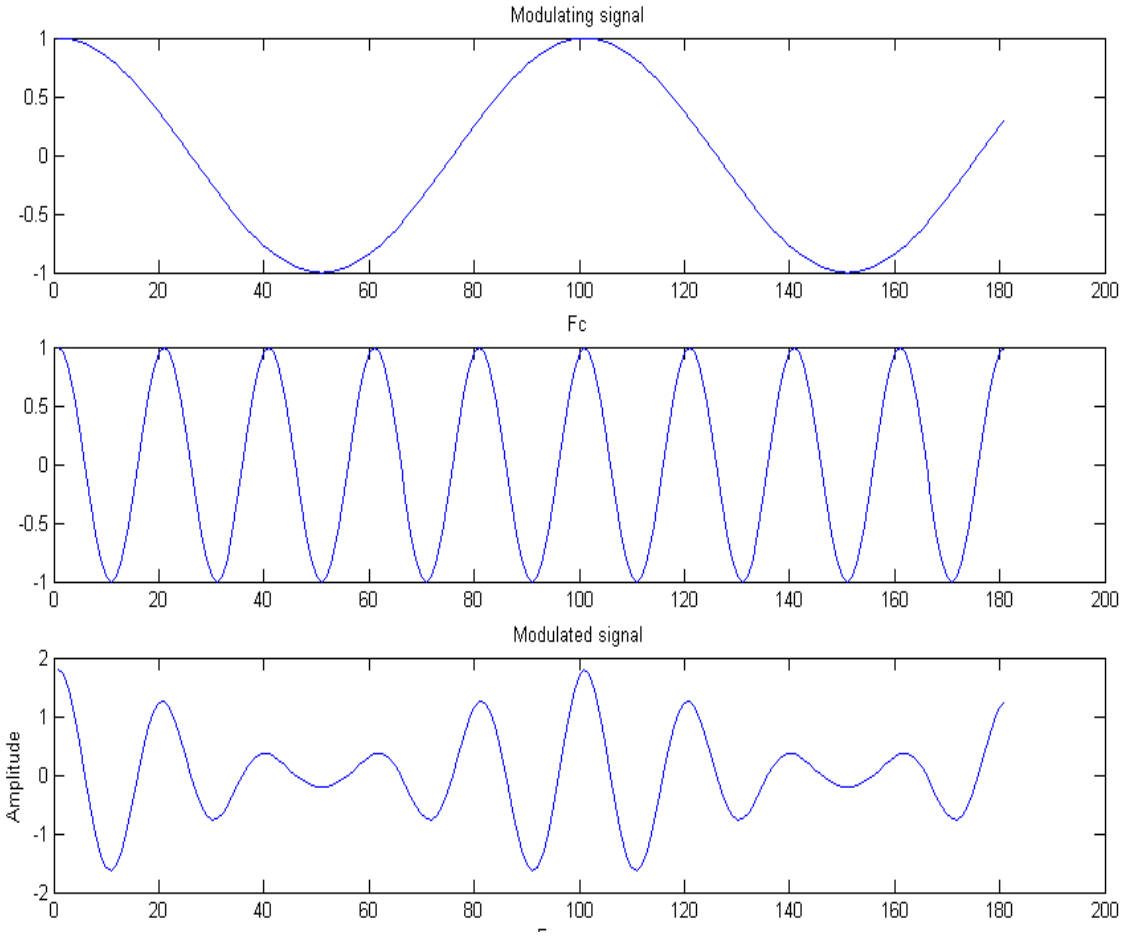
Prac.1	Plot S(t) in MATLAB ,if Fc = 50Khz,Fm = 10Khz, S(t) = [1 + Ma *cos(2*pi*Fm*t)]*cos(2*pi*Fc*t)

```
clc;
fm=input('enter modulated freq= ');
fc=input('enter carrier freq= ');
ma=0.8;
t=0:0.000001:0.00018;
for j=1:length(t)
   m(j)= cos(2*pi*fm*t(j));
   c(j)= cos(2*pi*fc*t(j));
   s(j)=[1+(ma*(cos(2*pi*fm*t(j))))]*cos(2*pi*fc*t(j));
end
subplot(3,1,1);
plot(m);
title('Modulating signal');
subplot(3,1,2);
plot(c);
title('Fc');
subplot(3,1,3);
plot(s);
title('Modulated signal');
xlabel('Frequency');
ylabel('Amplitude');
```

