a WLAN?

A wireless local area network (WLAN) is two or more computers joined together using radio frequency (RF) transmissions. This differs from a wired LAN, which uses cabling to link together computers in a room, building, or site to form a network.

Although WLANs can be independent they are more typically an extension to a conventional wired network. They can allow users to access and share data, applications, internet access or other network resources in the same way as wired networks.

Currently, Wireless LAN technology is significantly slower than wired LAN. Wireless LANs have a nominal data transfer rate of between 11 and 54 Megabits per second (Mbps) compared to most wired LANs in schools which operate at 100Mbps. Newly installed wired networks can now operate at up to 1,000Mbps (1Gb).

Wireless LANs are typically used with wireless enabled mobile devices such as notebook computers, PDAs and Tablet PCs. This allows users to take advantage of the flexibility, convenience and portability that WLANs can provide.

There are several wireless technologies in existence, but most wireless LANs use wireless Ethernet technologies based on IEEE 802.11 standards (see: Current Standards).

The term Wi-Fi (Wireless Fidelity) is often used to refer to 802.11 wireless networks. It comes from the testing and certification programmer run by the Wi-Fi Alliance (see below) to ensure wireless products from different manufacturers comply with standards and are interoperable.

1.3 WHY A WIRELESS LAN?

By using radio frequencies instead of conventional wires, WLANs enable organizations to realize flexibility and real-time access to information for people who need to be connected. The ease and speed of connecting and disconnecting wireless devices gives organizations a reliable, scalable and easy-to-integrate tool to increase productivity and save money. In today's ever-changing workplace, a Wireless LAN combines the power of freedom and information so people can access the resources of corporate information, the Internet and e-mail wherever and whenever they need it.

1.4 How WLANs Work?

Wireless LANs use electromagnetic airwaves (radio and infrared) to communicate Information from one point to another without relying on any physical connection. The Data being transmitted is superimposed (modulated) onto the electromagnetic airwaves And delivered to the receiving end. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. The Radio signal occupies more than a single frequency, since the frequency or bit rate of the Modulating information adds to the carrier. To extract data, a radio receiver tunes in one Radio frequency while ignoring all other frequencies. In a typical WLAN configuration an access point, this is outfitted with a transceiver Device connects to the wired network at a fixed location. At a minimum, the access point Receives, buffers and transmits data between the WLAN and the wired network Infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The access point (or the Antenna attached to the access point) is usually mounted high but may be mounted

Essentially anywhere that is practical as long as the desired radio coverage is obtained.4End users access the WLAN through wireless-LAN adapters. Adapters can be fitted out as PC cards in notebook computers, ISA or PCI cards in desktop computers, or integrated into hand-held computers. WLAN adapters provide an interface between the clients Network operating system (NOS) and the airwaves (via an antenna).

1.5 Using of WLANs

Wireless LANs frequently augment rather than replace wired LAN networks often when a wired network and the mobile user. Mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- **In business:** WLANs are increasingly being installed by business to provide flexible access, or for specific tasks such as stock taking in warehouses.
- **In the wider community:** Wireless networks can be used for public access to the Internet. Commercially available public access wireless networks are more commonly known as 'hotspots' and there are now thousands of these throughout the UK; located at railway stations, airports, hotels, in certain public libraries, in cafes and eating establishments, and at underground stations in London.
- **On transport:** Several airlines have in-flight WLAN availability.
  Wireless access is available on certain trains in many countries of the World. In the UK, several train operators have started on board wireless services

1.6 Advantages OF Wireless LANs:

With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following advantages:

- **Mobility**: Wireless LAN systems can provide users access to real-time information anywhere within the organization. This extra mobility supports productivity and service opportunities not possible with wired networks.

- **Flexibility & Scalability**: Deploying a wireless network eliminates the need to pull wires or cables through walls and ceilings. Wireless LAN gives organizations the flexibility to move people from office to office, re-organize departments or even

entire campuses almost effortlessly. Once Wireless LAN base units are located strategically throughout building, users simply insert an adapter card into their computer and are free to move about.

- **Cost Savings**: With the simple and flexible architecture of WLAN, organizations can save network management costs related to adds, moves and changes, guaranteeing a short term return on investment.

- **Installation Speed and Simplicity:** Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

1.7 Disadvantages OF Wireless LANs:

- **Less secure than wired LANs:** Wireless introduces some additional security problems beyond those associated with a wired network (which a wireless LAN shares). Considerable effort has gone into providing security to meet these problems, and a more detailed discussion is provided below. Some of the key issues are highlighted here. The signal from a wireless LAN will pass through walls, which means hackers do not even need to be inside the premises to access the LAN. If they can make use of the wireless LAN they are on the college or university network. Once inside, hackers can monitor the traffic on the network and so acquire user names and passwords. These are normally encrypted, but there are some doubts about the effectiveness of encryption.

- **Standards are still evolving:** The standards for wireless LANs are still evolving and not always compatible with one another. A number of different standards are used or defined by organizations which sometimes communicate only with themselves. Europe has been working on some standards for use in the EU, while the IEEE, based in the US, has been defining worldwide standards.

- **Management of the network is more complex:** There are a number of issues associated with managing wireless networks which add to the complexity of network management in a mixed wireless and wired LAN environment. These include the need to manage the wireless LAN as a single subnet if roaming is to work,

- **Cost of network cards:** While cards for wired Ethernet start at around £10, wireless cards start at around £60. Although they will become cheaper, they will never be as cheap as wired LAN cards because they are inherently more complex. How the wireless part of the LAN relates to the rest of the network and managing security. With modern wireless LANs management is for the most part undertaken centrally. However, some changes need to be made at the access points themselves.

- **Network performances degrades with additional users:** If many users are connected to the LAN via the same access point, the performance of the LAN can degrade quite rapidly by comparison with wired Ethernet systems. This is because the available bandwidth is shared between all the users, and because of the nature of the communications protocols needed to support wireless working. The overheads associated with setting up each message are much larger for wireless LAN than for a wired LAN, and the protocols enforce waiting times (of microseconds) at certain points. The decline in network performance is particularly great when two PCs are hidden from each other (for instance at opposite sides of the cell) but both are trying to communicate with the access point at the same time, so corrupting each other's messages.

- **Multi-path fading:** can be caused by signals bouncing off walls and other surfaces. As the signal is transmitted to the receiver a reflection of the signal may take slightly longer to arrive and will interfere with the original transmission; it may even arrive out of phase and cancel out the signal all together. Antenna diversity attempts to solve this problem, it involves having two antennas built into the

hardware, and allows the system to determine which signal is stronger and therefore the correct signal.

1.8 Components OF Wireless LANs:

802.11 defines two pieces of equipment, **a wireless station**, which is usually a PC equipped with **a wireless network interface card (NIC),** and an **access point (AP)**, which acts as a bridge between the wireless and wired networks. An access point usually consists of a radio, a wired network interface (e.g., 802.3), and bridging software conforming to the 802.11d bridging standard. The access point acts as the base station for the wireless network, aggregating access for multiple wireless stations onto the wired network. Wireless end stations can be 802.11 PC Card, PCI, or ISA NICs, or embedded solutions in non-PC clients (such as an 802.11-based telephone handset).

An 802.11 WLAN is based on a cellular architecture. Each cell (BSS) is connected to the base station or AP. All APs are connected to a Distribution System (DS) which is similar to a backbone, usually Ethernet or wireless. All mentioned components appear as an 802 system for the upper layers of OSI and are known as the ESS.

The 802.11 standard does not constrain the composition of the distribution system; therefore, it may be 802 compliant or non-standard. If data frames need transmission to and from a non-IEEE 802.11 LAN, then these frames, as defined by the 802.11 standard, enter and exit through a logical point called a Portal. The portal provides logical integration between existing wired LANs and 802.11 LANs. When the distribution system is constructed with 802-type components, such as 802.3 (Ethernet) or 802.5 (Token Ring), then the portal and the access point are the same, acting as a translation bridge.

The 802.11 standard defines the distribution system as an element that interconnects BSSs within the ESS via access points. The distribution system supports the 802.11 mobility types by providing logical services necessary to handle address-to-destination mapping and seamless integration of multiple BSSs. An access point is an addressable station, providing an interface to the distribution system for stations located within various BSSs. The independent BSS and ESS networks are transparent to the LLC Layer

1.9 Topology of Wireless LANs:

In a typical Wireless LAN configuration, a transmitter/receiver (transceiver) device, called an Access-Point (APs), connects to the wired network. This Access-Point is the actual interface between the wireless users and the wired backbone, receiving, buffering and transmitting data between the Wireless LAN and the wired network infrastructure. A single Access-Point can support a small group of users and can function within a range of up to one hundred meters.

End users access the Wireless LAN through wireless-LAN adapters, which are implemented as PC cards in notebook or palmtop computers (Wireless NIC cards), as PCI/ISA cards in desktop computers, or integrated within hand-held computers and laptops.

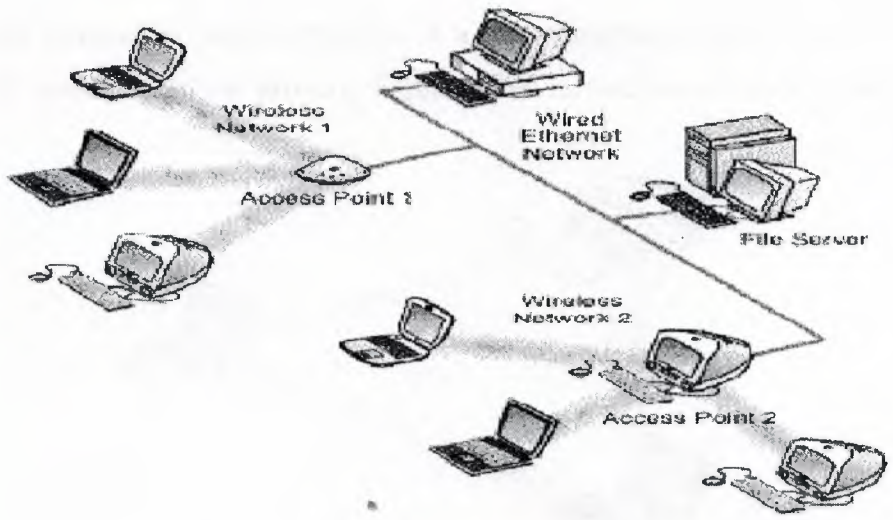

Figure1.1: WLAN topology

1.10 Types of Wireless LANs:

1.10.1 An ad-hoc or peer-to-peer wireless network:

Ad-hoc network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. (This is called "bridging")

Ad-hoc networks are the simplest form of wireless network created by two or more wireless enabled computers communicating with each other directly. These types of WLANs are useful for creating small dynamic networks. However, these ad-hoc networks have similar limitations as wired peer to peer networks and are only really suitable for occasional, small networks of a few computers. Ad-hoc networks cannot provide the same security as properly implemented infrastructure mode networks

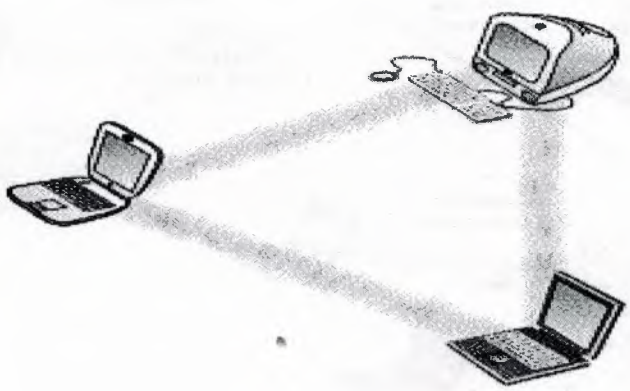

Figure 1.2: Ad-Hoc or Peer-to Peer Networking.

1.10.2 Infrastructure wireless network:

Can also use an access point (APs), or base station. In this type of network the access point (APs) acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

Requires one or more access points (APs) through which the network cards communicate. In a typical wireless LAN, a transmitter/receiver (transceiver) device, called an access point, is normally physically connected to the wired network using standard Ethernet cabling. It acts as a bridge between the wired network and the remote computer(s). At a minimum, the access point receives, buffers, and transmits data between the wireless LAN and the wired network infrastructure, using radio frequencies to transmit data to each user.

Access points can have a varying amount of intelligence and functionality built-in. There are two main types of AP. "Thick" APs are fully functional and can handle all processes. "Thin" APs only include radios and antennas and rely on controllers (WLAN switches/appliances) for other functionality including managing APs, security and authentication. There is also a third hybrid category with some limited radio frequency management functionality, but that still need controllers to function fully.

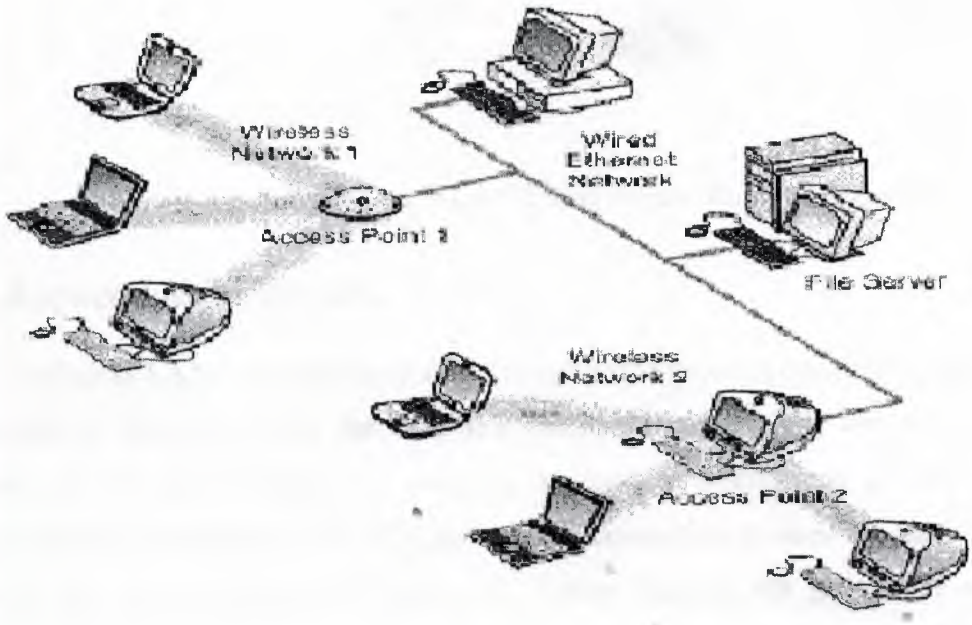

Figure 1.3: Infrastructure wireless network

1.10.3 Independent WLAN Using Access Point as Repeater:

Access points can extend the range of ad-hoc LANs by acting as a repeater, effectively doubling the distance between wireless PCs (See Figure 1.3).

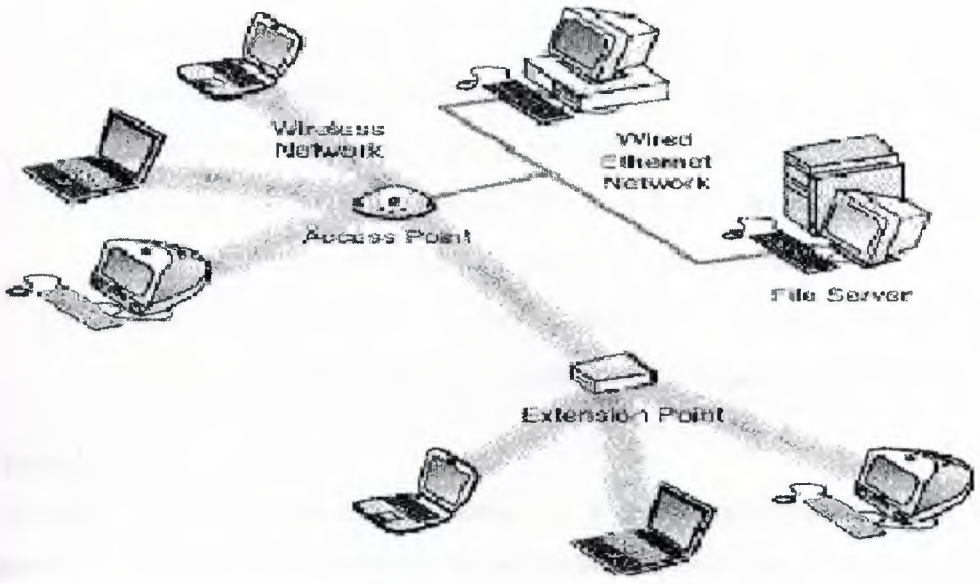

Figure 1.4 Independent WLAN Using Access Point as Repeater

1.11 Applications of WLAN:

Wireless LANs are frequently added to the wired network rather than being used to replace it, often providing the final few meters of connectivity between a wired network and the mobile user. The ongoing decrease in pricing and the increase of integrated WLAN technology in PCs and mobile computing devices by many leading network and mobile computing vendors is further fuelling the growth of wireless networking at home, in the enterprise environment and also in public spaces like hotel lounges & airports.

The following list describes some of the many applications made possible through the power and flexibility of Wireless LANs:

- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks and other changes with Wireless LANs.

- Network managers installing networked computers in older buildings find that Wireless LANs are a cost-effective network infrastructure solution.
- Wireless LANs are the ideal solution for temporary networks on exhibitions and seminars.
- Warehouse workers use wireless devices to exchange information with central databases, thereby increasing productivity.
- Network managers implement Wireless LANs to provide backup for mission-critical applications running on wired networks.
- Office workers can roam from meeting to meeting throughout the building, remaining constantly connected to the enterprise network

1.12 Security

Security is one of the major issues in wireless networking. In a wired environment in a building, someone has to get inside the building to make a physical connection with a client to the existing network before he can access the network resources.

Because Wireless LAN works with radio signals, the physical connection is not necessary. Someone standing outside the building could (if the Access Points are not configured properly) make a connection to the network resources by intercepting the radio signals. Although this is possible, it is not that easy. Different measures exist to prevent unauthorized access to the network via Wireless LAN. The eventual goal of these measurements is a secure access to the network for valid users.

There are basically three approaches to securing access to an 802.11b network:

- Built in 802.11b mechanisms:
- Virtual Private Network-based (VPN) security solution
- 802.11X security standard

1.13 The standards relating to Wireless LANs

The Institute of Electrical and Electronics Engineers (IEEE) is the leading authority in the specification and ratification of standards relating to technology. Current Wireless standards have originated from the IEEE; thus IEEE 802.11a, IEEE 802.11b etc.

In the field of wireless LAN there are currently three main operational standards: IEEE 802.11a, 802.11b and 802.11g. There are also a number of other standards relating to security, functionality and interoperability. Further WLAN standards are still in development. For example the 802.11e Quality of Service (QoS) standard is expected by mid 2005 and the IEEE has set up a Working Group to develop the 802.11n standard for higher bandwidths over wireless LAN.

