DEPLOYING A WIRELESS NETWORK WITH HIGH AVAILABILITY AND SECURITY BOTH IN WAN & LAN CONNECTION

(A CASE STUDY OF SIFAX SHIPPING COMPANY PLC)

YUSUF KARIMOT OMOLAYO
NID/0/FN/019

Department Of Networking And System Security Engineering
Dalewares Institute Of Technology

May, 2012.

DECLARATION

I solemnly declare that, this project is based on a study undertaking by me, under the supervision of MR. FEMS BUBARAYE STEVEN. All ideas and views expressed herein are produce of my personal findings and where the views of others have been expressed, they have been duly acknowledged.

SIGNATURE: ----------

NAME: ----------

MATRIC NO: ----------

DATE: ----------

APPROVAL OF SUBMISSION

I certify that this project **DEPLOYING A WIRELESS NETWORK WITH HIGH AVAILABILITY AND SECURITY BOTH IN WAN AND LAN CONNECTION** was carried out by **YUSUF KARIMOT OMOLAYO** has met the required standard for submission in partial fulfillment of the award of National Diploma in Networking and System Security at Dalewares Institute of Technology.

Approved by:

Signature : _____

Supervisor : MR. FEMS BUBARAYE S.

Date : _____

DEDICATION

This research project is dedicated to God Almighty for his guidance and protection over me all throughout the completion of this programme.

To my wonderful husband, parents, friends and family members for their support.

ACKNOWLEDGEMENT

First and foremost, my sincere gratitude and appreciation goes to God Almighty for being my source of knowledge and strength even in the darkest times. Also, I show my sincere appreciation to my project supervisor MR. BUBARAYE STEVEN who in spite of his crowded workload still had the time to buttress me all-through on this work and I have a great respect for his sense of directions, tolerance, and objectivity. May God continue to provide for him.

I must also let out my special appreciation and gratefulness to my parents, Mr. and Mrs. Yusuf and my wonderful Mr. Hakeem Adesiyan for their love, understanding and financial support channeled towards the success of this programme. A very big thank you to my siblings, Sofiat, Habeeb, Kabir and Seleem and friends in persons of Adebayo Oluseye, Frederick Ozagha, Gideon Animashaun, my immediate family Aisha, Sodiq, Rasheedat, Balikis, Jamiu, Shakirudeen, Muqsit, Sammy and Muiz for their immense contribution and consideration to the success of my education.

To all graduating student of this great citadel of learning, Dalewares Institute of Technology, Lagos, to mention but few Mustapha dare, Akindele Olawunmi, Ekibade John, Tosin, Andrew and Balikis, I say bravo for the pursuit and attainment of academical excellence. Thank you all for your love and support.

ABSTRACT

Today's technology imposes restricted requirements on the corporate users for constant access to their corporate resources. Few instances of these resources are corporate e-mail or web services. Many of these corporate users are mobile, either traveling far or near the physical location of their office. Sometimes it is essential for these remote users to have immediate access to their company resources. Wireless WANs provide the most rapid way of accessing these resources. Cellular Digital Packet Data (CDPD) network is one of the most common wireless infrastructures that is being implemented nationwide today. A CDPD network is an overlay service on top of the existing AMPS (Advanced Mobile Phone Systems) cellular voice networks. A mobile unit in a CDPD Key fingerprint = AF19 FA27 2F94 998D System (MES) is a computer 4E46 a CDPD network, also known, as Mobile End FDB5 DE3D F8B5 06E4 A169 with modem. It has adequate capability for being mobile while connected to the CDPD network.

The CDPD network, on the other hand, guaranties the packet delivery to the MES, while MES constantly changes its physical location. In order for an MES to have access to a CDPD network it must be authenticated either directly by Mobile Data Intermediate System's (MDIS) Mobile Home Function (MHF), while an MES' is in its home area or through MDIS's Mobile Serving Function (MSF) while roaming. After a successful authentication MES can access public networks such as internet. Although CDPD networks provide some level of encryption and authentication, the authentication scheme is unilateral, i.e. only

MES are being authenticated by MHF. Neither MHF nor MSF will be authenticated by MES. In the meantime the traffic encryption is only available over the radio frequency. The lack of a bilateral authentication and partial route encryption are two of the major security concerns in CDPD networks. In this paper the security architecture of a CDPD network will be scrutinized and some possible solutions will be investigated.

The emergence of IEEE 802.11 standards has significantly contributed to the popularity of Wireless Local Area Network (WLAN) implementations over recent years in business organizations, government bodies and even home environment. While WLAN provides greater mobility and flexibility, it also poses security risks that must not be overlooked.

This paper focuses on the security issues of WLAN and attempts to put in place a set of security guidelines to help organizations and home users in securing their WLANs.

TABLE OF CONTENTS

Chapter 1 – Introduction

1.0 Background of the Study

Today's technology imposes restricted requirements on the corporate users for constant access to the corporate resources. Few instances, of these resources are e-mail access or information service access to a centralized IS server. Many of these corporate users are mobile either travelling far or near the physical location of their office. In any case they don't have access to the corporate resources any more. It is sometimes essential for a user to have immediate access to this information. For instance law enforcement agents may need a rapid response for a background check of a suspect. Having the ability to access corporate resources on the fly with minimal wait time is one of the ideas behind wireless network.

Over the years desktop computers have changed from stand alone workstations into networked clients which rely on connectivity. E-mail, remote storage services and the Web are just a few of the uses that are common place in most institutions, both educational and commercial. In addition, computing is becoming more mobile, handheld and notebook computer sales are growing each year. A report from Dataquest Inc. has shown that Notebook sales have increased by 20% each year for the last three years and show no sign of slowing.

This move towards mobile use and a reliance on the network has caused increasing problems for computing departments in all areas of industry and education. To address these problems Radio and Infrared technology is being used to connect mobile users and network buildings which previously would have been impossible. What was once a fledgling technology is being transformed by improved systems into a viable cost effective solution?

Wireless networks can be divided into two areas in much the same way that traditional wired networks are: Local Area Networks (LANs) and Wide Area Networks (WANs). As with wired networks, wireless LANs have a higher data rate and are confined to small areas, either a building or campus. Wireless WANs can cover anything from a city to a continent. The work carried out concentrated on Local Area Networks and much of the content of this study is dedicated to wireless LANs, however, a brief description of wireless WANs is included.

1.1 Project Aims

The aim of this study is to provide you with an understanding of wireless network, its use, application and the technology behind it; it also aims to provide you with solutions to problems in wireless network. This will be achieved by:

- introducing you to what the wireless network consists of
- explaining to you the basic technology underlying the wireless network
- explaining to you the cellular design concept
- helping you to understand the various modulations, diversity and multiple access techniques.

1.2 Course Objectives

To achieve the aims set out above, the study has a set of objectives. On successful completion of this project, you should be able to:

- explain the concept and evolution of wireless network
- identify the various component of wireless network
- discuss in detail difference between wireless data network
- know the difficulties of wireless LAN
- demonstrate the availability of the wireless through W/LAN.
- have a clear view of the wireless network using WAN/LAN
- know the extent to which wireless network can be increased.
- determine the performance of wireless network in information technology.
- determine the level at which wireless network can transmit signals.

- determine the flexibility of the wireless network.

1.3 Brief History of Wireless Communications

1.3i Before the "Birth of Radio" 1867-1896

- 1867 - Maxwell predicts existence of electromagnetic (EM) waves
- 1887 - Hertz proves existence of EM waves; first spark transmitter generates a spark in a receiver several meters away
- 1890 - Branly develops coherer for detecting radio waves
- 1896 - Guglielmo Marconi demonstrates wireless telegraph to English telegraph office

1.3ii "The Birth of Radio"

- 1897 – "The Birth of Radio" - Marconi awarded patent for wireless telegraph
- 1897 - First "Marconi station" established on Needles Island to communicate with English coast
- 1898 - Marconi awarded English patent no. 7777 for tuned communication
- 1898 - Wireless telegraphic connection between England and France established

1.3iii Transoceanic Communication

- 1901 - Marconi successfully transmits radio signal across Atlantic Ocean from Cornwall to Newfoundland
- 1902 - First bidirectional communication across Atlantic
- 1909 - Marconi awarded Nobel Prize for physics

1.3iv Voice over Radio

- 1914 - First voice over radio transmission
- 1920s - Mobile receivers installed in Police cars in Detroit
- 1930s - Mobile transmitters developed; radio equipment occupied most of Police car trunk
- 1935 - Frequency modulation (FM) demonstrated by Armstrong
- 1940s - Majority of Police systems converted to FM

1.3v Birth of Mobile Telephony

- 1946 - First interconnection of mobile users to public switched telephone network (PSTN)
- 1949 – Federal Communication Commission (FCC) recognizes mobile radio as new class of service
- 1940s - Number of mobile users > 50,000
- 1950s - Number of mobile users > 500,000
- 1960s - Number of mobile users > 1,400,000
- 1960s - Improved Mobile Telephone Service (IMTS) introduced; supports full-duplex, auto dial, auto trunking
- 1976 - Bell Mobile Phone has 543 pay customers using 12 channels in the New York City area; waiting list is 3700 people; service is poor due to blocking

1.3vi Cellular Mobile Telephony

- 1979 – NTT Communications Corporation Japan deploys first cellular communication system
- 1983 - Advanced Mobile Phone System (AMPS) deployed in US in 900 MHz band: supports 666 duplex channels
- 1989 - Group Spècial Mobile defines European digital cellular standard, GSM

- 1991 - US Digital Cellular phone system introduced
- 1993 - IS-95 code-division multiple-access (CDMA) spreadspectrum digital cellular system deployed in US
- 1994 - GSM system deployed in US, labelled "Global System for Mobile communications"

1.3vii PCS and Beyond

- 1995 - Federal Communication Commission (FCC) auctions off
- frequencies in Personal Communications System (PCS) band at 1.8 GHz for mobile telephony
- 1997 - Number of cellular telephone users in U.S. > 50,000,000
- 2000 - Third generation cellular system standards. Bluetooth standards.

1.4 Scope Of The Study

The scope of this study covers the following areas:

- Physical Security;
- Confidentiality and Integrity;
- Key Management;
- User Authentication;
- Access Control;
- Client Security;
- User Awareness;
- Administration of access points;
- Availability and
- Logging and Audit Trail

1.5 Motivation

Network security is an interesting and stimulating field, whose development has enabled technological growth in various organization, were by unauthorized user

cannot get access to your system. To further this development, it is essential to fully know understand the concepts involved in wireless network & security.

1.6 Conclusion

Chapter one presents a general introduction to the project report. It begins with the aims of the project and some of the background knowledge necessary for writing the report. The course objective was discussed; follow by the scope of the study and motivation for carrying out the project. The next chapter shall be the technical background related to the project. It gives a description of the Wireless Network Overview, LAN & WAN, Devices, LAN difficulties and security options used in the development of the project.

Chapter 2 - Technical Background

2.0 Introduction

This chapter discusses the technical background of the project in its entirety and the unique constituent sections addressed in the project. First an overview of the wireless network is discussed. Finally, each individual component of wireless network is discussed in detail.

2.1 Wireless Network Overview

Wireless network is a type of computer network where communication or exchange data among various devices on the network are carried out without the use of cables, This means, the connection and exchange of data between computers and other devices in a particular network is made possible by radio signal frequency (RF) or electromagnetic waves in the atmosphere instead of cables.

2.1.1 Wireless Networks

Wireless networks, the medium of connection or mode of transmitting are radio waves, space, or microwaves. Wireless networks may include the home wireless connection between a wireless router and a computer with a wireless network card, the global wireless connection between two ground stations, or the communication between devices on earth and satellites then received via the internet.

2.1.2 Features of Wireless Networks

- Data are transmitted and received through airwaves.
- It also infrared light to transmit signals
- It 10 mbps to transmit signals i.e. wireless LAN
- Some of its devices used is WAP (Wireless Access Point), W/LAN Card, Antenna, Radio, VSAT, Satellite devices etc

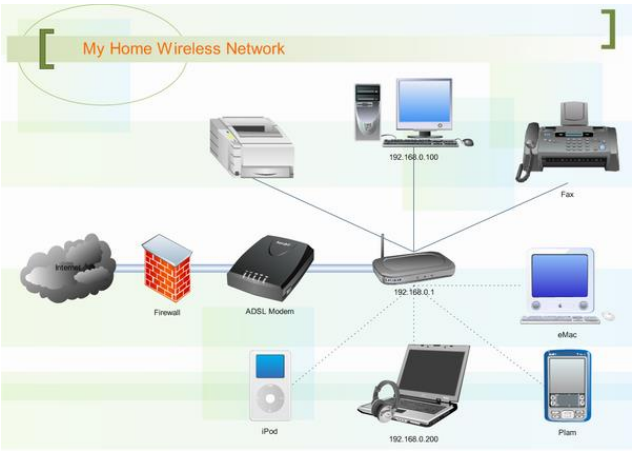


Fig. 1

2.1.3 Devices and Media

Devices and media are the physical elements or hardware of the network. Hardware is often the visible components of the network platform such as a laptop, a PC, a Switch, Router or the cabling used to connect the devices. Occasionally, some components may not be so visible. In the case of wireless media, messages are transmitted through the air using invisible radio frequency or infrared waves.

