NEAR EAST UNIVERSITY

Faculty of Engineering

Department of Electrical and Electronic Engineering

WIRELESS AND MOBILE COMMUNICATION

Graduation Project
EE-400

Student: Ibrahim hajjaj (990982)

Supervisor: Professor
Fakhreddın Mamedov

Lefkoşa-2003

ACNOWLEDGMENTS

First I want to thank Prof. Fakhreddın Mamedovto be my advisor. Under his guidance, I successfully overcome many difficulties and learn a lote about Wireless and Mobile CommunicationS. In each discussion, he explained my question patiently, and I felt my quick progress from his advises.He always helps me alot either in my study or my life. I asked him many questions in Electrons and Communication and he always answered my questions quickly and in detail.

Special thanks to Asst.Prof. Fa'eq, Dr. Meherdad, Prof. Adnan, Ms. Filiz, Dr. Özgür, and Asst.Prof. Kedri. Withe thier kind help, in many field during my earies in N.E.U. Thanks to faculty of Engineering fore having such a good computational environment.

I also want tothank my freinds in N.E.U: Hüseyin Ernur, Khalid Shanable, Mohammad Oda, Khalid Faleh, Asa'd Alkhroof, Melın, Mertsan, Semih Ay, Ala'a Ensar, Mustafa Ahmmad, Aylınand Altuğ. Being with them make my 4 years in N.E.U. full of fun.

Finally, I want to thank my family, especially my parents. Without their endless support and love fore me, I would never achieve my current position. I wish my mother lives happily always, and my father in the heaven be proud of me.

And this project will be as a gift to my dear breather Reyad with his help not only with study but also in my life. Thanks a lot breather, all my life I will not forget you.

GLOSSARY OF TERMS

PDA	Personal Digital Assistant
GPS	Global Positioning System
FM	Frequency Modulation
IMTS	Improved Mobile Telephone Service
AMPS	Advanced Mobile Phone System
GSM	Global System for Mobile Communication
SDMA	Space Division Multiple Access
FDMA	Frequency Division Multiple Access
TDMA	Time Division Multiple Access
CDMA	Code Division Multiple Access
ITU	International Mobile Telecommunications
LEO	Low Earth Orbit
RF	Radio Frequency
FCC	Federal Communications Commission
NTIA	National Telecommunications and Information Administration
IEEE	Institute of Electrical and Electronics Engineers
MSA	Metropolitan Service Area
RSA	Rural Service Area
BTA	Basic Trading Area
PCS	Personal Communication Services
SMR	Specialized Mobile Radio
FSK	Frequency Shift Keying
PSK	Phase Shift Keying
BPSK	Binary Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
QAM	Quadrature Amplitude Modulation
MCM	Multicarrier Modulation
DSSS	Direct Sequence Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
MAC	Medium Access Control

CSMA	Carrier Sense Multiple Access
MACA	Multiple Access with Collision Avoidance
PCF	Point Coordinated Function
DCF	Distributed Coordinated Function
LAN	Local Area Network
SCO	Synchronous Connection Oriented
ACL	Asynchronous Connectionless Link
IP	Internet Protocol
LLC	Logical Link Control
MN	Mobile node
HA	Home agent
FA	Foreign agent
COA	Care Of Address
DHCP	Dynamic Host Configuration Protocol
DSR	Dynamic Source Routing

Abstract

Wireless and mobile communications is one of the most rapidly emerging and developing technologies in the world today. We have seen a surprisingly huge interest from different research organizations and companies in this field and much has been contributed to this field in the past two decades. This term paper provides the reader with the topics and issues in wireless and mobile communications. We have been using mobile and wireless communications since the late 19^{th} century. However in the past two decades the wireless industry has really taken off to the point that today we have more than 120 million mobile phone subscribers in the world . As one of the white papers from Cyprus Instruments puts "Utopia—or your worst nightmare—whatever your perspective, wireless and mobile communications is the future which is just over the horizon".

Wireless and mobile communications are significantly different from the traditional wired communications in the sense that transmission in wireless is broadcast and in air. When we do that we end up in a new realm with a whole lot of issues with respect to signal propagation, multiplexing, modulation, medium access and routing. All the above schemes in wireless and mobile communications are different from the traditional communication schemes used in wired networks. The wireless communications generally suffer from lesser data transfer rates, however in the recent past few years bandwidth efficient digital transmission schemes like CDMA (code division multiple access) have tremendously increased the performance and capacity of wireless systems. Also driven by the motivation and desire to be untethered to wires and ubiquitous access to the internet has led to the proliferation of wireless LANs. Finally the paper discusses the issues involved when routing data on a wireless network with a brief stint on adhoc (on-the-fly) networks.

TABLE OF CONTENTS

Introduction

When one mentions the term "Mobile", we define it as user mobility or device mobility. When we say a user is mobile we mean that the user can be mobile and the services can follow him. However with device mobility the communication device moves with or without the user. It is in such a case that the term wireless is used. So the term "mobile" may or may not mean wireless but the term "wireless" does mean mobile. Some of the mobile and wireless devices are sensors, embedded controllers, pagers, mobile phones, personal digital assistant (PDAs), palmtop/pocket computers, notebooks and laptops. Wireless and mobile communications can be used for in a variety of environments for different applications like vehicles having global positioning system (GPS), ambulances with high quality wireless connections to the hospitals, businesses allowing an employee to access the company information anywhere, replacing wired networks, location dependent services and many more.

Wireless and mobile communications is such a broad topic that it could put a writer in a state of quandary- what should I include, what topics should I talk about? This paper has been a humble attempt by me to encompass most of the basic issues and topics in mobile and wireless communications. I have buttressed the paper by a lot of figures as it is often said -"A picture is worth a thousand words". It is my belief that without these figures the material would have been difficult to follow. The material in the paper is fairly easy to understand. I tried to keep the flow of the paper interesting to the readers. I also tried to put forth and build the topics in this term paper in a logical manner. I have discussed the topics - history, market, frequency allocations and regulations, multiplexing, modulation, wireless LANs and network layer ; in that order.

1. Introduction to Wireless and Mobile Communications

1.1. Introduction

When one mentions the term "Mobile", we define it as user mobility or device mobility. When we say a user is mobile we mean that the user can be mobile and the services can follow him. However with device mobility the communication device moves with or without the user. It is in such a case that the term wireless is used. So the term "mobile" may or may not mean wireless but the term "wireless" does mean mobile. Some of the mobile and wireless devices are sensors, embedded controllers, pagers, mobile phones, personal digital assistant (PDAs), palmtop/pocket computers, notebooks and laptops. Wireless and mobile communications can be used for in a variety of environments for different applications like vehicles having global positioning system (GPS), ambulances with high quality wireless connections to the hospitals, businesses allowing an employee to access the company information anywhere, replacing wired networks, location dependent services and many more.

1.2. History of Wireless Communications

Wireless communication was demonstrated for the first time when Claude Chappe invented the optical telegraph in 1794. Following this the first commercial optical telegraph line between Washington and Baltimore was built in 1843. The light signals were transmitted using telescopes as relays. However this scheme was unsuccessful because the optical transmissions had their own share of problems. It was difficult to transmit light signals because of their high frequency. The higher the frequency the more difficult it is to transmit the signal. Furthermore obstacles like rain, fog and signal made the communication virtually impossible.

The discovery of electromagnetic waves and ability to modulate the same was a breakthrough in wireless communication. In 1831, Michael Faraday invented electromagnetic induction and later in 1920 Marconi demonstrated that wireless telegraphy could be possible by transmitting short waves in medium called the "ether". Since these waves could be reflected off the ionosphere, wireless transmission could now be done over greater distances. However the radio transmitters were extremely bulky and were difficult to house them in cars and

other such small facilities. It was then that Armstrong in 1933 came up with the invention of Frequency Modulation (FM) which greatly reduced the size of the transmitters and led to better quality radio transmission. After the II World War the focus and research in wireless communications really stepped up. There was a need to replace the current existing amplitude modulation (AM) technology by more efficient frequency modulation (FM). This led to companies like AT&T and Motorola developing better quality 2-way communications and portable mobile devices like the walkie-talkie. In the 1940s though there was the capability to provide 2-way mobile communications these devices had little capacity. They could handle only a few calls at a time and only a few channels were allocated to handle the calls. Cities like New York were limited to 12 callers at a time. In 1947, the AT&T was successful in providing greater capacities in wireless communications by using many transmitters scattered throughout the metropolitan area. This led to frequency reuse. The frequencies could then be reused across the city. This was called the "handing-off" where the call was handed from one transmitter to another as the user traveled from one place to another. The handing-off technology was more refined in the 1960s when improved mobile telephone service (IMTS) was introduced. It supported full-duplex, auto dial, auto trunking services.

In 1983, the advanced mobile phone system (AMPS) was introduced in the US. This was the dawn of a new era .Wireless telephones were introduced. There were many services offered besides voice transmission like fax and data transmission via modem. It was used in 900 MHz band and supported 666 duplex channels.

In the early 1990s we saw an advent of fully digital systems. A technology called the global system for mobile communication (GSM) was introduced. This worked at 900 MHz, used 124 full-duplex channels and provided full international roaming, automatic location services, authentication, encryption on wireless link and very high audio quality. However, soon the AMPS in US and GSM in Europe began to take the beat. They were not sufficient for the number of users subscribing to these services in large cities. While Europe chose to operate in a new frequency band of 1800 MHz, the US operated in the same spectrum with more efficient technologies like time division multiple access (TDMA) and code division multiple access (CDMA).

In 1997, IEEE introduced the 802.11 standard for local area networks. It works at 2.4 GHz and infrared providing transfer rates up to 2Mbps and up to 10 Mbps with modifications. In 1998, the international mobile telecommunications (ITU) recommended the ITU-2000 which defines a common framework for services, network architecture, radio interface, spectrum consideration, security and different transmission technologies.

Today wireless communications has come to a point that there every person here in the US can chose from 3 to 8 wireless providers. Currently the number of wireless users in the United States exceeds 120 million with the number increasing every day. The number of wireless subscribers is growing at the rate of 67000 per day.

The table below summarizes the chronological order of important events in mobile and wireless communications.

Table 1.1 History of Wireless Communications

Year	Events
1794	Claude Chappe invents the optical telegraph
1831	Michael Faraday invents the electromagnetic induction
1843	The first commercial telegraph line between Washington and Baltimore is built
1933	Armstrong invents Frequency Modulation (FM)
1947	AT&T provides scattered transmitters in metropolitan areas providing frequency reuse
1983	Advanced mobile phone system (AMPS) is introduced in the US
1991	Global system for mobile communication (GSM) is
1995	Qualcomm invents the CDMA
1997	IEEE 802.11 standard for wireless networks is introduced
1998	Wireless communications with satellites is introduced

1.3. Market for Wireless and Mobile Communications

The wireless and mobile communication industry is one of the fastest growing industries in the US economy. Mobile wireless communications have shown unprecedented growth in the past few years. More and more people use wireless phones, wireless technologies have been introduced in cars, wireless data services and

wireless local area networks are made use of in many places to the point that wireless and mobile communications have become ubiquitous.

The following figure shows tremendous growth rates of mobile phone users in most countries.

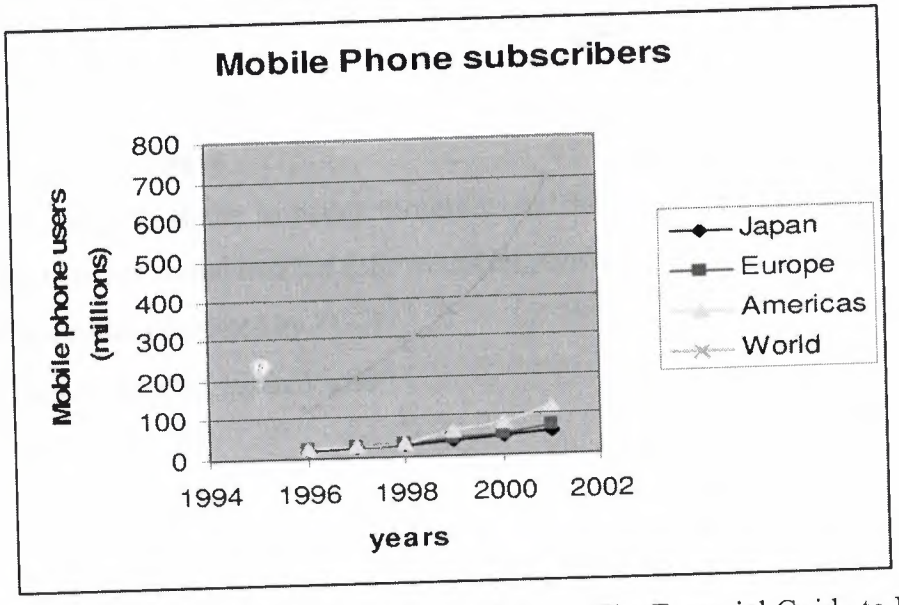


Figure 1.1 Mobile Phone Subscribers Adapted from "The Essential Guide to Business of US Mobile Wireless Communications"

The three main drivers for the field of wireless and mobile communications are:

- Digitalization
- Speed and power of information processing
- Mobility

Digitalization has tremendously influenced the way we live. Most of it is because digital communications are more efficient. With the advent of Internet, we have seen meteoritic increases in bandwidth consumption and demand. Most of the analog devices are being substituted for the better quality and more efficient digital devices. Digitalization has led to lower cost and smaller size devices like chips. One can clearly see that in the past few years digital images are taking over photography market, CDs and DVDs are taking over music and video market. With the advent of 3G networks the capacity of wireless and mobile communications has increased dramatically. Broadband access is available to the user giving him or her wide range of services. Speed and power of information processing is a dimension that has increased to the point that speeds like 2Mbps are possible over wireless and will continue to improve and refine in the near future. The first two factors further contribute to mobility.

Wireless internet access has been introduced in a big way. People want to be unrestrictive from phone lines, cables and other electrical wires. It has been predicted that virtually all voice communication traffic will be over wireless in the US in next 5-10 years. Thus wireless networking solutions are used almost everywhere. The mobile phones, PDAs, Pocket PCs are the fastest growing devices in the area of computing today.

1.3.1. Industry structure

In order to understand the industry structure and how it operates, the mobile and wireless industry is divided into the following components

- Network spectrum (allocated by FCC)
- Digital wireless network technologies
- Network suppliers
- Network service providers
- Network service consumers

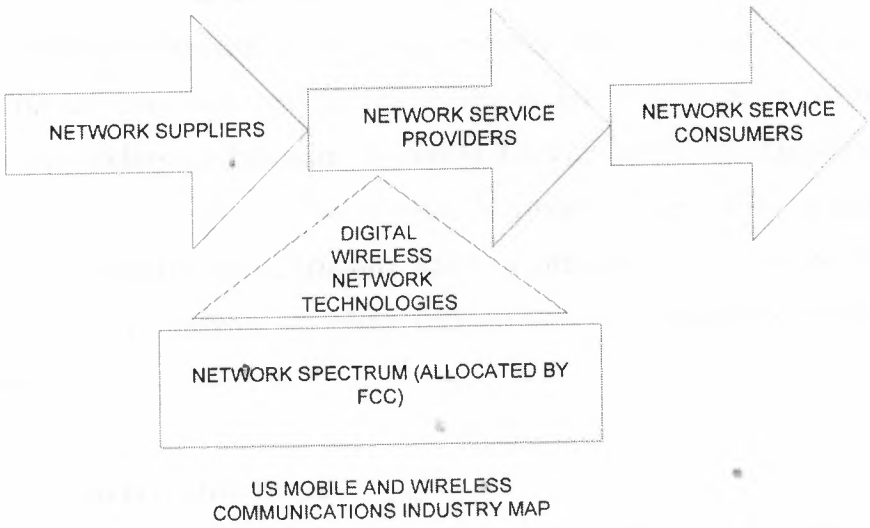


Figure 1.2 US Wireless Industry Map Adapted from "The Essential Guide to Business of US Mobile Wireless communications"

1.3.1.1. Network spectrum

A firm that is planning to offer wireless and mobile communication services acquires a license from the federal communications commission (FCC).The spectrum in the US is very precious and scarce resource. Companies have paid exorbitant prices to acquire the spectrum in the recent years.