1.14 Which standard to choose

The choice of which wireless standard to deploy will be based on a range of factors including: what equipment is already in use; the size of area to be covered by the network; the number of users to support; the applications to be used on the network; environmental conditions; and any interference present. A site survey (see below) will help determine some of these factors.

Manufacturers now provide dual mode and tri-mode equipment (access points, NICs), which support 802.11a/b, 802.11a/g and 802.11a/b/g. whilst slightly more expensive, this does provide considerable flexibility.
Most new notebook, laptop and tablet PCs ship with wireless connectivity as standard. Schools should consider this when purchasing new equipment and ensure that it is compatible with their existing wireless set up.

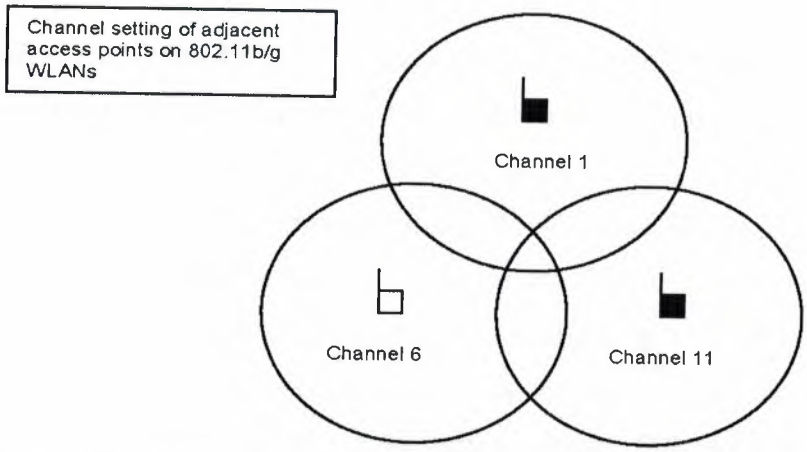

Figure 1.5: Channel setting of adjacent access points on 802.11 b/g WLANs

As 802.11b/g and 802.11a operate in a different frequency range they are not compatible with each other. However, 802.11b/g and 802.11a networks can be used side by side to increase capacity.

In general both 802.11b and 802.11g (as they work in the 2.4GHz frequency) have a greater range than 802.11a. In practice, to obtain the same network coverage, the user may require up to four times as many access points when using an 802.11a network. This may be more expensive as not only do you require more access points, but 802.11a access points are still currently more expensive than both 802.11b and 802.11g devices. However, the smaller range and greater number of channels of 802.11a allow more access points to be used in any given area improving network performance. The 5GHz frequency of 802.11a is also less congested than the 2.4GHz frequency used by 802.11b/g, reducing the chance of interference.

Schools or organizations that have already deployed 802.11b networks have several choices if they want to improve their wireless data rates:

- Increase the number of APs in order to lower contention ratios
- Build a new 802.11a wireless LAN alongside/replacing their existing 802.11b network
- Purchase new dual or tri band access points to allow for equipment with different wireless cards to co-exist

- Purchase Wi-Fi approved 802.11g equipment

If schools want to run a mixed 802.11b/g network there are a couple of issues relating to data rates notably that the actual data rates for 802.11g devices drop in the presence of 802.11b equipment. If 802.11g devices and 802.11b devices are in dialogue with each other then the data rates will be dictated by the 802.11b device. If two or more 802.11g devices are in dialogue with each other but there are 802.11b devices in the same network, then 802.11g data rates will drop but may well still be more than the practical rates of 802.11b. There are 802.11g access points, or dual or tri-band access point incorporating 802.11g which can be set to only recognize 802.11g equipment. This obviously prevents the 802.11b equipment from working on the 802.11g network but there are times when this may be desirable.

1.15 WLAN Issues

1.15.1 Security

Wireless LAN security problems have been widely publicized and have been a key barrier to take up. Security is always a balance between perceived risks and costs. Various factors need to be considered including the vulnerability of the network, the threat of attack, the value of the data to be secured and the costs involved. Securing WLANs, as with all networks, needs to be seen as a continuous process rather than a one-off step. Any security solution needs to be consistently and properly implemented with regular monitoring.

Anyone with a compatible wireless device can detect the presence of a wireless LAN, however if appropriate security mechanisms are put in place, this does not mean that they can access any data. The wireless LAN should be configured so that anyone trying to access the wireless LAN has at least the same access restrictions as they would if they sat down at a wired network workstation. Schools should be implementing a comprehensive security policy and incorporating standards like WPA/WPA2. However, there are a number of other security measures that can be taken.

All the suggestions below are practical steps that schools can put in place to improve wireless LAN security. A school can:

- Ensure that the devices with WEP security are upgraded to WPA/WPA2 where possible and that the encryption is enabled. WPA provides a high level of security for a wireless network. If an upgrade to WPA is not possible, schools should ensure that WEP is enabled.
- Educate users about security and implement an organization wide policy, Ensure that users know not to plug in their own access points that could leave the network open
- Restrict access to the Wireless network by only permitting devices with a recognized MAC (Media Access Control) address. Every computer has an individual alphanumeric identifier known as a MAC address. Within the software accompanying the access point, there is an Access Control List, which as its name suggests, controls access to the network. The access point can be configured to only permit recognized devices. This only gives an additional layer of security to the network; it is not a secure solution in itself as MAC addresses can be easily "spoofed". It should be noted that the management of these ACLs can become burdensome in larger networks.
- Change the default Service Set Identifier (SSID or network name) and administrator passwords. (SSID is the method wireless networks use to identify or name an individual wireless LAN.) Access points may be set to broadcast the SSID; this should be turned off where possible. This only adds an additional layer of security and is not a solution in itself. On access points where this is not possible, the network name can be made less recognizable by including non alphanumeric characters (like _*# etc)
- Avoid wireless accessibility outside buildings where it is not required; directional aerials can be obtained to restrict the signal to 180° or 90° from the access point.
- Switch off the power to the access point(s) 'out of hours' makes the wireless LAN unavailable at those times.
- Make sure that the network is regularly checked to ensure that only legitimate wireless access points and devices are connected to the network. This can be done by walking around with a wireless device and

software tools like nets tumbler.

- Put the Wireless LAN into its own DMZ so that all wireless nodes pass though a firewall to access the educational network.
- The security measures a school would consider for a standard LAN implementation can also be incorporated in to a WLAN (e.g. installing a firewall, using a DMZ, administrator file restrictions etc).
- Implement firewalls on client devices.
- Regularly update the firmware of all wireless equipment.
- Incorporate a Virtual Private Network (VPN). A VPN is a secure private network that uses a public network like the Internet to connect remote sites or users together. Anyone wishing to access files on the WLAN would first need to log on to the network via the VPN using a User name and Password. Data sent between the client device and the network is secure as it is encrypted / decrypted using VPN encryption. A VPN for wireless would provide a relatively high level of security for a school. Users would need to ensure they use sensible (i.e. not obvious) Password and Log-on details otherwise this level is security is easily compromised.

Several companies now offer third party security tools and management systems. These can provide various functions such as intrusion detection systems (IDS) that actively monitor airwaves for rogue access points/devices and disable any found. Some systems can limit the area from which devices are allowed to connect to the network using location based technology. These solutions add to the cost of WLAN deployment.

1.15.2 Performance

It is important to remember that transmission speeds for all wireless LANs vary with file size, number of users, distance from the access point, the environment and any interference present.

As the distance from the access point increases, the nominal data rate for 802.11a and 802.11g standard equipment drops from 54Mbps to 48, 36, 24, 18, 12, 9, or 6 Mbps. 802.11b standard equipment drops from 11Mbps to 5.5Mps, 2Mbps or 1Mbps. It is possible to boost the range of some access points by installing specialized antennae. Wireless clients will only send data when other devices are not transmitting. Interference from other wireless signals can cause clients to wait before sending data or cause dropped packets that have to be retransmitted, slowing down the network.

The environment of a WLAN can also affect the range and throughput. Buildings with many girders, thick walls, and concrete will often shorten the effective range and there may be areas that are effectively 'dead zones'. Water, glass and paper can also reduce a network's range.

1.15.3 Prices

The cost of access points depends on the quality and on built-in functionality, and includes:

- The quality of the antennae
- Antennae directionality
- Encryption included in the access point
- Whether the access point has DHCP (Dynamic Host Configuration Protocol – allows automatic assignment of IP addresses to new devices on the network) built in
- DSL access (which allows internet access direct from the access point) this is designed for small home network or small business use
- The number of user devices that can be listed in the Access Control Lists; is the number limited and if so is it sufficient for your network?
- The ability to centralize the control and management of access points

over the network

- Whether the access point can act as a bridge between other access points and the network
- Support for Power over Ethernet (PoE)

Enterprise class access points are significantly more expensive than consumer/SOHO class devices. They tend to include more features, more robust radios and better support and management tools.

Prices for WLAN equipment have fallen significantly in a short period. Access points are available from between £40 and £800. Wireless cards for notebooks start at around £10. In general 802.11a equipment is slightly more expensive than 802.11b of 802.11g. However, Multiband access points and cards that support 802.11a/b/g are increasingly common and as a result prices for 802.11a connectivity should continue to fall.

1.16 Implementing a WLAN

1.16.1 Planning

As wireless network technology has matured there has been a proliferation in manufacturer offerings of both equipment and management tools.

There are various factors that need to be considered before deploying a wireless network. These include what it is to be used for, the requirements for applications intended to be run on the network, the number of users and the size and location of the area to be covered. It is also important to have a good understanding of the technologies and standards involved.

It is recommended that a small pilot wireless network is set up to test applications and use before widespread deployment.

WLANs vary in their size and complexity. Schools may decide to cover a small area such as classroom/classrooms or to have blanket coverage over a wide area or entire site. The amount of coverage can be increased over time, but clearly defined aims need to be set out at the start of any WLAN project. Alternatively, many schools use "mobile" APs instead of fixed APs. These are usually fitted to a laptop trolley, which can be wheeled into a classroom and connected to a free network port. This provides an

inexpensive way of delivering wireless connectivity to a suite of laptops, which can be moved around the school. However, it does not provide the flexibility of "blanket" wireless coverage and relies on there being fixed wired network ports in classrooms.

1.16.2 Site survey

To determine the location of access points for infrastructure networks, it is recommended that a site survey is undertaken by a specialist. A site survey will also determine the number of access points required to give the desired coverage, the range of each access point, and its channel designation, signal strength and the presence of interference.

Before a site survey is undertaken, it is advisable to prepare a floor plan to show where coverage is required. Precise details should be sought from suppliers of 'network coverage' and 'data transfer rates' particularly towards the edge of the coverage area.

You should specify the level of coverage you require, as a supplier's definition may be as low as 1Mbps. It is also a good idea, if possible, to ensure that the site survey is carried out with the equipment anticipated to be used in the school. It is also advisable to build in some redundancy to provide better performance and reliability. This can be achieved with extra access points or by moving access points closer together.

For schools upgrading or adding to an existing 802.11b wireless network, a further site survey may be required since the coverage is likely to be different when compared to 802.11b. More access points may be required to maintain or improve data rates.

1.16.3 Positioning APs

The access point, or the antenna attached to the access point, will usually be mounted high in a classroom or in the ceiling space However, an access point may be mounted anywhere that is practical as long as the desired radio coverage is obtained. Larger spaces generally require more access points. APs will also need a power supply and these needs to be taken into consideration when planning the location and cost of installations. It is advisable for electrical installations to include remote power switches, so that APs in awkward locations can be easily powered down or rebooted.

1.16.4 Power over Ethernet (PoE)

Many enterprise class access points now support Power over Ethernet. Power over Ethernet (PoE) is a network standard (IEEE 802.3af) for sending DC power over data cabling to provide power for networked devices. PoE allows for greater flexibility in WLAN deployment as infrastructure can be installed in places away from power outlets and easily moved to meet requirements. Another key consideration is potential cost savings on installation and management. Using PoE devices reduces the financial and time costs of employing a qualified electrician to install mains sockets and cabling. The reduction in wiring and lack of mains voltage can also improve safety. Although PoE can be used over existing fast Ethernet Cat 5 and Cat 6 cabling (currently not gigabit Ethernet), the costs of mid-span PoE expansion modules, UPS, power supply units (PSU) and air conditioning to cope with the extra heat are not insignificant. PoE is not yet a widely used technology and the costs are a barrier to take up. However, it could be considered for larger WLAN deployments.

1.17 Network Management

Schools will need to allocate resources for network management in the same way as they would for a wired network. Tasks such as configuring MAC and IP addresses, changing security keys, managing radio strength, monitoring network performance, upgrading access points and generally ensuring system integrity, will need to be undertaken on a relatively regular basis.

Most access points will allow a certain amount of configuration, usually via a browser interface. In networks of more than a handful of access points, manual configuration of APs can become unmanageable. Enterprise class APs provide some management tools and will often allow some remote management using Simple Network Management Protocol (SNMP) via Management Information Bases (MIB). However, these management tools are proprietary and rely on all APs being from the same vendor. Alternatively, third party management and WLAN monitoring tools that can work with products from a variety of manufacturers are increasingly available.

The Wi-Fi Alliance is considering introducing a new certification for Wi-Fi equipment to make setting up secure wireless networks easier. Imposing easy to use

setup schemes on Wi-Fi equipment is seen as important for the increasing number of non-technical users using the technology. Some vendors have already introduced proprietary set-up solutions. The WFA has set up a working group to look at the problem.

Chapter 2

Technology and implementations of Wireless (WLANS)

2.1 INTRODUCTION

A wireless local area network (WLAN) is a flexible data communications system implemented as an extension to or as an alternative for, a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, wireless LANs combine data connectivity with user mobility.

Wireless LANs have gained strong popularity in a number of vertical markets, including health-care, retail, manufacturing, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today wireless LANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers.

There are two types of WLANs, infrastructure WLANs and independent WLANs. Infrastructure WLANs, where the wireless network is linked to a wired network, is more commonly deployed today. In an infrastructure WLAN, the wireless network is connected to a wired network such as Ethernet, via access points, which possesses both Ethernet links and antennas to send signals. These signals span microcells, or circular coverage areas (depending on walls and other physical obstructions), in which devices can communicate with the access points, and through these, with the wired network. In a wireless LAN, devices can move within and between coverage areas without experiencing disruption in connectivity as long as they stay within range of an access point or extension point (similar to an access point) at all times

2.2 Wireless LAN Technology's

Manufacturers of wireless LANs have a range of technologies to choose from when designing a wireless LAN solution. Each technology comes with its own set of advantages and limitations.

2.2.1 Radio Technologies

Radio network technology exists in two forms: narrow band technology and spread spectrum technology. Narrow band systems transmit and receive data on a specific radio frequency; the bands are kept as close together as possible and sharp filters are used to filter out other signals to make efficient use of the bandwidth. In order to prevent different signals from interfering with each other, a regulatory body has been established to licence the frequencies and monitor their use. These licences are very expensive and in the past have prevented manufacturers from using narrow band technology: An example of a narrow band network would be a commercial radio station [In the early 1990s, the regulatory bodies around the world set aside a band at 2.4GHz (the Instrumental, Scientific and Medical band, ISM) for use by new technologies. However, 2.4GHz is just one in several ISM bands. The 40.66-40.7 MHz segment is another example of an ISM band, available for use by remote controlled devices such as alarms and door openers]. The bands can be used without a license making it more accessible for private networks. Consequently manufacturers soon started to produce products, which used the new bands, one of which is centered at 2.4GHz.

Spread spectrum technology spreads the signal over a range of frequencies preventing concentration of the signal in any one place. This allows large numbers of users to share the same bandwidth. There are two different methods involved in spread spectrum technology, Direct Sequence and Frequency Hopping, with both having advantages and disadvantages associated with them

2.2.1.1 Narrowband Technology

A narrowband radio system transmits and receives user information on a specific radio frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communications channels is avoided by carefully coordinating different users on different channel frequencies.

A private telephone line is much like a radio frequency. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. In a radio system, privacy and noninterference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency. From a customer standpoint, one drawback of narrowband technology is that the end-user must obtain an FCC license for each site where it is employed.

2.2.1.2 Low-Power Narrowband Technology

An alternative approach to spread spectrum that some wireless LAN vendors are using is to transmit narrowband signals at low-power levels, a method allowed by FCC CFR 15.249 rules. By transmitting at low-power levels, vendors do not have to use spread spectrum, which gives them the ability operate at higher data rates. RadioLAN's product uses this approach and operates at 10 Mbps in the 5.8-GHz band with 50 milli-watts (mW) of peak transmission power. The price of this higher performance is a reduced transmission range of about 30 meters (100 feet) in an office environment.

2.2.1.3 Spread Spectrum Technology

Most wireless LAN systems use spread-spectrum technology, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread-spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the

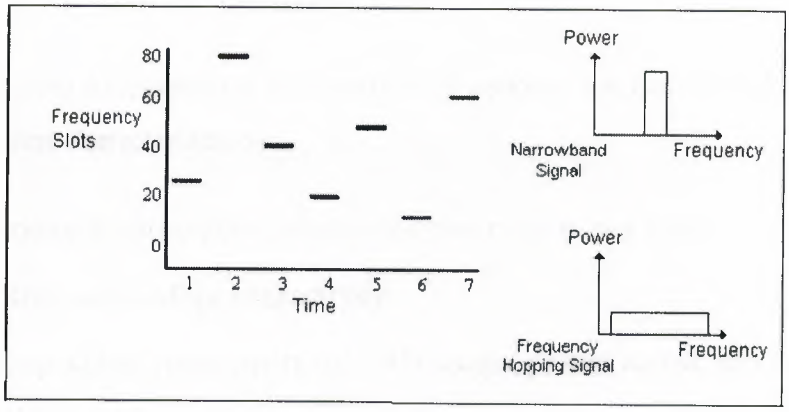

Figure 2.2: Frequency Hopping Spread Spectrum

2.2.1.6 HiperLAN Technology

HiperLAN, an abbreviation for Higher Performance Radio LAN, is a wireless technology standard developed by the European Telecommunications Standards Institute. It boasts very impressive capabilities, including a data rate of about 24 Mbps using a channel width of 23.5 MHz. In Europe, spectrum is available in the 5.15 to 5.3 GHz range, allowing for five separate channels. This type of throughput readily supports multimedia applications. Unfortunately, no commercial products are yet available. But the technology is under consideration for new spectrum in the United States in the 5-GHz band as part of the U.S. Unlicensed National Information Infrastructure band.

2.2.2 Infrared Data Association (IrDA) Technology

Infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide limited range of approximately 3 feet and typically are used for personal area networks. Occasionally directed systems are used in specific wireless LAN applications. High performance directed IR is impractical for mobile users and is therefore used only to

implement fixed sub-networks. Diffuse or reflective IR wireless LAN systems do not require line-of-sight, but cells are limited to individual rooms.