2.2 Network Devices

There are specially designed network devices that are used to interconnect LANs. Configuring, installing and maintenance of these devices require expert skills by

skilled technicians for the management of the organization's network. These devices are specific to WAN environment, and they are:

2.2.1 Modem

Modem enables digital data to be sent over an analogue medium during transmission and receiving of information

A voice band modem converts the digital signals produced by a computer – the 1s and 0s- into voice frequencies that can be transmitted over the analogue lines of the telephone network. On the other side of the connection, another modem converts the sounds back into a digital signal for input to a computer or network connection.

2.2.2 CSU/DSU

Channel Service Unit / Data Service Unit CSU/DSU are combined piece of equipment used for monitoring clocking and frame synchronization on a line. It also performs error detection at the physical layer, It could be called a Modem sort of.

2.2.3 Access Server

Concentrates dial-in and dial-out user communications. An access server may have a mixture of analogue and digital interfaces and support hundreds of simultaneous users.

2.2.4 Routers

Routers are generally known as intermediate systems, which operates at the network layer of the OSI reference model, routers are devices used to connect two or more networks (IP networks) or a LAN to the Internet.

The router is responsible for the delivery of packets across different networks. The destination of the IP packet might be a web server in another country or an

e-mail server on the local area network. It is the responsibility of the router to deliver those packets in a timely manner. The effectiveness of internetwork communications depends, to a large degree, on the ability of routers to forward packets in the most efficient way possible.

Routers are now being added to satellites in space. These routers will have the ability to route IP traffic between satellites in space in much the same way that packets are moved on Earth, thereby reducing delays and offering greater networking flexibility.

ROUTER *Fig. 2*

2.2.5 Advantages of A Router

In addition to packet forwarding, a router provides other services as well. To meet the demands on today's networks, routers are also used:

- To ensure steady, reliance availability of network connectivity. Routers use alternative parts in the case the primary part fails to the delivery of packets.
- To provide integrated services of data, video, and voice over wired and wireless networks.

For security, router helps in mitigating the impact of worms, viruses, and other attacks on the network by permitting or denying the forwarding of packets.

2.2.6 Switches

A Network switch is a device that filters, forwards, or floods frames based on the destination address of each frame. A switch is a very adaptable Layer 2 device; it replaces a hub as the central point of connection for multiple hosts. In a more complex role, a switch may be connected to one or more other switches to create,

manage, and maintain redundant links and VLAN connectivity. A switch processes all types of traffic in the same way, regardless of how it is used.

A switch moves traffic based on MAC addresses. Each switch maintains a MAC address table in high-speed memory, called content addressable memory (CAM). The switch recreates this table every time it is activated, using both the source MAC addresses of incoming frames and the port number through which the frame entered the switch.

Switches perform their routing functions at the layers 2 model of the OSI. Some switches process data at the Network Layer (layer 3), this types of switches are referred to as layer 3 switches or multilayer switches. Switches form an integral parts in networking LAN or WANs. Small office, Home office (SOHO) applications normally, use a single or an all purpose switches.

Fig. 3 **SWITCH**

As mentioned earlier, switches operates at the data-link layer of the OSI model, switch function is to create a different collision domain per switch port. Let take an example, Four computers **PC 1**, **PC 2**, **PC 3**, **PC 4** attached to switch ports, then PC 1 and PC 2 can transfer data between them so as PC 3 and PC 4, simultaneously without interfering with each other's conversations. Unlike a hub, which allows the sharing of bandwidth by all port, run in half-duplex and is prone to collisions of frames and retransmissions?

2.3 Cabling Network Devices

2.3.1 Types Of Cables (Media)

Choosing the right cable necessary to make a successful Local Area Network (LAN) or Wide Area Networking (WAN) connection requires deliberation of the different media or cable types. For the benefit of beginners, there are many different Physical layer implementations that support multiple cable types:

- **UTP (Category 5, 5e, 6, and 7)**
- **Fibre-optics**
- **Wireless**

2.3.2 Advantages and Disadvantages of Cables

Some of the factors to consider are:

- **Cable length** – how far will the cables have to go around the room or building?
- **Cost** - Does the budget allow for using a more expensive media type?
- **Bandwidth** – this is one of the criteria to focus your thoughts on. Does the technology used with the Cable provide adequate bandwidth?
- Susceptible to Electromagnetic interference also called radio frequency interference (**EMI/RFI**) - Is the local environment going to interfere with the signal?
- UTP cabling connections are specified by the Electronics Industry Alliance/Telecommunications Industry Association (EIA/TIA).

2.3.3 RJ-45

The RJ-45 connector is the male part crimped on the end of the cable. When viewed from the front, the pins are numbered from 8 to 1. When viewed from above with the opening gate facing you, the pins are numbered 1 through 8, from

left to right. The standard lengths for this cable are 1.83m (6ft) and 3.05m (10ft). This orientation is important to remember when identifying a cable.

Fig. 4

RJ45 Top View

Fig. 5

A B

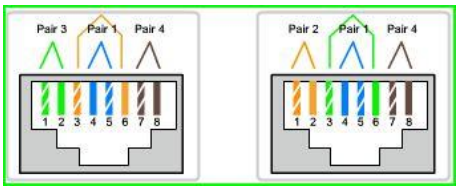


Fig. 6

RJ45 Cable Orientation

2.4 Wireless Networks Vs Wired Networks

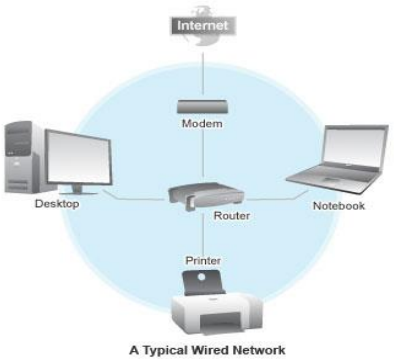
Although it was once common practice, having a single computer and solitary Internet connection in the home is hardly the norm these days. Waiting in line to use the Internet connection is now almost a thing of the past (if not having enough computers aren't an issue). Of course, whether you have a wired network or a wireless local area network (WLAN), multiple users on the same Internet line put a strain on the connection's speed, and download time will be affected.

One of the primary benefits of LANs is the ability to share files (images, documents, mp3 music files, etc) and even external hardware (printers, scanners, and so forth), which makes for a much more convenient system of home

computing. However, this requires one computer to be established as a main (or "server") computer, with other computers on the network then needing to connect to that, rather than the "router" (which cannot share files). (A "router" is a device that is plugged into the telephone socket on your wall in order to harness your Internet connection and then broadcast it to other computers). Computers can be "networked" with wires or wirelessly, so one questions remains: which way is best? A mostly wire-free home network (using a wireless-enabling router) or a cable-interconnected "plug in" type system (via router or modem)?

2.4.1 Differences between Wired and Wireless Networks

There are a couple of big differences between setting up a wired network and setting up a wireless network. Wireless networks are generally accepted to be the easiest to set up, with a "network wizard" or "network assistant" instructional set-up tool found in all Macs and PCs. This guides you through the process of creating your network on the first computer gaining access; the computer essentially setting up the network. It also helps you to join a network if you are using the assistant tool on an additional computer thereafter. Wireless networks require a router for Internet access. Computers that are hardwired do not necessarily need a router for Internet access if there is not more than one computer. That considered, such a system would hardly qualify as a "network", with only one computer connected. The point specifically is that a modem cannot be accessed wirelessly and so a router is needed for any number of computers gaining access via wireless connection, be it one or 100.



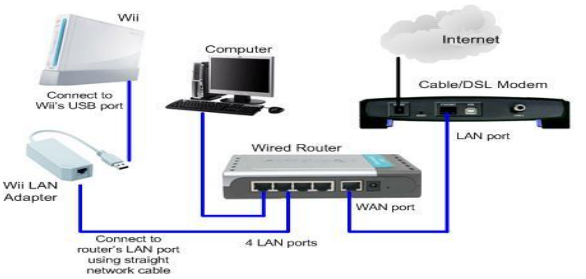


Fig. 7 **Wired Network** *Fig. 8* **Wireless Network**

2.4.2 Wireless Network Pros

- ✓ Very convenient in the home, especially for laptops
- ✓ Easy to set up (you can get your Internet Service Provider, or "ISP", to set it up for you if you're having problems, for an additional fee).
- ✓ Less clutter

2.4.3 Wireless Cons

- ✓ Slower transfer rate
- ✓ Can 'drop out' occasionally
- ✓ Not as secure

2.4.4 Wired Network Pros

- ✓ Faster transfer rate
- ✓ More secure

2.4.5 Wired Cons

- ✓ Requires a little knowledge to set up (but it could be argued that configuring wireless networks also requires at least a basic computer knowledge)

- ✓ Not convenient if you wish to use your laptop anywhere in the house

If you're thinking about setting up a home network to make sharing of Internet access and files possible (or your laptop more mobile), it's best to consider what your needs are: how many computers will need to join the network? Are they mainly laptops or desktops? Is security the top concern for you? It is hardly worth setting up a wired network if your computers are mainly laptops and you trust the security of your router. Likewise, it may not be worthwhile compromising security by setting up a wireless network if you are only using two desktop computers in the same room. Whatever your needs, networking is a hugely convenient way to facilitate multiple-user Internet and peripheral hardware device access and can help to save the most crucial of all resources; time.

2.5 Wireless LAN

Wireless networks are a reality, with installations being common place in hospitals and trading rooms everywhere. The recent ratification of the IEEE 802.11 Standard for Wireless LANs has legitimized the systems which are widely available and given consumers the confidence to start investing in wireless technology. The intention of the wireless LAN is not to replace the wire, as reduced speed and other complications have meant that wired systems will always be more cost effective in a typical environment. Wireless systems are designed to solve problems which wired solutions cannot address. The most obvious scenario would be the mobile user who needs to access network resources from his or her portable computer. A wireless network would allow them to work from any location within the wireless LAN and access the network resources with the minimum of effort. In contrast to the mobile solution, a wireless system could be used with desktop computers, for example, in a listed building, where regulations prevent cables being installed. A wireless solution would allow the desktop computers to connect to a network without disturbing the structure of the building. Another use might be a temporary network, for

example at an exhibition. A wireless LAN could be set up within minutes and then dismantled after the exhibition has finished leaving no trace.

Wireless networks can be implemented in two ways. Those listed above are examples of structured networks, where the wireless LAN is an extension of the existing LAN. Another type of wireless network is the ad-hoc, peer to peer network which may be set up quickly between several laptop computers for the duration of a meeting. This form of wireless network is the simplest, requiring no infrastructure and, depending on the number of users, little or no administration. Structured wireless LANs are more complex. They consist of Access Points (AP) spread around a building and connected together or onto the wired LAN using copper cable. Mobile users in range of an AP can connect to other wireless users or to network resources. As a user moves around the building the AP hands off responsibility for that user to the next AP.

2.5.1 Wireless LAN 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 networked computing 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 this 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 and can take at least 30 to 50μs to determine if the channel is clear; by itself a nontrivial portion of the packet transmission time. Coupled with this, the hidden terminal problem has been identified in wireless systems and is caused by problems in collision detection. 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.

The solution involves sending a small packet (Request To Send, RTS) to the intended recipient to prompt it to send back a packet (Clear To Send, CTS). 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 contain the length of the impending data transmission so stations overhearing either of the frames know how long the transmission will take and when they can start to send themselves. Carrier sense is also used to help prevent station transmitting RTS packets at the same time.

Another problem can be caused by signals bouncing off walls and other surfaces, known as multipath fading. 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, as it involves having two antennas built into the hardware, and so allows the system to determine which signal is stronger and therefore the correct signal.

2.5.2 Wireless LAN Agencies

There are some international agencies that create standard on behalf of wireless lan.