1.3.1.2. Digital wireless network technologies

These are used to transmit and receive the signals between the mobile device and the base station or between mobile devices. The three main digital transmission technologies used in the US are code division multiple access (CDMA), time division multiple access (TDMA) and global system for mobile communications (GSM). CDMA uses the spectrum more efficiently than TDMA and GSM in the sense that it is a more bandwidth efficient technology than TDMA and GSM. This will be discussed later in the paper.

1.3.1.3. Network suppliers

Wireless networks have their own infrastructure though not as extensive as wired networks. It mainly consists of the base stations which act like switches. The investment on infrastructure may be a substantial investment. Some of the major infrastructure providers are Ericsson, Motorola, Lucent and Nortel. These companies form the network suppliers in the market. Network suppliers are generally the manufacturers of wireless infrastructure and in some cases may involve third party agents who sell and service wireless infrastructure on behalf of the primary manufacturers.

1.3.1.4. Network service providers

Network service providers can be divided into three major categories- one that provide cellular voice and data services like AT&T, Verizon and Sprint PCS ;two, that provide data-only services like Bell South Wireless data; three, that provide paging service like Metrocall.

1.3.1.5. Network service consumers

Network service consumers subscribe to the services offered by the network service providers. Network service consumers may fall into three categories-retail

consumers that use the wireless services for communication and convenience,business consumers which are those firms that use the network services to increase the productivity and value-added consumers that use the wireless network to provide their own added service like wireless internet service.

1.3.2. Industry size and focus

Wireless communications has been one of the most profitable and successful businesses in the last decade. The number of mobile phone users in the US alone exceeds 120 million. When we talk about the difference of US wireless and mobile communications market with rest of the world is the range of transmission technologies employed. The US has focused on a wide variety of standards ,while most of Europe has stuck to one standard by using the GSM. According to John P. Burnham "In spite of the much ballyhoo about other parts of the world being much ahead of US in the field of wireless and mobile communications ,the fact remains that US by far is the largest single market for mobile and wireless communications in the world.

The following figure shows the number of mobile terminal units shipped in the US in the recent years and projected estimates.

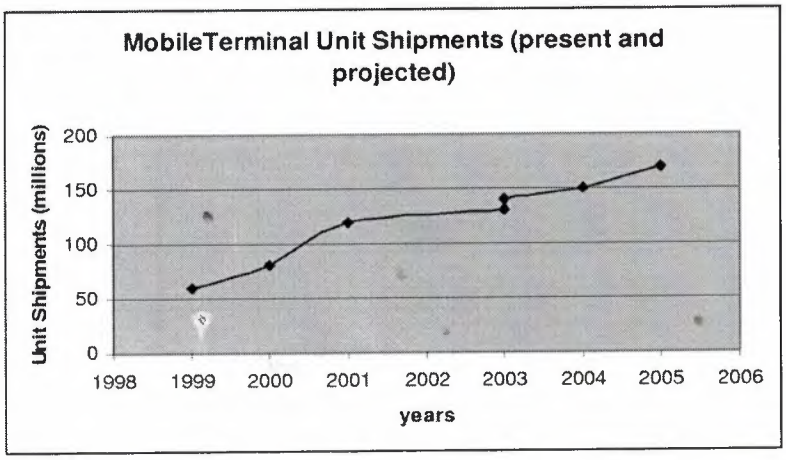


Figure 1.3 Shipment of mobile terminal units. Adapted from "The Essential Guide to Business of US Mobile Wireless communications

2. Regulation and FCC

Radio frequencies are scarce resources and so there is a need to ration these frequencies to companies. In the United States the allocation of the spectrum is done by the Federal Communications Commission(FCC) and National Telecommunications and Information Administration(NTIA).The FCC is an independent regulatory agency which is responsible for the allocation of the spectrum for commercial use and NTIA is responsible for the allocation of the spectrum for the government use.

The demand for spectrum from both government and other private firms far exceeds its supply.Hence, there has been a lot of competition among companies to acquire parts of the spectrum. FCC plays a major role in the allocation of the spectrum in the wireless and mobile communication industry today. The firms that need to use the spectrum need to take permission from the FCC in the form of a license. The major consumers of wireless radio frequency(RF) spectrum include wireless communications, television broadcasting, radio broadcasting and the department of defense. The radio spectrum used commercially is between 9 KHz and 38GHz.The following figure shows the major users of the wireless spectrum.

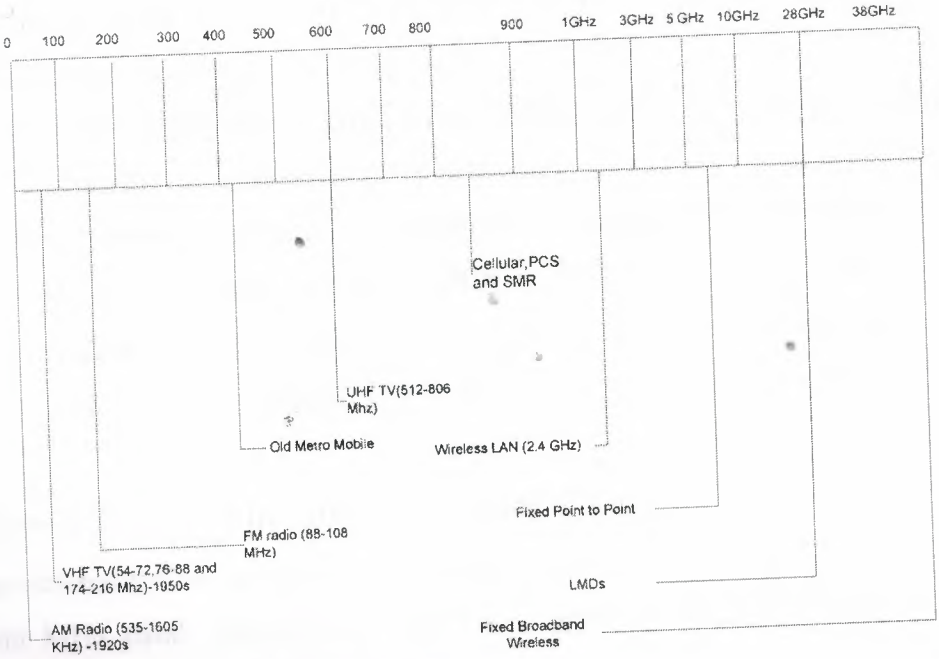


Figure 2.1 US wireless Frequency allocation. Adapted from "The Essential Guide to Business of US Mobile Wireless Communications"

2.1. Cellular spectrum allocation

The FCC allocated the radio spectrum for cellular service at 824-851 MHz and 869-896 MHz. The country was divided into 306 Metropolitan Service Areas (MSAs) and 428 Rural Service Areas (RSAs).Each MSA and RSA were to have two cellular service providers to promote competition. One 25 MHz license was given to a local exchange carrier (LEC) such as Verizon or Bell South (B block license) and the other 25 MHz license was given to a nontelephone company(A block license).The giving away of B block licenses was done to build up healthy competition in the wireless communication industry. However, the A-Block licenses were allocated through a lottery based scheme. Many companies formed alliances before the lottery to increase their chances of winning and ended up in a partial ownership of licenses.

2.2. PCS Spectrum allocation

The need for more spectrum capacity led the congress direct the FCC to allocate more spectrum for wireless communications .As a result of this the FCC decided to auction off the 120 MHz band of 1850-1990 MHz for personal communication services (PCS).The spectrum was divided into six segments: A,B,C,D,E and F blocks.

The A and B blocks were 30MHz each in the 51 major trading areas MTAs which included multiple cities or states.

The C (30 MHz) and D through F (10 MHz) serviced the Basic Trading Areas (BTAs) which included only one metropolitan area.

The government in order to increase the competition disallowed the already existing cellular providers to enter the PCS market. In the auction for A, B, D and E block licenses the major winners were Sprint PCS and AT&T Wireless, while in the C and F blocks biggest winner was Nextwave Personal Communications.

2.3. Specialized mobile radio spectrum allocation

The specialized mobile radio (SMR) spectrum occupies a 26.5 MHz of spectrum in the 800-900 MHz band. The FCC allocated this spectrum on a first-come first-served basis and Nextel acquired most of this spectrum.SMR is primarily used for voice services but more recently we have seen data services like paging, inventory tracking and credit card authorization.

2.4. Unlicensed Spectrum

The unlicensed spectrum is free to use. As a result many wireless devices operate in this range as the manufacturers don't have to worry about license procurements. They include cordless phones, card door remote controls, garage door remote controls and many others. This spectrum is present in 2.4 GHz frequency band. One of the most recent and rapidly growing use of this spectrum is for the bluetooth which transfers data over very short distances like 10 m at the rate of 721 kbps.

2.5. Total spectrum and total caps

At the end of the spectrum allocations the US mobile wireless communications was divided as 50 MHz for cellular, 120 MHz for PCS and 26.5 for SMR. The FCC also in order to promote competition limited the amount of bandwidth a carrier could own which was limited to 45MHz in metropolitan market and 55 MHz for rural market.

2.6. Spectrum auctions and reauctions

As the number of wireless services grew there was more and more need for spectrum. As a result the FCC decided to reauction 2 regions of the spectrum. The first one was the 1.9 GHz PCS spectrum reauction. The FCC had maintained a right to take the spectrum back if the service was not deployed in the original allocted spectrum before certain deadlines. One such company to suffer due to this policy was NextWave Communications which had to surrender its licenses to the FCC.The 1.9 GHz spectrum was reauctioned in an aggressive bidding with Verizon winning the most licenses. The FCC is also planning to auction the 700 MHz Spectrum Allocation. This spectrum has been an object of desire for many companies as it allows for long distance wireless transmissions and it is suitable for 3G wireless which needs bands that are at least 10 MHz wide. This spectrum is currently occupied by the television broadcast channels (60-69).This spectrum is due to be returned to the FCC when 85% of the subscribers change to digital broadcasting which is due by 2006.The FCC has taken a lot of flak and has been criticized for allocating this spectrum free for television broadcasting. The 700 MHz spectrum allocation has been already delayed many times. After much controversy, the

government has once again scheduled the auction for June 19, 2002. The 2 licenses (10 and 20 MHz) are to be allocated for the 6 regions of the United States.

The following figure shows the existing TV channels for broadcast and the proposed frequency allocation of the 700 MHz spectrum.

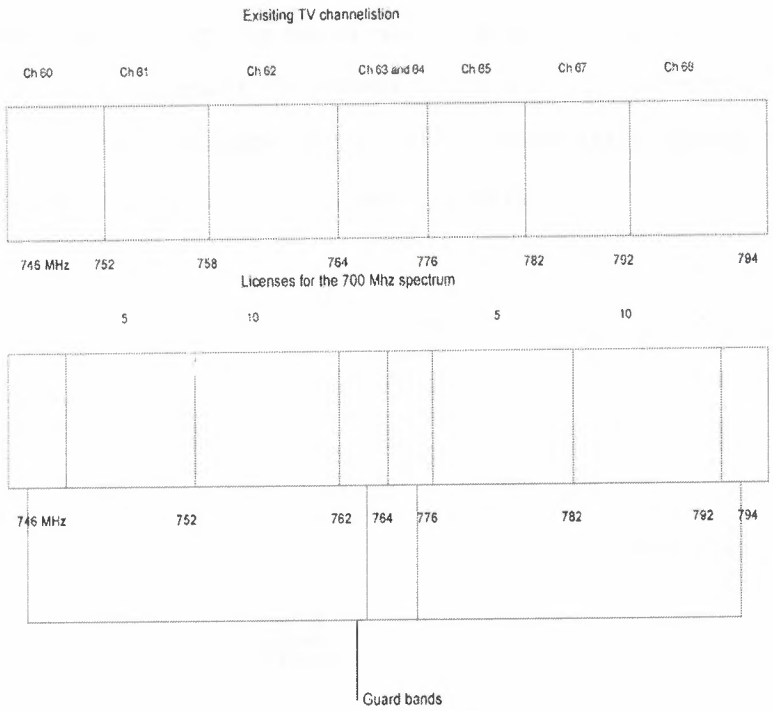


Figure 2.2 Existing and proposed frequency allocation for 700 MHz spectrum

2.7. Worldwide spectrum bands

At the World Radio Conference (WRC 2000) three spectrums for 3G wireless systems were identified: 806-960 MHz, 1710-1885 MHz and 2500-2690 MHz for worldwide 3G services. In the US, the primary occupants of this band are analog cellular, phone carriers, the department of defense, fixed wireless services and satellite broadcasting.Unless some part of this spectrum is reallocated by FCC, the WRC 3G services are unlikely to be used at least in the near future.

3. Wireless Transmission Signal

3.1. Signal propagation

Signals represent data. If one were to exchange data in a wireless scenario, it has to be done through signals. In wired networks there exists a physical link literally between a sender and receiver. So the signal has a sense of which direction it has to propagate if it were to reach the receiver. However a wireless networks, the medium being broadcast changes this situation considerably. Hence there arises a concept of concentric cells, which would look like as below.

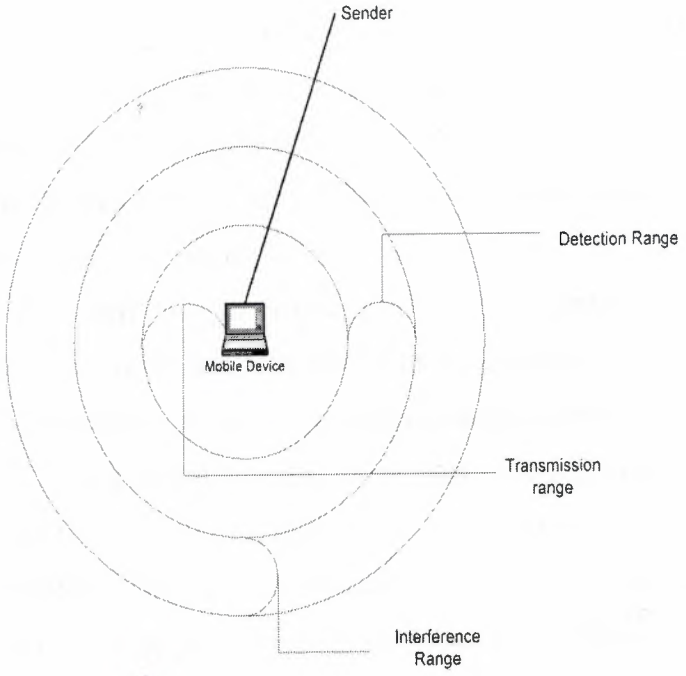


Figure 3.1 Ranges in a wireless transmission

Transmission range

In this range the sender's transmission reaches the receiver at very low error rates which is acceptable to it. The receiver can also act as a sender in this case.

Detection range

In this range the receiver can hear the sender's transmission but the error rates are substantially higher to establish good communication.

Interference range

In this range the receiver will not be able to detect the sender's transmission and may interfere (it is too weak when it reaches the receiver and is interpreted as noise) with

other signals that it may be receiving.

Signal propagation in wireless communications has its own set of issues. The radio signals experience a "free-space loss" when they travel thorough air/vacuum. The signal received at the receiver is inversely proportional to the square of the distance i.e. the greater the distance of the receiver from the sender the greater loss of signal strength (also called the inverse square law). Also the radio waves can penetrate the objects depending on its frequency. The lower frequency the frequency the better the penetration or to put it in other words the higher the frequency of a radio wave the more difficult it is to transmit the same because they have lesser penetration power.