The Infrared Data Association is a consortium of vendors that has defined low- cost IR communications characterized by:

- Directional point-to-point communications of up to one meter
- 115-Kbps and 4-Mbps connectivity
- Walk-up ad hoc connectivity for LAN access, printer access, and portable computer to portable computer communications

Many laptops today include IRDA ports, though devices such as LAN access points and printers with IR capability are not yet very common. The IRDA estimates some 60 million IRDA ports in the market.

2.2.2.1 Direct Infrared Technology

Direct infrared light needs a clear line of sight to make a connection. The most familiar direct infrared communication device is the TV remote control. A connection is made by transmitting data using two different intensities of infrared light to represent the 1s and 0s. The infrared light is transmitted in a 30-degree cone giving some flexibility in orientation of the equipment, but not much. Some disadvantages exist with direct connections one of which is range, usually restricted to less then 3 meters. Also because it needs a clear line of sight, the equipment must be pointing towards the general area of the receiver or the connection is lost. However, advantages include low cost, and a high, reliable data rate.

In order to promote the use of direct infrared systems an organization called the Infrared Data Association (IrDA) has been established. IrDA is an association of over 130 companies, including IBM, Intel and Motorola, formed to create interoperable, low cost infrared data interconnection standards. The first of these standards (IrDA 1.0) supported data rates of 115.2Kbits/s, the newer standard (IrDA 1.1) now supports higher data rates of 1.15 & 4Mbps. Today most new laptop computers come with IrDA ports as standard as

well as printers and a whole range of network and access products designed to take advantage of the new technology.

What would appear to be a restrictive wireless technology is actually quite well suited to wireless LANs. The technology is ideal for creating a BSS network (ad-hoc or peer- to-peer network). As most laptops already have IrDA ports, users in a meeting would simply be able to point their laptops towards each other and the network would be formed. As far as infrastructure networks go, access points do exist which allow IrDA equipped laptop computers to connect directly to the network, although restrictions in range make roaming and true mobility a little difficult.

This does not necessarily rule out the use of direct infrared technology in wireless systems. An office for example which had access points liberally spread around on

Desks and benches would allow mobile users to sit down and connect without the inconvenience of having to plug in to the network. This forgoes the advantage of mobility during use. However, how many users are likely to type when walking around anyway? In addition, when one considers the cost, typically $150 per infrared access point compared with $300 per radio network card (which still requires a radio AP retailing at $1500 plus), the systems becomes more attractive.

Despite these advantages, in order for this technology to be useful as a replacement to traditional methods of connecting to a network the infrared link would have to perform at 4Mb/s the IrDA1.1 standard [9].

2.2.2.2 Diffuse Infrared Technology

Diffuse infrared technology operates by flooding an area with infrared light, in much the same way as a conventional light bulb illuminates a room. The infrared signal bounces off the walls and ceiling so that a receiver can pick up the signal regardless of orientation.

Diffuse infrared technology is a compromise between direct infrared and radio technology. It combines the advantages of high data rates from infrared and the freedom of movement from radio. However, it also inherits some disadvantages. For example, although it transmits at 4Mbits/s twice that of current radio systems, this must be shared among all

users, unlike direct infrared. And although a user can roam around freely, which is an advantage over direct infrared, the signal is still confined to individual rooms unlike radio signals, which can pass through walls.

Diffuse infrared technology is still in its infancy, and consequently there are very few manufacturers of this technology. One of the few is Spectrix Corp., which was established in 1987, and mainly designed and implemented wireless LANs for trading floors. The SpectrixLite system uses hemispheres mounted on walls or in ceilings to communicate with receivers which connect to portable computers using PCMCIA cards. The hemispheres are connected to a central hub that powers each hemisphere and acts as a bridge onto the wired LAN (See figure 2.3 below).

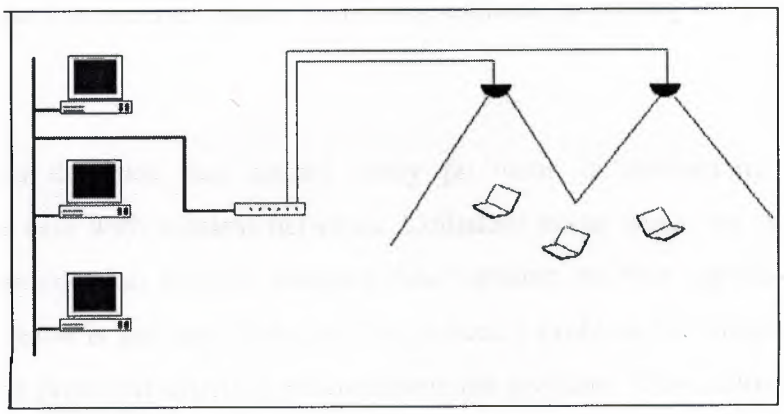

Figure2.3: Overhead Diffuse Infrared Hemispheres connected to A Network through a Hub

SpectrixLite uses a proprietary protocol called CODIAC (Centralized Operation Deterministic Interface Access Control). This protocol was tailor made to suit wireless networks and includes features, which conserve battery power, supports large numbers of users and can be tailored to various applications. The system guarantees service levels by offering different classes of data rate ranging from the lower of 1.2Kbit/s to 230.4Kbits/s and supports features of wireless LANs such as seamless roaming.

Diffuse infrared technology has begun to establish itself as a real alternative to radio in wireless LAN systems. However, lack of movement towards this technology by the large

networking manufacturers (IBM for example recently abandoned it's diffuse infrared product) has meant very few systems are commercially available. Those that do exist do not show the refinement of the radio systems produced by the large manufactures. Despite these initial problems, the technology has the potential to provide very high data rates and good coverage for most applications.

2.3 Wireless LAN Technologies Difficulties

Two types of technology exist to form a wireless LAN: radio and infrared. However, manufacturers using either of these technologies face the same problems when attempting to implement a wireless LAN solution. Multiple access protocols that enable devices to share a medium, such as Ethernet, are well developed and understood. Yet the nature of the wireless medium makes traditional methods of sharing a common connection more difficult.

Collision detection has caused many problems in networking and this is particularly the case with wireless networks. Collisions occur when two or more nodes sharing a communication medium transmit data together, the two signals corrupt each other, and the result is garbage. This has always been a problem for computer networks and the simplest protocols often do not overcome the problem. More complex protocols check the channel before transmitting data. This is very simple with Ethernet as it merely involves checking the voltage on the wire before transmitting. However, the process is considerably more difficult for wireless systems. It can take at least 30 to 50s to determine if the channel is clear, which is a long time when compared to the amount of time taken to transmit a packet.

Other problems exist with collision detection, the hidden terminal problem being one of them. In traditional shared medium networks if node A can hear node B and node B can hear node C, then node A can hear node C. In a wireless environment this is not a safe assumption. Obstructions and distance between A and C may cause C to be hidden from A with neither one detecting a collision when transmitting to B, causing the network to become unreliable.

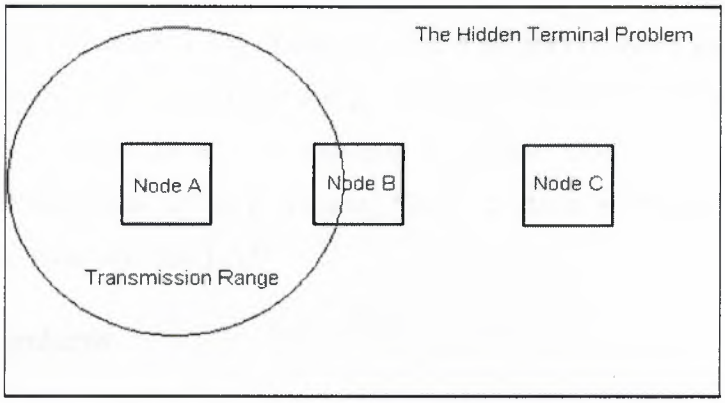

figure2.4: Collision Detection with a Hidden Terminal Problem

The solution to this problem, involves sending a Request To Send (RTS) packet to the intended recipient to prompt it to send back a Clear To Send (CTS) packet. This process informs any nearby stations that data is about to be sent, helping them to avoid transmitting and causing a collision. Both the RTS and the CTS packets contain the length of the impending data transmission so stations overhearing either of the packets know how long the transmission will take and when they can start to send themselves. Carrier sense is used to help prevent station transmitting RTS packets at the same time.

Another problem, known as mutlipath fading, can be caused by signals bouncing off walls and other surfaces. As the signal is transmitted to the receiver a reflection of the signal may take slightly longer to arrive and will interfere with the original transmission; it may even arrive out of phase and cancel out the signal all together. Antenna diversity attempts to solve this problem, it involves having two antennas built into the hardware, and allows the system to determine which signal is stronger and therefore the correct signal.

2.4 The standards relating to Wireless LANs

The Institute of Electrical and Electronics Engineers (IEEE) is the leading authority in the specification and ratification of standards relating to technology. Current Wireless standards have originated from the IEEE; thus IEEE 802.11a, IEEE 802.11b etc.

In the field of wireless LAN there are currently three main operational standards: IEEE 802.11a, 802.11b and 802.11g. There are also a number of other standards relating to security, functionality and interoperability. Further WLAN standards are still in development. For example the 802.11e Quality of Service (QoS) standard is expected by mid 2005 and the IEEE has set up a Working Group to develop the 802.11n standard for higher bandwidths over wireless LAN.

2.4.1 Current standards

2.4.1.1 IEEE 802.11b

802.11b is the most mature and widely deployed wireless network standard. It is also the standard used by most public wireless "hotspots". The 802.11b standard derived from the 802.11 standard, and was ratified by the IEEE in 1999.

- The 802.11b standard operates in the 2.4GHz spectrum
- Has a nominal data transfer rate of 11Mbps. In practice the actual data transmission rate is approximately 4-7Mbps, which is shared by all clients using an access point.
- Provides 3 non-overlapping channels (see below)

This is adequate for accessing most data or applications, including Internet access, but might be insufficient for multimedia applications or for instances when a large number of simultaneous users want to access data from a single access point.

The 2.4GHz frequency is also used by other electronic devices, notably Bluetooth devices, cordless telephones, microwave ovens and some lighting. 802.11b can encounter electromagnetic interference in the presence of these devices or other 802.11b equipment.

2.4.1.2 Wi-Fi Alliance (WFA)

Initially, not all 802.11b items of equipment were compatible with each other. To rectify this, an alliance of manufacturers and interested parties was set up (Wireless Ethernet Compatibility Alliance – (WECA). WECA officially changed its name to the Wi-

Fi Alliance in December 2002) and a distinct Wi-Fi certification mark was established.

In principle, any item with the Wi-Fi certification mark has been tested for compliance with IEEE standards and should be interoperable with other equipment (even from other manufacturers) bearing the Wi-Fi certification mark. In practice, this may not always be the case. It is advisable to ensure that all wireless equipment purchased is Wi-Fi certified.

The Wi-Fi mark has now been extended to the 802.11a and 802.11g standards and denotes that equipment of the same standard is compatible. The Wi-Fi label now also states which standard(s) is supported by that particular piece of equipment. From August 2003, to receive Wi-Fi approval, new 802.11b and 802.11g products were required to conform to the WPA (Wi-Fi Protected Access) security standard. This also applied to all 802.11a products from September 2003. The Wi-Fi Alliance began testing and issuing certificates for products conforming to WPA 2 (see below) in September 2004.

2.4.1.3 IEEE 802.11g

The 802.11g standard was ratified in June 2003 and the first devices to receive Wi-Fi approval were announced in July 2003. It is intended to offer the same data rates as 802.11a (54Mbps), whilst working in the same frequency range as 802.11b (2.4GHz) for backwards compatibility. 802.11g is widely used in consumer wireless equipment and has also been installed by many organizations.

802.11g:

- Operates in the 2.4GHz spectrum
- Has nominal data speeds of 54Mbps
- Has an actual data speed of 18-30Mbps. These drop to around 60% of the available data rate in the presence of 802.11b equipment
- Offers three non-overlapping channels (see below)
- Is backwards compatible with 802.11b equipment? (All Wi-Fi certified 802.11g equipment should permit the use of 802.11b equipment, however it is possible to

configure access points to only allow 802.11g clients.)

- Can suffer from interference from other devices in the 2.4GHz frequency
- 802.11g is less power efficient than 802.11g, so 802.11b may continue to be more common in some mobile devices such as PDAs
- Uses Orthogonal Frequency Division Multiplexing (OFDM), so benefits from some resiliency to RF interference and multi-path distortion

2.4.1.4 IEEE 802.11a

The 802.11a standard was ratified by the IEEE in 1999 and adopted in the USA and other parts of the World. However, 802.11a equipment was restricted in the UK and the rest of Europe because it uses the 5GHz frequency, parts of which are traditionally used by national governments for defense purposes. This slowed adoption of the standard, especially with the emergence of 802.11g. 802.11a was made available without license in February 2003. Band A for indoor use (5.15GHz to 5.35 GHz, 200mW EIRP3) and Band B for indoor and outdoor use (5.47 GHz to 5.725 GHz 1W, EIRP) are open for wireless LAN services.

Multiband a/g or a/b/g wireless cards are increasingly common and falling in price.
802.11a has:

- Nominal data rate of 54Mbps with actual rates of between 17-28Mbps.
- 802.11a has a signal range of about 50 meters from an access point and data rates begin to drop at a range of 10-15 meters from the access point (dependent on environment and equipment).
- The 802.11a standard uses OFDM
- The 5 GHz band provides much greater spectrum than the 2.4 GHz band. This results in 802.11a being able to deploy eight non-overlapping channels in the UK compared to only three in an 802.11b/g environment (see below)

802.11a is particularly suited to environments with multiple users using applications with high data throughput. In a school environment this might be a class group using multimedia, digital video, or database packages.

2.4.1.5 IEEE 802.11h

This is an addition to the 802.11a standard that meets European requirements for use of 5 GHz frequencies. It includes Transmit Power Control (TPC) to limit transmission power and Dynamic Frequency Selection (DFS) to protect sensitive frequencies. These changes protect security of military and satellite radar networks sharing some of this spectrum. It is possible to use 802.11h to reduce AP cell sizes to increase the density of AP coverage. The standard was finalized in September 2003 and has been included in some wireless equipment, but Wi-Fi certification for products is not expected until later in 2005.

2.4.2 Future standards

2.4.2.1 IEEE 802.11e

Quality of Service (QoS)

WLANs operate on a contended basis meaning all devices on a particular AP share the bandwidth and data packets are dealt with in the order received. This is usually sufficient for data applications such as office suite and basic internet browsing, as users will not be continuously accessing the network. However, voice and streaming media can be seriously disrupted. There are proprietary QoS solutions available, but an IEEE standard, 802.11e, is in development and is expected to be ratified in mid-2005.

There are two strands to the standard.

1) Enhanced Distributed Coordination Access (EDCA)
2) Hybrid Coordination Controlled Channel Access (HCCA)

The Wi-Fi Alliance will certify products with Wi-Fi Multimedia Enhancements (WME), based on EDCA, and Wi-Fi Scheduled Multimedia (WSM), based on HCCA. WME priorities packets according to different categories. WSM will measure the available

bandwidth and reserve a dedicated portion of it. WME is expected to be implemented on all equipment, but WSM may be reserved for particularly time sensitive applications such as VoIP.

In September 2004 the Wi-Fi Alliance launched an interim Quality of Service certification for wireless products. It is intended to bridge the gap until the ratification of the full QoS wireless standard next year. WMM (Wi-Fi Multimedia) is aimed at consumer electronics devices and classifies data packets into voice, video, best effort and background.

All 802.11e certified products are expected to be backward compatible with existing 802.11 wireless LAN products (a, b and g). It should be possible to upgrade existing 802.11 equipment to comply with 802.11e through relatively simple firmware upgrades once they are available.

2.4.2.2 IEEE 802.11n

Increasingly, users are expecting wireless connectivity to be available and as the number of wireless devices grows, faster data rates will be needed. This, coupled with more bandwidth hungry applications such as video and voice, has created the need for wireless technology capable of extra speed, capacity and reliability. To meet this need the IEEE formed 802.11 Task Group N (TGn) in September 2003 to develop a wireless standard capable of real world speeds greater than 100Mbits/sec However, products using 802.11n are not expected for two to three years.

There are two main proposals before the IEEE Task Group and a standard is not expected until late 2006. Both 802.11n proposals use Multiple Input Multiple Output (MIMO) technology. MIMO involves the use of at least 2 antennas for transmitting data and an equal or greater number for receiving. The multiple antennas are tuned to the same channel, but each transmits a different data stream. This method of setting up multiple parallel data paths within the same channel requires the use of sophisticated algorithms to reassemble the data at the receiving end. MIMO allows for more efficient use of the spectrum and greater transmission ranges. However, there are cost and power implications in having multiple RF units.

Several manufacturers are launching pre-standard "802.11n" wireless networking equipment using MIMO technology. The pre-standard equipment claims to offer better coverage and throughput even when used with existing 802.11b/g devices. However, the "n" label is misleading, due to the lack of a ratified standard and is seen by some analysts as market manoeuvring to gain an advantage in the standards setting process.

2.4.2.3 IEEE 802.16/ WiMAX

IEEE 802.16-2004 was ratified in June 2004 and is intended to provide fixed wireless broadband access at a theoretical shared peak rate of 72Mbps with a maximum range of 50km. It is designed for several applications including delivering broadband over the last mile, backhaul for other solutions such as Wi-Fi and Wireless MANs. Many major companies including Intel are backing the technology. The WiMAX (Worldwide Interoperability for Microwave Access) Forum is the industry group that promotes and oversees the technology in much the same way as the Wi-Fi Alliance. The first wireless broadband services using WiMAX have recently been launched. WiMAX is initially expected to be complementary to Wi-Fi, but a mobile version of the standard (802.16e) is in development and could provide competition in the future.

2.5 Roaming

Roaming is the ability of a client to seamlessly switch between access points while moving or for load balancing purposes. The client should associate with the access point with the strongest signal. To do this APs need to be on the same subnet (to avoid needing to acquire a new IP address) and have the same SSID and encryption keys.

The 802.11b and 802.11g standards working in the 2.4 GHz frequency range have 13 channels available in the UK. However, to avoid crosstalk and interference there are effectively only 3 non-overlapping channels that can be used (usually set at 1, 6 and 11).

Adjacent APs need to be set to different channels. This means that only 3 access points can be used in parallel. 802.11a has 8 non-overlapping channels allowing many more APs to be used in parallel.

A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box.

Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

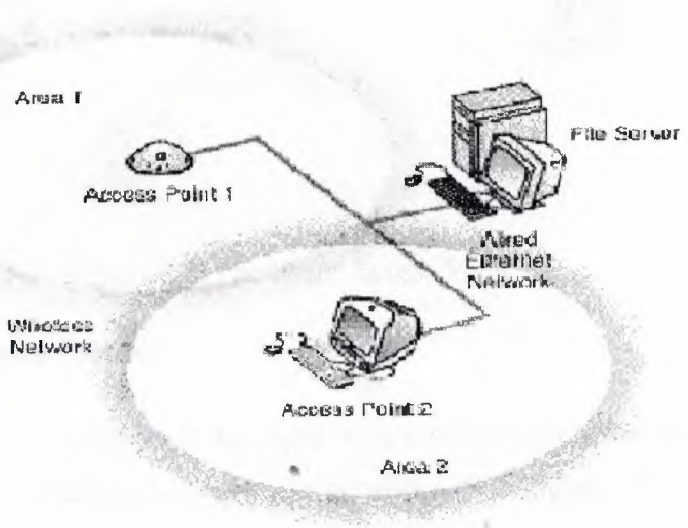

Figure 2.5: Roaming between tow APs

A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the best signal. Not all access points are capable of being configured to support roaming. Also of

note is that any access points for a single vendor should be used when implementing roaming, as there is no official standard for this feature.

2.6 Types of (APs) access points:

There are two types of access points:

2.6.1 Dedicated hardware access points (HAP):

Such as Lucent's WaveLAN, Apple's Airport Base Station or WebGear's AviatorPRO. (See Figure 2.6) Hardware access points offer comprehensive support of most wireless features, but check your requirements carefully.

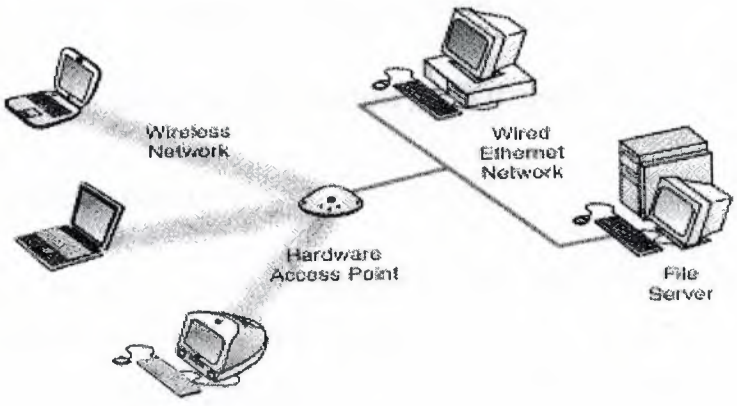

Figure 2.6: Hardware Access Point.

2.6.2 Software Access Points:

Which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network? (See Figure 2.7) The Vicomsoft InterGate suites are software routers that can be used as a basic Software Access Point, and include features not commonly found in hardware solutions, such as Direct PPPoE support and extensive configuration flexibility, but may not offer the full range of wireless features defined in the 802.11 standard. With appropriate networking software support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa.

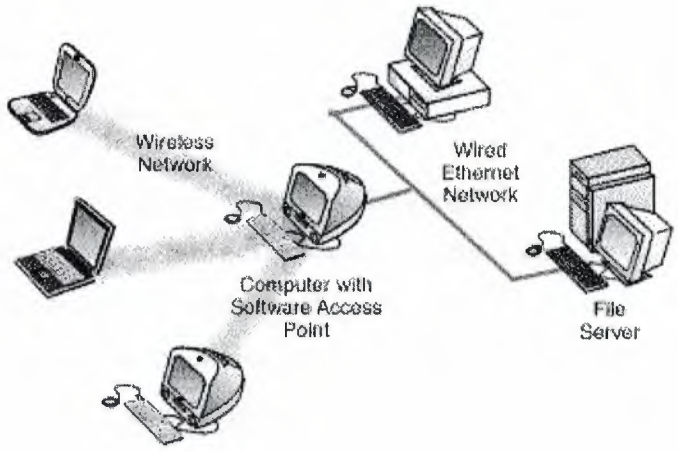

Figure 2.7: Software Access Point.

2.7 Implementation and Configuration of Wireless LAN

2.7.1 A wireless peer-to-peer network

Wireless LANs can be simple or complex. At its most basic, two PCs equipped with wireless adapter cards can set up an independent network whenever they are within range of one another. This is called a peer-to-peer network. On-demand networks, such as in this example, require no administration or preconfiguration. In this case each client would only have access to the resources of the other client and not to a central server

Figure 2.8: A wireless peer-to-peer network

2.7.2 Client and Access Point

Installing an access point can extend the range of an ad hoc network, effectively doubling the range at which the devices can communicate. Since the access point is connected to the wired network, each client can have access to server resources as well as to other clients. Each access point can accommodate many clients; the specific number depends on the number and nature of the transmissions involved. Many real-world applications exist where a single access point services from 15-50 client devices.

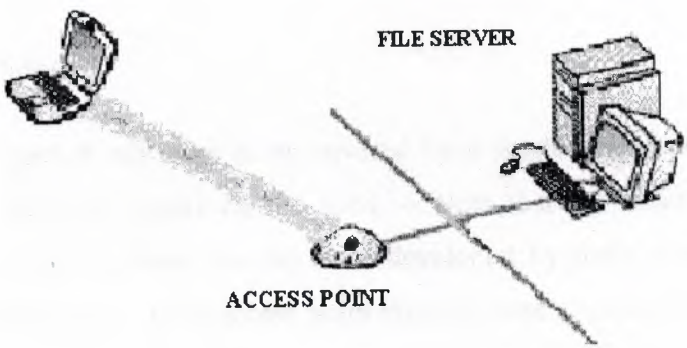

Figure 2.9: Client and Access Point

2.7.3 Multiple Access Points.

Multiple access points can be connected to a wired LAN, or sometimes even to a second wireless LAN if the access point supports this.

In most cases, separate access points are interconnected via a wired LAN, providing wireless connectivity in specific areas such as offices or classrooms, but connected to a main wired LAN for access to network resources, such as file servers. (See Figure 2.10)

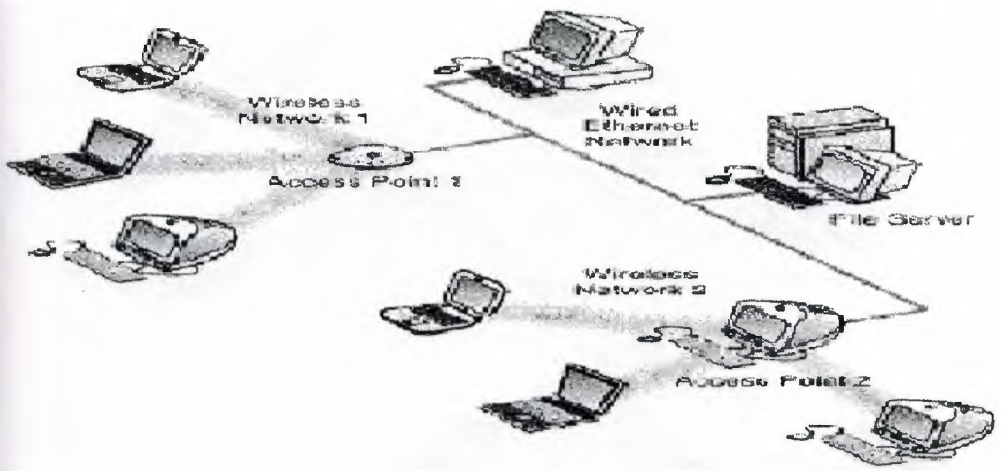

Figure 2.10: Multiple Access Points.

2.7.4 Extension Point.

If a single area is too large to be covered by a single access point, then multiple access points or extension points can be used. -- Note that an "extension point" is not defined in the wireless standard, but has been developed by some manufacturers. When using multiple access points, each access point wireless area should overlap its neighbors. This provides a seamless area for users to move around in using a feature called "roaming."

Some manufacturers produce extension points, which act as wireless relays, extending the range of a single access point. Multiple extension points can be strung together to provide wireless access to far away locations from the central access point. (See Figure 2.11)

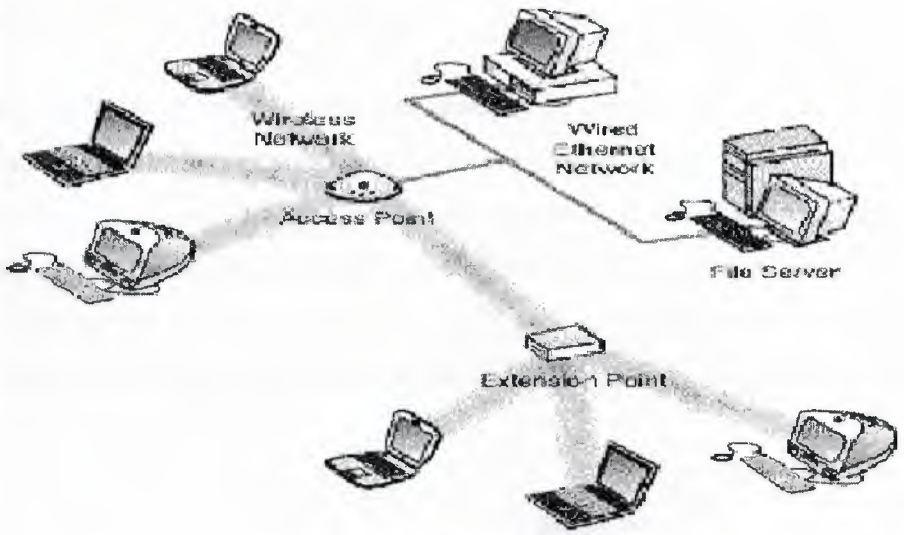

Figure 2.11: Extension Point.

2.7.5 LAN to LAN Wireless Communications

Wireless networking offers a cost-effective solution to users with difficult physical installations such as campuses, hospitals or businesses with more than one location in immediate proximity but separated by public thoroughfare. This type of installation requires two access points. Each access point acts as a bridge or router connecting its own LAN to the wireless connection. The wireless connection allows the two access points to communicate with each other, and therefore interconnect the two LAN's. (See figure 2.12)

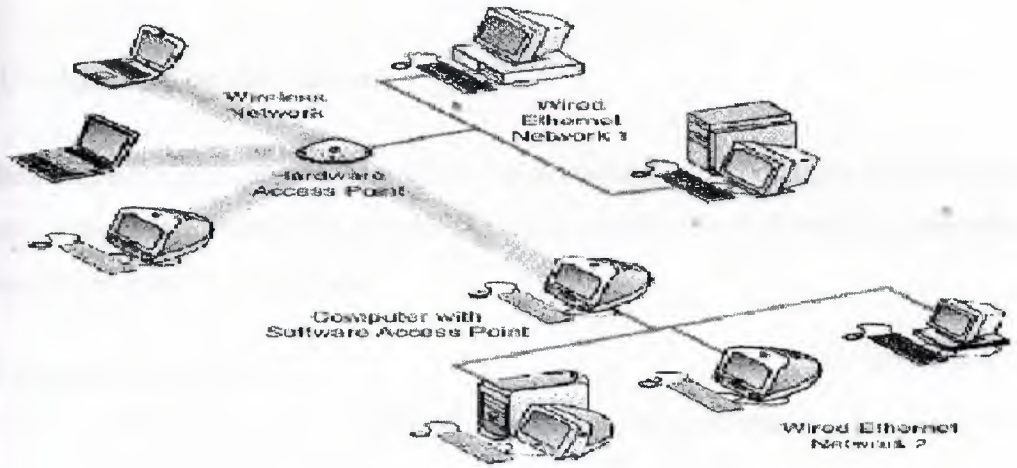

Figure 2.12: LAN to LAN Wireless Communications

2.7.6 The use of directional antennas

One last item of wireless LAN equipment to consider is the directional antenna. Let's suppose you had a wireless LAN in your building A and wanted to extend it to a leased building, B, one mile away. One solution might be to install a directional antenna on each building with each antenna targeting the other. The antenna on A is connected to your wired network via an access point. The antenna on B is similarly connected to an access point in that building, which enables wireless LAN connectivity in that facility. (See figure 2.13)

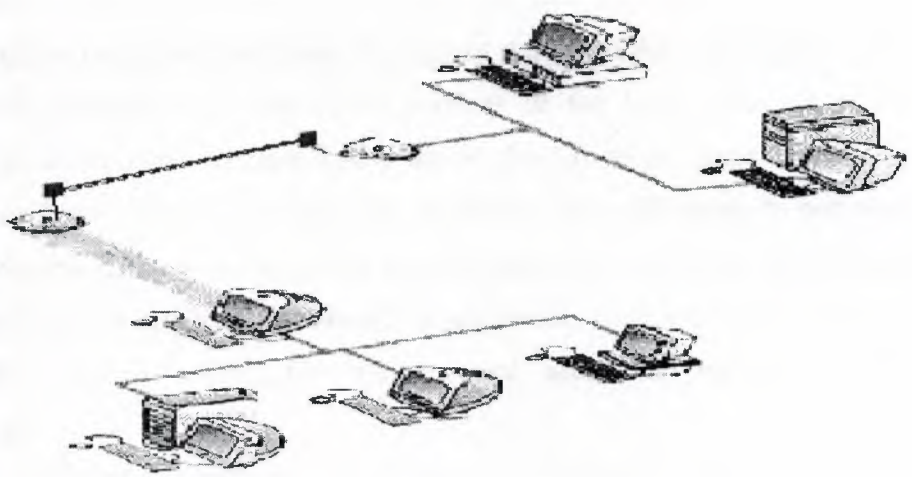

Figure 2.13: The use of directional antennas

2.8 Customer Considerations

While wireless LANs provides installation and configuration flexibility and the freedom inherent in network mobility, customers should be aware of the following factors when considering wireless LAN systems.

2.8.1 Range and coverage

The distance over which RF waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, including

walls, metal, and even people, can affect how energy propagates, and thus what range and coverage a particular system achieves. Solid objects block an infrared signal, which imposes additional limitations. Most wireless LAN systems use RF because radio waves can penetrate most indoor walls and obstacles. The range (or radius of coverage) for typical wireless LAN systems varies from under 100 feet to more than 300 feet. Coverage can be extended and true freedom of mobility via roaming, provided through microcells.

2.8.2 Throughput

As with wired LAN systems, actual throughput in wireless LANs is product- and set-up-dependent. Factors that affect throughput include the number of users, propagation factors such as range and multipath, the type of wireless LAN system used, as well as the latency and bottlenecks on the wired portions of the LAN. Data rates for the most widespread commercial wireless LANs are in the 1.6 Mbps range. Users of traditional Ethernet or Token Ring LANs generally experience little difference in performance when using a wireless LAN. Wireless LANs provide throughput sufficient for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, Internet access, file transfer, and access to multi-user databases and applications.

As a point of comparison, state-of-the-art V.90 modems transmit and receive at data rates of less than the advertised 56.6 Kbps. In terms of throughput, a wireless LAN operating at 1.6 Mbps is (almost thirty times faster than the state-of-the-art V.90 modem)

2.8.3 Integrity and Reliability

Wireless data technologies have been proven reliable through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the home or workplace. Robust designs of proven wireless LAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

2.8.4 Compatibility with the Existing Network

Most wireless LANs provide for industry-standard interconnection with wired networks such as Ethernet or Token Ring. Wireless LAN nodes are supported by network operating systems in the same fashion as any other LAN node through the use of the appropriate drivers. Once installed, the network treats wireless nodes like any other network component.

2.8.5 Interoperability of Wireless Device

Wireless LAN systems from different vendors may not be interoperable. For three reasons. First, different technologies will not interoperate. A system based on spread spectrum frequency hopping (FHSS) technology will not communicate with another based on spread spectrum direct sequence (DSSS) technology. Second, systems using different frequency bands will not interoperate even if they both employ the same technology. Third, systems from different vendors may not interoperate even if they both employ the same technology and the same frequency band, due to differences in implementation by each vendor.

2.8.6 Interference and Coexistent

The unlicensed nature of radio-based wireless LANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a wireless LAN system. Microwave ovens are a potential concern, but most wireless LAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple wireless LANs. While wireless LANs from some manufacturers interfere with wireless LANs, others coexist without interference.

2.9 Licensing Issues

In the United States, the Federal Communications Commission (FCC) governs radio transmissions, including those employed in wireless LANs. Other nations have corresponding regulatory agencies. Wireless LANs are typically designed to operate in portions of the radio spectrum where the FCC does not require the end-user to purchase a license to use the airwaves. In the U.S. most wireless LANs broadcast over one of the ISM (Instrumentation, Scientific, and Medical) bands. These include 902-928 MHz, 2.4-2.483 GHz, 5.15-5.35 GHz, and 5.725-5.875 GHz. For wireless LANs to be sold in a particular country, the manufacturer of the wireless LAN must ensure its certification by the appropriate agency in that country.

2.9.1 Simplicity/Ease of Use

Users need little new information to take advantage of wireless LANs. Because the wireless nature of a wireless LAN is transparent to a user's network operating system, applications work the same as they do on wired LANs. Wireless LAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need these tools.

Wireless LANs simplify many of the installation and configuration issues that plague network managers. Since only the access points of wireless LANs require cabling, network managers are freed from pulling cables for wireless LAN end users. Lack of

Cabling also makes moves, adds, and changes trivial operations on wireless LANs. Finally, the portable nature of wireless LANs lets network managers preconfigured and troubleshoot entire networks before installing them at remote locations. Once configured, wireless LANs can be moved from place to place with little or no modification.

2.9.2 Security

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

2.9.3 Cost

A wireless LAN implementation includes both infrastructure costs, for the wireless access points, and user costs, for the wireless LAN adapters. Infrastructure costs depend primarily on the number of access points deployed. The number of access points typically depends on the required coverage region and/or the number and type of users to be serviced. The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms.

The cost of installing and maintaining a wireless LAN generally is lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, a wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because wireless LANs simplify moves, adds, and changes, they reduce the indirect costs of user downtime and administrative overhead.

2.9.4 Scalability

The design of wireless networks can be extremely simple or quite complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.

2.9.5 Battery Life for Mobile Platforms

Since end-user wireless products are designed to run off the AC or battery power from their host notebook or hand-held computer, wireless products have no direct wire connectivity of their own.

2.9.6 Safety

The output power of wireless LAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health affects have ever been attributed to wireless LANs.

2.10 Summary

Flexibility and mobility make wireless LANs both effective extensions and attractive alternatives to wired networks. Wireless LANs provide all the functionality of wired LANs, without the physical constraints of the wire itself. Wireless LAN configurations range from simple peer-to-peer topologies to complex networks offering distributed data connectivity and roaming. Besides offering end-user mobility within a networked environment, wireless LANs enable portable networks, allowing LANs to move with the workers that use them.