- IEEE: Institute of Electrical Electronics Engineering

- They create and maintain operational standard of wireless LAN and their website is ieee.org.
- FCC: Federal Communication Commission
- It regulates the use of wireless devices in U.S. Their website is www.fcc.gov.
- ETSI: European Telecommunication Standard Institute
- They produce common standard of wireless network in Europe. Their website is www.etsi.org.
- WIFI: Wireless Fidelity
- It is an alliance between different wireless producing vendors to promote and test for wireless lan inter-operability. Their website is www.wifi.org.
- WLANA: Wireless LAN Association
- They educate and raise consumers' awareness regarding wireless LAN. Their website is www.wlana.org.

2.6 IEEE 802.11

The IEEE 802.11 standard has been drafted to allow manufacturers to develop equipment which is compatible with other manufacturer's product. The IEEE 802 standard was originally developed for wired local area networks but as technology has progressed subsets of the standard have been published. The standard defines a single MAC layer and three Physical layers (PHY). The physical layer includes two specifications for radio operating in the 2.4GHz - 2.4835GHz ISM band: Direct Sequence Spread Spectrum Radio, Frequency Hopping Spread Spectrum Radio, together with a Diffuse Infrared PHY layer. Data rates of 1Mbit/s and 2Mbit/s have been specified for all the technologies.

The MAC layer has specifications for two modes of operation,

• Independent configuration

Stations communicate directly with each other, without the need for access points, a so called 'ad-hoc' network. This form of network has been defined as a **Basic Service Set.**

• Infrastructure configuration

Stations communicate with an access point which is connected to a wired network providing access to network resources. The area around the access point is considered to be a Basic Service Set (BSS), with several BSSs being defined as an **Extended Service Set.**

In addition, the MAC layer will provide the following nine services split between the Access Point and the mobile Client: Authentication, deauthentication, privacy, MSDU delivery, association, disassociation, distribution, integration and reassociation.

The IEEE 802.11 working group has also set up a study group to investigate future enhancements of the standard. Two projects currently awaiting approval aim to investigate a PHY layer operating in the 5GHz band and a PHY layer for higher speeds in the 2.4GHz band. Both projects hope to yield improved performance for radio wireless LANs.

2.6.1 Wireless Standards 802.11 Committees and Functions/Purpose.

- 802.11a: Supports 54mbps, 5ghz standards.
- 802.11b: An enhancement to 802.11 to support 5.5 mbps and 11mbps.
- 802.11c: Support bridge operation procedures and is included in the 802.10 standard.
- 802.11d: Support international roaming extension.
- 802.11e: Support quality of service QOS.
- 802.11f: Support inter access-point protocol.
- 802.11g: Support 54mbps, 2.4 GHz standard.
- 802.11h: Support dynamic frequency selection DFS and transmit power control TPC at 5 GHz.
- 802.11i: Support enhanced security 802.11j.

- 802.11k: Support radio resource measurement and enhancement.
- 802.11m: Support the maintenance of this standard such as odds and ends.
- 802.11n: Support higher throughput improvement using MIMO antenna.
- 802.11p: Support wireless access for the vehicular environment.
- 802.11r: Support fast roaming.
- 802.11s: Support extension service set ESS mesh networking.
- 802.11t: Support wireless performance prediction.
- 802.11u: Support inter-networking with non 802 networks such as cellular or mobile phone.
- 802.11v: Support wireless network management.
- 802.11w: Support protected management frames.
- 802.11y: Support 3650 to 3700 operations in the U.S.

2.7 Wireless WAN

The most familiar form of wireless network is a Mobile Phone network. Millions of people around the world use mobile phones to connect them to a Public Switched Telephone Network. Mobile phone service providers invest an enormous amount of capital into creating an infrastructure which links antennas, known as base stations, through mobile switching offices to a central office then onto the phone network. Several different standards for mobile phone technologies have been developed in the USA and Europe based on either Analogue or Digital Radio technology.

Instead of attempting to create a separate wireless WAN for data traffic, although this has been attempted by some companies, most service providers in the industry are attempting to offer a service using their current mobile phone network. Using the existing mobile phone infrastructure has several advantages over specialized wireless WAN ventures. These advantages include the instant coverage of large geographical areas, an existing administrative system for billing and maintenance, and a service which has already been established as reliable and

cost effective in the eyes of most potential customers. These advantages have been highlighted by many industry analysts as a sound basis for the service providers to offer a commercially viable voice/data network. This network could offer three different types of service: a datagram's service used for applications such as credit card transactions, a broadcast service used for road traffic announcements and other advisory services and, finally, a fully interactive service allowing client/server connections. However, attempting to integrate data traffic onto a voice network introduces many problems associated with transmitting data over a medium designed for voice. The earlier mobile phones were based on analogue technology and are still widely used in the USA and to a lesser extent in Europe. A data network service provided across these older technologies is all but impossible, although some services do exist. Low capacity, low security, high noise and high cost are just some of the disadvantages of analogue systems, making them less than ideal for data transmission.

Cellular Digital Packet Data (CDPD) networks are an attempt to overcome the problems of data transmission over analogue systems. The technology uses channel hopping to transmit data in the analogue channels used by mobile phones. The system is able to coexist by only using the channels during times when they are idle and in cases when a conflict occurs, giving voice traffic priority. This service successfully addresses the problems of analogue data transmission, providing higher security, higher data rates and other features such as message broadcast, roaming, compression and authentication. CDPD, however, is only likely to be an interim solution as it still runs over an analogue infrastructure.

An alternative to using existing Mobile Phone networks is to use a specialized wireless WAN. Two such systems are already implemented in parts of the USA and Europe: ARDIS from IBM/Motorola and MOBITEX from Bell/Ericsson. The technology used is still analogue and very similar to mobile phone systems; however, only data is transmitted across these networks. The ARDIS system was

set up to support IBM field engineers, but has been expanded to offer a commercial service. Some 400 cities in the USA have base stations allowing access to the ARDIS network. The performance of the system is not very high with data rates of less than 2400 bits/s but a faster system of 19,200 bits/s is being planned. The MOBITEX network is a newer system and already supports 19.2Kbit/s data rates, although subscriber throughput is less than this figure. Due to the relatively small market base and the expense of the radio transceivers, the systems have not been widely subscribed to.

The future of fully integrated data/voice networks is Digital Cellular Technology. Digital Cellular services are already widely used in Europe and Asia using the Global System for Mobile Communication (GSM). Although predominantly used for voice transmissions, the
service offers all the requirements for a data network. High security with the use of encryption, increased capacity and performance, better recovery from noise using error correction are just a few of the features incorporated into the original standard from the system. The standard was designed from scratch as an integrated data/voice network and was not hindered with the need for backward computability as with the US and the Japanese systems. Consequently, it has been because of this that the system has been adopted by over 50 countries around the world making it ideally placed as a future standard for global wireless WANs.

2.8 Security

With any network security is an important consideration. Unauthorized access can result in several forms of attack such as information theft, denial of service; where an attacker attempts to make the network unusable, and the most common form of attack, intrusion; where an attacker desires access to computers or resources on the LAN. Once an unauthorized user has gained access to the flow of data over a network, promiscuous monitoring of the network can lead to user names and passwords being intercepted and used for further attacks.

Traditionally, the physical security of a building and the offices in that building afforded some security to the LAN. Yet the nature of the wireless medium means that signals cannot be controlled as easily and even a secure environment cannot prevent radio signals from passing through walls and beyond confines of a company's buildings or grounds. The problem has already been encountered in the industry, with a case brought to court in America involving a service vendor which intercepted a rival's customer list as it was being transmitted over the ARDIS network.

In the past wireless network manufacturers have relied on the complexity of the technology to provide security. This assumption was essentially sound when one considered that the technology was originally developed by the military. In practice this approach works to a degree, because with radio, for example traditional methods of intercepting radio transmissions cannot detect a spread spectrum signal. This model breaks down though when the same vendor's equipment is used by unauthorized people to access the LAN. To overcome this flaw some manufacturers use encryption to encode transmissions and so make the signal indecipherable if intercepted.

Complete confidence can only be achieved when a wireless network is treated in a similar manner to an Internet connection, where data is being transmitted over an unsecured medium susceptible to interception. Similar precautions to those put in place to accommodate an Internet connection should be implemented for a wireless network. A gateway with functions such as authorization and authentication, possibly even encryption, could be implemented, creating a firewall to secure a network from the vulnerabilities of a wireless network.

2.8.1 Security Threats

The security risks in WLAN extend beyond those in a wired network to include the new risks introduced by the weaknesses in wireless protocols. The security threats posed by WLAN include: Eavesdropping –Intercepting information that is

transmitted over the WLAN is generally easier as it can be done from a distance up to kilometres3 outside of
the building perimeter without any physical network connection required. The information intercepted can be read if transmitted in clear or easily deciphered if only WEP encryption is used.

2.8.1i Traffic Analysis

The perpetrator gains intelligence by monitoring the transmissions for patterns of communication, information flow between communicating parties and deciphering of encrypted traffic captured. This may result in disclosure of sensitive information.

2.8.1ii Data Tampering

The information transmitted over the WLAN can be deleted, replayed or modified by the perpetrator via man-in-the-middle attack4. This may result in a loss of data integrity and availability. 3 With high gain antennas, the distance can vary up to kilometres even when the nominal or claimed operating range of wireless device is less than a hundred meters. An antenna with 24dBi gain can reach as far as 32miles and it is widely available via the Internet. 4 Using devices to masquerade as a trusted wireless access point, the perpetrator can manipulate all wireless traffic transmission between the wireless client and the backend systems.

2.8.1iii Masquerading

The perpetrator gains unauthorized access to the information and network resources within the WLAN or other interconnected network by impersonating

the identity of an authorised WLAN user. The perpetrator can create further havoc by launching attacks or introducing malicious codes that will disrupt operations. Denial of Service (DoS) – The perpetrator can jam up the entire frequency channel that is used for wireless data transmission using a powerful signal generator, microwave or massive network broadcasting traffic from a rouge wireless device. With high gain antennas and WLAN attack tools, the perpetrator can cause denial of service without close proximity to the targeted WLAN. Furthermore, it is not possible to locate the perpetrator base on current detection solutions. This attack can cause a denial of service and unavailability of information and network resources.

2.8.1iv Wireless Clients Attacks

The perpetrator can potentially gain access to the information shared or stored in the wireless client when it was connected to an unprotected ad hoc WLAN or an untrusted third party WLAN. Furthermore, the compromised wireless client can potentially serve as a bridge to the corporate internal network, thus allowing perpetrator to gain access or launch attacks against the corporate internal network and resources.

2.8.2 Why Is Security Important?

Where there is a network, wired or wireless; there are threats. Some people are easily put off setting up a home or office network with the fear that anything stored in their hard drive could be accessed by neighbours' or hackers .The types of potential threats to network security are always evolving .Constant computer network system monitoring and security should be an ultimate priority.

If the security of the network is compromised, there could be serious consequences, such as loss of privacy, and theft of information. When it comes to network security, the main concern is making sure that any wireless connections are protected against unauthorized access.

Most business transactions are done over the internet. In addition, the rise of mobile commerce and wireless networks demands that security solution become flawlessly integrated, more transparent, and more flexible. The internet has grown over the years and still growing, this is due to the flexibility of its design.

Network attack tools and methods have evolved. Back in the days when a hacker had to have sophisticated computer, programming, and networking knowledge to make use of rudimentary tools and basic attacks. Nowadays, network hackers, methods and tools has improved tremendously, hackers no longer required the same level of sophisticated knowledge. People who previously would not have participated in computer crime are now able to do so.

2.8.3 How To Secure Wireless Network

There are certain steps which ensure that your Wi-Fi traffic is not interrupted by anyone and here are few steps: Some or the other time we have always jumped on someone's Wi-Fi network causing insecurity to data. But if you have no wrong intentions and are a good soul still there is little harm in it.

But as no two people in this world are alike so it's very difficult and scary to trust anyone if you own some unsecured network as some dishonest people may do their job well causing harm. But don't worry as there are few basic steps to fix the problem.

2.8.3i Wireless Router.

Encryption is the first step towards your Wi-Fi network security as the data is well encoded when transmitted between PC and wireless router. But still there are many routers which have the encryption just turned off and this allows many users to leave themselves open towards unsecured web as their identity is being traced. If the router's encryption is not completely enabled then encryption is very strong asset to support your network. As technology is changing and so the

routing protocols too. Like the Wireless Protected Access and WPA2 are latest in encryption technology so it has surpassed the less secured Wireless Encryption Protocol.

Fig. 9

WEP is easy to crack as today WPA or WPA2 are best possibly used today. (You should not fuse WEP and WPA and have to use same form on all devices). As the key used are same so it makes them very difficult to hack. The password used should not be weak and must comprise of numerals, alphanumeric characters, and must be more than 14 characters.