The atmospheric conditions like rain, fog, snow, dust particles play an important role in influencing wireless transmission over large distances. They can cause attenuation of the signal. Another form of attenuation called blocking or shadowing occurs when the radio waves are reflected or scattered from the object's (obstruction) surface. The obstruction will reflect the radio wave if its wavelength is greater than that of the radio wave and will scatter the same if its wavelength is less than or equal to that of the radio wave.

One of the most serious factors that effect signal propagation is the multipath propagation. Since radio waves are transmitted as a broadcast there may be multiple paths between the sender and the receiver. So the signal propagated from the sender may reach the receiver through multiple paths. Also since the signals traversed multiple paths they may reach the receiver at different times. This effect is called delay spread. So with a single impulse at the sender the receiver may end up getting many weaker impulses. In fact some of these pulses may be too weak to be detected and will appear as noise.

Another effect of multipath propagation is intersymbol interference. Two pulses from the sender may interfere at the receiver to appeat as one pulse. In such a case there may be an energy spill between these pulses causing transmission errors.

3.2. Multiplexing

Multiplexing describes a method of several users being able to share and transmit signals on a medium. The main objective to do multiplexing is to reduce interference and maximize the channel utilization. Multiplexing in wireless communications is generally done in four dimensions

- Space
- Time
- Frequency
- Code

3.2.1. Space Division Multiplexing

When we talk about Wireless communications we talk about wireless channels on which the data has to be transmitted. Consider a case where there are six channels and three senders. They may represented as below

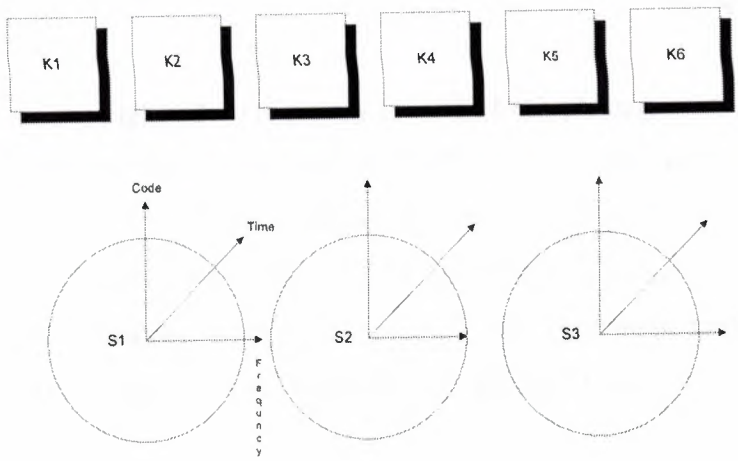


Figure 3.2 Space Division Multiplexing

Each of the three senders (SI to S3) may map to any of the channels Kl to K6 and in a sense they are separated by space. Infact had there been only three channels – Kl to K3, each of the senders could have been mapped to each of the channels. Hence space division multiplexing may lead to wastage of space. Also radio stations that use space division multiplexing are separated by appropriate distances so that their transmissions don't interfere. However if multiple stations are trying to transmit to the same station their transmissions may collide and in such a case space division multiplexing cannot be used.

3.2.2. Frequency Division Multiplexing

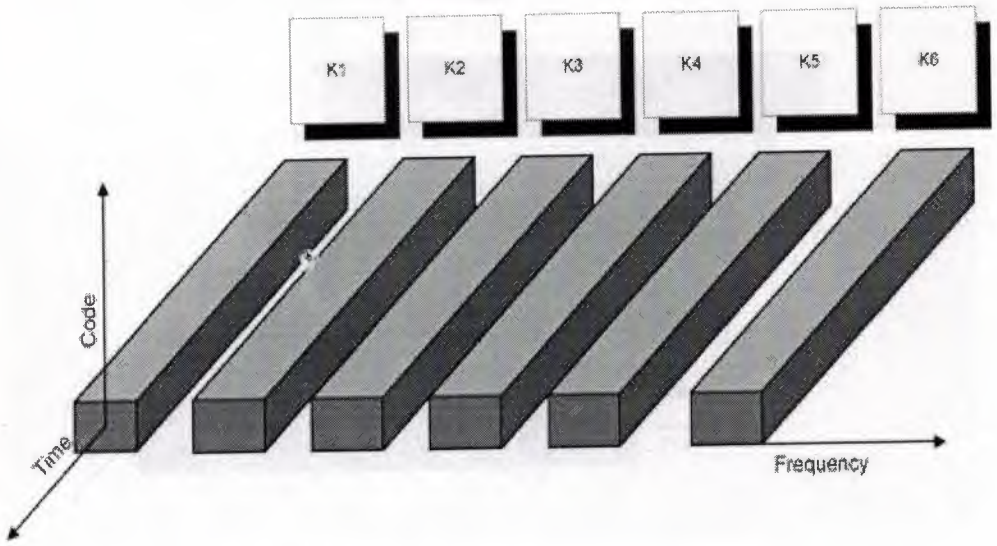


Figure 3.3 Frequency Division Multiplexing

In this scheme each of the channels kl to k6 have their own set of frequencies at which they operate. Each of these channels may be separated from a guard frequency space to avoid interference. So a radio station that needs to broadcast will transmit at the frequency allocated to it. However this is an extremely inefficient scheme because the station may not be transmitting all the time and scarce resource (frequency) is wasted.

3.2.3. Time division Multiplexing

In this scheme the all the channels Kl to K6 is given the entire bandwidth for a certain amount of time. So the senders (kl to k6) use the same frequency, but only for a certain amount of time. One of the requirements of the scheme is that the senders should keep their clocks synchronized for they need to know at what point in time, it is their turn to send. The figure below demonstrates Time division Multiplexing.

Time and frequency division multiplexing can be combined where the sender can send at a particular frequency for a certain period of time. This scheme has a greater overhead than the above as not only do the senders and receivers need to synchronize with each other but also need to know when to switch to a particular frequency. The figure below demonstrates combined frequency and time division multiplexing.

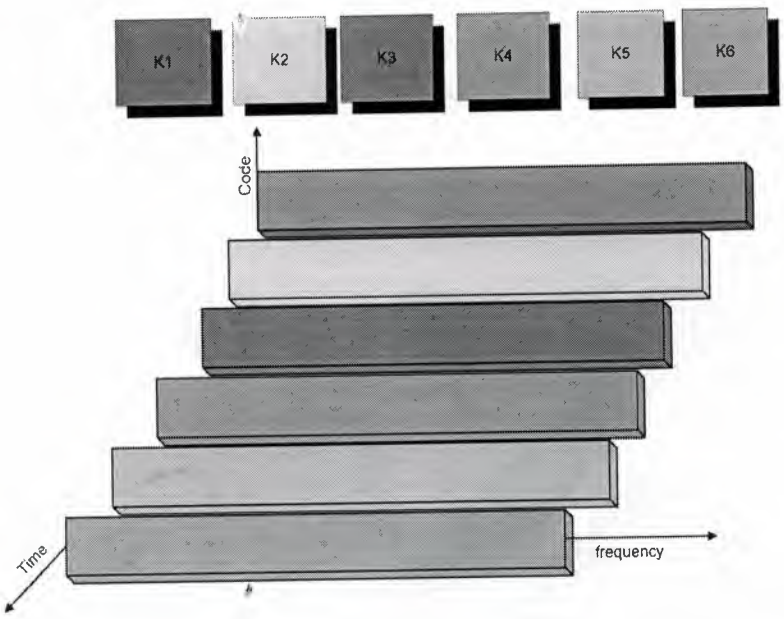


Figure 3.4 Time DivisionMultiplexing

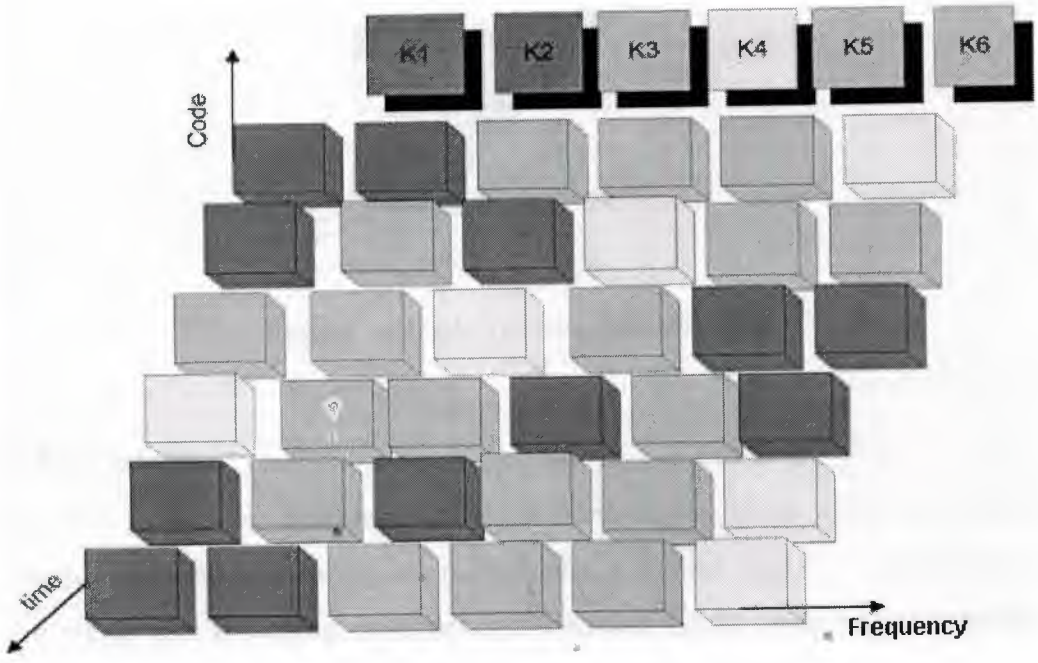


Figure 3.5 Frequency and Time Division Multiplexing

3.2.4. Code division Multiplexing

This scheme is a relatively new multiplexing scheme for mobile communications. Here the guard spaces are implemented by using codes. Each of the channels Kl to K6 uses the same frequency during the transmission. Each channel has its own code and thus there is an inbuilt property of security in the above scheme[55]. The receiver can listen to all the transmission but will only tune in the code that it needs to listen to.

This scheme clearly utilizes the bandwidth very efficiently but has a disadvantage that the receiver needs to separate the channel from the user data. This form of multiplexing is immune to interference and tapping. The following figure shows how code division multiplexing works.

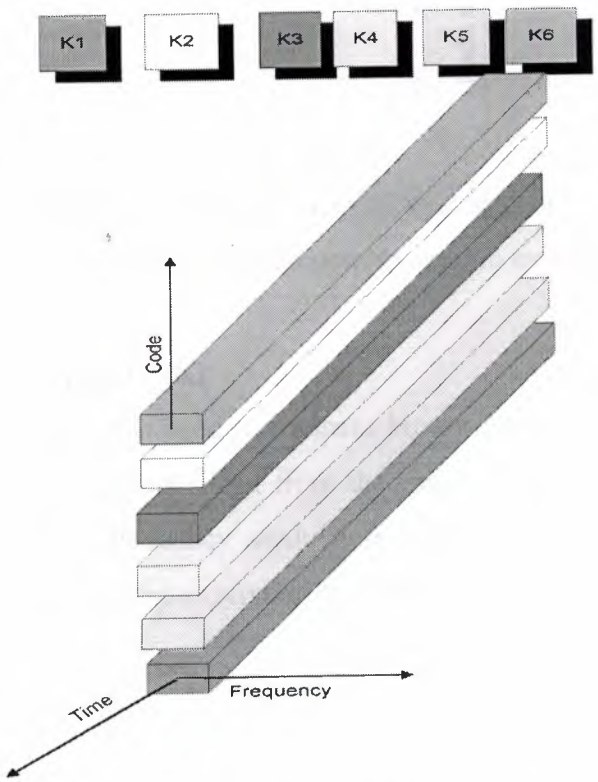


Figure 3.6 Code Division Multiplexing

3.3. Modulation

Modulation in wireless communications is done in two steps - digital modulation and analog modulation. In digital modulation a digital signal is converted to an analog signal and in analog modulation the analog signal generated also called the base band signal is mixed with a carrier and transmitted. This is necessary because at higher frequencies more bandwidth is available for the signal and also the carrier frequency can give certain characteristics to the base band signal, which may be necessary to avoid interference, scattering and diffraction.

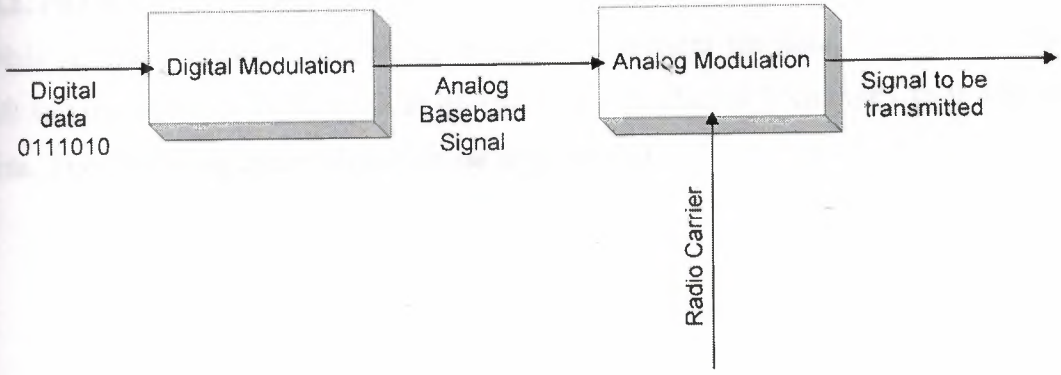


Figure 3.7 Modulation in wireless system

The following are the modulation schemes commonly used in mobile communications

3.3.1. Frequency shift keying (FSK)

In this scheme a frequency fl is used to transmit binary 1 and frequency f2 is used to transmit a binary 0 which slightly offset from the carrier frequency Generally to avoid sudden phase shifts special frequency modulators called continuous phase modulators (CPM) are used. The following figure represents frequency shift keying.

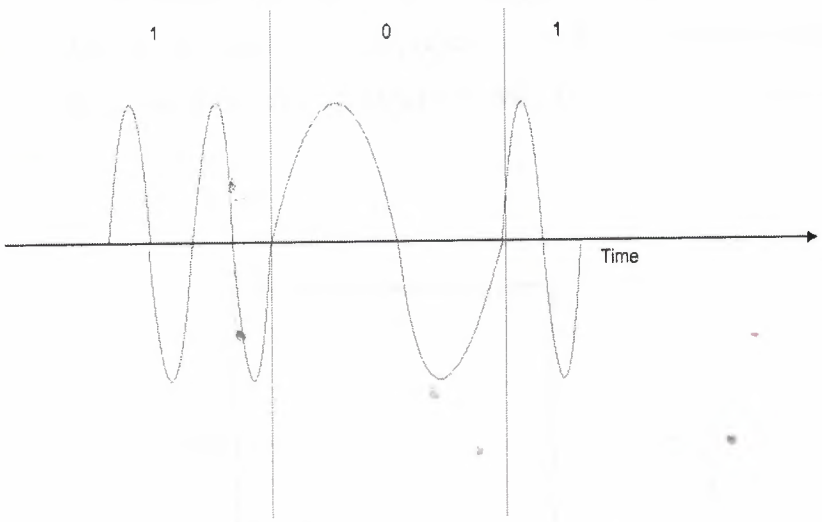


Figure 3.8 Frequency Shift Keying

In wireless communications a variant of the above called the minimum shift keying (MSK) is used. In this scheme we use 2 frequencies fl and f2 such that f2 = 2fl. The data bits are separated into odd and even bits and duration of bit is doubled. Depending on the value of odd and even bits (0 or 1) in a bit time the frequency fl or f2 is chosen.