Chapter 3

Security of Wireless Local Area Networks

Overview

When the wireless communications is coming to the offices and the homes, there are some new security issues to be taken care of. Today we have continuously growing markets for the wireless LANs, but there is big black hole in the security of this kind of networks. This paper gives an overview of the security functions specified in two wireless LAN standard, namely in the IEEE 802.11 and the HIPERLAN. There is also some discussion about the threats and vulnerabilities in wireless networks compared to wired networks. And last but not least the protocols and mechanisms needed in the secure wireless LAN are described

3.1 Introduction

802.11 wireless LANs continue to gain market momentum. Higher speeds, larger bandwidth and improved quality of service are helping businesses realize the potential business benefits that wireless networking delivers. Now, with this growing adoption of 802.11 wireless LANs, security has become a focal point regarding the decision to deploy a wireless LAN.

While wireless networking has several advantages over a traditional wired LAN, it introduces security risks that a wired LAN is not susceptible to. Without a robust wireless security solution, organizations leave themselves vulnerable to attack through their WLAN. Although malicious attacks are a non-controllable reality, companies can take action to integrate a solid wireless security solution that prevents unauthorized users from accessing confidential company information.

Authentication and data encryption are the key components of wireless LAN security to help prevent unauthorized users from accessing the network and compromising confidential information. Standard 802.11 securities have two major issues:

1) Authentication of wireless clients is missing, so unauthorized users may be Able to access network resources.
2) Weak encryption results in minimal effort for attackers to decipher data Transmissions.

3.2 Why secure the WLAN?

If you only surf the Web and send occasional emails, the risk of being hacked appears low. However, it's not as simple as that. Firstly, if someone manages to hack into your WLAN and piggybacks onto your Internet connection, even if it's only a slow modem link, they are stealing your bandwidth. If they only download the odd email and Web page you might not notice, but if you start a big download and it takes an hour instead of a few minutes, it costs you time and money.

Worse, anyone on your WLAN will be using the same Internet protocol (IP) address as you. To others on the Internet they appear to be you – the intruder has hijacked your identity. This means that they could send spam, fill in forms on Web pages and generally be a nuisance at best or, at worst, conduct criminal acts. And when the authorities trace the IP address, they see yours, potentially rendering you liable for prosecution.

There's a honeypot effect too. A relatively new phenomenon known as warchalking also means that hackers can tell others where there's an accessible Internet connection by chalking marks on the pavement. A "free" Internet connection could entice others to come and piggyback your connection. Most of them do it not to steal data, but simply because they can.

3.3 How much security is enough?

Security involves the application of common sense, bearing in mind the whole risk. The key is to reduce the risk to a level you're comfortable with.

For example, when deciding how much to spend on home security, you calculate how much security you need given the risks involved and balance that against the cost and any inconvenience it might entail.

It's the same when determining the right level of WLAN security. Questions to answer are:

- How valuable is the information you are guarding?
- How much inconvenience are you prepared to tolerate?
- How much are you willing to pay?

Let's examine the risks using a simple example. For a home-based WLAN, the odds are low that anyone will want to steal information since its value to anyone else is likely to be minimal. However, they might want to steal your bandwidth.

This means you need to stop intruders connecting to the AP by using hardware filtering to disallow them from registering a client PC at the AP – see below for details. This is the minimum level of security you should apply. It also makes sense to prevent potential eavesdroppers from spying on your data stream, so a combination of filtering and encryption will provide all the security you need. Best of all, they require no intervention once you've configured the AP and clients, and they're free.

So there's no right or wrong answer to the question of how much security is enough – only you can determine the answer based on your individual circumstances. That said, it makes sense to use whatever security measures that come free with the system if only for your peace of mind.

3.4 Security Threats and Types of Attacks

Before examining the security solutions available today, it is important to define some of the security risks faced by WLANs. All LANs, wired or wireless, are vulnerable to two types of attack: 1) active attacks; hackers gain access to the LAN to destroy or alter data and, 2) passive attacks; hackers gain access to the LAN, but can only eavesdrop to transmitted data. Wireless LANs are more susceptible to both types of attacks because hackers do not require a physical connection to the premises.

3.4.1 Active Attacks:

A direct attack by intruders, with specific intent to disrupt network operations or access data. These are profiled below:

3.4.1.1 Spoofing:

One of the most basic types of active attacks whereby the intruder configures their wireless terminal to appear to have the same MAC address as an authorized access point or wireless terminal. When spoofing an access point, the intruder's terminal appears as the authorized access point, with the intent to associate with an authorized wireless terminal and access the data on that device. When spoofing a wireless terminal, the intruder's terminal appears as the authorized terminal, with the intent to gain unauthorized access to the wireless network.

3.4.1.2 Denial of Service (DoS):

A denial of service attack disrupts a network by flooding the bandwidth with meaningless data to bring the network to a halt. To initiate a DoS attack, the intruder discovers an access point on the wireless network and then sends it a continuous stream of meaningless information. The data stream overwhelms the access point, causing it to become unusable. DoS attacks may be as sophisticated as spoofing 802.11 disassociation management frames to the wireless terminals, or as simple as using an RF generator in the 2.4 GHz band to jam the RF channel.

3.4.1.3 Replay Attacks:

The intruder monitors and captures transmitted packets between a wireless terminal and access point. This is achieved via a passive monitoring utility called a 'sniffer'; such as Air Snort, which is readily available on the Internet as freeware. Once the packet is captured, the hacker can do one of two things:

- Initiate a DoS attack by repeatedly transmitting through the access point. Because the packet contains valid data, the access point forwards it to the host server to process and respond with a data receipt message. The host server overloads if the packet is transmitted with enough frequency.
- Accelerate the data flow on the network to reduce the time required to collect enough data to crack a WEP encryption key.

3.4.2 Passive Attacks:

One of two types; 1) collect data in transit, without the interruption of communication between authorized devices, or 2) penetrate a wireless network through a security hole. 802.11 wireless technologies are inherently open to data interception by any 802.11 radio. Consequently, a passive attack does not require sophisticated methods or tools in order to eavesdrop and collect data.

3.4.2.1 War-driving:

The most common form of passive attack. The RF signal of 802.11 networks may extend beyond the confines of a building. With a wireless laptop or terminal, a hacker simply drives through business districts passively listening for a strong RF signal. Without good security, little effort is then required to penetrate the network.

3.4.2.2 Man-in-the-Middle:

An attack that requires sophisticated software and can cause significant disruption or data loss. The hacker inserts themselves between an access point and a wireless terminal to capture packets in transmission. The wireless terminal sees the hacker as an authorized access point, while the access point sees the hacker as an authorized wireless terminal. Both authorized devices fail to detect the intruder and continue transmitting information. The intruder captures legitimate Information and is also able to inject false data into the network, or

Initiate a DoS attack. Attacks by unauthorized users are not the only threats to WLAN's. Many 802.11 networks are installed without proper measures to secure configuration and management functions. Also, companies may not enforce security policies or provide education to help employees understand the wireless network and its security implications. For example, in an effort to minimize the time to get a WLAN up and running, some wireless equipment vendors offer their devices with certain features turned off; including security mechanisms. This can cause undue exposure to an attack. It is important to understand and properly manage WLAN equipment in order to minimize the risk of an attack.

An example of an internally caused network risk could be an employee that introduces an unauthorized 'rogue' access point into the company network. Today's plug-and-play wireless equipment requires minimal configuration, and the individual can quickly have their own wireless network up and running. Without proper security mechanisms, the individual has unintentionally created a security hole. If the RF signal is sufficiently strong, a 'war-driver' could pick up the signal and gain access to the company network.

3.5 Security Standards

This section describes two existing wireless network standards concentrating on the security functions they provide. The proprietary solutions (like Lucent Technologies WaveLAN), existing mobile telephone networks (like GSM) and future technologies (like wireless ATM or UMTS) are out of the scope of this paper.

3.5.1 HIPERLAN

HIPERLAN is ETSI's wireless broadband access standard, which defines the MAC sublayer, the Channel Access Control (CAC) sublayer and the physical layer. The MAC accesses the physical layer through the CAC, which allows easy adaptation for different physical layers. Currently defined physical layers use 5.15 - 5.30 GHz frequency band and support 2 048 Kbps synchronous traffic and up to 25 Mbps asynchronous traffic. HIPERLAN has following properties:

- It provides a service that is compatible with the ISO MAC service definition in ISO/IEC 15 802-1
- Its operations are compatible with the ISO MAC bridges specification ISO/IEC 10 038 for interconnection with other LANs
- It may be deployed in pre-arranged or an ad-hoc fashion
- It supports node mobility
- It may have a coverage beyond the radio range limitation of single node
- It supports both asynchronous and time-bounded communication by means of a Channel Access Mechanism (CAM) with priorities providing hierarchical independence of performance

- Its nodes may attempt to conserve power in communication by arranging when they need to be active for reception

The HIPERLAN specification defines an encryption-decryption scheme for optional use in the HIPERLAN. In this scheme, all HM-enties of a HIPERLAN shall use a common set of shared keys, referred as the HIPERLAN key-set. Each of these keys has a unique key identifier. Plain text is ciphered by XOR operation with random sequence generated by confidential algorithm, which uses as an input the secret key and initialization vector send in every MPDU (see figure3.1). ETSI claims that defined scheme utilize.

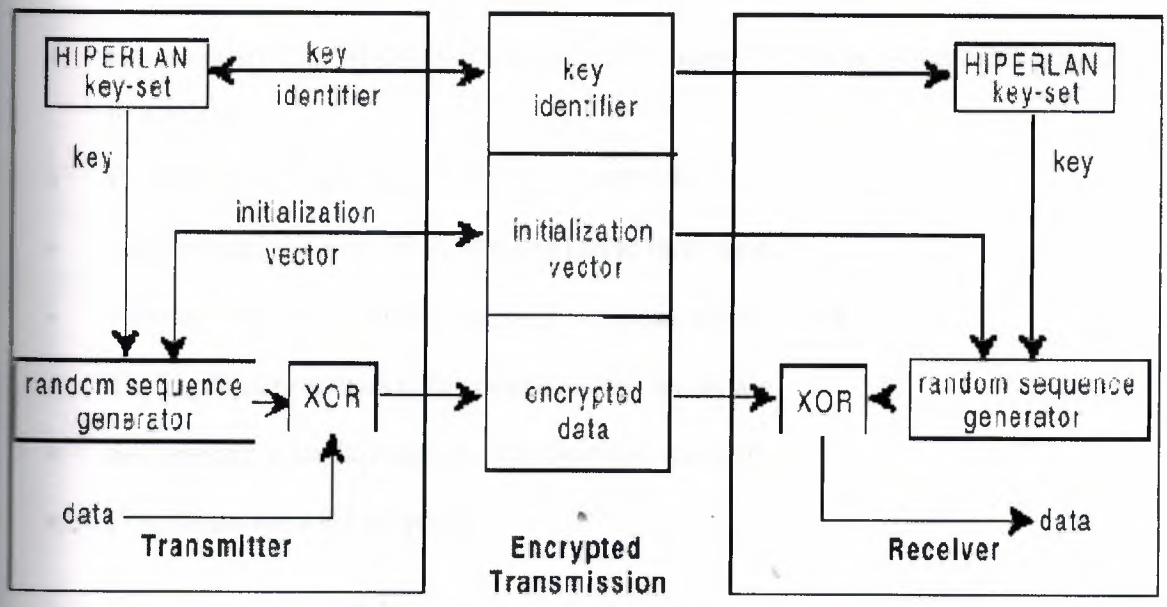

Figure 3.1: HIPERLAN encryption-decryption scheme

It is impossible to say anything for sure about the protection level that the WEP offers, because the algorithms are not available. But the lack of the independent and public analysis arouses some suspicions about the strength of the algorithms. The HIPERLAN standard does not define any kind of authentication, which sounds very strange for this kind of system. In my humble opinion one should not trust the security

level offered by the HIPERLAN specification in any sensitive application, but use some additional mechanism to gain the security requirements sat to the wireless LAN.

3.5.2 IEEE 802.11

The IEEE 802.11 standard defines the physical layers and the MAC sublayers for the wireless LANs. There are three different physical layers: Frequency Hopping Spread Spectrum Radio, Direct Sequence Spread Spectrum Radio and Baseband Infrared. All physical layers can offer 2 Mbps data rate, the radio PHYs uses 2 400 - 2 483.5 MHz frequency band. The MAC layer is common for all three PHY and has the following features:

- Support of Iso-chronous as well as Asynchronous data
- Support of priority
- Association/Disassociation to an AP in a BSS or ESS
- Re-association or Mobility Management to transfer of association from one AP to another
- Power Management to save in the battery time
- Authentication to establish identity of the terminals
- Acknowledgment to ensure reliable wireless transmission
- Timing Synchronization to coordinate the terminals
- Sequencing with duplication detection and recovery
- Fragmentation / Re-assembly

The IEEE 802.11 defines two authentication schemes: Open System Authentication and Shared Key Authentication. The former is actually a null authentication; all mobiles requesting the access are accepted to the network. The later one uses shared key cryptography to authenticate the mobile. When a mobile request authentication, the base sends 128 octet (1024 bits) long random numbers to the mobile encrypted using shared key. The mobile decrypts the random number using the same shared key than the base and sends that back to the base. If the number that the base receives is correct, the mobile is accepted to the network. All mobiles allowed to

connect to the network uses the same shared key, so this authentication method is only able to verify if the particular mobile belongs to the group of the mobiles allowed to connect to the network, but there is no way to distinct the mobiles from each other. There are also no means to authenticate the network by the mobile. The IEEE 802.11 does not define any key management functions.

The IEEE 802.11 defines an optional Wired Equivalent Privacy (WEP) mechanism to implement the confidentiality and integrity of the traffic in the network. WEP is used at the station-to-station level and does not offer any end-to-end security. WEP uses the RC4 PRNG algorithm based on a 40 bit secret key and a 24 bit initialization vector (IV) send with the data. WEP includes an integrity check vector (ICV) to allow integrity check. One MPDU frame contains the clear text IV and ICV and the cipher text data block, so receiver is always able to decrypt the cipher text block and to check the integrity. The IV can always be new or reused for a limited time the scheme is illustrated in (figure 3.2)

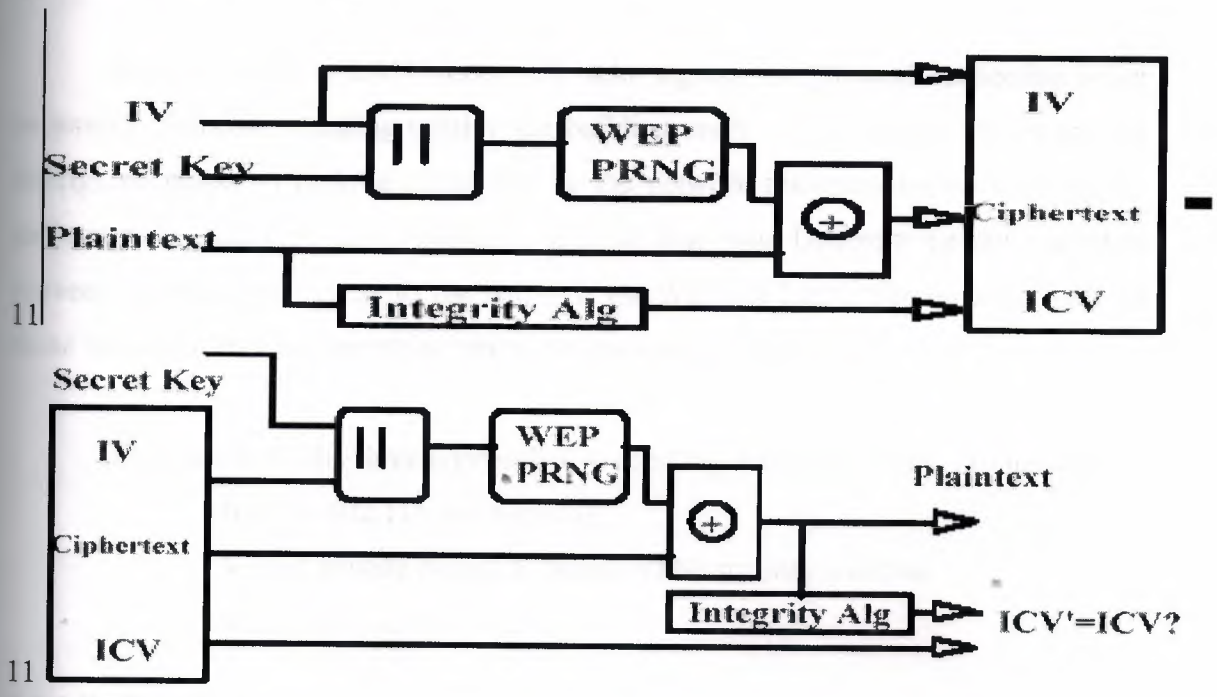

Figure3.2: WEP mechanism

The PRNG algorithm used in IEEE 802.11 is RC4 from RSA Inc. The actual algorithm is not public, but has been studied in independent research laboratories under nondisclosures agreements and no weaknesses has not yet been reported, which

does not guarantee that these does not exist. Anyway the secret key used is only 40 bits long, which can be solved by brute-force attack in 2 seconds with $100 000 hardware and 0.2 seconds with $ 1,000,000 hardware according the 1995 figures; today the hardware prices are significantly lower. And even with some additional strength gained with variable IV the protection level of WEP may not be considered strength enough for the most sensitive applications. The Shared Key Authentication scheme could be easily fooled using for example the play-back attack. So anyway an additional authentication mechanism is needed.

3.6 Security Mechanisms

Security is one of the major issues in wireless networking. In a wired environment in a building, someone has to get inside the building to make a physical connection with a client to the existing network before he can access the network resources.

Because Wireless LAN works with radio signals, the physical connection is not necessary. Someone standing outside the building could (if the Access Points are not configured properly) make a connection to the network resources by intercepting the radio signals. Although this is possible, it is not that easy. Different measures exist to prevent unauthorized access to the network via Wireless LAN. The eventual goal of these measurements is a secure access to the network for valid users.

There are basically three approaches to securing access to an 802.11b network:

- Built in 802.11b mechanisms:
- Virtual Private Network-based (VPN) security solution
- 802.11X security standard

3.6.1 Built in 802.11b mechanisms

Currently there are three methods that are defined in the 802.11b standard:

- Service Set Identifier (SSID)
- Media Access Control (MAC) address filtering
- Wired Equivalent Privacy (WEP)

Network administrators can choose to implement one or more of these methods. Standard none of these methods is turned on. This is mainly done by the vendors to allow easy set-up of the product by it's customers.

3.6.1.1 Service Set IDentifier (SSID)

Network access control can be implemented, using an SSID associated with one or more Access Points. Each Access Point is programmed with an SSID corresponding to a specific wireless network. A building, for example, can be configured using different SSID's. The client computer has to be configured with the correct SSID to connect to the specified Access Point. If the client computer hasn't got the correct SSID, it can not make a connection to the Access Point.