You must check for 128-bit WEP keys if you are using WEP support router and must also check the website of manufacturer for updating WPA support after adding it. If this is not suitable option for you then you can update the old router models and adapters with WPA. You can also look for router that is on hybrid mode (WPA + WPA2). This supports strong encryption called WPA2 with adaptors supporting it so that compatibility is always maintained with WPA adapters. The default network name and password on the router must always be changed. If this is done then it becomes very difficult for hackers to get in router settings.

As the firewall is into your router so internet access cannot be given to particular router and hence its secured from hackers. But this will not prevent people from getting over the Wi-Fi signal on the network and with high performance equipment and latest Wi-Fi signal one can reach the clear down block. But all the Wi-Fi traffic tools can be used by anyone without any encryption and precautions.

You can also run software firewalls on respective PC’s for high level protection on particular network. You can easily download some good options like Zone

Labs' Zone Alarm Security with Agnitum's Firewall. As not many public places use encryption facilities so it's difficult that Internet traffic will be secured as you are exposed globally.
The hotspot should be legitimate: At some nefarious hotspots, pirate routers have been set up with familiar SSID names like "way port" or "t-mobile" and then these are being used in capturing unsuspecting information of users and several private data.

The software firewall of your PC must be turned on, file sharing windows feature must be off and it should be off by default with Service pack 2. You will find this setting in control panel and choose Windows Firewall then you can also see that in Security Centre first of XP or Vista. You can see in the Programs and Services and find the XP exception tab to make sure that "File and Printer Sharing" is not checked. You can follow the instructions of XP in Change Settings in Vista and then the exceptions tab should be selected.

You should never exchange confidential and important data like credit card numbers, bank details, debit cards pin over unsecured sites: First find the lock icon in bottom right corner and the URL address of the browser such that the address bar comprises of https. These sites have their own encryption.

If you are not at hotspot then you can always turn off the radio: The create peer-to-peer Wi-Fi network connections are created by hackers only in computer for direct access.
You should always subscribe to paid network connections to have enhanced security and tunneling protocols. The connection software used provides one easily with automatic and secured sessions.

VPN is virtual private network which allows protecting the common wireless link and is best, cost effective way for security. Just by keeping secured tunnels by which the private data travels are ensured for safe communication. The Vpn

services are provided to mobiles and workers too. You can check with the IT department for connection instructions.
A paid service like the Boingo's VPN is available for free trial with Witopia, JiWire Hotspot Helper at an average cost of $25 to $40 per year. These services are very simple in use and very easy to install.

As this is the best security option so connecting through your home and office is not a problem. The public hotspots can be used with ultimate security for remote access programs like LogMeIn, GoToMyPC

2.9 CDPD Network Components

2.9.1 Mobile End System (MES)

The mobile unit, also known as Mobile End System (MES) is an independent network component, which helps a network end user to have access to CDPD network. Usually it is in a form of a specialized modem with a small footprint that can be used by a computer system for wireless access to CDPD network. MES communicates through the airlink with other network components. The CDPD network, on the other hand, guaranties the packet delivery to the MES. Providing such services by the network it is required to identify each individual M-ES in different locations. Mobile end systems use protocols defined up to OSI layer 3, which makes MES capable of having an IP address.

2.9.2 Mobile Database Station (MDBS)

Mobile Data Base Station (MDBS) performs two functions. First, it is a device that

arbitrates the activities on a channel that it manages. In a CDPD network much like the Ethernet, an RF channel is shared between several MES. In this case MDBS is arbitrators in CDPD MAC scheme, also known as digital sense multiple

access. Upon successful reception of bit stream it relays everything back to mobile data intermediate system.

2.9.3 Intermediate System (IS)

Intermediate System is a physical device responsible for routing and forwarding packets either using a Connectionless Network Protocol (CLNP) or Internet Protocol (IP). CLNP is being used for routing datagram between Mobile Data Intermediate Systems. However, IP can be used for forwarding and routing of datagram between MDIS and MES. Other functions of IS are route calculation, fragmentation and congestion mitigation. In other words is a multi-protocol router.

2.9.4 Mobile Data Intermediate System (MDIS)

MDIS is responsible for routing functions based on the MES location. It employs two different routing functions: Mobile Home Function (MHF) and Mobile Serving Function (MSF), which provide network services to MES regardless of its location. The idea behind the MHF is that each MES logically belong to a home area managed by home MDIS. The MHF keeps track of all of its MES community, either when they are in the home area or in serving area while roaming. When MES are roaming the packets that are addressed to them will be forwarded to the MSF in each serving area. On the other hand the MSF of an MDIS acting as a routing function for the visiting MES and it provides the necessary services for those MES. During the MES registration the MSF forwards all the registration requests to home MDIS's MHF module.

2.9.5 Fixed End System (FES)

FES is any system that is not mobile. It may be external or internal to the CDPD networks. The external F-ES may be located on any network anywhere in the Key fingerprint = AF19 FA27 2F94 998D instance some of 06E4 A169 4E46 are the

world connected over a landline. For FDB5 DE3D F8B5 the external FES hosts that mobile end users connect to send email or accessing some web pages. Internal FES can be used by CDPD service providers to operate administrative services on the network.

2.10 Problem Definitions

2.10.1 Security Handling in CDPD Networks

In contrast to many other network protocols, CDPD specifications took into consideration the potential security issues [13] and it supports a set of primary security functions over the air link. These functions are:

- **Confidentiality** of the data link, after determining a secret key all the traffic between the MES and MD-IS are encrypted in both ways.

- **Key Management,** The encryption algorithm guaranties the message privacy over the A interface. The key exchange and management is based on Diffie-Hellman algorithm.

- **MES Authentication,** The MHF module of the home MDIS authenticates the KeyMES based AF19 shared historical FDB5 DE3D F8B5 06E4 A169 4E46 a tuple

- **Fingerprint =** on a FA27 2F94 998D record (SHR) and NEI. SHR is two numbers: a 16 bit authentication sequence number (ASN) and a 64 bit authentication random number (ARN).

2.10.2 Encryption and Authentication in CDPD Networks

During MES registration process and while it is roaming through Mobile Network Registration Protocol (MNRP) MES requests for a temporary network identification number (TEI) from MSF module of the serving MDIS. In response

the serving MDIS assigns a TEI to the MES and establishes a link. After the assignment of TEI the serving MDIS initiates a key exchange algorithm. The key management is based on Diffie and Hellman [3] key exchange procedure.

Fig. 10

The key exchange procedure is initiated by sending a MDIS key exchange (IKE) datagram also known as protocol data unit (PDU) to MES. The IKE PDU contains a triplet of:

2.10.3 Security Loopholes In CDPD Network

CDPD specs is designed so that all MES can be authenticated by home MDIS. Besides, the traffic on the A-interface is also encrypted and privacy of the messages between the MES and serving MDIS is provided by the MSF. However, CDPD network does not provide any bilateral authentication between all parties. For instance, neither MES authenticates the MSF nor MSF authenticates MES. In other words, there is no bilateral authentication process between the visiting MES and serving MDIS.

Chapter 3 – Design

3.0 Introduction

This chapter describes the design of the wireless network deployment both in LAN/WAN. It begins with the use of Radio and Infrared Technology. Then the more specific designs and implementations for wireless networks are discussed in detail.

3.1 Radio Technology

Radio network technology exists in two forms: narrowband technology and spread spectrum technology. Narrowband systems transmit and receive data on a specific radio frequency; the bands are kept as close together as possible and strong 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 was set up to licence the frequencies and monitor their use. These licences are very expensive and in the past have prevented manufacturers from using narrowband technology; an example of a narrowband 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) for use by new technologies. This band could be used without a license making it more accessible for private networks, and consequently manufacturers soon started to produce products which used the new band. However, one condition of using the ISM band was that signals must share the airwaves with one another, and as narrowband methods did not allow this, spread spectrum technology was used instead.

Spread spectrum technology spreads the signal out over the whole band preventing concentration of the signal in anyone 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.

3.1.1 Direct Sequence Spread Spectrum

Direct Sequence Spread Spectrum works by adding redundant data called 'chips', to the signal, at least 10 chips per bit are added to the signal. The code used to modulate the transmitted data is called the spreading code and only receivers which know the spreading code can decipher the signal. This unique spreading code is what allows multiple direct sequence transmitters to operate in the same area. As the transmission is spread across a wide frequency band (a result of the spreading process), transmission power is lower than that of narrowband transmissions enabling it to be used in the ISM band. To other radio users the direct sequence transmission appears to be low power background noise. Because the signal is low power and spread across a wide frequency the signal is susceptible to noise. However, in cases of signal corruption the redundant data helps to recover the original signal, the number of chips is directly proportional to the immunity from interference.

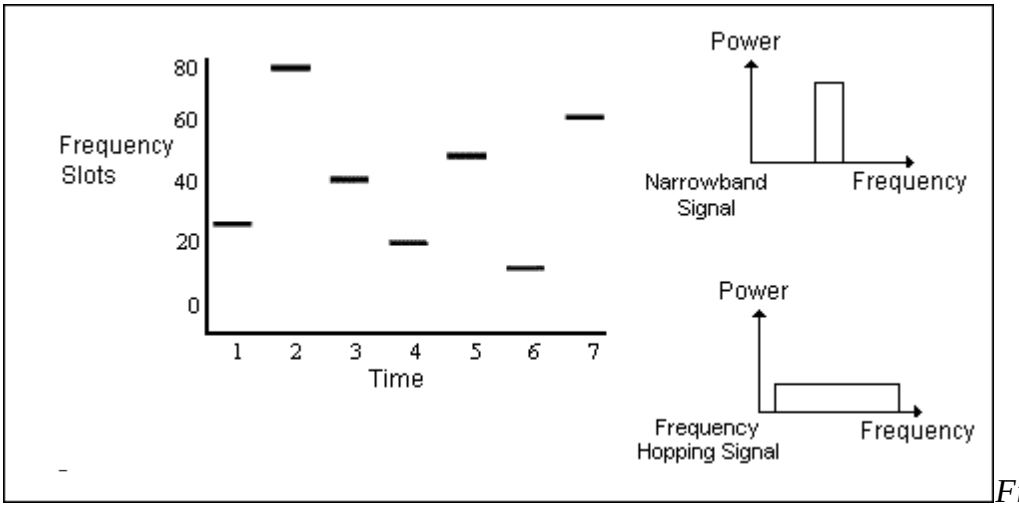


Fig. 11

Direct Sequence gives a higher throughput and is more immune to interference than frequency hopping. Unfortunately it uses two to three times more power and

tends to be more costly. The wireless LAN industry seems to be split equally between Frequency Hopping and Direct Sequence. AT&T are one user of DSSS and are a major producer of wireless LAN products, they also play a large part in the IEEE 802.11 standard for Wireless LANs.

3.1.2 Frequency Hopping Spread Spectrum

Unlike Direct Sequence spread spectrum which chops the data into small pieces and spreads them across the frequency domain, Frequency Hopping splits the data up across the time domain. A short burst of data is transmitted on a narrowband and then the transmitter quickly retunes to another frequency and transmits again. The sequence of hops the transmitter makes is pseudorandom and is known by the receiver, enabling it to receive each short burst of data. As the transmitter and receiver are synchronized the stream of data appears to be constant. There are certain rules governing how a frequency hopping device must behave to make sure a device doesn't use too much bandwidth or linger too long on a single frequency. In North America, the ISM band is separated into 75 hopping channels and the power transmitted on each channel must not exceed 1W. To other radio users the frequency hopping signal appears as short bursts of noise.