3.3.2. Phase shift keying (PSK)

In this scheme, the shifts in phase are used to represent the data. In a simple phase shift keying there is a phase shift of 180 degrees when a 1 changes to 0 and vice versa. The following figure shows phase shift keying.

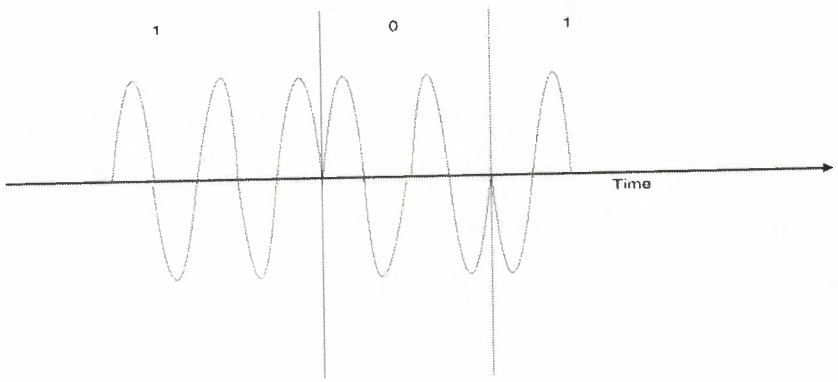


Figure 3.9 Phase Shift Keying The scheme described above is called binary phase shift keying (BPSK).

However the phase changes can be represented in steps of 90 degrees to give a quadrature PSK (QPSK) scheme. The phase shifts can be related to a reference signal. A phase shift of zero means that the signal is in phase with the reference signal. In QPSK a phase shift of 45 degrees will represent 11,135 degrees will represent 10, 225 degrees will represent 00 and 315 degrees will represent 01.The below figure represents this.

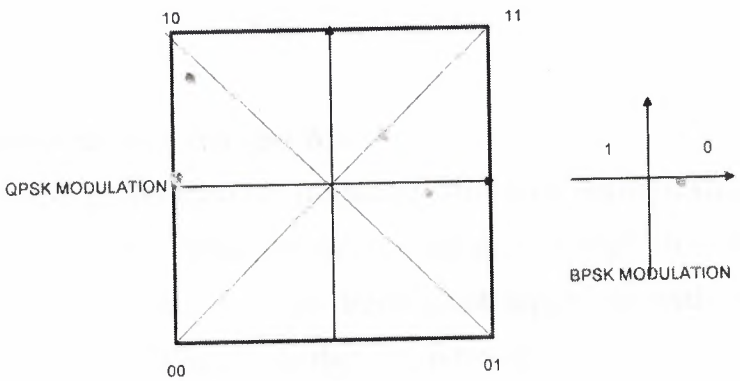


Figure 3.10 Phase ShifKeying

However QPSK has a problem that the sender and the receiver should be synchronized as the receiver should compare the incoming signal with respect to the reference signal. To overcome this problem another scheme called the differential QPSK (DQPSK) is implemented where the phase shift is not relative to the reference signal but depends of the phase of the previous 2 bits.

The phase shifting in steps of different angles can be implemented to represent more and more bits for a phase shift .For example 4 bits can be used to represent 16 phase shifts from 0-360 degrees.

The PSK and FSK schemes can be combined to give a scheme called the quadrature amplitude modulation (QAM) where 3 different amplitudes and 12 angles are combined to give a coding of 4 bits per phase/amplitude change. The following figure illustrates QAM

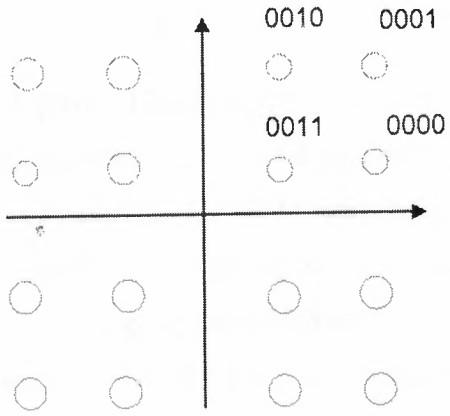


Figure 3.11 QAM

3.3.3. Multi-carrier modulation (MCM)

This is also called as orthogonal frequency division multiplexing (OFDM) or coded OFDM. The MCM scheme divides the signal with high bit rate into multiple lower bit rate streams which are then transmitted separately with an independent carrier signal. The result of which is that the inter-symbol interference is reduced. For example if the bit rate of the signal is n symbols/sec and there are c sub-carriers then the each of the c sub-carriers can transmit at the rate of n/c symbols/sec.

3.4. Spread Spectrum

This is a technique that is used to spread the signal to reduce the narrowband interference. When a signal is spread it is converted to a broadband signal which is spread over a greater frequency range. The following steps illustrate the spreading and

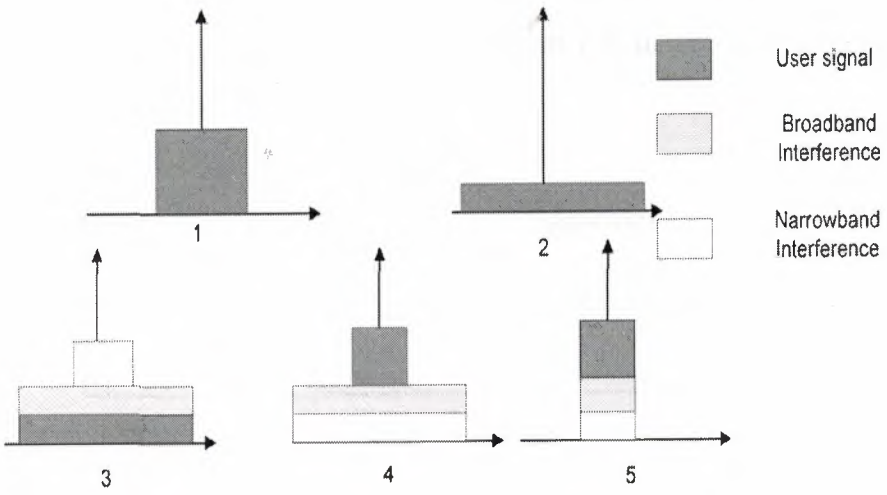


Figure 3.12 Spread Spectrum Steps

in step 1 the sender has to transmit a narrowband signal. In step 2, the sender converts this narrowband signal to a broadband signal by spreading. In step 3, the broadband signal is transmitted and received at the receiver during which the narrowband interference and broadband interference get added to the signal. In step 4 the receiver applies despreading to convert the signal back to a narrowband signal. This process spreads the narrowband interference while the broadband interference remains the same. In step 5, the receiver filters off the frequencies to the left and right of the narrowband signal and the original signal is retrieved.

Spreading of the spectrum can be achieved using 2 schemes

3.4.1. Frequency hopping spread spectrum (FHSS)

In this scheme the channel is split into many channels of smaller bandwidth. The transmitter and receiver hop from one channel to another and stay on a particular channel for a certain amount of time called the dwell time. FHSS comes in 2 forms- slow hopping and fast frequency hopping.

In slow hopping, the transmitter uses the same frequency for many bit times/periods. The slow hopping systems are easier to implement. In fast hopping the transmitter changes frequencies many times during a bit period. Since the

transmitter dwells for a lesser time on a particular frequency the interference and fading effects are lower compared to slow hopping.

In the first step the signal to be transmitted is modulated to produce a narrowband signal .This narrowband signal is presented with a hopping sequence of frequencies say fl, f2... fn from a frequency synthesizer that produces a spread spectrum signal with frequency fi+ fO if the user data is a 0 and fi+ fl if the user data is a I. The value of i here varies from 1 to n. The following figure shows slow and fast hopping in FHSS.

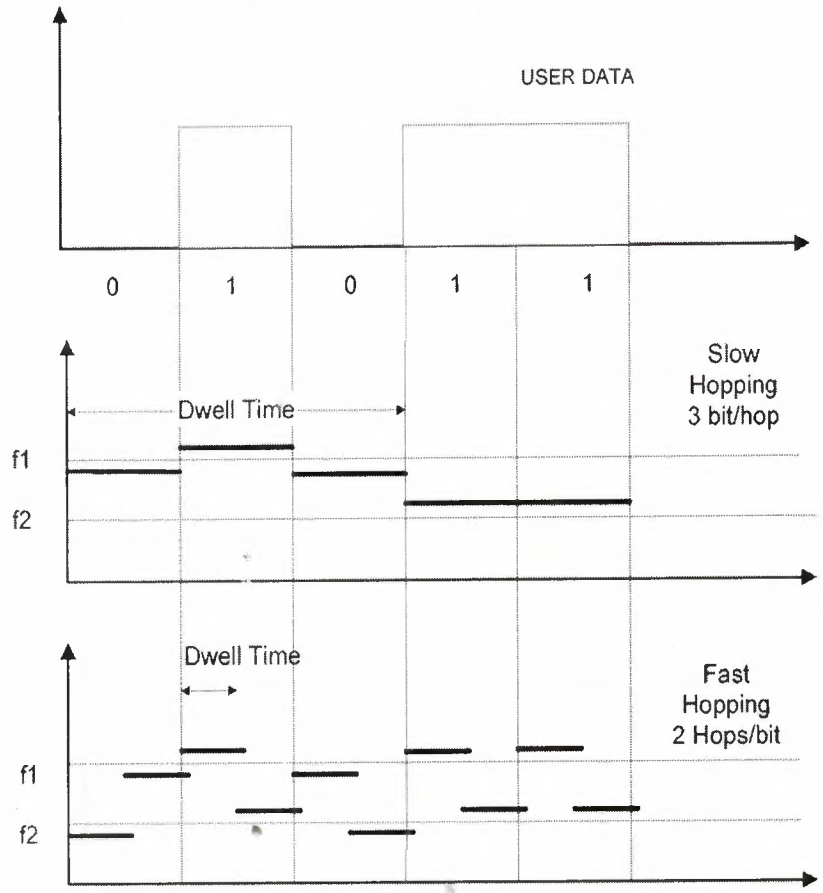


Figure 3.13 FHSS

3.4.2. Direct sequence spread spectrum (DSSS)

In this scheme the user data is XORed with a chipping sequence or code (one such is the barker sequence) to produce a spread spectrum signal. This spread spectrum signal is modulated to produce a transmit signal. The receiver then demodulates and applies the chipping sequence to get back the user data that was transmitted. Since the receiver too has to apply the chipping sequence to get back the user data

the sender and the receiver have to be kept tightly synchronized. The receiver applies a product of the chipping sequence and transmit signal and collects sum of all the products using an integrator.

Then during each bit time a decision unit samples the sum to decide whether the user data transmitted was a 1 or a 0. One of the disadvantages of direct sequence spread spectrum is that of the complex function of the receiver. However this scheme is extremely resistant to fading and multi-path propagation effects. Also the DSSS signals are difficult to compromise because a spreading code is used. In fact tapping of DSSS signals is virtually impossible.

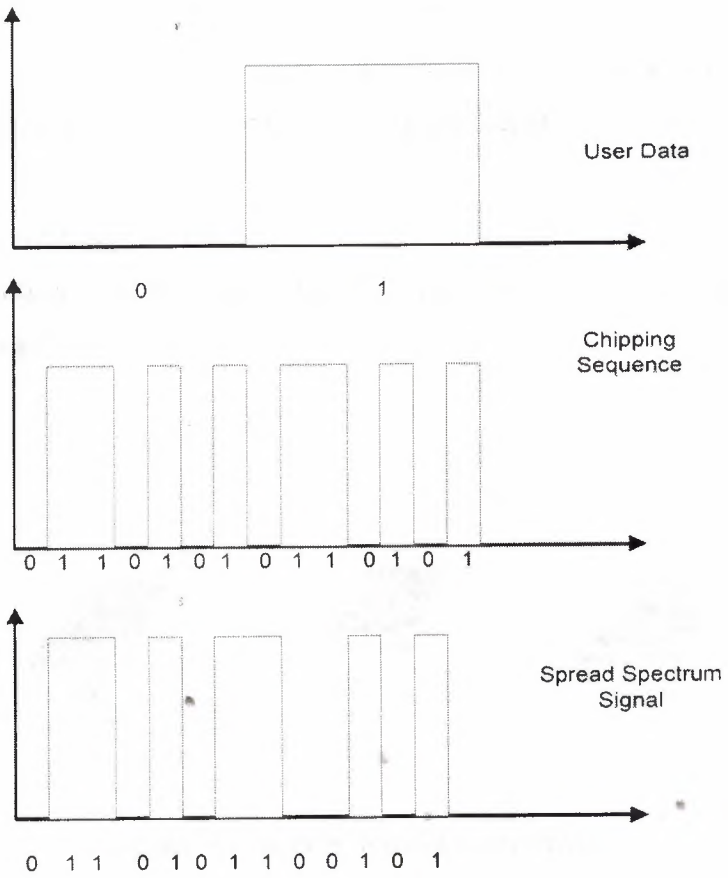


Figure 3.14 DSSS

FHSS is simpler to implement compared to DHSS and uses only a portion of the bandwidth at a time.

4. Medium Access Control

4.1. Why the specialized MAC?

The medium access control (MAC) protocol is used to provide the data link layer functionalities in a wireless domain. The wireless domain is a medium that the users must contend to access. Unlike wired networks where accessing a medium means accessing a wired link where a user knows in which direction the transmission is to be done, in a wireless scenario the directional is most cases is omni directional. It is important to understand in a wireless scenario that the contention for the medium is both at the sender and the receiver. However in a wired scenario contention resolution of the medium at the sender is enough to guarantee that the medium is free to transmit. The contention resolution only at the sender leads to a peculiar situation called the "Hidden and Exposed terminal" problem for wireless scenario as mentioned below.

4.1.1. Hidden terminal problem

Consider a situation as below where the three terminals A, B and C are trying to talk or send data to each other.

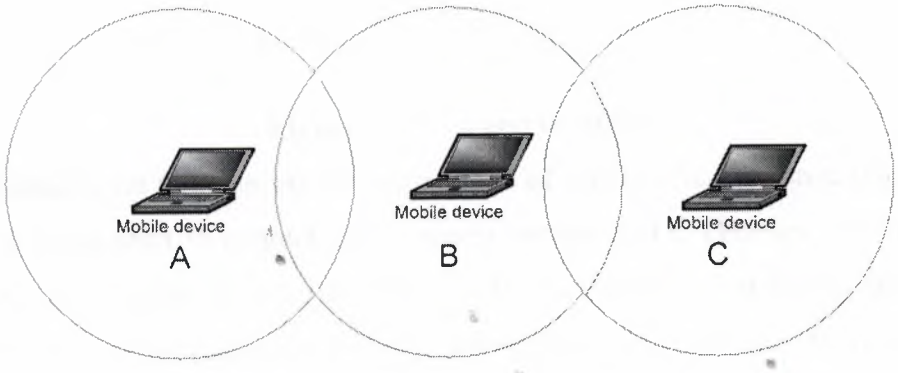


Figure 4.1 Sample Wireless transmission

A is in the transmission range of B and B is in the transmission range of A and C and C is in the transmission range of B. So if A is trying to transmit data to B at the same time when C is trying to transmit data to B, both A and C sense the channel as free if we were to do contention resolution according to a wired medium where the resolution is done at the sender. So the transmissions of A and C collide at B and so we say that A is hidden from B and vice versa.Clearly there is a need for a scheme to overcome this.

4.1.2. Exposed terminal problem

Using the same situation as shown above consider a situation where A is trying to send data to some mobile device not in the interference range of B and C when B is already sending data to C. In this case A senses the medium as busy as A can hear Bs transmission it being in Bs range and chooses not to transmit. However such a decision is undesirable because the transmission of A to some other mobile device when B is already transmitting to C would not collide with each other. This is called the exposed terminal problem. A does not send the data sensing that the medium is busy even though this is not necessary!