A typical user has more than one profile, so he can use different Access Points within the company. By doing so, some Access Points can only be available for a specific group of users.

Because a client computer has to give the correct SSID to the Access Point, the SSID works as a password and, thus, provides a measure of security.

However, if the Access Point is configured to broadcast the SSID, it transmits it's SSID to all the clients within the range. By doing so, the client can easily intercept the SSID and access the Access Point. Therefore, it is strongly recommended that Access Points be configured with broadcast mode disabled.

3.6.1.2 Media Access Control (MAC) Address Filtering

While an Access Point or group of Access Points can be identified by its SSID, a

client computer can be identified by its unique MAC Address[11] of its 802.11 network card. To increase the security, each Access Point can be configured to give only access to a list of MAC Addresses. This means that only those persons with the correct Network Card can get access through the Access Point.

MAC address filtering, together with SSID, give improved security to the network. However, this is only recommended in small networks, where the list of MAC

addresses can be efficiently managed. After all, each Access Point must be manually programmed with the list of MAC addresses and the list must be up-to-date.

3.6.1.3 Wireless Equivalent Privacy (WEP)-based Security

The 802.11 standard works with WEP to increase the security of the solution. WEP is based on encrypting the data with a symmetric key. The basis for the WEP protocol is Ron's Code 4 Pseudo Random Number Generator (RC4 PRNG).

All clients and Access Points on a wireless 802.11b network use the same key to encrypt and decrypt data. The key is placed in every client computer and in every Access Point on the same network.

WEP specifies the use of a 40-bit or 104-bit encryption key. The encryption key is combined with a 24-bit "initialization vector" resulting in a 64 or 128-bit key. This key is put into a generator of pseudo random numbers. The resulting sequence is then used to encrypt the data.

On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.)

WEP encryption has been proven to be insufficient for a sufficiently secure network. Today scripting tools exist that can be used to take advantage of weaknesses in the WEP key algorithm. The industry and IEEE are working on a new standard that will allow more security and hence a network that is even tougher to hack: 802.1x

3.6.2 Non 802.11b built-in security

Besides the mechanisms that are implemented in the 802.11b standard, there are also other security solutions available that are not implemented in the 802.11b standard. To enforce the security of your network, a Virtual Private Network solution (VPN) for wireless access is currently the most suitable alternative to WEP and MAC address filtering. Besides the VPN solution, there exist also proprietary solutions. This means that the solutions are only available with one vendor.

Cisco has the most advanced proprietary security solutions available in the Wireless LAN market today, making them the best solution for secure Wireless LAN.

The Access Points are configured for open access with no WEP encryption, but the wireless access is separated from the network resources by using a VPN server. The connection between the Access Point and the VPN server is done by a Virtual LAN. Authentication and encryption are done by the VPN server; also the gateway to the private network resources is done by the VPN server.

This VPN solution is scalable for a very large numbers of users. The VPN server can be administered centrally.

3.6.3 How it works

The communication begins with an unauthenticicated network client device attempting to make a connection with an access point. Then the Access Point responds by telling the network device which port it can use. The port will only accept EAP packages (cf. supra) from the client to an authentication server located on the wired side of the Access Point. The Access Point blocks all other traffic such as HTTP and DHCP until it receives a GO from the authenticication server (e.g. a RADIUS server). Then the Access Point will open the port for all traffic.

Some Wireless LAN vendors offer dynamic key management using 802.1x as a delivery mechanism. The authentication server can return session keys to the access point along with the accept message.

The 802.1x standard doesn't actually give the authentication mechanisms. It only provides a more secure way to use the existing authentication mechanisms, such as Transport Layer Security. The software supporting the EAP-mechanisms stays on the authencation server and within the operating system of the client device.

3.7 Emerging 802.11 security standards.

3.7.1 IEEE 802.11i Enhanced Wireless Security standard.

The IEEE 802.11 TGi working group is currently working on ratifying (expected early 2004) the 802.11i Enhanced Wireless Security standard, also known as Robust Security Network (RSN).

802.11i incorporates user authentication mechanisms and stronger data encryption, effectively representing second-generation 802.11 security to address security concerns for legacy hardware and new hardware in AP and ad-hoc (peer-to-peer) based 802.11 networks. 802.11i specifies user authentication through 802.1X and data encryption through the Temporal Key Integrity Protocol (TKIP) and Counter Mode with CBC-MAC Protocol (CCMP).

TKIP targets legacy 802.11 equipment and will be available as a firmware or software upgrade. TKIP implements counter-measures to reduce the rate at which a hacker can make message forgery attempts, down to two packets every 60 seconds; after which new encryption keys are generated. The counter-measures reduce the probability of successful forgery and amount of information an attacker can learn about a key.

By contrast, CCMP requires new 802.11 hardware with greater processing power and increased memory. Based on the Advanced Encryption Standard (AES), CCMP is a FIPS-197 certified algorithm approved by NIST. AES replaces the Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) for all government transactions.

AES operates in a Counter Mode within 802.11i with CBC-MAC (CCM). Counter Mode is used for data privacy and CBC-MAC (Cipher Block Chaining Message Authentication Code) is used for data integrity and authentication. Message Authentication Code (MAC) provides the same functionality as MIC, used with TKIP.

3.7.2 Wi-Fi Protected Access (WPA).

The Wi-Fi Alliance realizes the immediate need for stronger wireless security and has teamed with the IEEE to introduce Wi-Fi Protected Access WPA; a subset of 802.11i security with many of the same data encryption and user authentication components. WPA fills the security gap until the ratification of 802.11i, and WPA certification of 802.11 hardware began in February 2003. WPA will be mandatory for Wi-Fi certification before the end of 2003.

WPA utilizes TKIP to provide strong data encryption, and offers two user authentication and key management methods. In enterprise environments with a centralized AS, user authentication is based on 802.1X and mutual authentication based EAP. In home or office environments where a centralized authentication server or EAP framework is not available, user authentication is based on a 'Pre-Shared Key' method (PSK). With Pre-Shared Key authentication, the home or office user manually enters a password (Master Key) in the Access Point or Wireless Router and enters the same password in each client device that accesses the wireless network. The manually configured WPA password (Master Key) automatically starts the TKIP data encryption process.

The first version of WPA addresses security requirements for AP-based 802.11 networks only. The Wi-Fi Alliance will adopt the full 802.11i security standard as WPA version 2, featuring security requirements for AP-based and ad-hoc (peer-to-peer) 802.11 infrastructures.

3.8 Vulnerabilities of standard 802.11 security.

Today's tools and knowledge enable hackers to easily compromise first generation 802.11 security. In 2000, researchers from the University of California Berkley published a paper detailing WEP vulnerabilities, including ways to compromise it. Vulnerabilities include weak encryption (keys no longer then 40 bits), static encryption keys, and a lack of a key distribution method. Various academic and commercial studies show that persistent hackers can quickly breach WLAN security

even with WEP enabled. WEP is only effective against casual snoopers, and the Wi-Fi Alliance warns against WEP as a standalone security solution by stating:

Another modest security technology is SSID (Service Set Identifier) that acts as a network name or password for the WLAN. In an open system architecture, the access point transmits its SSID in clear-text, allowing any correctly configured wireless client to connect to any access point. In an effort to increase security, many wireless equipment vendors use a closed system architecture where the access point does not transmit its SSID - only clients configured with the same SSID as the access point are granted access. However, this provides minimal defense against a malicious attack as the SSID is broadcast in clear-text in and can be intercepted by an intelligent hacker with the right tools.

The greatest risk attack comes when no security measures are implemented. Although WEP vulnerabilities have been documented, it still requires effort to compromise and should be enabled whenever possible.

3.9 Security Solutions for today's 802.11 WLAN

To combat standard 802.11 security weaknesses, organizations such as the IEEE, Cisco Systems and Fortress Technologies have introduced enhanced security solutions developed around standards based technologies. The IEEE's 802.1X Port Based Network Access Control standard provides strong authentication and network access control for 802.11 networks. Cisco developed the Lightweight Extensible Authentication Protocol (LEAP); built on the principles of the Extensible Authentication Protocol (EAP). Fortress Technologies' Air Fortress FIPS 140-1 certified security solution is built on the National Institute of Standards and Technology (NIST) cryptographic standards and provides strong data encryption for 802.11 networks. Information on each of the technologies can be found below:

.9.1 IEEE 802.1X Port Based Network Access Control

802.1X is a standard that provides a means to authenticate and authorize devices or network access; a security mechanism absent from 802.11. 802.1X provides a port-based network access control solution for networking technologies such as Ethernet, 02.11, Token Ring and FDDI.

802.1X has three components that combine to deliver authentication: the Supplicant, Authenticator and Authentication Server (AS). The wireless terminal is the supplicant and the access point is the authenticator. The most common type of AS is RADIUS (Remote Authentication Dial-In User Service) - typically a stand-alone software package installed on a standard PC platform. Authentication requests occur during system initialization and are initiated by wireless terminals or access points, after the terminal has associated to the access point. Various authentication methods such as digital certificates, smart cards and one-time passwords can be used to provide credential information for authentication. Of course, without successful authentication, network access is denied.

The 802.1X authentication process uses the Extensible Authentication Protocol (EAP) to pass authentication information between the supplicant and the AS. EAP effectively creates a session with the AS for the terminal to forward its credentials. If the EAP version supports mutual authentication, then the AS provides its credentials to the wireless terminal within the same session. The EAP session allows a wireless terminal limited access to the network for terminal authentication purposes only. Once authentication is complete, the session is terminated and the wireless terminal is granted access.

EAP is a general protocol and is 'extensible' in that it supports multiple authentication mechanisms. 802.1X supports such EAP types as Message Digest 5 (MD-5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS) and Protected Extensible Authentication Protocol (PEAP).

The authentication dialog between the terminal and authentication server is carried in EAP frames. The encapsulated form of EAP, known as EAP over LAN, or EAPOL, is used for all communication between the supplicant and authenticator.

The access point acts as an EAP proxy between the terminal and AS, accepting EAPOL packets from the terminal and forwarding them to the AS over a protocol such

as RADIUS. In turn, the access point forwards all AS EAP packets over EAPOL to the wireless terminal.

Figure 3.3 Illustrates the IEEE 802.1X setup. The supplicant sends its authentication credentials to the AS via the authenticator. The AS confirms the supplicant's credentials and directs the authenticator to allow supplicant access to the network. The access point communicates with the wireless terminal and submits the terminal credential information to a suitable AS to determine correct authorization.

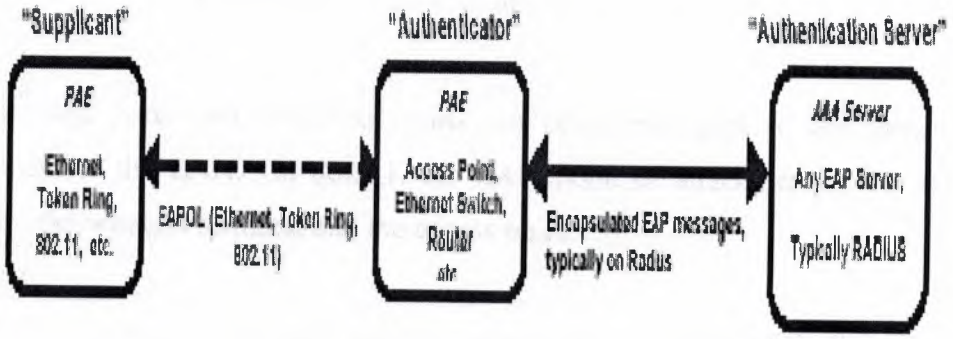

Figure 3.3: The IEEE 802.1x Setup

Figure 3.4 Illustrates how 802.1X port-based access control has the effect of creating two distinct points of access to the authenticator system's point of attachment to the LAN. The two distinct points of access are referred to as the "controlled" port and "uncontrolled" port.

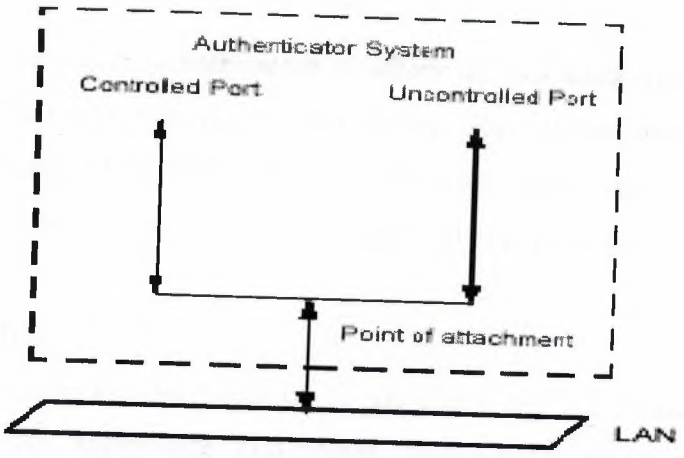

Figure 3.4: Controlled and Uncontrolled ports

Uncontrolled ports and controlled ports are considered part of the same point of attachment to the LAN. In 802.11, the LAN point of attachment is the association between the wireless terminal and the access point.

The controlled port only accepts packets from authenticated clients - the MAC address is on the list of authenticated MAC addresses. The access point uses the uncontrolled port to exchange EAP protocol information between the wireless terminal and the AS. Protocol exchanges between the access point and the authentication server can be conducted via one or more of the access point's controlled or uncontrolled ports.

EAP/MD5:

Simple, one-way handshake in which the AS authenticates the client. Credentials are based on mutual knowledge of a shared secret such as username and password. MD5 requires little memory and is simple to implement and manage; making it ideal for wireless terminals with limited memory and processing power.

EAP/TLS:

Two-way (mutual) authentication in which the AS authenticates the client, and in turn, the client authenticates the server. This mutual authentication secures against man-in-the-middle-attacks. TLS uses digital certificates to provide credential information and secures against dictionary attacks.

EAP/TTLS:

Two-way (mutual) authentication of the client and AS based on TLS. TTLS only requires server-side certificates, eliminating the need to install and configure certificates for each wireless client. User authentication occurs via a security database already in use on the corporate LAN, such as Windows domain controllers, SQL, or LDAP. TTLS securely forwards client authentication information after a TLS tunnel is established.

EAP/PEAP:

Similar in functionality to TTLS in that, it too specifies mutual authentication, uses TLS to establish a secure tunnel between the wireless client and authentication server, and only requires server-side certificates. The difference is that you would deploy an authentication method defined by EAP on the wireless client.

WEP is used in conjunction with 802.1X to protect packets from eavesdroppers. 802.1X EAP types such as TLS, TTLS and PEAP introduce strong improvements to how WEP keys are generated, managed and distributed by enabling 'per user/per session WEP keying'.

Per user/per session keying:

Once mutual authentication is successfully complete, the client and authentication server each derive the same high-level encryption key, known as a session key. Using a secure channel on the wired LAN, the authentication server sends the session key to the access point, which the access point stores. The access point generates a set of WEP keys that it transmits to the wireless

terminal as multiple EAP protocol messages, which are protected by encrypting the messages with the session key. The terminal uses its derived session key to decrypt the EAP protocol messages to get at the WEP keys that are used for encrypting subsequent data transmissions. The result is per-user, per-session WEP keys. The length of a session is defined on the authentication server. When a session expires or the client roams from one access point to another, re-authentication occurs and a new session key is generated, which in turn generates new WEP keys. The re-authentication is transparent to the user.

Even if an intruder intercepts a WEP key, a new WEP key is generated after a specified period of time rendering the captured key invalid.

3.9.2 LEAP

LEAP is Cisco's solution for providing strong authentication and is supported with Cisco's Aironet wireless infrastructure; client credentials are based on username and password. By enabling WEP, LEAP mitigates the risk of a hacker intercepting and cracking a WEP key through dynamic generation of per user/per session WEP keys, as described above.

The Cisco Secure Access Control Server (ACS) or the Cisco Access Registrar (AR) RADIUS server determine session length. When a session expires or the client roams from one access point to another, re-authentication occurs and generates a new session key – totally transparent to the user. Figure 3.5 Illustrates the LEAP authentication process and the derivation of the dynamic WEP key.

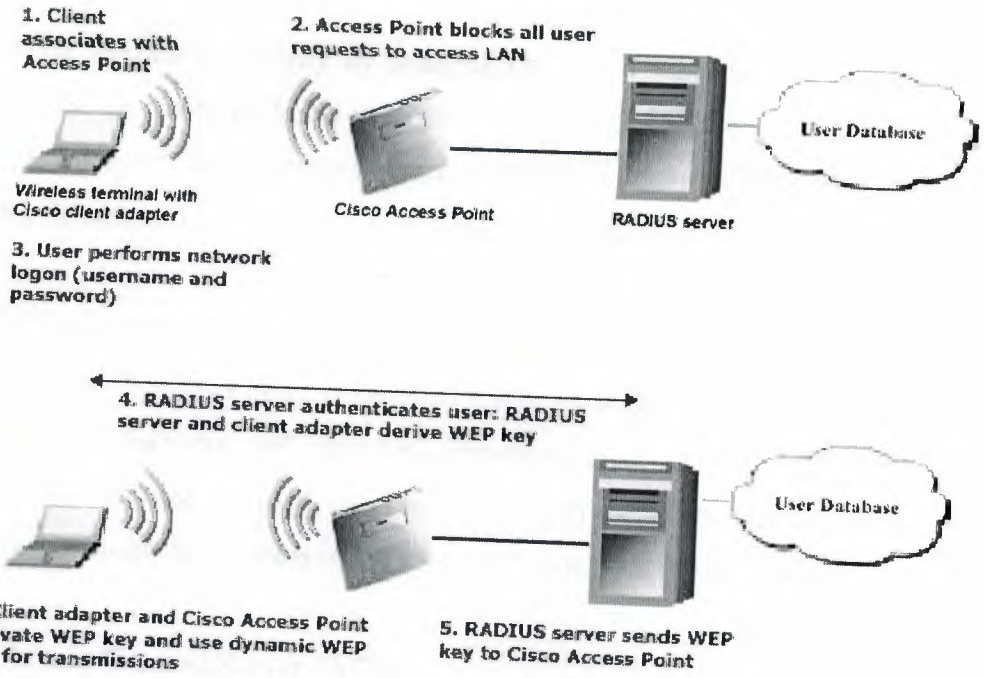

Figure 3.5: Cisco LEAP authentication

Cisco recently announced a no-cost licensing program called the Cisco Compatible Extensions program (CCX), specific to wireless client products. CCX makes Cisco technology (including LEAP) available to industry leading silicon suppliers that manufacture embedded and stand-alone wireless clients. CCX participants include Agere Systems, Atheros, Atmel, HP, IBM, Intel, Intersil, and Texas Instruments. Many have already begun integrating Cisco extensions into their product designs. Extensive third party testing ensures interoperability between CCX products and Cisco Aironet products.