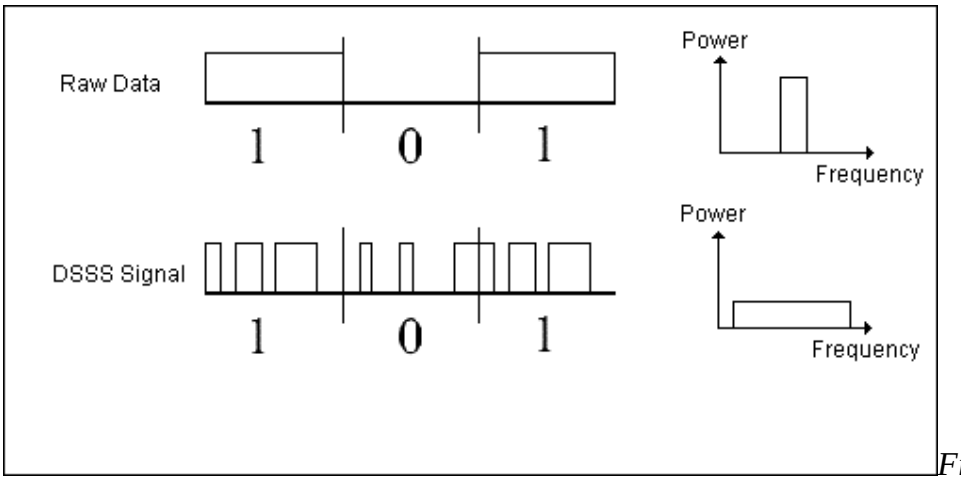


Fig. 12

Frequency Hopping devices have different characteristics when compared to Direct Sequence. They use less power and are generally cheaper. However, performance, compared with DSSS, tends to be lower and their immunity to

interference is lower too. Consequently if a burst of data is corrupted on one hop the entire data packet must be sent again. Despite this, Frequency hopping does have one major advantage in that several access points can coexists in the same area. Therefore if an access point is struggling to cope with large numbers of users then another access point can be added to take some of the load. This cannot be done with direct sequence access points as they would block each other from transmitting.

3.2 Infrared LAN Technology

Infrared is simply invisible light. It has all the properties of visible light except that our eyes cannot see it. It can't pass through walls or ceilings but it can bounce off flat surfaces and pass through open door ways. There are a number of advantages associated with using infrared systems. One is low power consumption which is useful when considering notebook computers. Others include the invulnerability to interference from traditional sources such as EMI and RF. Also the signals cannot escape from the building or be jammed from outside.

An infrared signal can be either focused, as with a laser, directed, as with a television remote control, or diffuse like normal sunlight. All three of these technologies are used in one form or another in computer networks. Focused infrared is used in building to building links. This form of infrared technology is best able to capitalize on the high speed of infrared. Links of 10Mbits/s are common and 100Mbits/s links are also available. However, one disadvantage of focused infrared lasers is their sensitivity to atmospheric conditions. Heavy rain and fog can block a signal, and even on sunny days convection currents caused by heat from the sun can divert the beam from its target, cutting the link completely. Move over all of these problems are intensified by distance.

3.2.1 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 than 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, however, 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, 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, during our evaluation of these systems we have come across some drawbacks. In order to be useful as a replacement to traditional methods of connecting to the network the infrared link would have to perform at 4Mb/s the IrDA1.1 standard. Unfortunately, systems we tested, the HP Netbeam and the extended systems Jeteye did not support this standard. Only the older and slower IrDA 1.0 (115Kb/s) was supported despite claims to the contrary by both manufacturers. This was not dishonesty on the part of the manufacturers. The inconsistency was due to the laptop manufacturers. Both the HP and the extended systems used Microsoft's IrDA LAN driver V2.0 to access the network, but this driver officially only supports data rates of 115Kb/s. In order for the IrDA port to communicate with the MS IrDA LAN driver a module called the framer software needs to be provided by the laptop manufacturer. Some manufacturers, for example HP have written framer software which allows the MS IrDA 2.0 driver to transmit at 4Mb/s but, most have not. Microsoft is currently developing its IrDA LAN driver V3.0 which will transmit at 115Kb/s, 1Mb/s and 4Mb/s. Most laptop manufacturers have chosen to wait for version 3.0 before developing their 4Mb/s framer software rather than developing drivers for version 2.0.

Despite our experiences with these two systems, we still consider direct infrared technology to be a very useful solution for connecting laptop computers to the network. Although it is not known how soon Microsoft will release version 3.0 of it’s IrDA LAN driver, the beta development kit is already available to download from their web site. If one were considering using this technology today it is a simple matter of finding which laptops are compatible with the preferred access

point. HP Omnibooks and Sharp Notebooks are just two of the compatible models currently available on the market.

3.2.2 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 user is still confined to individual rooms unlike when using 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 the ceiling to communicate with receivers which connect to portable computers using PCMCIA cards. The hemispheres are connected to a central hub which powers each hemisphere and acts as a bridge onto the wired LAN (See Fig 6.).

SpectrixLite uses a proprietary protocol called CODIAC (Centralised 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 lowest of 1.2Kbit/s to 230.4Kbits/s and supports features of wireless LANs such as seamless roaming.

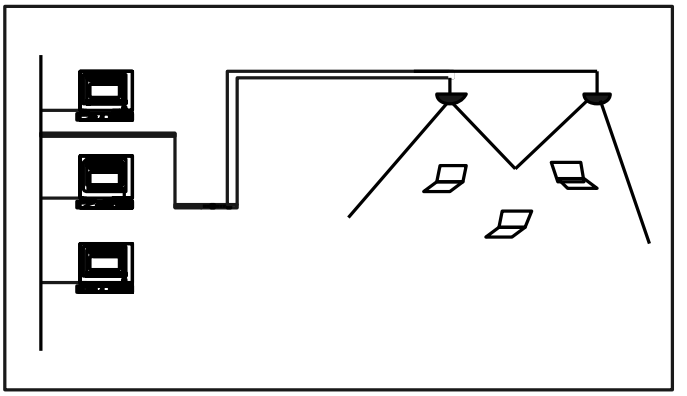


Fig. 13

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 its diffuse infrared product) has meant very few systems are commercially available. Those which 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.

Chapter 4 – Implementation

4.0 Introduction

This project commenced because Sifax Company views wireless LAN technology as a solution to the obstacles which hinder the advancement of information available. The company's on a site of historic importance in the Lagos and a substantial pressure is put in place due to the lack of available space to use for expansion. This prevents the Company from providing large numbers of dedicated computing offices which have become a vital part of routine. The Company's strategy for tackling this problem is to convert all rooms into offices capable of supporting a wireless network which will provide all the usual network and Internet facilities.

4.1 The Wireless LAN implementation

The project aims are to determine how best to use the technology available. Initially, this involved researching which products and systems were available. In order to gain some experience with the technology and to determine how well the systems performed, a series of tests was conducted. On the bases of these tests two systems have been selected to implement in a working system in the company to see if the original aims of the project are feasible. If the project is successful a full scale wireless network is planned.

For the initial test installation two systems were chosen, one radio and one infrared. We decided to include an infrared system in the study because we hoped it would make the study more valuable, as a direct comparison could then be

made between the radio and infrared systems. Full details of the systems and how we came to decide on them are discussed below.

4.2 The Radio Equipment

The decision of which radio equipment to use in the study was based on a number of factors. Some of the issues which needed to be considered included which technology to adopt, Direct Sequence (DSSS) or Frequency Hopping (FHSS) spread spectrum. Also important, was the performance of the systems under consideration (which was determined in earlier stages of the project), the design and construction of the hardware, and finally, the Net Wave Air Surfer system was chosen as it met most of our requirements.

The Net Wave Air Surfer uses Frequency hopping spread spectrum. This technology was favored as it offered some advantages over Direct Sequence, the most important of which was scalability. Signals from DSSS access points cause interference on other access points so a great deal of planning has to go into positioning access points to prevent this problem. FHSS does not have this problem, so several access points can coexist in the same area. This allows additional access points to be added to an area of heavy usage, enabling load balancing to increase performance. DSSS has higher throughput and can support a higher number of users per access point, but the ability of FHSS to balance a large number of users over several access points' results in greater flexibility and a more constant service per user than with DSSS.

The performance of FHSS is lower than DSSS, typically 33% - 50% less. This is the greatest disadvantage of FHSS and we are very much aware that the lower performance may affect the results of the study, especially when large numbers of users collect in the same area. However, we believe that the other features of the Net wave system make up for the lower throughput. Higher frequencies are currently being researched by the IEEE 802.11 group which will increase the

performance of both DSSS and FHSS systems and will hopefully address any problems caused by performance which may be faced during this study

The design and construction of the products we evaluated probably proved the greatest factor in our decision of which system to adopt. The wireless LAN manufacturers seem to be split into two camps based on the design of their laptop antennas. As discussed earlier, the antennas can be very small or quite large

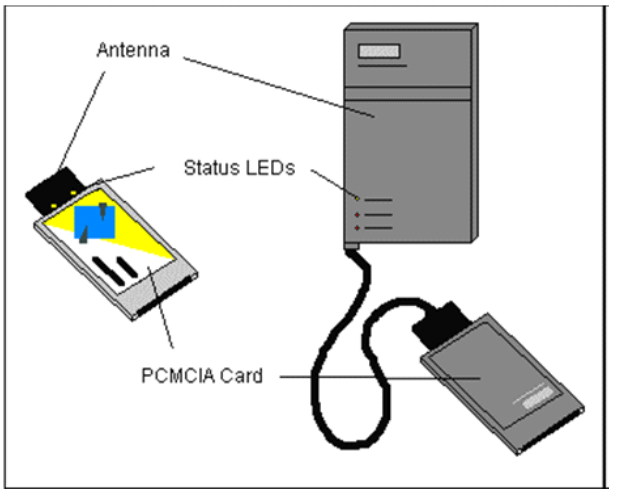


Fig. 14

As you would expect, the larger antennas give better range and throughput, but we decided on the smaller antennas because we believed they would be less intrusive and more user friendly, requiring little or no involvement with the user once they have been installed. In contrast, the larger antennas have to be plugged in and unplugged every session which could potentially result in wear and tear on the hardware.

However, we are operating on a limited budget and we believe the less expensive equipment will allow us to implement a larger test group and therefore will establish a more credible statistical base to work on.

4.3 The Infrared Equipment

We were left with little choice when deciding on which system to use as only one system is commercially available at the moment, namely the SpectrixLite system from Spectrix Corp.

The infrared system does not have the higher data rates of the radio systems (10 - 15 Kbytes/s compared with 40 - 70Kbytes/s respectively) and the infrastructure needed to support the network is greater (more wires connecting the access points to the central hub). However, there are no problems with the number of users as the system can support up to 1000 and the protocol is deterministic, so each user is still guaranteed a constant bit rate. Some concerns we have with the infrared system involve the design and construction of the hardware. We opted for the slower radio system because the antenna was smaller, unfortunately the infrared transceiver is a little larger than the largest radio antenna, which for the reasons outlined above, is undesirable. In addition, the hub used to power and connect the access points to the network needs a PC to act as a bridge onto the wired network. Despite these short comings, the infrared system still has a great deal of potential; the speed advantages alone would make a future product a real contender. Spectrix Corp is currently working on the next generation of the product, which will have performance more in line with the capabilities of infrared and the hardware will be redesigned to address some of the issues mentioned above.

4.4 The Users

This working test stage of the study will be spread over one year with either one or several test groups using the wireless network. The test groups will be made up of 5 staffs who will be using the radio network and 5 staffs who will be using the infrared network. Both groups will be issued with laptop computers and antennas. Staffs will be chosen from the wide range of users currently using the Company network. The staffs will be given training sessions on how to use the wireless network and will be made aware of what kind of performance to expect. A series of questionnaires and interviews will be used to gather data from the test group

and monitoring tools will be used to gain quantitative data on how the network is performing.

4.5 Design and Implement Local and Wide Area Networks Optimized For Wireless Access, Acceleration and Load Balancing.

Project Leadership can help your organization design, deploy, manage and maintain your LAN/WAN and wireless networks for improved wireless access and system availability. Implementing a solid infrastructure around your switches and routers will help your business achieve optimum connectivity to all servers, desktops and offices. You will also be able to greatly improve business continuity and disaster recovery capabilities for your entire organization.

4.5.1 Typical Wireless LAN Implementation

A WLAN can be configured in 2 modes, namely the ***ad-hoc*** or the ***infrastructure*** network mode. An *ad-hoc* WLAN allows wireless stations to connect directly to one another for sharing of files or resources. In an *infrastructure* WLAN, wireless stations communicate with one another via the access point, which also serves as the bridge that interconnects the WLAN and the wired network. Wired Equivalent privacy (WEP) and Service Set Identifier (SSID) are the two security mechanisms in IEEE 802.11b for providing confidentiality and access control.

W/Lan implementation in ad-hoc topology

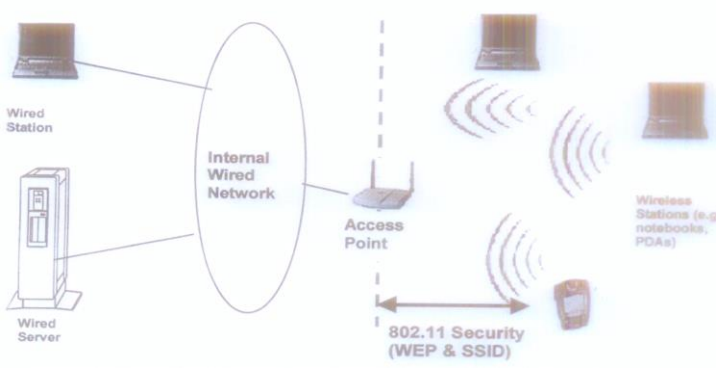


Fig. 15

W/LAN implementation in infrastructure topology

4.5.2 LAN/WAN Architecture & Deployment

Architect and deploy the best LAN/WAN business solution to meet the needs of single and multi-office locations for maximized connectivity, business continuity and disaster recovery.