4.1.3. Near and far Effect

A phenomenon called the near or far effect occurs quite often in wireless communications. Consider a scenario as shown below

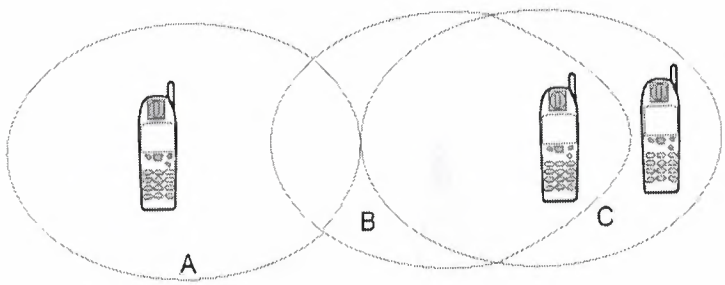


Figure 4.2 Near and far effect

In this scenario let C be an arbiter for a range of services in the sense that different mobile devices need to contact C to request service and C chooses one of them by applying a fairness scheme. However since A's transmission can barely make it to C as by the time the signal reaches C it is drained out, so C chooses B over A which is unfair. There has to be a mechanism of power control that one should implement when receiving from many senders in the above scenario. The different media access mechanisms are described as below:

4.2. Space Division Multiple Access (SDMA)

In this scheme the users are separated by space or in other words by distance. A typical application of this scheme would be where a user of a cell phone chooses a base station over others or in other words an optimal base station is allocated to the user. Clearly one can see that this scheme may not be optimal and involves a loss of space. Generally space division is used in conjunction with other schemes like frequency division multiple access (FDMA), time division multiple access (FDMA), code division multiple access (CDMA).SDMA is used in smart antennas where the signals are separated in space to the different users as shown below. SDMA requires careful choice of zones for each transmitter, and also requires precise antenna alignment. A small error can result in failure of one or more channels, interference among channels and confusion between surface coverage zones. The following figure shows how smart antennas send controlled energy to the users, one of the latest applications of SDMA.

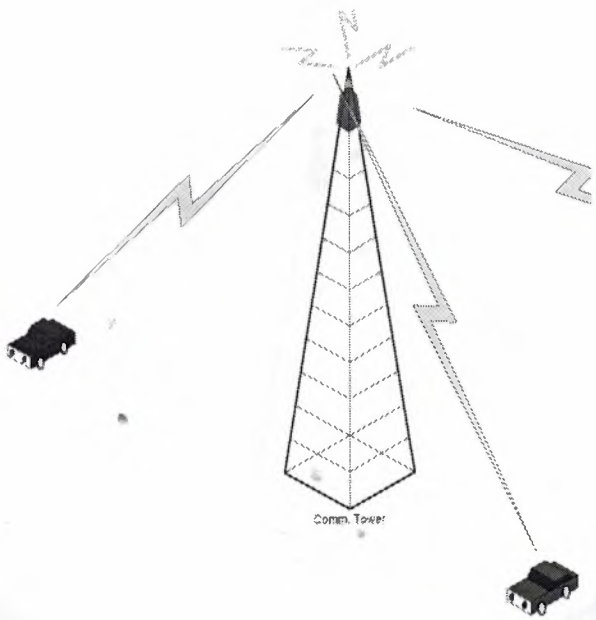


Figure 4.3 SDMA

4.3. Frequency Division Multiple Access (FDMA)

This scheme involves the division of frequencies to users. This effectively means allocating user to channel. FDMA may come in different flavors where channels are assigned the same frequencies called "pure FDMA" or where channels may change frequencies like frequency hopping scheme as described before. A scenario where FDMA is used is when the mobile device and the base station are trying to communicate to each other. They both establish full-duplex channels by using different frequencies in both directions. The direction from the mobile device to the base station is called the uplink and the direction from the base station to mobile device is called the downlink. The base station and mobile device predetermine the frequencies to be used for both directions. However in this scheme since a single user is allocated to a channel it clearly wastes bandwidth. The presence of interference bands which need to separate the channels and avoid interference also wastes bandwidth. The figure below shows how FDMA is used between the mobile device and base station.

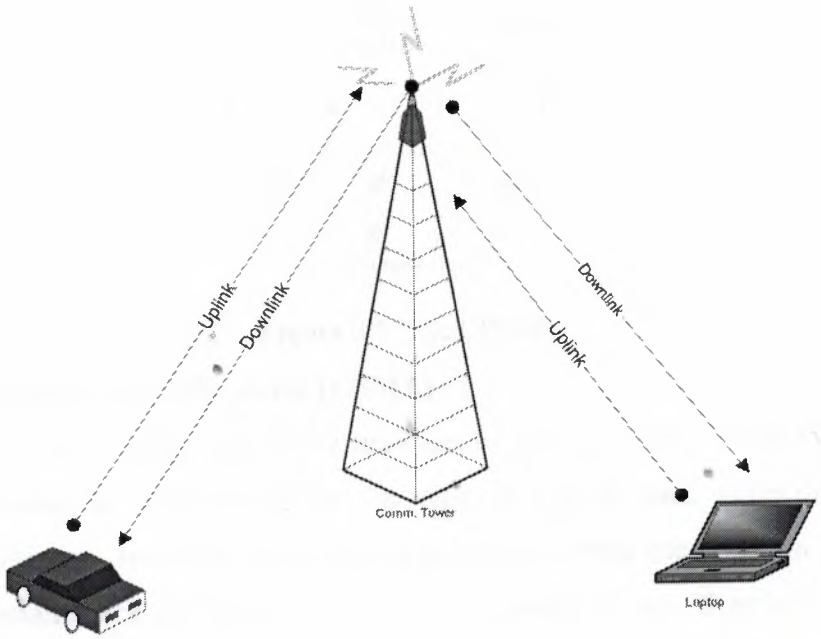


Figure 4.4 FDMA

4.4. Time Division Multiple Access (TDMA)

In this scheme the users can tune into the same frequencies for a specific amount of time called the "slot". The sender and receiver have to be synchronized in a sense that they both have to access the channel at the same time resulting in the need to keep the clocks synchronized.

Some of the different schemes used in TDMA are:

4.4.1. Fixed time division multiplexing (FTDM)

In this scheme a fixed time slot is allocated to the mobile station to access the duplex channel between itself and the base station. In the figure shown below, the mobile device can choose one of the slots for the uplink (1 to 4) and one of the slots for the downlink (1 to 4). These slots will remain idle if no mobile device accesses them. Also this scheme is not suitable to transfer a burst of data because the station/device may have to transfer the busty data over several slots.

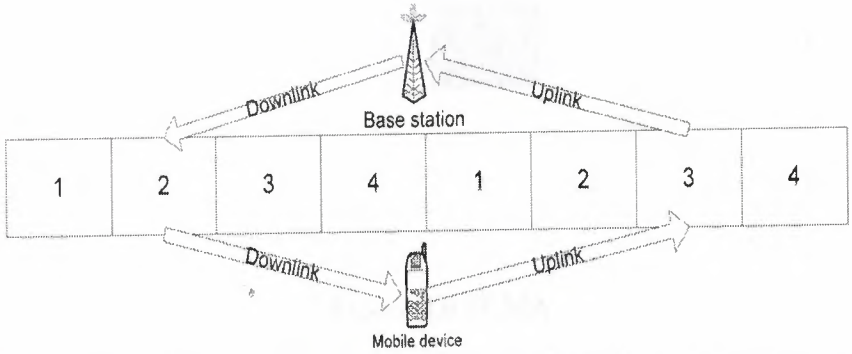


Figure 4.5 Fixed TDM

4.4.2. Carrier sense multiple access (CSMA)

In this scheme the sender senses the medium to find whether it is busy or not. In mobile and wireless communications the type of CSMA used generally is called collision avoidance. Here the wireless device when senses the medium to be busy chooses a certain back off which is the time for which it would go to sleep. After sleeping for back off interval the mobile device wakes up to find whether the medium is busy or not. If the medium is still busy it chooses a back off interval twice that it choose before and goes to sleep again. However if the medium is found free it accesses it to send data.

4.4.3. Packet reservation multiple access

In this scheme a certain number of slots form a frame, which is repeated. Each of these slots can be accessed by a mobile station at a time. The slot occupation information is sent as a broadcast by the base station as a reservation vector. A slot once assigned remains allocated to the mobile station as long as it has data to send and hence the term "reservation". The following figure shows the reservation vector and the frame which consists of a specific number of slots.

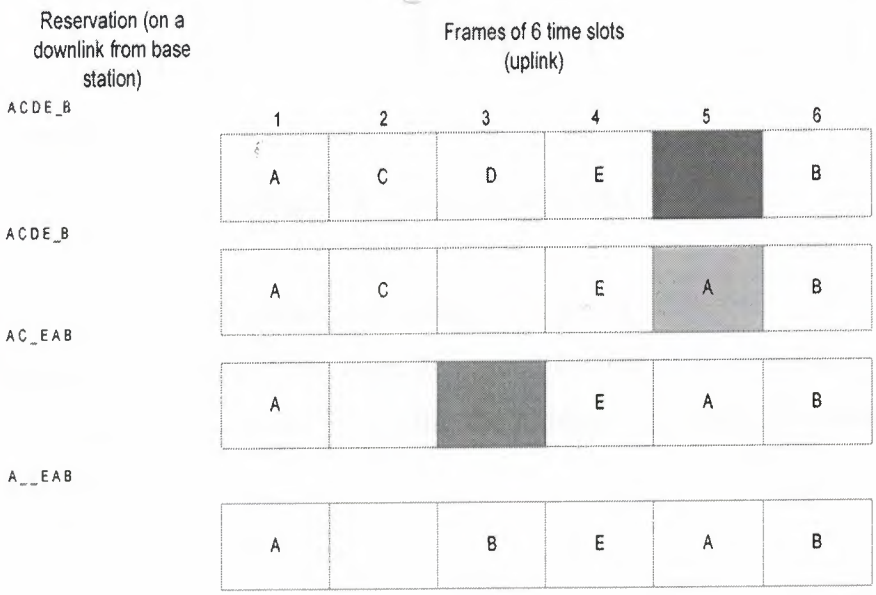


Figure 4.6 PRMA

In step 1 the stations receive ACDE_B which means that slot 5 is free. Many of the mobile stations try to access the slot and hence there is a collision. The slot is still not gets reserved by any station. In step 2 the stations again receive ACDE_B and slot 5 is successfully reserved by station A and station D stops transmitting in slot 3 and so the stations receive AC_EAB in step 3. The stations (many) now try to access slot 3 and there is a collision. Also station C stops transmitting in slot 2 and hence the stations receive A EAB in step 4.Finally, the station B is successful in accessing slot 3.

4.4.4. Reservation TDMA

In this scheme each of the N stations is given K data slots which are used to send data. Hence the number of the data slots are N*K .This is shown below in the figure. Preceding the data slots are the N mini-slots which represent whether a station is

currently using its K data slots. Stations can use the K data slots of the other stations which have to be accessed in a round-robin fashion. This scheme clearly optimizes the bandwidth utilization by providing a best-effort service which basically means that whenever there is data to be sent and bandwidth is available, the data is transmitted.

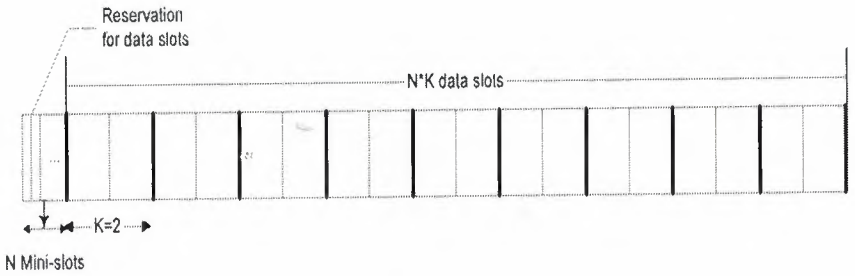


Figure 4.7 Reservation TDMA

4.4.5. Multiple access with collision avoidance (MACA)

This TDMA scheme is one of the more advanced and latest TDMA schemes used in mobile communications. It helps in solving the hidden and exposed terminal problem mentioned before.

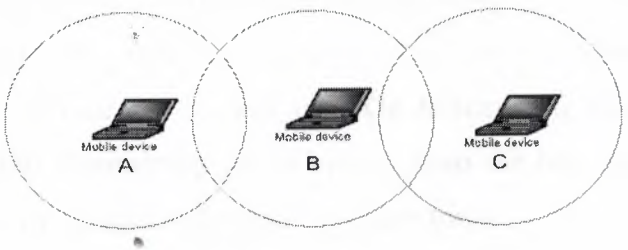


Figure 4.8 Reservation TDMA

Consider a situation again as shown above where A and C are hidden from each other. The hidden terminal problem can be overcome by resolving collisions are at the sender and receiver. I could not emphasize this point more enough. So, when A wants to send data to B it sends a frame called the request to send (RTS) indicating the duration of data transfer it intends to make to B. When B receives this RTS packet it copies the duration of transfer and sends out a clear to send (CTS) packet .All the stations that receive the CTS packet shut up for a time equal to the data transfer. In this case C will choose not to transfer data to B because it hears CTS from B and hence transmissions from A and C will not collide at B.

In the exposed terminal situation like explained before, B sends an RTS when it has to send data to A while C is wants to send data to someone else besides B and A. A on hearing the RTS sends a CTS back to B. However C does not hear this CTS and goes ahead with its transmission which is what is desired.

4.4.6. Inhibit sense multiple access (ISMA)

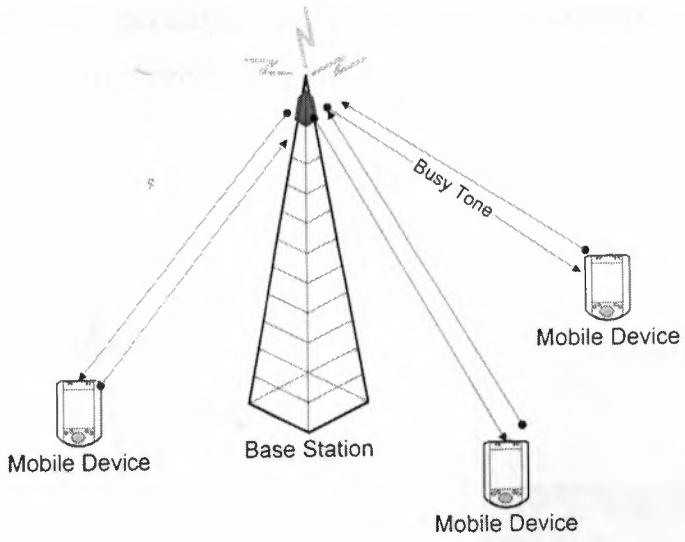


Figure 4.9 ISMA

This is a scheme used in packet transmissions from the base station to mobile device. The base station sends a busy tone to the mobile devices on a downlink asking the mobile device not to transmit. On hearing the busy-tone the mobile devices refrain from transmitting on an uplink. Also the base station sends positive and negative acknowledgements through this busy tone.

4.5. Code division Multiple Access (CDMA)

CDMA is a digital wireless technology that was pioneered and commercially developed by QUALCOMM. CDMA is the most advanced digital media access wireless technique present today. In this scheme codes are used to separate different users without causing any interference. Consider a situation where there are four simultaneous users speaking at the same time in four different languages English, German, French and Spanish. There is a receiver in the audience who understands only English, so he will tune according to the English speaker and tune out the other three. In the same way in a scheme like CDMA the channel is coded

for each user and all the users use the same frequency band. The user then decodes the conversation according to his code for the channel. Since the frequency band is shared by different users CDMA is extremely efficient in bandwidth utilization. CDMA uses the spread spectrum technique for encoding which involves spreading the signal over a larger bandwidth. The signal appears like pseudo-random with noise-like properties and hence the term "pseudorandom encoding". Every time a spreading is done a unique code is used. On the other side the receiver uses dispreading to perform decoding and gets back the original transmitted data. Both the sender and the receiver have to be tightly synchronized during the transmission of data.