3.9.3 AirFortress

AirFortress provides a simple, efficient and robust Layer 2 encryption security solution for 802.11 wireless networks. Developed by Fortress Technologies Inc, AirFortress is a FIPS 140-1 approved security technology (Certificate # 231) that supports current and legacy operating systems for a total solution.

The AirFortress solution is comprised of three components:

3.9.3.1 Wireless Security Gateways:

Provide perimeter security by bridging encrypted wireless communications to the wired LAN, or remotely between point-to-point connections. The Wireless Security Gateway encrypts and decrypts communication to/from a Secure Client or other Wireless Security Gateway, thereby preventing unauthorized network access.

3.9.3.2 Secure Client:

A DOS or Windows based driver that secures a wide range of mobile devices. The Secure Client encrypts and decrypts communication to/from a Wireless Security Gateway and during peer-to-peer communication between mobile devices thereby preventing unauthorized access to the mobile device from other devices.

3.9.3.3 Access Control Server (ACS):

ACS is a software application database designed to monitor and manage the authentication and access control of wireless clients.

The AirFortress solution utilizes a number of methods to enhance security. Frame Manipulation hides the entire Layer 3 (Network Layer) header and utilizes a unique MAC protocol ID only recognized by AirFortress products. Frame Authentication ensures integrity through SHA-1 hashing, preventing session hijacking. Payload Compression disguises original frame length and its contents to combat analytical and brute force attacks. Dynamic per Session Keys are generated using an encrypted dual Diffie-Hellman key exchange to prevent man-in-the-middle attacks and spoofing. The encryption of ARP packets and unique bridging design prevents ARP poisoning attacks. Replay Protection guards against data being captured and then being re-injected into the network after it has been compromised.

A unique Access ID prevents unauthorized clients and intruders from performing a key exchange by providing a mechanism to segment communications and control network access. A Physical Device ID is a system generated, unique hardware identifier bound to a specific device and used to distinguish AirFortress devices. The closed architecture design restricts both the wireless client and security gateway to encrypted communications to deliver the protection of a firewall without the complexity. Figure 3.6 illustrates an AirFortress implementation:

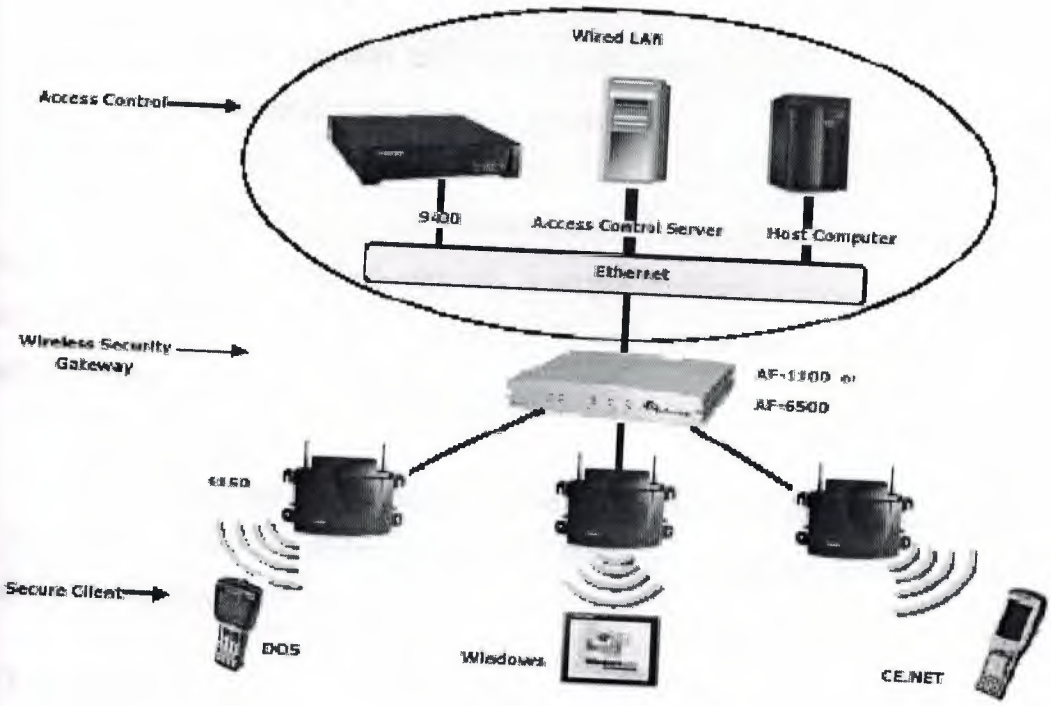

Figure 3.6: AirFortress implementation

The AirFortress solution is based on Wireless Link Layer Security (wLLS) - a true security protocol that operates on the Data Link layer and provides point-to-point encryption of wireless communications. wLLS is designed using standard encryption methods and a dual Diffie-Hellman key exchange to automatically build security associations. wLLS uses industry standard algorithms including AES, 56-bit DES, 128-bit IDEA or 168-bit 3DES - if necessary, other algorithms can be customized into the product.

10 The Future of wireless security: 802.1x

The problem, as mentioned above, is that with the current standard 802.11b, the WEP allocation has to be done manually. If this is for only a small group of users, than the task can be done on a regularly basis, without having to do monumental tasks. If there is a large group of users for the Wireless LAN, then the task of changing the WEP becomes inmanageable.

The 802.1x standard provides a solution for:

- authenticicating
- controlling user traffic to a secure network
- dynamically varying encryption keys

It bundles EAP (Extensible Authentication Protocol) to both the wired and the wireless media. This protocol supports multiple authenticication methods, such as Kerberos, certificates, etc. This mechanism is well on its way to become an industry leading standard.

The standard has been ratified in June 2001. The EAP-protocol is implemented in the Aironet Products under the name LEAP, by Windows EAP-TLS which is available in Windows XP.

3.11 Summary

802.11 wireless LAN deployments will continue to grow with each passing year. Higher data rates, increased bandwidth and improved quality of service coupled with ncreased productivity through mobility are making wireless LANs an attractive etwork solution for many customers. Along with improved wireless technology erformance, organizations such as the IEEE, Wi-Fi Alliance, Fortress Technologies nd Cisco Systems are providing enhanced security solutions for 802.11 networks to revent unauthorized access to confidential data.

ompanies that are deploying a wireless network should become familiar with 802.11 ireless technologies to help them create a more efficient and secure network. It is portant to understand today's security solutions in order to choose the right solution r their requirements. Enhanced wireless security solutions such as 802.1X, rFortress, LEAP and WPA deliver the significant benefit of security to the other tures of a wireless network.

Chapter 4

Applications of Wireless Local Area Networks

4.1 INTRODUCTION

Wireless LANs are frequently added to the wired network rather than being used to replace it, often providing the final few meters of connectivity between a wired network and the mobile user. The ongoing decrease in pricing and the increase of integrated WLAN technology in PCs and mobile computing devices by many leading network and mobile computing vendors is further fuelling the growth of wireless networking at home, in the enterprise environment and also in public spaces like hotel lounges & airports.

The following list describes some of the many applications made possible through the power and flexibility of Wireless LANs:

- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks and other changes with Wireless LANs.
- Network managers installing networked computers in older buildings find that Wireless LANs are a cost-effective network infrastructure solution.
- Wireless LANs are the ideal solution for temporary networks on exhibitions and seminars.
- Warehouse workers use wireless devices to exchange information with central databases, thereby increasing productivity.
- Network managers implement Wireless LANs to provide backup for mission-critical applications running on wired networks.
- Office workers can roam from meeting to meeting throughout the building, remaining constantly connected to the enterprise network.

4.2 How Wireless LANs Are Used in the Real World

Wireless LANs frequently augment rather than replace wired LAN networks often providing the final few meters of connectivity between a wired network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- Doctors and nurses in hospitals are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- Consulting or accounting audit teams or small workgroups increase productivity with quick network setup.
- Students holding class on campus greens can access the Internet to consult the catalog of the Library of Congress or class notes.
- Network managers in dynamic environments minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.
- Training sites at corporations and students at universities use wireless connectivity to access information, information exchanges, and learning.
- Trade show and branch office workers minimize setup requirements by installing pre-configured wireless LANs needing no local MIS support.
- Warehouse workers use wireless LANs to exchange information with central databases, thereby increasing productivity.
- Senior executives in meetings make quicker decisions because they have real-time information at their fingertips.

4.3 Applications of WLAN in Government Organization

The application of wireless LAN is seen everywhere .Not only it is applied in medical science and in institution, it can be easily applied in government organization so that data sharing among various department can be made easy and also the productivity can be increased.

Moreover in government organization, WLAN can be applied with more ease at various fields such as:-

4.3.1 Traveling Workers

Workers are on the move--from office to office, marketing and engineering personnel need a secure, convenient, and low-cost means to conduct business away from the office with the same ease as a worker on the corporate campus. When away from your desk, a wireless LANs is a great solution for staying productive on the corporate campus.

4.3.2 State and Local e-Government

Technology is fundamentally changing the way organizations operate and deliver services, and the institutions of state and local governments are no exception. In fact, many governments have formed e-government commissions to proactively evaluate and implement opportunities available thanks to advanced technology.

With e-initiatives, state and local governments are beginning to redesign business processes to meet the demands of citizens who question why, if e-commerce is available for enterprises of all types, it isn't available for government services like permitting, payment of property tax, licensing and more.

4.3.3 Extending Availability

Government agencies have implemented technology as a series of tools that enables workers to be more efficient in their daily tasks, but today the opportunity exists to extend that technology beyond government employees to the community at large. Easy, low-cost access to the Internet now offers citizens a new opportunity to interact with government.

In the past, citizen interaction with a government agency required travel to a government facility and direct contact with a government employee. Today, such contact can often be completed via the Internet. This means of "virtual" access can operate in conjunction with the face-to-face way of doing business with little to no impact on facility space allowing the existing facility to handle all future growth. Additional and short-term programs, which would require additional staffing, can be easily implemented in an e-government environment for direct digital access by individual consumers.

E-government transactions account for less than 5% of all government transactions today. As the ability to interact electronically expands, the potential to automate a majority of transactions will grow. At the same time, however, those transactions that by their nature require face-to-face interaction will remain in their current form. Importantly, the ability for government to interact with its suppliers currently exists in some form for vendors of all types. Government interaction with constituents provides the greatest opportunity for growth with the greatest payback; automated offerings can handle large transaction loads around the clock with no affect on staffing.

4.3.4 Designing and Planning for Rapid Growth

Once implemented, automated transactions are embraced quickly and often experience tremendous growth within just a few months of being placed online. The networking infrastructure that facilitates these applications must be planned, designed and executed with adequate bandwidth to accommodate the growth that will occur or with a modular design to add bandwidth as needed. Other concerns are the institution of process control features within the infrastructure to allow prioritization of bandwidth and security.

Information dissemination, on-line transactions and interactive conferencing (audio, video and data) are tools being planned and put into place in government agencies at all levels. Implementing these tools can be a challenge if the networking infrastructure is not adequate in both bandwidth and features. As a result, technology planning should address the overall infrastructure to ensure adequate capacity and features to allow ongoing

processes to continue without interruption as well as to provide for new automated service offerings to be added.

4.3.5 Financial Services

The financial services industry is at a crossroads. To meet customer demands, traditional "brick and mortar" organizations—from small retail banks to large investment institutions, from discount brokers to insurance companies, and all their "on-line" counterparts—are literally changing the way an entire industry conducts business.

In this new global environment, web-enabled technology makes systems and applications more accessible, allowing customers to access financial information and transact business 24 x 7. Critical business applications—like those for enterprise resource planning and customer relationship management—capture and store important information so institutions can more effectively meet the needs of their customers. State-of-the-art technology maximizes resources and ensures that employees have access to information when—and where—they need it.

And, this is all accomplished with the highest level of security, ensuring that the privacy of a customer's information is always protected.

4.3.6 Working toward the Bottom Line

- **Expanding business—electronically.** More and more consumers are turning to the Internet for services and information. To attract new customers (and retain their existing customer base), financial services organizations are seeking to provide on-line electronic commerce and vital interactive customer service and support around the clock and around the globe. To institutions that expand with e-commerce, this focus on the customer can mean significant revenue generation.
- **Making the most of valuable resources.** High-performance technology maximizes IT dollars as powerful wired and wireless infrastructures enable financial-services organizations to use employee and financial resources efficiently and effectively.

And this is essential as customers and employees alike require unprecedented levels of performance, accessibility and security.

- **Ensuring network availability.** In today's global economy, time or place doesn't limit bank, brokerage and insurance customers so scheduling even routine network maintenance can be a challenge. When an institution's profitability depends on meeting the highest availability standards, making sure that the network is up and running 24 x 7 is essential. Global network management solutions and Quality of Service that prioritizes data like constantly changing market data feeds over e-mail and web surfing are just two ways to increase availability.
- **Taking advantage of critical business applications.** In a financial-services environment, demand for network bandwidth is high. Traders, for example, may have crowded desktops, but they can't afford crowded pipes. With five to six market data feeds on the desktop, traders need a high-bandwidth network to ensure that each trade gets through. In addition, organizations are looking to customer relationship management and call centers, as well as distance learning, live streaming, and converged voice, video and data traffic as they expand the business with new services.
- **Maximizing security.** Of course, security is a critical concern for financial institutions of all sizes and types as they seek to protect themselves against threats and intruders from the outside as well as from unauthorized access from within. Importantly, vital security features can be enabled without any impact on network performance, meaning that secure data gets through to those who need it, when they need it.

4 Application of WLAN in Manufacturing.

Wireless LAN can be easily applied in numerous areas including manufacturing.

The presence and impact of Wireless LAN has changed the concept of anufacturing firm and in result increases the productivity and borne out new management tiatives.

e application of Wireless LAN in manufacturing can be seen as:-

- Fast and reliable data sharing among customers, dealers, partners companies, and suppliers.
- Use in implementation of manufacturing initiative like ERP, CRM.
- Static and local e-government.
- Security purposes.
- Traveling workers.
- Use in production unit.
- Wireless LAN in Manufacturing and Warehousing

4.1 Wi-Fi the Easiest to Install

It's much easier to install a wireless LAN at home than a wired network. A typical meowner won't consider running cables throughout the house. It's time consuming and uires stringing wires through the walls, which can be tricky and frustrating.

The installation of a wireless system, however, only requires the connection of a eless LAN router to the broadband modem and the installation of Wi-Fi cards in the ops and PCs (if they don't already have them). You'll be ready to start networking in than an hour. Thus, installing a wireless LAN at home is much faster and easier than alling a wired network, the main reason why wireless in homes is flourishing.

Flexible Access Makes Life Easier

With a wireless LAN, employees can bring laptops home from work and continue ing just as they do from their offices. For many professions, this makes it possible for e to work from home more effectively, whether it's to spend a few more hours rching stuff on the Internet or enable telecommuting on a daily basis.

Of course with a wireless laptop, you truly can work from anyplace in the house. 's nothing tying you down to a desk in a particular room. You're free to use the et or access files on other computers while relaxing in a comfy chair in front of a TV,

lounging on the patio breathing fresh air, or sitting at a desk in a quiet bedroom, just like you see in the commercials.

As an independent consultant, I do much of my work from home. Without any defined work hours (a good thing), I tend to work off and on from morning to late evening (a bad thing). With this type of work schedule, I like the idea of working in the presence of family, which enables me to socialize a bit despite my work habits. With my wireless laptop, I can easily go back and forth to work.

Wireless LANs at home are good for PCs as well. Unlike companies, Ethernet cabling in homes is nearly nonexistent. That makes wireless the best way to connect stationary PCs to the network. You'll have much more flexibility in locating a PC to any part of the house without being near the broadband modem.

4.4.3 Internet Connection Sharing

Many homes now have more than one computer. After purchasing a new PC, homeowners will generally hold on to the older PC. It may not be the best for running some of the newer games, but it still offers a good station for browsing the Web and interacting with e-mail. Of course some people will also bring a laptop home from work or purchase one instead of upgrading to a newer PC.

With multiple computers, it's extremely beneficial to have them interface to the same Internet connection. Because of the ease of installation, a WLAN is the best solution for sharing the Internet service. Thankfully, for most, the days of dialup are over. Just be sure to install a WLAN router (not an access point) to ensure that you have Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) services necessary for all of the computers to share a single, official IP address supplied by your Internet service provider. (You would use an AP just to get wireless access to an existing wired network.)

4.4.4 Printer Sharing Increases Usability

Without a WLAN, most home users must cable their printer directly to a PC or the Ethernet connector on the broadband modem. This limits the number of places that the printer can reside. Generally, it must sit within a few feet of the PC or modem.

A Wi-Fi print server, however, enables the printer to be accessible over the network. This makes printer placement extremely flexible. For example, you may find it most useful to have the printer in the family room where you do most of your laptop computing. Or, it might make more sense to have the printer just inside the door that leads to your patio. You can also easily move the printer to new locations whenever you want to.

Common applications, such as Web surfing and e-mail, perform very well over wireless LANs. All it takes is a browser and e-mail software on the client device. Users may lose a wireless connection from time-to-time, but the protocols in use for these relatively simple applications are fairly resilient under most conditions.

Beyond these simple applications, however, you will likely find the need to incorporate connectivity software that provides an interface between a user's client device and the end system containing an application or database. Applications could be warehouse management software running on an IBM AS/400, a modeling application located on a UNIX box, or a time management system resident on an old mainframe (define) system. The databases would be part of a client server system where part or all of the application software resides on the client device and interfaces with a database such as Oracle or Sybase.

In these cases, you need application connectivity software in addition to traditional WLAN components (i.e., wireless radio NICs and access points) to enable communications between the client device and the application software or databases located on a centralized server. The primary options you have available beyond using Web browser technology are terminal emulation, direct database connectivity, and wireless middleware. Let's take a closer look at each one of these.

4.4.5 Terminal Emulation

Terminal emulation (define) software runs on an end-user device and lets the client operate as a traditional terminal, communicating directly with application software running on a host-based system. The terminal merely presents screens to the use and accepts input rendered by the applications software. For example, VT220 terminal emulation communicates with applications running on a UNIX host, 5250 terminal emulation works with AS/400-based systems, and 3270 terminal emulation interfaces with IBM mainframes.

The advantage of using terminal emulation is its low initial cost. The wireless systems using terminal emulation, however, may not be able to maintain continuous connections with legacy applications, which have timeouts set for more reliable wired networks. Timeouts will automatically disconnect a session if they don't sense activity within a given time period. As a result, the corporate IT group may spend a lot of time responding to end-user complaints of dropped connections and the associated issues of incomplete data transactions. Thus, implementing terminal emulation can have a significant disastrous effect on long-term support costs.