4.5.3 Network Load Balancing

Utilize professional devices to help balance business loads across multiple parts of web or application services so no single piece of equipment is ever overloaded.

4.5.4 Wireless Architecture & Deployment

Architect and strategize implementation plans for wireless network solutions, both internal and external to client environment.

4.5.5 WAN Acceleration

Accelerate and optimize data transfers across the wide area network by implementing best practices in device usage.

4.5.6 Benefits

- ❖ Improve efficiency of LAN/WAN infrastructures.
- ❖ Optimize your network speed, security, stability and customer experience.
- ❖ Increase convenience and productivity by extending wireless networks.
- ❖ Improve disaster recovery and business continuity.

Enhance connectivity to all servers and desktops from disparate geographies and co-locations. Clients are connected to a wireless network through a wireless access point (AP) instead of an Ethernet switch. Each client uses a wireless adapter to gain access to the network through a wireless device such as a wireless router or access point.

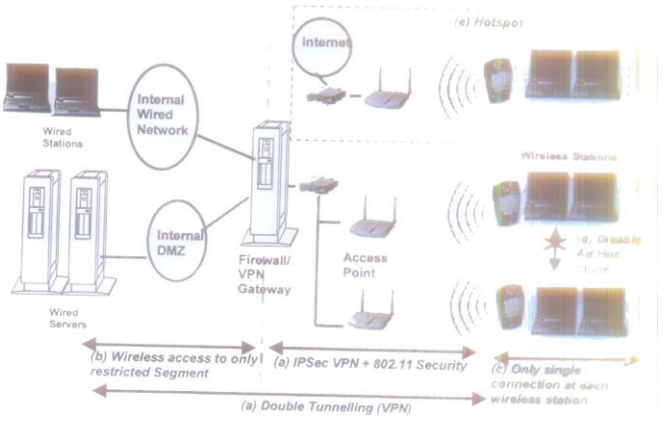


Fig. 16

Proposed W/LAN implementation in Office environment

The wireless adapter in the client communicates with the wireless router or access point using RF signals. Once connected to the network, wireless clients can access network resources just as if they were wired to the network.

Chapter 5 – Result and Discussion

5.0 Introduction

This chapter presents all information regarding the implementation of the project. The implementation of radio and infrared technology and are discussed in detail. The chapter concludes with the implementation of wireless LAN network layout in an office environment.

The next chapter describes the different tests performed to ensure wireless functionality. It describes the problems encountered during the testing phase and concludes with the ethical issues involved with the development of the project.

5.1 Performance Results

During the course of the study being carried out, seven separate wireless radio LAN systems have been tested. The systems were tested for performance, design and build quality, and ease of installation. Other issues, such as, range were not considered to be important as the area of coverage required for the final installation was well within the range of all the systems tested.

The test procedure involved using an FTP client to ftp files from a central network server to a laptop computer positioned at different places around the building. The test was quite crude; however we wanted to obtain data from an application point of view rather than focusing on the low level raw bit rate. A 100Kbyte, 500Kbyte and 1Mbyte file was FTPed 100 times each to the laptop and the average was used in the results. Care was taken to avoid some of the potential pitfalls involved in attempting to gain accurate measurements of a

networks performance. Among the points of particular concern were: to make sure that the sample size was large enough, to make sure that the samples were representative, to be aware of the specification of the system clock, to be sure nothing unexpected was going to happen which may affect results and to check the effect caching may have had.

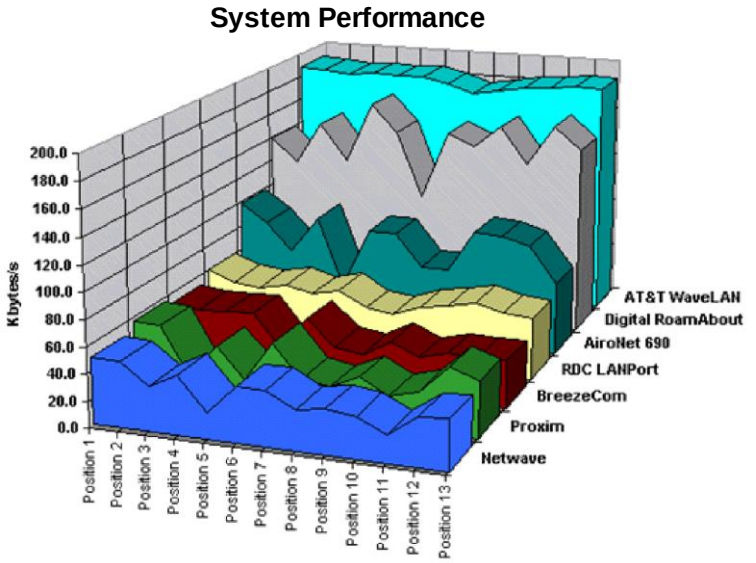


Fig. 17

The positions used in the study were mainly offices located on the two floors of the Computing Services building at the company. As they were all well within range of the AP their exact locations were not important. Only two positions were note worthy: position 7 and position 5. Position 5 was behind a lift shaft in relation to the AP which blocked a large part of the radio signal. Position 7 was in the main processor room where most of the servers are kept. This area was the most distant compared to the other locations and was separated by two internal walls. In addition to this, the interference caused by the servers may account for the dip in performance which some of the systems show.

The results of the systems in relation to each other are quite straight forward. Several factors account for the differences such as: whether the system was Direct Sequence or Frequency Hopping, what size and power rating the antennas were, and which driver versions were being used. The three highest performers

were AT&T, Digital and AirNet. All these systems used Direct Sequence Spread Spectrum which has a much higher performance then Frequency hopping, and they also used large antennas (see Fig. 18) which improved range and overall performance. The Digital system uses a badge antenna from the AT&T product, but with a redesigned Access Point. The results of these two systems should have been very similar but the Digital system showed a 23% drop in throughput which was due to the drivers being used in the tests. The Digital system was the first product to be tested, but shortly after these tests a bug was found in the drivers which caused a drop in performance. Digital have corrected the bug and passed the information onto AT&T who corrected the bug in the latest version of their own drivers. The AT&T equipment was tested roughly 4 months after the Digital equipment allowing ample time for the bug fix to have been implemented. The Digital equipment is currently being retested in order to give a true picture of it's performance.

The lower performing systems were all Frequency Hopping, the bottom three of which used small antennas (see Fig.18). The RDC system showed slightly better performance because it used a large antenna, similar to those used by the DSSS systems. The larger antenna provides greater range and penetration, accounting for the more consistent performance of the product.

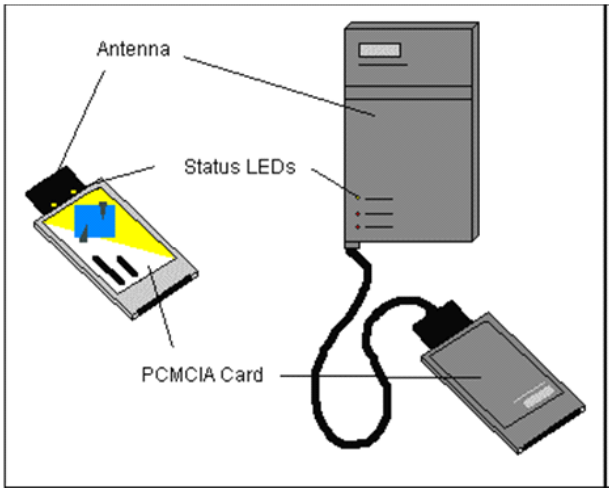


Fig. 18

Radio signals in wireless LANs are very sensitive to changes in their surroundings. People moving around and changes in the position of the antenna

in relation to the Access Point can all have a significant effect on the channel characteristics. Studies into indoor radio propagation have shown that received signal strength can fluctuate significantly within a period of 10 to 20 ms [5]. Most of the systems come with utilities to monitor the signal strength and performance allowing a user to adjust their orientation if necessary. However, during typical use over a prolonged period of time the overall performance lever would average out and for uses such as email and web browsing a user would not find it necessary to constantly monitor the signal strength.

Chapter 6 – Conclusion and Further Development

6.0 Introduction

This chapter concludes the project by providing a summary of the strengths, weaknesses, opportunities and threats concerning the final application followed by possible areas for further development.

6.1 Conclusions

The only right time to buy any product is when you need it. Wireless systems cannot compete with wired networks in terms of speed or price per connection, and so a wireless network should only be considered when a cabled solution is impossible or undesirable.

Of all the technologies discussed in this paper each has a niche was it is ideally placed. For a mobile user who works from his laptop and only wants to connect to the network when he's back in the office at his desk then direct infrared is the best solution. The connection is fast and reliable, the technology is cheap and widely available, if an office were equipped with a sensor on every desk then the system would fulfill all the needs of this case. For a more mobile solution, were a user's needs to access network resources on the move then radio or diffuse infrared are the logical choices. Each has advantages and disadvantages. Infrared is faster and can support many more users. If used in an office or educational environment the placement of access points can give a far great control over were the service is to be offered compared with radio. However, lack of investment in the area from the large manufacturers has meant that the solutions available today lack the refinement of radio systems. In the future though diffuse infrared has the

potential to compete with radio and even replace it. Radio by it's nature needs to be regulated and these regulations hinder the full exploitation of the medium. Infrared does not have this problem and, with time, wireless systems will begin to realize the full potential of infrared technology.

At this point in time though, a wireless LAN can most easily be achieved by spread spectrum radio. Whether direct sequence or frequency hopping, the radio systems available are well designed and constructed, are easy to install and maintain, and offer a range of performances based on cost and method of transmission. The IEEE 802.11 standard has emphasised the importance of the technology and the standard will prompt new manufacturers to produce systems and market forces will cause prices to fall making wireless systems more accessible to business. Wireless networks have cease to be a wonder and will become a more familiar sight in everyday life.

6.2 The Future of Wireless Networks

Wireless LAN sales are said to be approaching the $1bn mark from a level of only $157m in 1995[6]. This incredible growth in the market has prompted those networking manufacturers not currently offering systems to begin developing their own wireless products. More importantly, it has prompted those already established to begin research and development into new and improved wireless technologies. Research is being conducted by large companies such as British Telecom and in Universities throughout the world. Improved speeds and reliability along with new systems will help wireless technology maintain a footing in the ever increasing and competitive networking market. Some of the projects and advancements are discussed below.

As mentioned earlier, the IEEE 802.11 Working Group has set up a study group to develop the standard in order to take advantage of some the advancements being made in research and development. Current projects under review include

methods of achieving higher speeds in the current 2.4 GHz band and new systems which operate in the higher 5 GHz band which hope to yield improved performance. In addition to these, products are becoming available which use Quadrant Phase Shift Keying (QPSK) and Quadrant Amplitude Modulation (QAM). These methods, already used in modem technology, allow a greater number of binary combinations to be represented by a single signal increasing system performance [7]. Speeds of 3.2Mbits/s are capable, compared to 2Mbits/s with conventional techniques.

The University of San Diego's Centre for Wireless Communication [8] is currently working on a number of important projects regarding wireless LANs and WANs. Energy Constrained Wireless Communication is a project designed to investigate Battery Conservation in the mobile environment. The research revolves around how the wireless link can be used most efficiently with close examination of error detection and recovery to prevent packet retransmission.