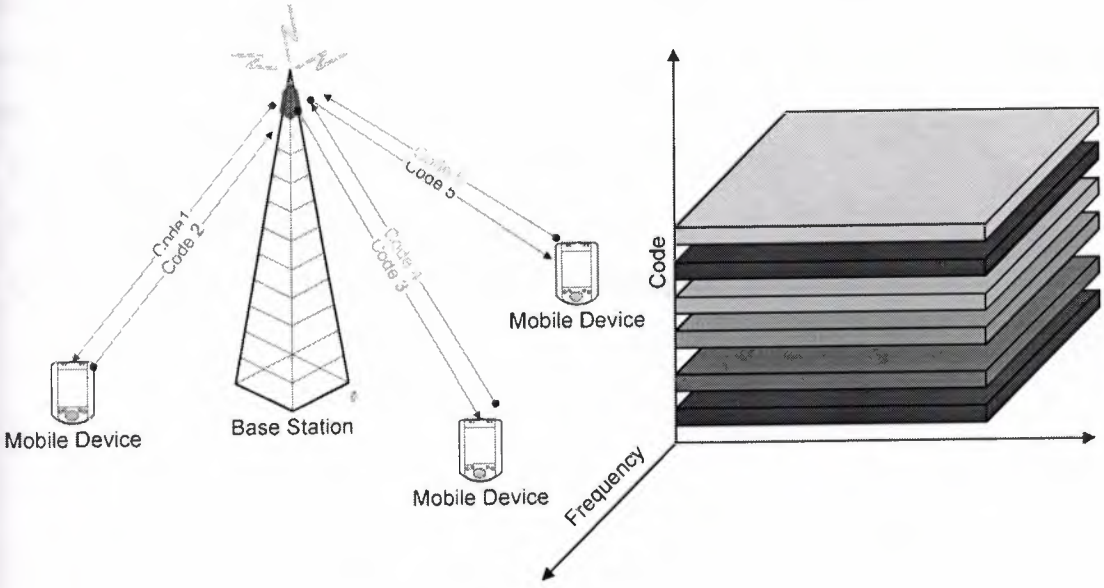


Figure 4.10: CDMA

It is clear from the figure that the CDMA uses a different code for both the forward channel i.e. the downlink from base station to the mobile device and the reverse channel i.e. the uplink from the mobile device to the base station.

CDMA is done using direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) techniques. Both of these spread spectrum techniques and their motivations for doing the same have been discussed before. To mention briefly in DSSS the narrowband data is multiplied by a wideband pseudo-random chipping sequence (Barker code), while in FHSS the available spectrum is divided into many bands of different frequencies and frequency is periodically changed as the transmitter hops from one different channel to another.

4.5.1. Advantages of CDMA

Some of the advantages of CDMA are:

- In the cellular technology the mobile devices have to be handed off as they move from one base station to another. In such a case since CDMA uses the same frequency band the shift from one cell to another is done in a smooth manner without disruption of the call. When the mobile device reaches the boundary of the cell it starts receiving signals from both he cells till a point where the mobile device is handed over to the other cell. This process is called "make before break" or "smooth handoff CDMA is a very inherently secure because of the channel coding that is used when transmitting information to each user.
- CDMA is known to exhibit something known as "soft capacity" where more and more users can be added to the cell, there is no hard-limit though the cell size may decrease when a number of users are added. However in FDMA/TDMA this is not the case.
- CDMA uses lesser power and leads to lesser interference.
- CDMA reduces multi-path fading effects.
- CDMA can coexist with previous analog technologies.

5. Wireless LANs

5.1. Overview

Wireless LANs are medium access control devices for wireless networks. The main motivations for a wireless LAN is that the current users want to be untethered to cables and wires as they access the network. There has been a lot of demand to replace the office cabling by wireless access to the network which the users can access by being mobile. The key is for one to be able to access information anywhere and all the time. In such a case wireless LAN comes into play where imagination is the only limiting parameter. Wireless LANs provide access to information and data where wiring is not possible say firewalls between buildings. Wired networks are susceptible to infrastructure breakdown during earthquakes or flood but wireless networks are typically more robust to such natural calamities. One cannot have copper cabling everywhere. Whether it's in the warehouse, conference room, or den, the handiest tool for making tough connections is a wireless LAN .Wireless LANs let you extend your network to every square inch of your campus, building, or residence.

5.2. IEEE 802.11

IEEE 802.11 is a wireless LAN standard developed by IEEE. IEEE 802.11 architecture can be of 2 typesInfrastructure-less or Adhoc scenario.

5.2.1. Types of IEEE 802 architecture

5.2.1.1. Adhoc scenario

An adhoc network is a group of nodes that come together to communicate with each other. Such a group of nodes don't have any existing architecture and depend of themselves to transfer the data from one node to another. The domain shown in the figure is called the basic service set (BSS) where all the nodes use the same frequency.

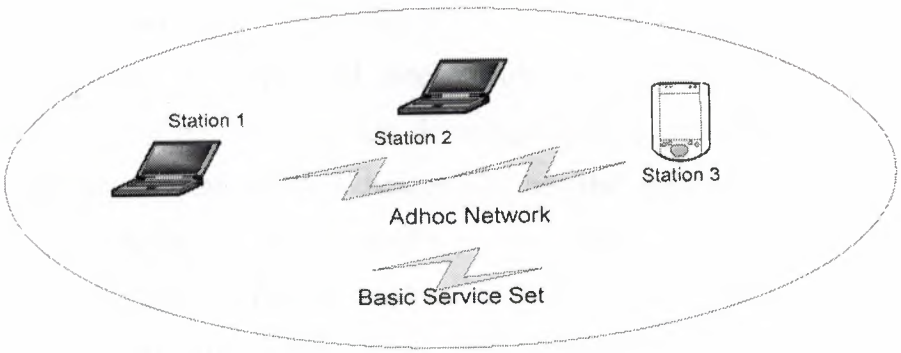


Figure 5.1 IEEE 802.11 Adhoc Architecture

5.2.1.2. Infrastructure based scenario

In this type of architecture the mobile nodes are connected to an access point which is the base station. All the nodes using the same base station or the access point are said to be in the same BSS. BSS's can be connected using a wired network. This interconnection network is called the distributed system (DS).

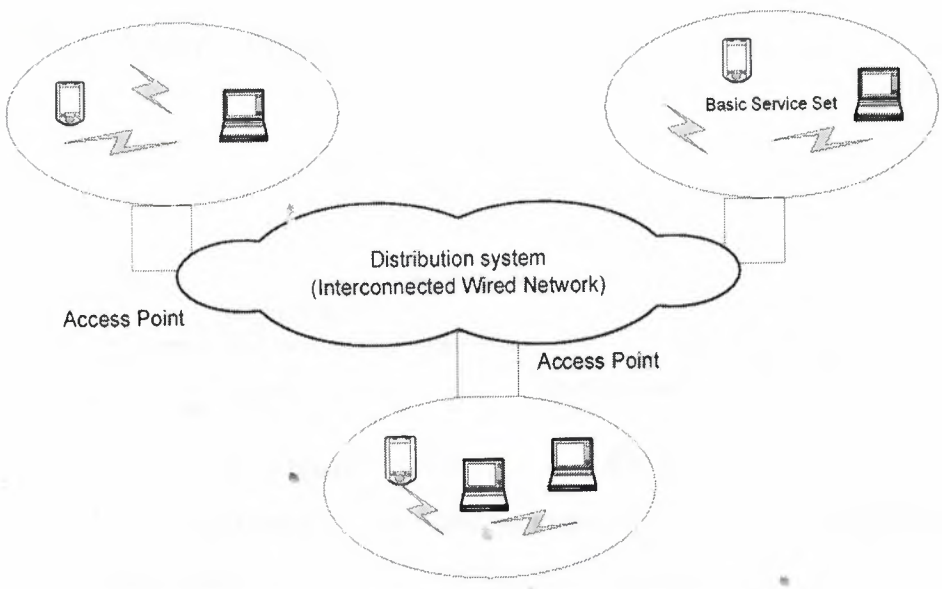


Figure 5.2 IEEE 802.11 Infrastructure based Architecture

5.2.2. IEEE 802.11 wireless LAN standard

IEEE 802.11 wireless LAN standard extends in two layers; the physical layer and the medium access control layer.

5.2.2.1. Physical layer:

The physical layer is subdivided into 2 sublayers -physical layer convergence protocol (PLCP) and physical medium dependent (PMD) layer. PLCP layer provides clear channel assessment which indicates whether the medium is busy or free and provides a service access point (SAP) to the MAC layer. The PMD layer is responsible for modulation and demodulation of the signal.

The physical layer is based on radio frequency transmission or infrared transmission. The FHSS scheme provides a data rate of 1 Mbps while the DSSS scheme provides a data rate of 1 to 2 Mbps.

5.2.2.2. Medium Access layer

The MAC layer provides controlled medium access. The basic services offered by MAC are asynchronous data service and time bound service. The former is a best effort delivery of the data. The delay bounds in the delivery are not taken into consideration and the latter involves delivery of packets with time constraints. Distributed Coordinated function (DCF) provides asynchronous data service.

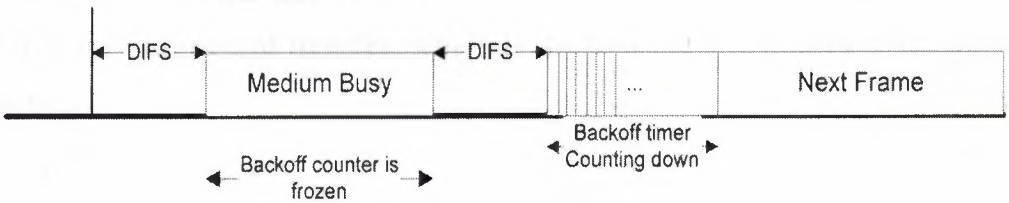


Figure 5.3 CSMA/CA in 802.II

The station when needs to access the wireless channel waits for a time period called the DCF inter-frame spacing (DIFS). If the medium is free for DIFS the station enters a contention phase where it starts counting the timer from a value called the back off. When the timer expires the node accesses the channel. So in addition to the time DIFS the nodes also wait for an interval called the back off before they access the channel. Different nodes choose different back off values which may be chosen on different parameters. This makes the access mechanism fairer. This mechanism above is called carrier sense multiple access with collision avoidance (CSMA/CA).

When the station that accesses the channel sends data after a time period DIFS, the receiver sends an acknowledgement (ACK) back to the sender after

waiting for a period SIFS. The period SIFS is shorter than DIFS because the receiver needs to access the channel before other stations to send the ACK back. The other stations wait for DIFS plus back off time before they access the channel after the data transfer is complete.

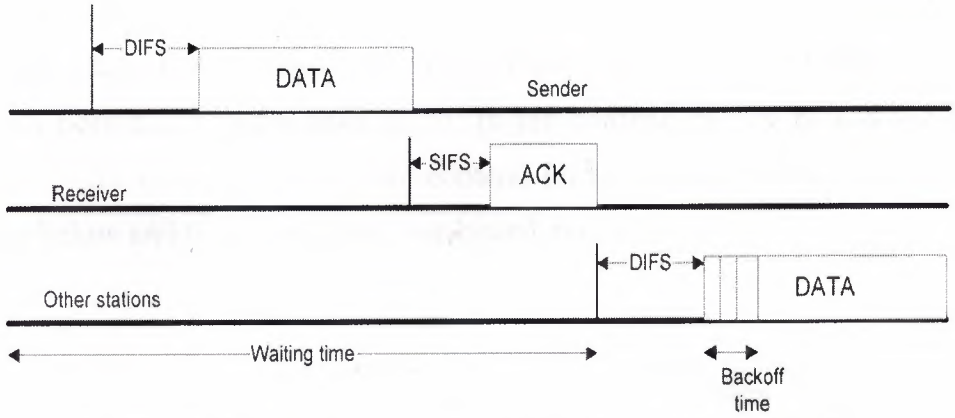


Figure 5.4 Data transfer for DCF in 802.11

The above mechanism can be improved using a RTS and CTS hand-shake to solve the problem of hidden and exposed terminals. When the sender has data to send, it waits for a time period called DIPS and sends the RTS. The receiver hears the RTS and sends a CTS back after a time period SIFS. The sender then sends the data after SIFS. All the stations hearing RTS and CTS set its net allocation vector (NAV) to the duration of transfer, which is the time for which they defer access to the channel.

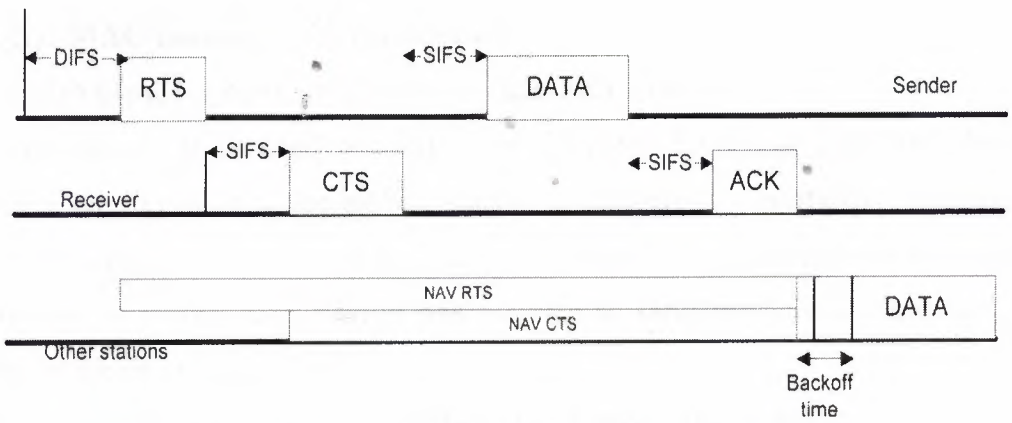


Figure 5.5 Data transfer using RTS and CTS for DCF in 802.11

Point Coordinated function (PCF) provides asynchronous and time-bound service. It uses a point coordinator (PC) which is the access point. This polls the stations when they have data to send or it has to send data to the stations. The

coordinator waits for a time period PCF inter-frame space (PIFS) before it sends data downstream to a station. The station replies after a SIFS. Now the point coordinator polls another station by sending D2 downstream. If the station has data to send it sends data upstream (U2) after SIFS. The PIFS is smaller than DIFS hence the coordinator is given more preference when it has to send data to the stations and ensuring time bound delivery. However after SIFS if the PC does not receive any data it can send contention free period end notification and the contention period can begin once again. In the contention free period the use of PCF ensures that other stations cannot contend for the channel indicated by NAV in the figure below and thus providing time bound deliveries.

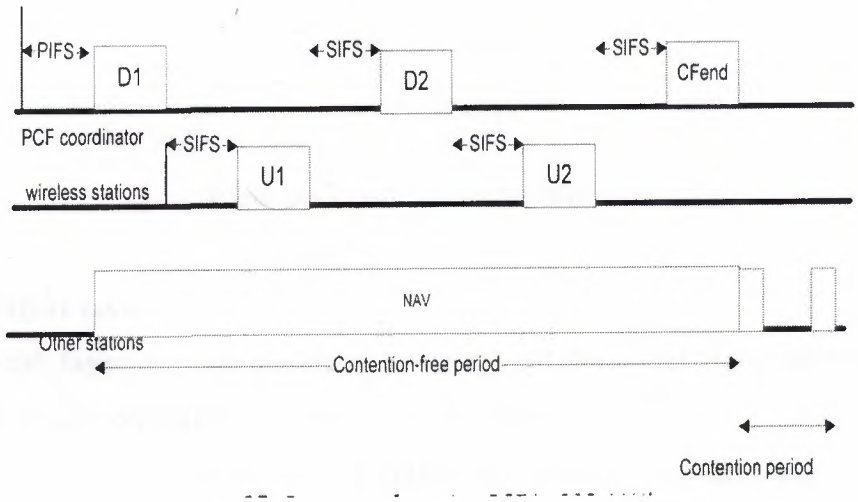


Figure 5.6 Data transfer using PCF in 802.11

5.2.2.2.1. MAC management functions

802.11 also provides MAC management functions like

Synchronization: It is used to find other wireless LANs and generate beacon signals as an invitation to the mobile station to indicate base stations' presence.