4.4.6 Direct Database Connectivity

Direct database (define) connectivity encompasses application software running on a client that interfaces over TCP/IP directly with a database located on a server. With this configuration, the software on the end-user device provides all application functionality. This enables flexibility when developing applications because the programmer has complete control over what functions are implemented and is not constrained by the legacy applications on the host. Direct database connections are often the best approach if you need a lot of flexibility in writing the application software.

A problem, however, is that the direct database approach relies on TCP/IP (define), which is not well suited for traversing a wireless network. TCP/IP uses a significant amount of bandwidth overhead when re-establishing connections after a break, and supports the transmission of packets with relatively large headers.

4.4.7 Wireless Middleware

Wireless middleware (define) software, offered by vendors such as Wavelink and Connect, provides intermediate communications between end-user devices and the application software located on a server. The middleware, which generally runs on a dedicated platform attached to the wired LAN, processes the packets (define) that pass between the LAN and the wireless access point. It provides efficient and reliable communications over the wireless network, while maintaining appropriate connections to application software and databases on the server via the more reliable wired LAN.

The following are features to look for in middleware products:

- **Optimization techniques**: Many middleware products include data compression at the transport layer to help minimize the number of bits sent over the wireless link. Some implementations of middleware use header compression, where mechanisms replace traditional packet headers with a much shorter bit sequence before transmission.

- **Intelligent restarts**: With wireless networks, a transmission may be unexpectedly cut at midstream. Intelligent restart is a recovery mechanism that detects the premature end of a transmission. When the connection is reestablished, the middleware resumes transmission from the break point instead of at the beginning.

- **Data bundling**: Some middleware is capable of combining smaller data packets into a single large packet for transmission over the wireless network, which can help lower transmission service costs of wide area networks. Since some wireless data services charge users by the packet, data bundling results in a lower aggregate cost.

- **Store-and-forward messaging**: Middleware queues traffic to ensure delivery to users who become disconnected from the network. Once the destination station comes back online, the middleware sends the stored packets.

- **Screen scraping and reshaping**: The development environment of some middleware products allows developers to use visual tools to "scrape" and "reshape" portions of existing application screens to more effectively fit data on the smaller display of some non-PC wireless devices, such as PDAs and bar code scanners.

- **End system support**: Wireless middleware interfaces with a variety of end system applications and databases. If you have multiple types of applications and data bases that clients need access to, then wireless middleware can act as a concentrator. For example, a user can use the middleware connection to interface with applications on an AS/400 and UNIX box simultaneously without needing to be concerned about running the correct terminal emulation software.

- **Security controls**: In addition to application management, middleware products often offer access control and encryption mechanisms that counter the issues of 802.11 wired equivalent privacy (WEP) (define). Some middleware is beginning to include the ability to identify and counteract the presence of rogue access points and denial of service attacks.

- **Operational support mechanisms**: Some offer utilities and tools to monitor the performance of wireless appliances, enabling you to better troubleshoot problems.

4.5 Applications of WLAN in Health Care Organization

When disaster strikes, the Red Cross Disaster Service operates like a huge mobile warehouse, setting up, on a moment's notice, locations for receiving and storing thousands of pallets of food, supplies and equipment, and efficiently distributing those supplies to disaster victims. These operations often take place under extreme conditions: heavy storms, power and telephone outages, continuing floods and other logistical difficulties posed by the preceding destruction. Field houses for relief operations must be swiftly set up and often moved during the course of the operation.

When relief needs have been met, they must be shut down quickly and the equipment made ready for immediate deployment to a new disaster site. Voice and data

communications are critical to the Red Cross operations and wireless solutions are a natural choice.

Prior to adopting a wireless application, the Red Cross used paper-based inventory systems. Richard Hoffman, senior systems programmer with the American Red Cross National Headquarters, said recent disasters demonstrated the need for a high-capacity, automated system.

The primary requirements for the new system were mobility, reliability, ease-of-use by staff and volunteer workers, and the ability to provide six to eight hours of continuous battery operation in the event of a power failure. Secondary requirements included tight tracking of accounting and traceability records of materials and donated goods used during the operation, in order to meet IRS tracking requirements. The system tracks everything from perishables and water to equipment such as fax machines, cellular phones and tables and chairs. The system also maintains warehouse data and transmits that data to a central logistics database at the local disaster operational headquarters. (The Red Cross central logistics database enables it to provide a current inventory of all relief material on hand for the entire operation.).

4.6 Applications of WLAN in Education and Research Organization

Wireless Andrew is a 2Mbit/s wireless local area network connected through access points to the wired Andrew network, a high-speed Ethernet backbone linking buildings across the Carnegie Mellon campus. The combination of networks gives high-speed access to any user with a portable computer and a wireless LAN card from any building covered by access points. In addition, a low-bandwidth wide area network that covers the greater Pittsburgh area provides researchers and others with off-campus wireless access to campus networks. Campus network services include e-mail and file transfer, access to audio and image data, access to the library and other databases, and full Internet access.

The Institute's wireless initiative not only serves the campus community by increasing high-speed access to campus networks, it also provides an infrastructure for research in wireless communication. As the university's Dr. Ben Bennington points out, "What makes us different from other wireless technology customers is that we're not

implementing an application; we're implementing infrastructure, a kind of 'honey pot' to attract people to mobility research".

In the area of infrastructure, Carnegie Mellon has anticipated the need for the next generation of systems to integrate wired and wireless networks by giving researchers a platform for developing and testing "middleware" - software that allows seamless access to the various wired and wireless networks which a roaming computer encounters.

As for mobility research, the system will provide a major test bed for Carnegie Mellon and its sponsors, giving researchers in many fields, inside and outside the university, a way to explore the uses of mobile computing. Programs include systems research, development of computer platforms for mobile use, compression research, and research on the human factors of mobile computing. The Institute's ongoing development is resulting in numerous innovative uses of wireless LANs, including emergency response, health care, and vehicle maintenance. One project involves communication with trains to download diagnostic data. Another involves "wearable Computers" - a project for developing innovative maintenance systems that free technicians' hands while still giving them access to engineering drawings and other information. Benefits: Increased Access to Campus Networks and Creation of Leading Research Platform.

4.7 SUMMARY

Wireless LANs frequently augment rather than replace wired LAN net-works—providing the final few meters of connectivity between a backbone network and the in-building or on campus mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- Doctors and nurses in hospitals are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- Consulting or accounting audit teams or small workgroups increase productivity with quick network setup.
- Network managers in dynamic environments minimize the overhead of moves, adds, and changes with wireless LANs, thereby reducing the cost of LAN ownership.
- Training sites at corporations and students at universities use wireless connectivity to facilitate access to information, information exchanges, and learning.
- Network managers installing networked computers in older buildings find that wireless LANs are a cost-effective network infrastructure c t u re solution.
- Retail store IS managers use wireless networks to simplify frequent network reconfiguration.
- Trade show and branch office workers minimize setup requirements by installing preconfigured wireless LANs needing no local MIS support.
- Warehouse workers use wireless LANs to exchange information with central databases and increase their productivity.
- Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
- Restaurant waitresses and car rental service representatives provide faster service with real-time customer information input and retrieval.
- Senior executives in conference rooms make quicker decisions because they have real-time information at their fingertips.

CONCLUSION

The project has investigated the theory of the Wireless LAN systems. In addition, the standards associated with such systems have been described in detail. Security is an important issue in all types of network related systems. But, the security is much more important in Wireless LAN systems where the components of the system can be located remote from each other, and it is easier for unauthorized people to have access to.

Chapter 1 of the project described in detail the theory of Wireless LAN systems, its advantages and disadvantages.

Chapter 2 has investigated the technological aspects of Wireless LAN systems. The components of typical Wireless LAN systems have been described in this chapter. In addition, the advantages and the disadvantages of various network components have been described in detail.

The important issue of security has been investigated in Chapter 3. It is shown in this chapter that unless a Wireless LAN system is protected, it is easy for unauthorized people to gain access.

Finally, the various application areas of Wireless LAN systems have been investigated in detail in Chapter 4. The application of such systems in manufacturing, education, finance, industry, health, research, and many other application areas have been investigated and the typical application problems have been outlined with examples.

REFERENCES

[1] R.O. LaMaire et al., "Wireless LANs and Mobile Networking: Standards and Future Directions," IEEE Commun. Mag., vol. 34, no. 8, Aug. 1996, pp. 86–94.

[2] ETSI TC-RES, "Radio Equipment and Systems (RES); High PerformanceRadio Local Area Network (HIPERLAN); Functional Specification," ETSI, 06921 Sophia Antipolis Cedex, France, draft prETS 300 652, July 1995.

[3] Wireless Medium Access Control and Physical Layer WG, IEEE DraftStandard P802.11, "Wireless LAN," IEEE Stds. Dept, D3, Jan. 1996.

[4] K. C. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, vol. 8, no. 5, Sept. 1994, pp. 50–63.

[5] W. Diepstraten, "A Wireless MAC Protocol Comparison," IEEE P802.11-92/51.

[6] J. Weinmiller, H. Woesner, and A. Wolisz, "Analyzing and Improving theIEEE 802.11-MAC Protocol for Wireless LANs," Proc. MASCOTS '96, San Jose, CA, Feb. 1996, pp. 200–6.

[7] D. Bantz and F. Bauchot, "Wireless LAN Design Alternatives," IEEE Network, vol. 8, no. 2, Apr. 1994, pp. 43–53.

[8] B. Crow et al., "Investigation of the IEEE 802.11 Medium Access Control (MAC) Sublayer Functions," Proc. INFOCOM 97, Kobe, Japan, Apr. 1997, pp. 126–33.

[9]"LANMANStandardsoftheIEEEComputerSociety.WirelessLANmediumaccesscontrol(MAC)andphysicallayer(PHY)specification.IEEEStandard802.11,1997Edition,"19

[10].Walker,"Unsafeatanykeysize:ananalysisoftheWEPencapsulation,"Tech.Rep.03628E,IE EE802.11committee,March2000.http://grouper.ieee.org/groups/802/11/Documents/ DocumentHolder/0-362.zi%p.

[11].Borisov,I.Goldberg,andD.Wagner,"InterceptingMobileCommunications:TheInsecurity of802.11."http://www.isaac.cs.berkeley. edu/isaac/wep-faq.html.

[12].BlunkandJ.Vollbrecht,"PPPExtensibleAuthenticationProtocol(EAP),"Tech.Rep.RFC2 284,InternetEngineeringTaskForce(IETF),March1998.

[13]Lucent Orinoco, User's Guide for the ORiNOCO Manager's Suite, November2000.

[14].Walker,"Overviewof802.11security."http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3% -Overview-of-802-11-Security.ppt, March2001.

[15]EEE802.11WorkingGroup.http://grouper.ieee.org/groups/802/11/index.html

[16] Academic writing. http://www.lascomm.com/tutorials/tut_WLANbasics.htm.

[17] Documentation, http://www.cisco.com/univercd/home.htm.

[18] Documentation, http://www.commspecial.com/introductiontoWLANS.htm.

[19] Documentation, http://www.connectworld.net/computer/kitco/connectors.htm.

[20] Search, http://www.google.com.

[21] Search, http://www.yahoo.com

GLOSSARY

cess point (APs) The hardware node of a wireless network that local Computers connect to or through. Some hold a PC (PCMCIA) card which can be replaced to upgrade to later
Standards. Always on A connection (especially to the internet) that is instantly available because it is constantly connected (as opposed To dial-up).

-Hoc Mode A client setting that provides independent peer-to-peer connectivity in a Wireless LAN. An alternative set-up is where PCs communicate with each other through an Access-Point.

ndwidth The amount of data that may pass over a connection, Determined by the speed at which it will pass:
2 megabits per second (basic broadband) or 56 kilobits Per second (the fastest domestic modem – narrowband).

uetooth A very short-range wireless link system particularly Suitable for personal technologies such as mobile phone To headset, laptop to printer, or PDA to desktop Computer; operating around 1Mbps.

oadband A faster form of connection (usually applied to the Internet) commonly providing a minimum of 2Mbps, With 8Mbps widely seen as the minimum currently Acceptable for secondary schools, 2Mbps for smaller Primaries. Bandwidth needs can be expected to rise Continually for some years.

SMA/CA (Carrier Sense Multiple Access/Collision Avoidance):
CSMA/CA is the principal medium access method employed by IEEE 802.11 WLANs. It is a 'listen before talk' method of minimizing (but not eliminating) collisions caused by simultaneous transmission by multiple radios. This principle uses a random back-off timer.

ontention ratio Sharing bandwidth between users, possibly resulting in Slowing transmission; measured by the number of users Sharing the given bandwidth, typically 8:1 for the Number of users sharing an access point on a WLAN.

SSS and FHSS Wireless LAN products are available in three different technologies – direct-sequencing spread-spectrum (DSSS), frequency-hopping spread-spectrum (FHSS) and infrared. DSSS and FHSS are spread-spectrum techniques

	that operate over the radio air-waves in the unlicensed ISM band (industrial, scientific, and medical). DSSS uses a radio transmitter to spread data packets over a fixed range of the frequency band. With FHSS the transmitted signal hops between several frequencies at a specific rate and sequence as a way of avoiding interference.
up	A connection through a modem or terminal adapter (ISDN) that is initiated by dialing each time it is needed And closed down again afterwards.
yption	Scrambling data so it is not readable by unauthorized Users. Usually automatically interpreted for those using The correct password.
rnet	The ubiquitous set of standards for computers to Communicate across networks, with varieties for wireless or wired transmission and standards of cabling.
	Interoperability Term describing ability of equipment from different sources to work together.
astructure Mode	A client setting providing connectivity to an Access-Point. As compared to Ad-Hoc Mode where PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central Access-Point. The Access-Point not only mediates wireless network traffic in the immediate neighbourhood, but also provides communication with the wired network. See Ad-Hoc and Access-Point above.
N	Integrated Services Digital Network – a digital service Run over telephone lines (dial-up) that typically offers About twice the speed or bandwidth of a modem (128Kbps) or multiples of that. Incurs a charge per Minute used.
s	Kilobits per second – a measure of the speed of data Transfer or bandwidth. 1000Kbps = 1Mbps.
N	Local area network – a medium-range network Connecting computers and peripherals within a building
N	Metropolitan area network – medium-to long-range Networking available in some major cities, typically at

22+Mbps.

Megabits per second – a measure of the speed of data Transfer or bandwidth. One Mbps = 1000 Kbps.

A set of computer-related equipment linked together to allow the sharing of files, peripherals such as printers and, sometimes, applications usually operating through one or more central servers which service the needs of The others (see also 'Peer to peer').

Personal area network, very local linking – eg, desktop Computer to PDA, (see Bluetooth).

Shorthand for a PCMCIA card.

Fixed internal card for a desktop computer to provide Additional circuitry such as to connect to a wireless Network. Some act as a holder for a PCMCIA card, which Can be replaced to upgrade to later standards.

card Removable thick credit-card-sized plug-in for laptop Computers providing extra functions such as wireless Networking (also becoming available in smaller formats Such as 'compact flash' and 'secure digital' for PDAs).

Personal digital assistant (type of small handheld Computer).

a network of linking computers, of equal status, without A server.

Moving seamlessly from one Access-Point coverage

Area to another with no loss in connectivity.

A device, connected to at least two networks, which Determines the next point to which data that reaches it Should be forwarded to its destination.

Low cost centrally managed computing device that uses Applications running on a central server.

Wide area network – long range, linking between Different buildings in or beyond a town, even Internationally.

Wi-Fi protected access – the later, improved form of Security protection for data transmitted over WLANs, Replacing WEP.

Wireless wide area network – a WAN using wireless Technology – radio, microwave or laser, the latter two Being restricted to line of sight (search www.becta.org.uk for 'wireless wide area network' for More information). To become increasingly common Using advanced mobile phone technologies such GPRS and 3G.

Wired equivalent privacy – the first and basic security protocols available on all Wi-Fi supporting software; defaults to disabled, switchable through at least two levels to a maximum of 128bit. Now replaced by WPA.

Short for 'wireless fidelity' - the popular name for 802.11-based technologies that have passed Wi-Fi certification testing. This includes IEEE 802.11a, 802.11b, and 802.11g technologies. Also used for equipment that contains both 802.11a and 802.11b (or 802.11a and 802.11g) technologies – commonly called 'dual band' or containing a/b/g technologies referred to as tri-band. Wi-Fi certification now also denotes what level of security a piece of equipment offers.

s network A network of computers and peripherals (printers etc) linked without wires, usually through radio transmission.

Wireless local area network, normally achieved using Radio transmission.

LIST OF ABRIVATIONS

D	Accessing Device
H	Authentication header
P	Access Point
A	Certificate Authority
NS	Domain Name Server
SSS	Direct Sequence Spread Spectrum
TSI	European Telecommunications Standards Institute
SP	Encapsulation Security Payload
HSS	Frequency Hopping Spread Spectrum
MAC	key Hashing for Message AuthentiCation
EE	Institute of Electrical and Electronics Engineers
E	Internet Key Exchange
AKMP	Internet Security Association Key Management Protocol
N	Local Area Network
AC	Media Access Control address
T	Massachusetts Institute of Technology
A	National Security Agency
DM	Orthogonal Frequency Division Multiplexing
I	Open Systems Interconnection
S	Perfect Forward Secrecy
I	Public Key Infrastructure
DIUS	Remote Authentication Dial-In User Service
A	Ron Rivest, Adi Shamir, and Len Adleman
D	Security Association Database
EP	Simple Certificate Enrolment Protocol
A	the Secure Hash Algorithm
D	Service Det IDentifier
	Secure Socket Layer
CACS+	Terminal Access Controller Access Control System Plus
	Virtual Private Network
P	Wireless Equivalent Privacy

N	Wireless Local Area Network
	Binary Phase Shift Keying
	Basic Service Set
	Complementary Code Keying
M or OFDM	(coded orthogonal frequency division multiplexing)
	cyclic redundancy check
/CA	Carrier Sense Multiple Access with Collision Avoidance
/CD	Carrier Sense Multiple Access with Collision Detection
	Clear to Send
	Distribution Coordination Function
	Dynamic Host Configuration Protocol
	distribution system
	direct sequence spread spectrum
	Extended Service Set
	Federal Communications Commission (USA)
	Frequency Hopping Spread Spectrum
	Independent Basic Service Set
	Institute of Electrical and Electronics Engineers
	Internet Engineering Task Force
	Internet Protocol
	Internet Protocol security
	Industry, Scientific, and Medical
	International Organization for Standardization
	Logical Link Control
	Media Access Control
	management information base
	network interface card
	network operating system
	Point Coordination Function
	Peripheral Component Interconnect
K	Quadrature Phase Shift Keying
	Ron's Code or Rivest's Cipher
	Request to Send

SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WLAN	wireless local area network
WLANA	Wireless LAN Alliance