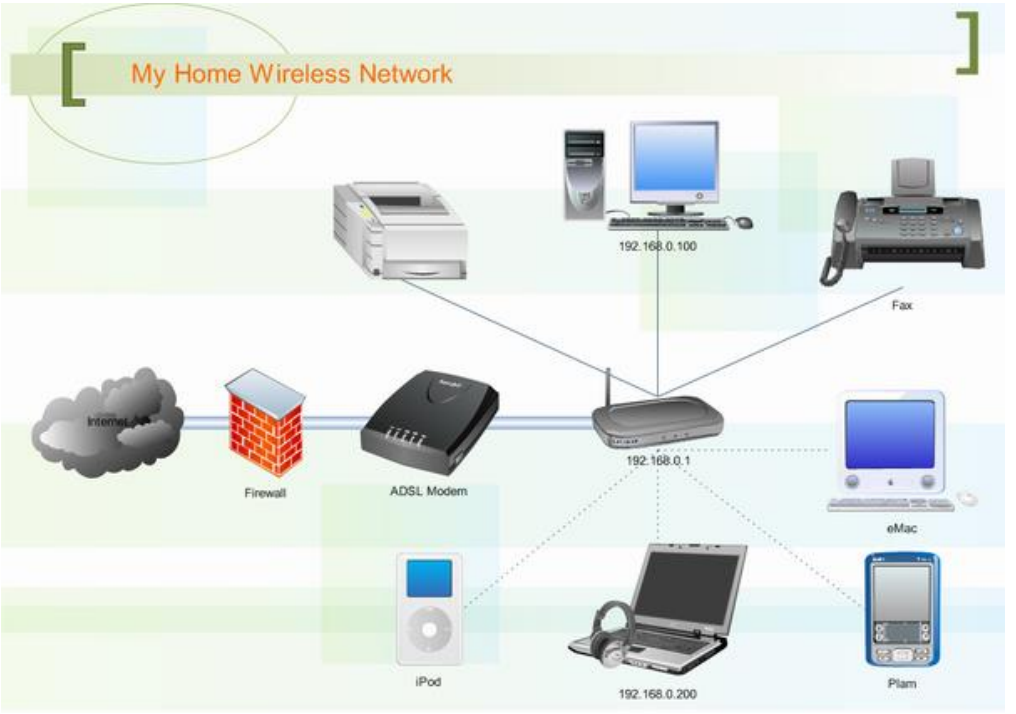
Asynchronous Transfer Mode (ATM) networks are rapidly becoming an important area of network technology and many papers have been written on wireless ATM [9]. The major ATM standards bodies have yet to define any standards for wireless ATM. Despite this, several projects have been undertaken by Industry and Education. Two such projects are WAND (Wireless ATM Network Demonstrator) which aims to develop a 20Mbit/s ATM air interface in the 17 GHz frequency and MEDIAN (Wireless Broadband CPN/LAN for Professional and Residential Multimedia Applications) which operates at 155Mbit/s in the 60 GHz band.

British Telecom is a large investor in research and development and has done considerable work in wireless communication. A recent publication has demonstrated how BT are committed to wireless LANs in the office and home. They have developed a new type of access point which they have named the 'passive picocell'. The picocell emits radio waves which can be used to communicate data over a network; the picocell is connected back to a central

network server using fibreoptic cables which carry the radio waves on a carrier pulse of light. This feat is achieved using an alloy based on indium phosphide which translates radio waves into light and vice versa. The unit has several advantages, namely that no power is required and the units are small, inexpensive and maintenance free. The units could cost as little as £35 each and the technology should be commercially available by 2005.

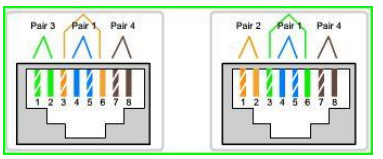
Appendices

Appendix 1 - Networking Devices



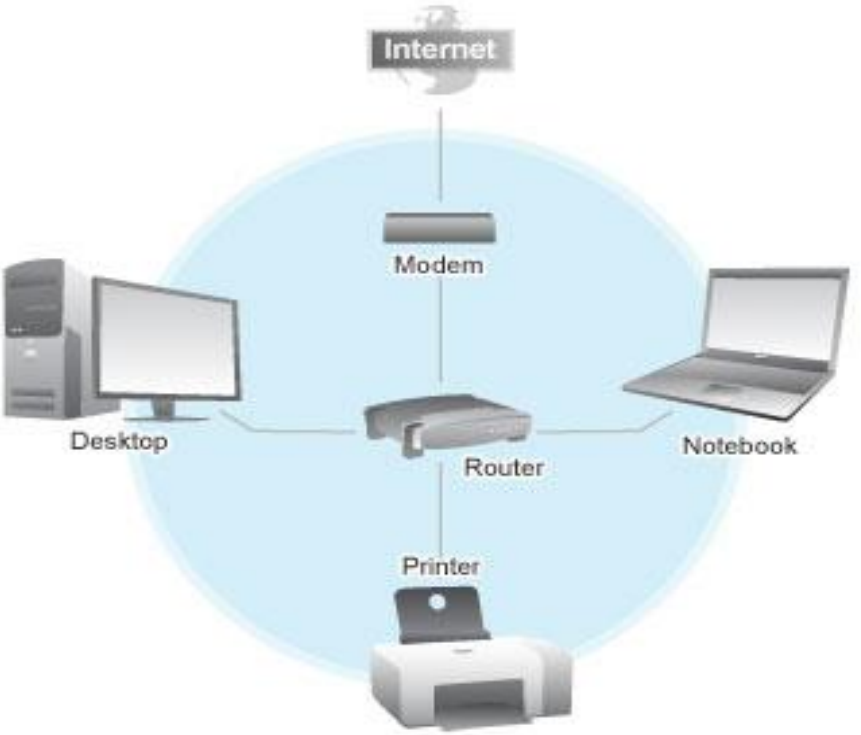
Router

Switch



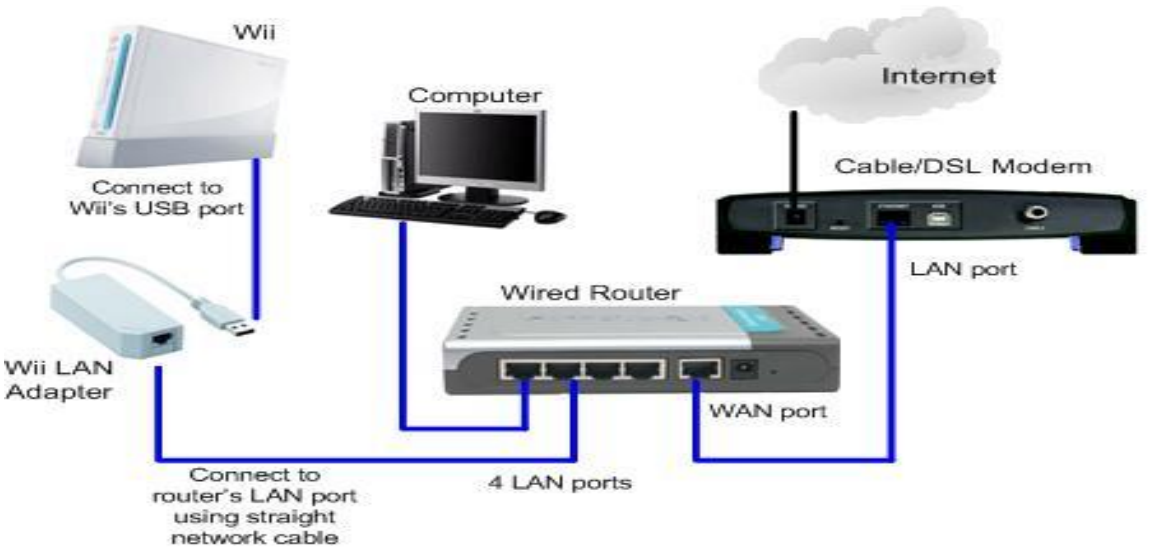
RJ-45

Appendix 2 - Wired & Wireless Network



A Typical Wired Network

Wireless Network



Wireless Network

Deploying a wireless network with high availability and security both in WAN & LAN connection

Appendix 3

Wireless LAN Agencies

International agencies that create standard on behalf of wireless lan.

- IEEE: Institute of Electrical Electronics Engineering
- They create and maintain operational standard of wireless LAN and their website is ieee.org.
- FCC: Federal Communication Commission
- It regulates the use of wireless devices in U.S. Their website is www.fcc.gov.
- ETSI: European Telecommunication Standard Institute
- They produce common standard of wireless network in Europe. Their website is www.etsi.org.
- WIFI: Wireless Fidelity
- It is an alliance between different wireless producing vendors to promote and test for wireless lan inter-operability. Their website is www.wifi.org.
- WLANA: Wireless LAN Association
- They educate and raise consumers' awareness regarding wireless LAN. Their website is www.wlana.org.

Wireless Standards 802.11 Committees and Functions/Purpose.

- 802.11a: Supports 54mbps, 5ghz standards.
- 802.11b: An enhancement to 802.11 to support 5.5 mbps and 11mbps.
- 802.11c: Support bridge operation procedures and is included in the 802.10 standard.
- 802.11d: Support international roaming extension.
- 802.11e: Support quality of service QOS.
- 802.11f: Support inter access-point protocol.
- 802.11g: Support 54mbps, 2.4 GHz standard.

- 802.11h: Support dynamic frequency selection DFS and transmit power control TPC at 5 GHz.
- 802.11i: Support enhanced security 802.11j.
- 802.11k: Support radio resource measurement and enhancement.
- 802.11m: Support the maintenance of this standard such as odds and ends.
- 802.11n: Support higher throughput improvement using MIMO antenna.
- 802.11p: Support wireless access for the vehicular environment.
- 802.11r: Support fast roaming.
- 802.11s: Support extension service set ESS mesh networking.
- 802.11t: Support wireless performance prediction.
- 802.11u: Support inter-networking with non 802 networks such as cellular or mobile phone.
- 802.11v: Support wireless network management.
- 802.11w: Support protected management frames.
- 802.11y: Support 3650 to 3700 operations in the U.S.

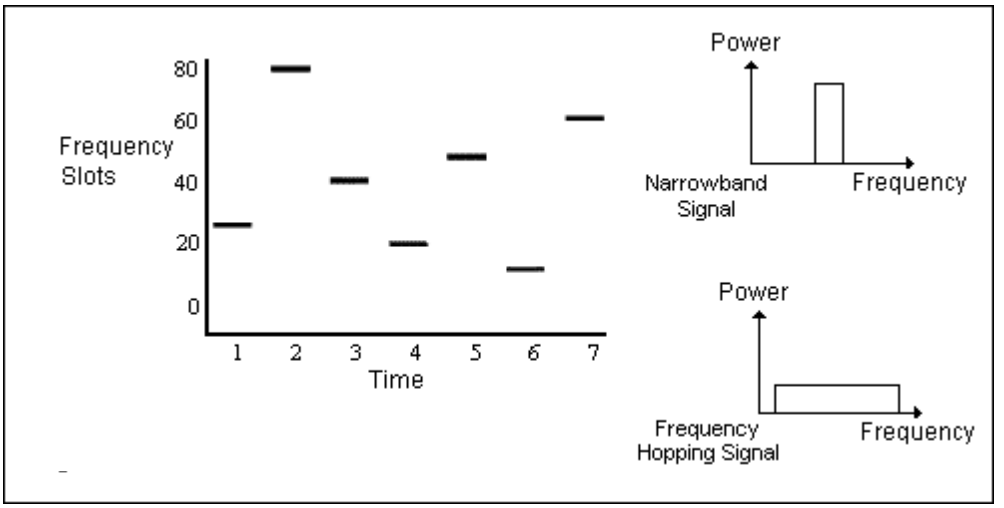
Appendix 4 - Tables of Acronym

CDPD	-	Cellular Digital Packet Data
LAN	-	Local Area Network
V/LAN	-	Virtual Local Area Network
W/LAN	-	Wireless Local Area Network
WAN	-	Wide Area Network
MES	-	Mobile End System
MDBS	-	Mobile Database Station
IS	-	Intermediate System
MDIS	-	Mobile Data Intermediate System
FES	-	Fixed End System
FM	-	Frequency Modulation
FCC	-	Federal Communication Commission
PSTN	-	Public switched telephone network
IMTS	-	Improved Mobile Telephone Service