Power management: It is used to reduce the power consumption in the mobile station say when the base station has no data to send to the mobile device the mobile device switches itself off.

Roaming: it is used to provide a hand-off mechanism as the user travels from one basic service set (BSS) to another

Management Information database (MIB) the base station stores all the state information of the mobile device.

5.3. HiperLAN

It is a wireless LAN standard developed for high performance of LAN in wireless networks. It operates in 5.15 -5.3 GHz and 17.1 -17.3 GHz. It has a maximum radio range of 50 m providing data rates of 20 Mbps. It allows topology discovery i.e. of other HiperLANs, data encryption and decryption and power saving mechanisms. The architecture of HiperLAN looks as below

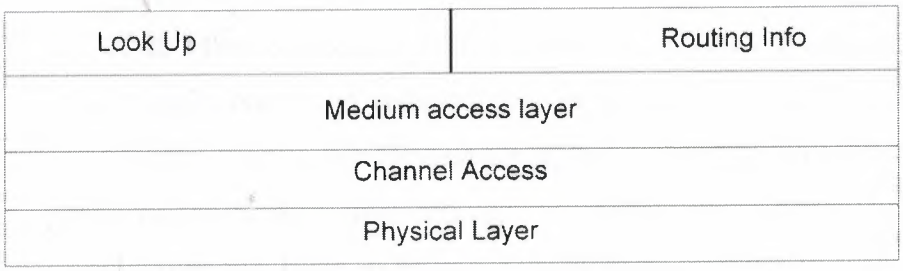


Figure 5.7 HIPERLAN architecture

5.3.1. Physical layer

The physical layer is responsible for the modulation and demodulation of the signal and synchronization between the sender and the receiver. The HiperLAN provides 2 modes of data transfer- low transmission rates and high transmission rates. The low transmission rates are around 1.4 Mbps. The sender and receiver don't have to be tightly synchronized in this case and a simple frequency shift keying is used. In high transmission rate we have speeds of 20 Mbps. The sender and the receiver have to be tightly synchronized in this case. In this only data packets are sent and no acknowledgement packets are received. For high bit data transfer minimum phase shift keying (MPSK) is used.

5.3.2. Medium Access

The Channel access sublayer is responsible for medium access. In HiperLAN a scheme called the elimination yield non-preemptive priority multiple access (EY-NPMA) is used which is explained as below. The medium access is subdivided into 4 phases:

• Prioritization: In this phase the node that has the highest priority is selected to access the medium. It might so happen that many nodes may have the highest priority, in that case all the nodes remain selected at the end of this phase.

• Contention: In this phase the nodes that remain after prioritization send a channel elimination burst .If a node senses the channel idle during elimination survival verification period then the node survives the contention phase .All the other nodes

yield to this node.

• Transmission: In this phase the node selected in contention phase transfers with a high transmission rate of 20 Mbps or low transmission rate of 1.5 Mbps. At the end of the three phases above only one node remains that involves in a data transfer. The medium access sublayer is responsible for data encryption and decryption, power saving and priority class transfer of data units. Encryption of the data is done using a key generated with an initial identifier to give a pseudo random number. This is then XORed with the user data to give encrypted data. Power saving is done using nodes called p-supporters that are responsible for a particular set of nodes called the p-savers that go to sleep. The p-supporters buffer the data destined to p-savers under it. Also a p-supporter tells its p-savers the time duration it has to go to sleep. This sublayer provides priority class traffic using a policy explained below. First, a data unit with highest priority is selected, if many such data units with high priority exist, one with smallest residual time is selected (time-bound packet).Thus the decision is made on the priority and then on residual times to break ties.

• The look up and routing layer provides topology information and routing functions. This layer maintains different types of information bases:

1) Route Information base (RIB): It maintains information about the routes (hops) to destinations.

2) Neighbor information base (NIB): It maintains information about a node's neighbors and the fact whether it shares a symmetric link with it.

3) Hello information base (HIB): It maintains neighbors who are forwarders and non-forwarders (can act as routers).

4) Topology information base (TIB): This maintains information about the entire topology of the network.

Duplicate detection information base (DDIB): In some cases the route to the destination is not known, in that case it is best to broadcast the packet. The duplicates of a packet that reach a node have to be discarded. So DDIB maintains duplicate information.

5.4. Bluetooth

Bluetooth is a technology that aims at providing cheap and reliable adhoc personal networking for short ranges. Bluetooth operates in the 2.4 GHz free license band. Bluetooth provides data rates like 115 Kbps. Some of the scenarios where Bluetooth is used are:

- The peripheral devices like mouse, headsets, speakers of a computer can be connected using bluetooth so that the users don't have to be hindered by wires
- Adhoc networking for PDAs and other devices.
- Home networking where the data from the PDA is synchronized with the desktop computer.

All the bluetooth devices form something known as a piconet as shown below. A typical piconet can have 1 master device and upto 7 slave devices.

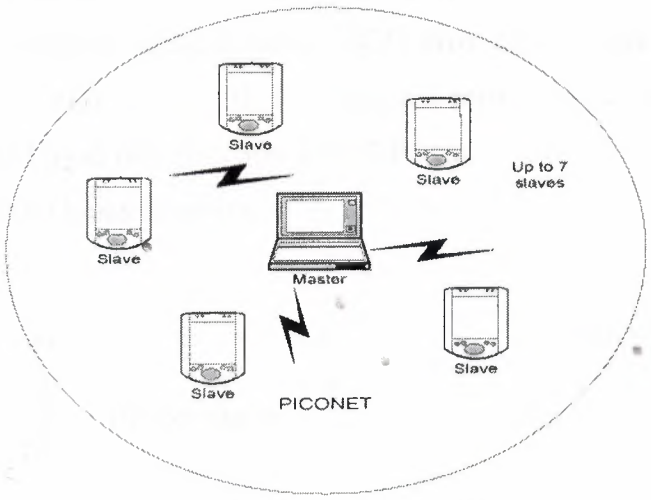


Figure 5.8 PICONET

5.4.1. Bluetooth Architecture Layers

5.4.1.1. Physical layer

Bluetooth devices operate with transmission range of 10 m to 100 m and power levels of 100 mW. It uses a frequency hopping scheme for transmission. Bluetooth devices go into 3 different power saving modes:

- Park State. In this state the device releases its MAC address. It listens to page message when it again wants to synchronize with the piconet.
- Hold State: In this state the device does not release its MAC address and the device goes to sleep for a time called the hold time and wakes up to synchronize with the piconet.
- Sniff State: In this state the device listens to the piconet at a reduced rate and hence the power consumption is not as low as the previous 2 modes.

5.4.1.2. MAC Layer:

Bluetooth offers two different types of services -Synchronous connection-oriented (SCO) link where a two-way point to point link between the sender and the receiver is established and asynchronous connectionless link (ACL) where master uses a polling scheme to transfer data to slave. SCO provides 60kbps voice data traffic between the master and slave with 1/3 forward error correction(FEC) and ACL provides upto 700 kbps in one direction and 57.6 kbps in other direction

A packet in Bluetooth looks as below

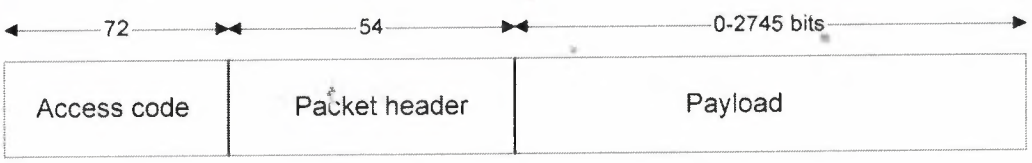


Figure 5.9 Packet Format in Bluetooth

Bluetooth uses one-third rate FEC. So, actually the packet header is only 18 bits, but with the error correction the header size comes to 54 bits.

5.4.2. Networking in Bluetooth

A piconet can be formed by upto 8 active Bluetooth devices. Each of the Bluetooth devices initially send an inquiry message to other devices. One of them becomes a master while the other become slaves. All the devices in a piconet share time and frequencies when sending data to each other. Two or more piconets can come together to form a scatternet. By doing so more devices share the same bandwidth however they may be more collisions (same collision domain). A device that wants to participate in say 2 piconets in a scatternet has to synchronize with the hopping sequence (essentially frequency) of that piconet. If a master of one piconet joins other piconet, all traffic in the master's piconet is suspended. If a slave of one piconet joins other piconet, it informs its master that it won't be available for some period of time.

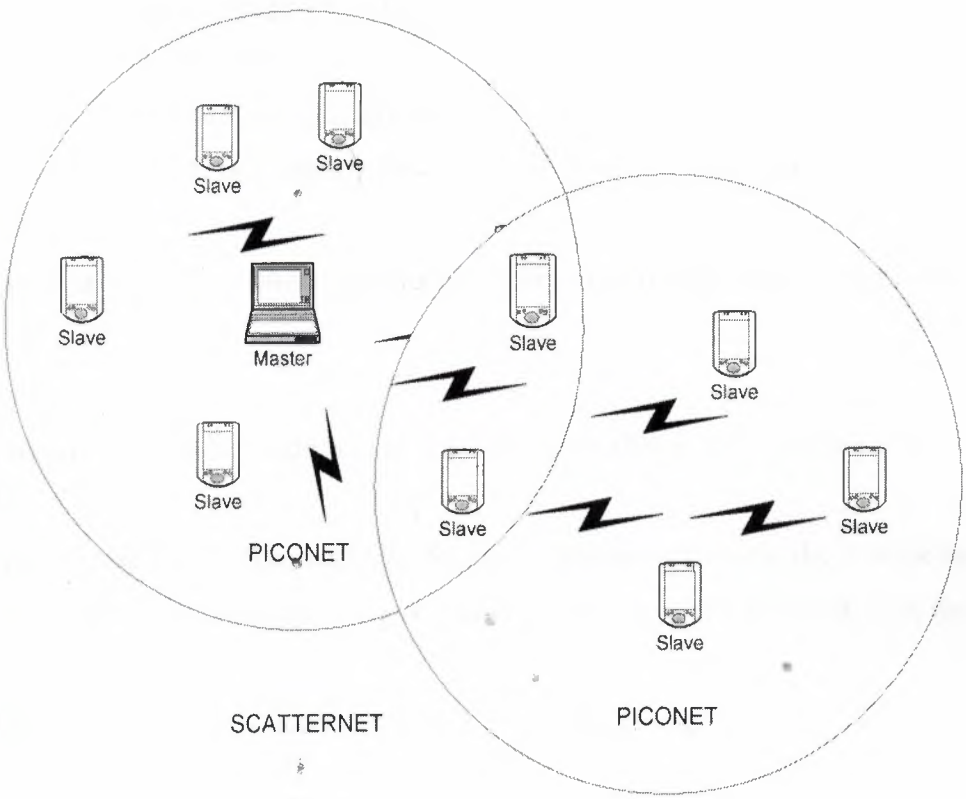


Figure 5.10 Scatternet in Bluetooth

6. Network Layer

6.1. Overview

Mobile networking has become one of the biggest needs in wireless networks. As the mobile hosts are on a constant move there is need to develop a routing protocol that works well under conditions of dynamic change in connectivity because of mobility. This involves developing a support for mobility in network layer protocol, namely internet protocol (IP).

6.2. Mobile IP

Mobile IP is the extension to the internet protocol (IP) developed by the Internet Engineering Task Force (IETF) working group. In brief, the mobile hosts continue to receive messages from other mobile hosts or stationary hosts as long as they plug themselves to the internet.

The following are the terms and entities used in mobile IP

Mobile node (MN). It is a mobile device that moves in the network from one location to

another. When a mobile node changes a location it may choose to keep or change its

IP address.

Home agent (HA) Home agent is a host or router that is responsible for the mobile

host in the sense that it maintains the location information about the mobile host.

Foreign agent (FA) Foreign agent is a host or router in the network that the mobile

node has moved to and is currently in that network (foreign).

6.2.1. The three steps of mobile IP

6.2.1.1. Agent discovery.

When a mobile node moves from its home network where its home agent is present to a new network, mobile node (MN) has to find its new agent by capturing the beacon or advertisement messages sent by the foreign agent. The advertisement

messages are sent by the foreign agent periodically. When the advertisement messages are received by the mobile node it receives a care of address (COA) message which is in most cases the IP address of the foreign agent. In another variant the mobile node can acquire a COA dynamically using a scheme like dynamic host configuration protocol (DHCP).

6.2.1.2. Registration

When the mobile node has received a COA it has to inform its home agent (HA) of its current location. This is necessary because the mobile agent actually belongs to the home network and at that instance of time has moved to a foreign network. The home agent is responsible for the current location of the mobile host. The mobile host sends the registration message to its home agent through the foreign agent. The foreign agent after receiving this registration message creates a mobility binding in it database mapping the mobile node's (MN) IP address with the COA address. However in a case where the MN comes back to its home network after roaming the registration request is send to HA directly. This can be summarized in the picture below.

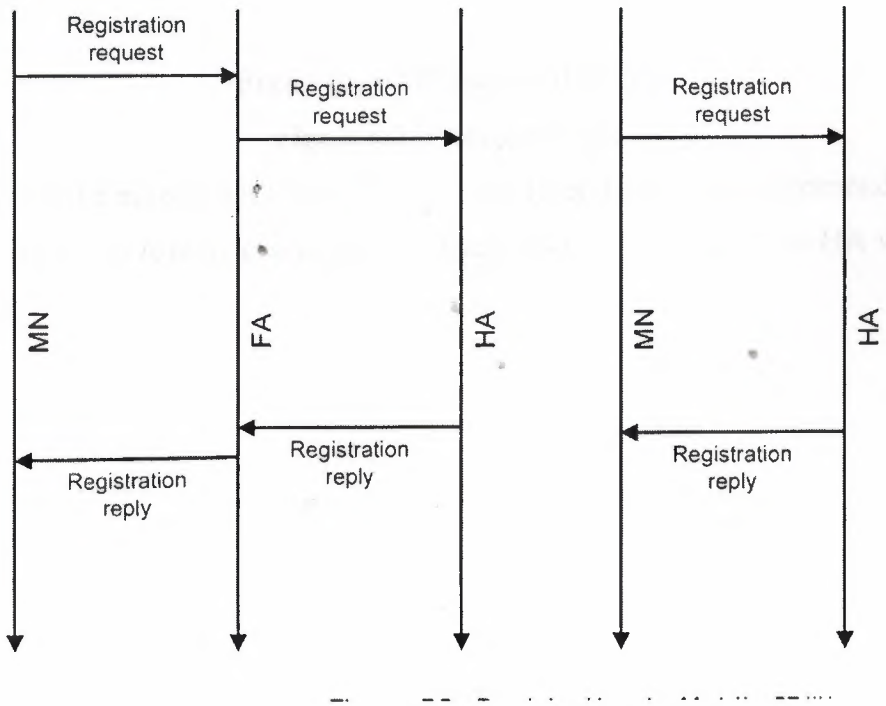
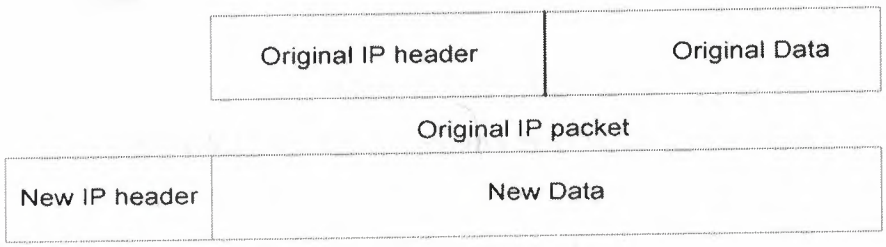


Figure 6.1 Registration in Mobil IP

6.2.1.3. Tunneling and encapsulation

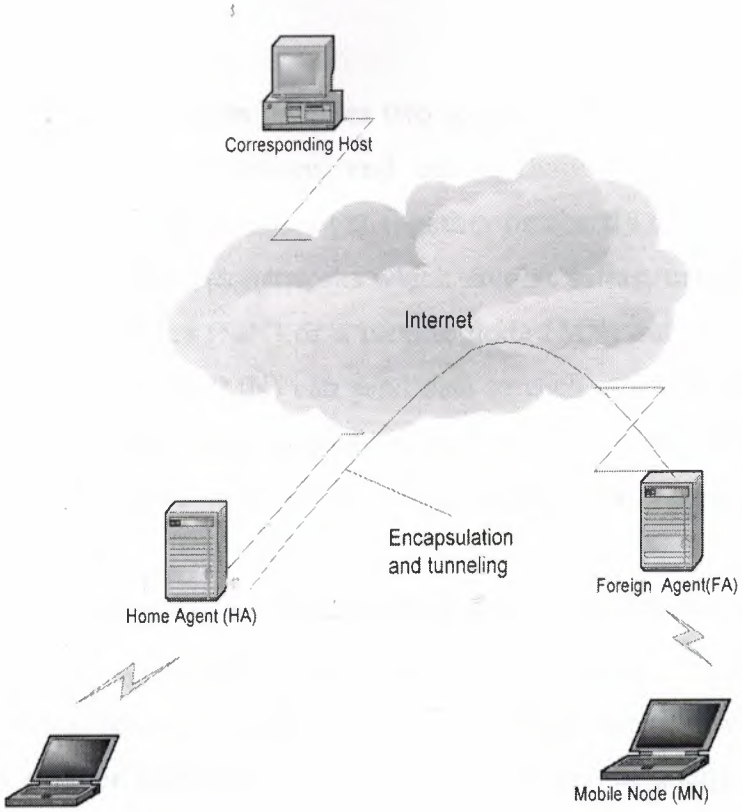
When a corresponding host in the network which is not mobile needs to send data to a mobile host (MN), the datagrams sent reach the home agent which has the responsibility of delivering this packet to the mobile node (MN).Since the MN is not in the home network and is in a foreign network, the home agent encapsulates the packet with a new header and destines the received packet from corresponding host to the foreign agent. The home agent knows the care of address (COA) of the mobile node as it has registered its new location at the home agent. The foreign agent when receives the packet strips the header of the packet and delivers it to the mobile node(MN) which is in its network.Since the IP packet here is encapsulated to create another IP packet ,this process is called "IP-in-IP encapsulation". The path from the home agent to the foreign agent is a tunnel through which the packet goes though intact.



Encapsulated IP packet (IP in IP)

Figure 6.2 IP encapsulation

When the mobile node (MN) wants to deliver data to the corresponding node (CN) the packet is routed as a normal IP packet where the FA or the HA will act as a router.



Mobile Node (MN)

Figure 6.3 Data Transfer from CH to MN in FA domain

6.2.2. The characteristics of the mobile IP protocol

- The mobile IP systems should be able to work with the systems that don't implement mobile IP. Mobile IP is a protocol that modifies only the IP layer and not the lower layers like the medium access control (MAC) or logical link control (LLC) and the higher layers like TCP.
- The messages in mobile IP that include the location of a mobile node have to be authenticated by the requestor to prevent remote attacks.
- The number of administrative messages regarding the host mobility and location is minimized as far as possible.
- Mobile IP places no limitations on the IP address assignment to the mobile hosts.

6.3. Routing

Routing in wireless networks involves two scenarios- one where there is support for infrastructure with base stations and one without infrastructure called adhoc networks where a group of nodes get together on the fly to exchange information or data. Routing in wireless networks which involve infrastructure can use mobile IP where two mobile nodes (MN) or a mobile node (MN) and a corresponding node (CN) and a mobile node (MN) can send data to each other though the intermediate wired network. However in a situation without infrastructure we need to use routing capabilities of the mobile nodes (MN) to relay packets across them.

6.3.1. differences between wired and adhoc scenarios with respect to routing

- Adhoc networks can have asymmetric links. When an adhoc node A receives data from another adhoc node B nothing can be told about the link from A to B. So the routing information collected in one direction may not be adequate for the links in the other direction.
- Adhoc networks have a lot of interference since the medium is broadcast. When a node A wants to send data to another node B that is many hops away, A's transmission can be heard by other nodes. Such nodes that hear this transmission are called promiscuous nodes. They may infact help in routing or interfere with A's transmission.
- The links are always changing; links may come up and down because of the mobility of the nodes. So the routing information collected may go stale before the route is used. The following 2 describe the most common algorithms used in adhoc networks.

6.3.2. the most common algorithms used in adhoc networks.

6.3.2.1. Dynamic source routing (DSR)

When a node has to send data to a destination it broadcasts a route request (RREQ) packet. Each node on receiving such a packet broadcasts the RREP packet to its neighbors. The route request (RREQ) packet may reach many nodes in an adhoc network before it finally reaches the destination. The destination looks into the packet and identifies the packet for itself and stops the broadcast. When the packet

traverses the network it collects the route that it has traversed. The destination reverses the route and sends the route reply (RREP) back to the source. The source may receive many such RREP packets and chooses the RREP packet which has the least hop count or based on some other metric and sends data on that path that is present in the chosen RREP. The destination on receiving the data then sends back the acknowledgement back to the sender/source. Since the routing of the packet is done using a source route the term "source routing" is used. One of the optimizations of dynamic source routing is that the intermediate nodes in the path from the source to the destination can cache the route and the RREP of a route to the destination can be send back to the sender immediately reducing the discovery time of the route. The disadvantages of DSR are that the source routes may make the packet very large. Also the links are assumed to be bidirectional if not the RREP packet sent by the destination may not reach back the source.

6.3.2.2. Hierarchical algorithm

The DSR described above is not a very scalable algorithm. In a case where the source and destination are many hops away the route discovery may take a long time. In such a case a hierarchical algorithm is used. The nodes are grouped in a cluster. Each cluster has a cluster head that is responsible for the topology information of the cluster. When the cluster changes only the nodes in the cluster are informed about the topology changes, the other nodes need not know the node movement in this cluster but rather to only reach this cluster. Thus the update information that needs to be broadcasted on a topology change is reduced. The clusters can further be grouped into super-clusters, regions and so on until we run out of names for aggregation!

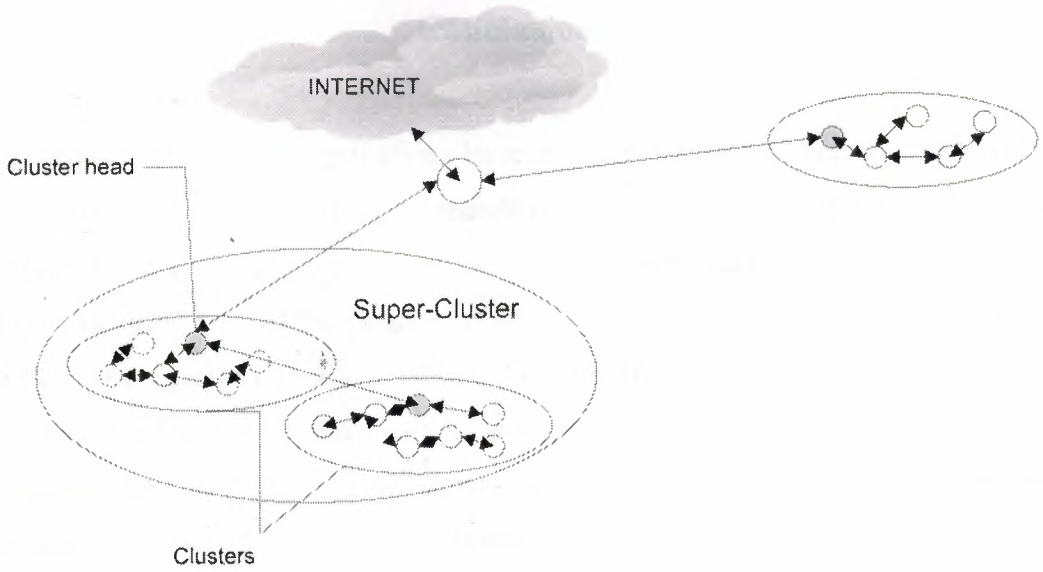


Figure 6.4 Hierarchical routing in wireless networks

Conclusions

Wireless and mobile communications have still not reached its zenith. There is lot a lot of scope for development and research in this area. The next generation will see a plethora for wireless applications rolled out in the time frame of 2000 -2010. For all we know the paradigm of the future may be wireless devices assisting the human user to access the internet in an unobtrusive and ubiquitous way more than ever. The concept of being unrestrictive is something that the people would cheerfully embrace. Technologies like CDMA have been on the forefront to provide substantial data rates. Wireless LANs have substituted the wired LANs in buildings and avoiding the drudgery of cabling in the buildings.

However wireless and mobile communications have its limitations. The transmission rates are lesser compared to wired networks. The medium is also inherently error prone and insecure. One must have to take special measures to overcome these glitches.

Despite its limitations, wireless and mobile communications have an attractive future. Its advantages far out-weigh it disadvantages. This is probably one of the reasons why development in this area has been resolutely encouraged by the companies and research institutions. Though this area may this may not successful in usurping the wired systems, it surely is jockeying for dominance.

REFERENCES

[1] Mamedov F. S., Control System Engineering, Lecture notes, Near East University Press, Lefkoşa, 1999.

[2] Hicks, Cheshunt, " History of Wireless ", *Asbury Field Home page* <http://www.albury-field.demon.co.uk/hisrad9.htm>, 1998.

[3] Jochen Schiller, "Mobile communications ", Addison-Wesley 1998.

[4] Anish Shah, "Wireless Communications - History" , *RPI Website,* <http://www.rpi.edu/~shaha/honsem/history.htm >, 2000.

[5] Ira Brodsky," Debunking the Myth of Europe's Wireless Supremacy", *Network World Fusion Website,* <http://www.nwfusion.com/columnists/2000/0117brodsky.html>, 1999.

[6] John P. Burnham ," The Essential Guide to the Business of US Mobile and Wireless Communications",2000.

[7] "How the Wireless Industry Is Structured", *Wow Website,* <http://www.wow-com.com/consumer/howitworks/articles.cfmPID-69> ,2001.

[8] "Cellular Telephone", *University of Oklahoma Website,* <http://coecs.ou.edu/vdebrunn/www/wireless/cellular.pdf>, 1998.

[9] Specialized Mobile Radio Service", *FCC Website,* <http://wireless.fcc.gov/smrs/>, 2001.

[10] Bob Weber," selected papers", *Kellogg faculty Website,* <http://www.kellogg.nwu.edu/faculty/weber/PAPERS/pcs auc.htm>, 1997.

[11] "Wireless Spectrum for dummies", *Business 2.0 Website,* <http://www.business2.com/docs/CheatsheetB12.pdfK, 2000.

[12] "700 MHz Band: Fact Sheet and Releases", *FCC Website,* <http://wireless.fcc.gov/auctions/31/K, 2001.

[13] "3G news Feb 2001", *3GNewsroom Website,* <http://www.3gnewsroom.com/3g news/feb 01/news O252.shtml>,2001.

[14] " The World Radiocommunication Conference (WRC 2000) Istanbul, Turkey" *GSMworld Website,* <http://www.gsmworld.com/news/articles/wrc2k 3.html>, 2001.

[15] "Code Division Multiplexing: Draft", *Transcend Website,* <http://www.transend.com.tw/~cryptext/CDM.htmlK>,1998.

[16] Randy Katz ,"CS:294-7 Digital Modulation", *Personal Website,* <http://www.sss-mag.com/pdf/lmodulation.pdf>,1996.

[17] "Phase Shift Keying", *TechTarget Website,* <http://whatis.techtarget.com/definition/0,,sid9 gci213937,00.html>,2000.

[18] Jim Geier, "Spread Spectrum Techniques" , *Wireless-Nets Website* , <http://www.wireless-nets.com/whitepaper spread.htm >,1999.

[19] Jeff Tyson, "Wireless Networking" ,*how-stuff-works Website,* <http: //www. howstuffworks.com/wi re'ess-networkl. htm > ,1998.

[20] Nigel Davies, "CS 630-01 :Special Topics in Mobile and Ubiquitous computing", *University of Arizona Website* , < http://www.cs.arizona.edu/classpage/cs630-l/lecture3.PDF> ,2001.

[21] "Smartant", *Mobile Choice Website* <http://www.mobilechoice.co.kr/leftwork/leftl2e.htm>,Circa1999.

[22] Rajesh Gupta, "Design Technology for Building Wireless Systems", *UC Irvine Website,* < http://wwwl.ics.uci.edu/~rgupta/iccad97/partl.pdf>, 1997.

[23] Randy Katz, "Media Access :Aloha and CSMA",t/C *Berkeley Website,*<http://www.sss-mag.com/pdf/1 mediaaccess.pdf> ,1996.

[24] Jos Nijhof /'Mobile Communications", *Delft University of Technology Website,* <http://wwwtvs.et.tudelft.nl/EDUCAT/COURSES/ET4-153/SHEETS/mc 03b.PDF>, 2000.

[25] Robert Xu, "Introduction to CDMA technology", *UT Dallas Website,* <http://www.utdallas.edu/~xu8589/cs6390/intro.html>, 1998.

[26] "Qualcomm CDMA technologies :Advantages of CDMA", *Qualcomm Website,* <http://www.cdmatech.com/about cdma/faq/cdma adv.html>,2001.

[27] Brian. P. Crow, Indra Widjaja, Jeung G. Kim, Prescott T. Sakai," IEEE 802.11 Wireless Local Area Networks", <http://ieeexplore.ieee.org/iell/35/13503/00620533.pdf>, ri1997.

[28] Victor Bahl," Future Directions - HIPERLAN, Wireless ATM, and FPLMTS", *MicrosoftCorporation,* <http://research.microsoft.com/~bahl/present/ms wireless98.pdf>, 1998.

[29] Karen," Medium Access Control Sublayer", *University of Toronto Website,* <http://www.comm.toronto.edu/~karen/projects/24.HiPerLANl/main/mac.htm>, 2000

[30] Dennis Sweeny and Max Robert, "Bluetooth Tutorial", *Virginia Tech Website,* <http://www.mprg.ee.vt.edu/tech xfer/ppt/bt tut.pdf>, 2000.

[31] Goal Labs, " Bluetooth" *personal Website,* <http://www.boing.org/~alokem/bt/>, 2000.

[32] Charles E. Perkins ," Mobile IP: Design, Principles and Practices", Addison Wesley,1998.

[33] David B. Johnson and David A. Maltz, " Dynamic Source Routing in Ad Hoc Wireless Networks". *In Mobile Computing* ,1996.

[34] Suman Banerjee, Samir Khuller ,"A Clustering Scheme for Hierarchical Control in Wireless Networks", *University of Maryland at College Park, INFOCOM 2001,* <http://citeseer.nj.nec.eom/cache/papers/cs/17918/http:zSzzSzwww.cs.umd.eduz Sz~samirzSzgrantzSzbk01.pdf/a-clustering-scheme-for. pdf > ,2001.