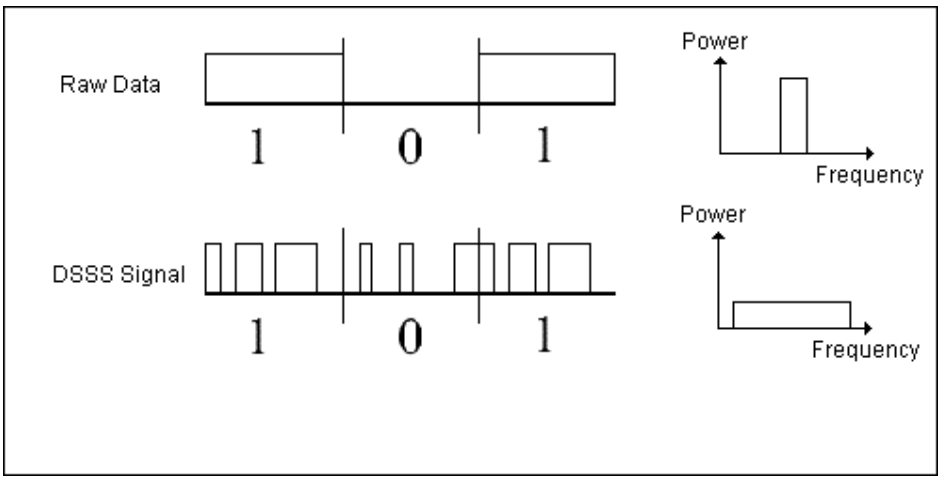
AMPS	-	Advanced Mobile Phone System
MHz	-	Mega Hertz
GHz	-	Giga Hertz
CDMA	-	Code Division Multiple Access
PCS	-	Personal Communications System
RF	-	Radio Signal Frequency
WAP	-	Wireless Access Point
CSU	-	Channel Service Unit
DSU	-	Data Service Unit
EIA	-	Electronics Industry Alliance
TIA	-	Telecommunications Industry Association
ISP	-	Internet Service Provider
BSS	-	Basic Service Set
ESS	-	Extended Service Set
DoS	-	Denial of Service
WPA	-	Wireless Protected Access
WEP	-	Wireless Encryption Protocol
VPN	-	Virtual Private Network
CLNP	-	Connectionless Network Protocol
IP	-	Internet Protocol
MNRP	-	Mobile Network Registration Protocol
PDU	-	Protocol Data Unit
DSSS	-	Direct Sequence Spread Spectrum
FHSS	-	Frequency Hopping Spread Spectrum
IrDA	-	Infrared Data Association
CODIAC	-	Centralised Operation Deterministic Interface Access Control
SSID	-	Service Set Identifier
WEP	-	Wired Equivalent privacy

Appendix 5

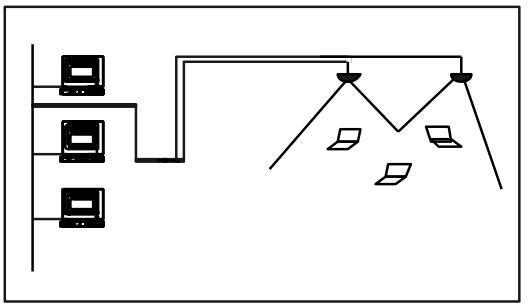
Direct Sequence Spread Spectrum



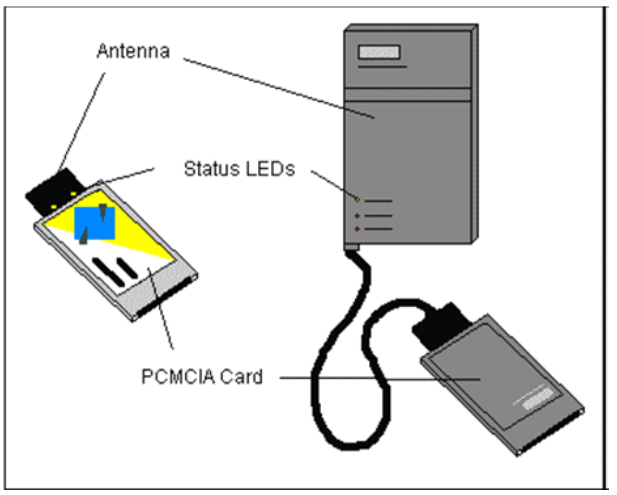
Frequency Hopping Spread Spectrum



Diffuse Infrared Technology

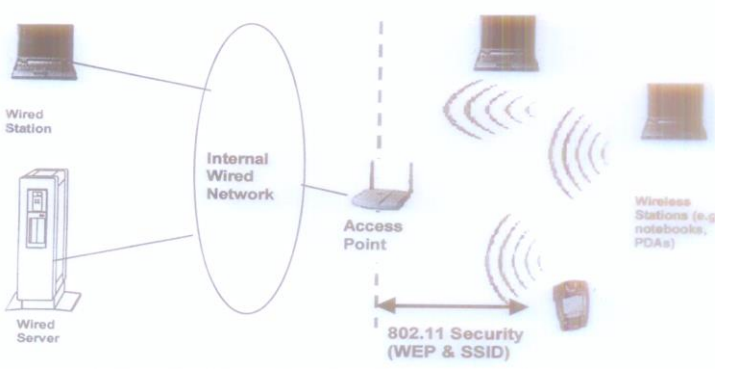


The Radio Equipment



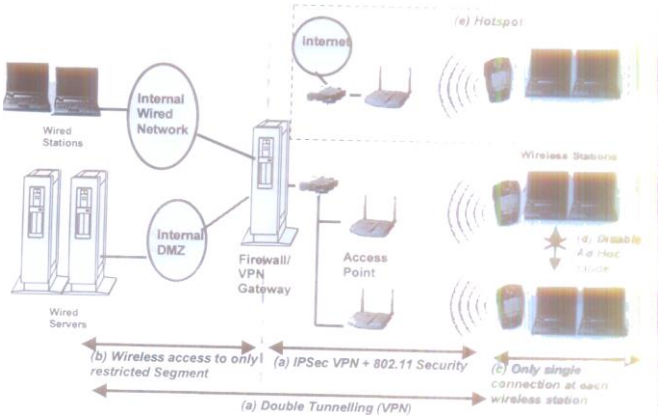
Design and Implement Local and Wide Area Networks

W/Lan implementation in ad-hoc topology

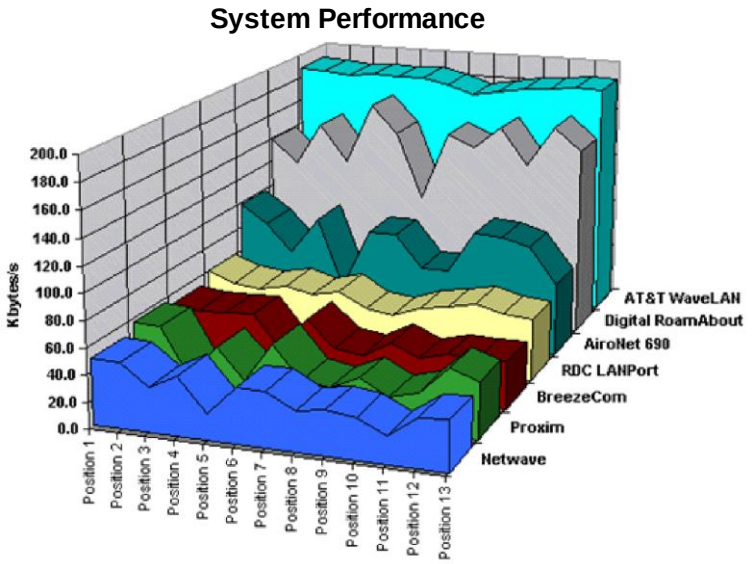


W/LAN implementation in infrastructure topology

Proposed W/LAN implementation in Office environment



Performance Results



References

J. Agusta, T. Russel 1997 CDPD Cellular Digital Packet Data Standards and Technology. New York, McGraw-Hill.

M. Sreetharan, R. Kumar 1996 11111111111Cellular Digital Packet Data. Boston, Artech House.

M. Banan, et al 1996 Prentice-Hall.

W. Stallings 1993. SNMP, SNMPv2, and CMIP The Practical Guide to Network Management Standards. New York: Addison Wesley.

D. Russell and G. T. Gangemi 1992. Computer Security Basics. California: O'Reilly & Associates.

Y. Frankel 1997 Security Issues in a CDPD Wireless Network, http://swig.stanford.edu/pub/summaries/wireless/security_cdpd.html.

D. Smith, et al 1995 Trails of Wireless Secure Electronic Mail. IEEE Personal Communication.

D. Pharr, et al..2001. The Growing Acceptance of Cellular Digital Packet Data as a Communication Method for Oil and Gas Telemetry http://www.bandwidthmarket.com/resources/speeches/sat/pharr/paper.doc

Rivest 1992 The MD-5 Message-Digest Algorithm. Request for Comments 1321, Internet Activity Board. Mobile Info 2001 Wireless and Mobile Computing Security,http://www. mobileinfo . com/Security/ problems.htm

F. Hatefi et al 2001 Prospect of Secure Real-Time Video Transmission over CDPD network, NSF Workshop on an Infrastructure for Mobile and Wireless Systems Sierra Wireless 2002 Wireless Security: Data Security in Wireless

Networks
http://www.sierrawireless.com/news/docs/21
30223_Wireless_Security.pdf,

Lightweight and Efficient Application Protocols (LEAP)
Forum 2000 CDPD Securityhttp:// www.
leapforum. org/published/ internetwork
Mobility/split/node97.html

S. Issacson 1997 CDPD Security, http://www.refreq.com/
downloads/cdpdsec.pdf

J. Geier 2000 CDPD Concepts, http://www.wireless-
nets.com/articles/whitepaper_cdpd.htm

J. R. Walker, "Unsafe at any key size; An analysis of the
WEP encapsulation", IEEE 802.11-00/362,
October 2000.
http://grouper.ieee.org/groups/802/11/Docum
ents/DocumentHolder/0-362.zip

W. A. Arbaugh, N. Shankar and Y. C. J. Wan,
"Your 802.11 Wireless Network has No
Clothes", University of Maryland,
Department of Computer
Science, March 2001.
http://www.securityfocus.com/data/library/wi
reless.pdf

Tom Karygiannis and Les Owens, “Wireless Network Security: 802.11,
Bluetooth, and Handheld Devices”, NIST Special
Publication SP 800-48, November 2002.
http://csrc.nist.gov/publications/nistpubs/800-
48/NIST_SP_800-48.pdf

Bob Fleck and Jordan Dimov, Cigital Inc,
“Wireless Access Points and ARP Poisoning:
Wireless vulnerabilities that expose the wired
network”.

http://www.cigitallabs.com/resources/papers/download/arppoison.pdf

Mishra, A & Arbaugh, W, "An initial security analysis of the 802.1x standard", Feb 2002. http://www.cs.umd.edu/~waa/1x.pdf

Scott Fluhrer, Itsik Mantin and Adi Shamir, "Weakness in the Key Scheduling Algorithm of RC4".http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

J. Philip Craiger, June 2002. "802.11, 802.1X and Wireless Security", http://www.sans.org/rr/wireless/80211.php

Christopher W. Klaus, Security "Wireless LAN Security FAQ", Internet Systems (ISS), October 2002. http://www.iss.net/wireless/WLAN_FAQ.php

"CISCO Aironet Wireless LAN Security Overview", August 2002. http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

Robert Braid and Mike Lynn, "Advanced 802.11b Attack", July 2002. http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#Baird

Mike D. Schiffman, "The Need for 802.11b Toolkit", July 2002. http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#MikeD.Schiffman

J.O'Dwyer (Dataquest Inc.), 1996 "PC Quarterly Statistics European Overview"

B.Egan (Digital Corp), "Wireless Data Communications" 1995

RACOTEK Inc., "Wireless Data Security 1996", http://www.racotek.com

Project Home Page, "http://www.canterbury.ac.uk/research/wireless-net"

C.Huang and R.Khayata, "Delay Spread and Channel Dynamics Measurement at ISM Bands" 1992

P.Healy (ComputerScope), "Unwired … But still Plugged In" Aug 1996

WaveAccess Wireless Communications, "Jaguar PC132 – Wireless LAN Adapter" 1997

UCSD Centre for Wireless Communication, "http://cwc.ucsd.edu"

J.Mikkonen, "Wireless ATM Overview" On-line paper, "http://www.tele.pw.edu.pl/Pliso/~kwrona/watm/wireless.html"

Hamer (New Scientist), "The Box That Banished Office Wiring" Jun 1997

Linnartz, J. P. G (2001). "Performance Analysis of Sychronous MCCDMA in Mobile Rayleigh Channels with Both Delay and Doppler Spreads", IEEE, 50(6), 1375-1387.

Linnartz, J. P. G. (1995). Cellular Telephone Network. (Online) http://wireless.per.nl/reference/about.htm

Sharma, S. (2006). *Wireless and Cellular Communications*. S.K. Kataria & Sons. New Delhi:

Yee, N. & Linnartz J. P.G (1994). "Wiener Filtering for Multi-Carrier CDMA", IEEE/ICCC Conference on Personal Indoor Mobile Radio Propagation Communications (PIMRC) and Wireless Computer Networks (WCN), 4, 1344-1347

Yee, N., Linnartz, J. P.G & Fettweis, G. (1993). "Multi-Carrier CDMA in Indoor Wireless

Radio Network", IEEE Personal Indoor and Mobile Radio Communications (PIMRC) International Conference, Yokohama, Japan, 109-113