Simulation Result:

enter modulated freq= 10000

enter carrier freq= 50000



Prac.2	Analyze Gaussian and Raleigh Distribution

Gaussian Distribution:

The Impulse response of the Gaussian filter gives rise to a transfer function that is highly dependent upon 3-db bandwidth. The Gaussian Low Pass Filter has a transfer Function Given by

$$H_G(f) = \exp(-\alpha^2 f^2)$$

Rayleigh Distribution:

The Rayleigh distribution is a special case of the Weibull distribution. If A and B are the parameters of the Weibull distribution, then the Rayleigh distribution with parameter is equivalent to the Weibull distribution with parameters and . If the component velocities of a particle in the x and y directions are two independent normal random variables with zero means and equal variances, then the distance the particle travels per unit time is distributed Rayleigh. The Rayleigh pdf is

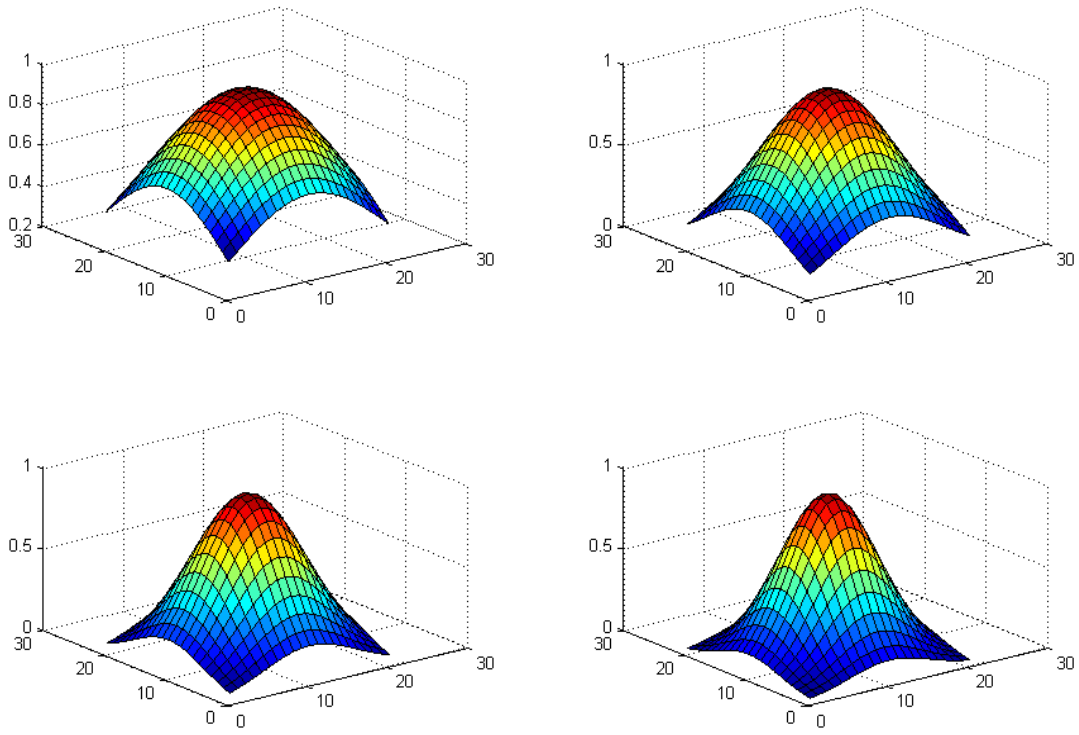
$$y = f(x|b) = \frac{x}{b^2} e^{\left(\frac{-x^2}{2b^2}\right)}$$

A] Gaussian Distribution:

```
x=-1:0.1:1;
y=-1:0.1:1;
a=0.5:0.5:2; % Value of  α increase
for k=1:length(x)
  for i=1:length(x)
    for j=1:length(y)
      z(i,j)=exp(-a(k)*(x(i)*x(i)+y(j)*y(j)));
  end
end
subplot(2,2,k);
surf(z);
```

end

Simulation Result:



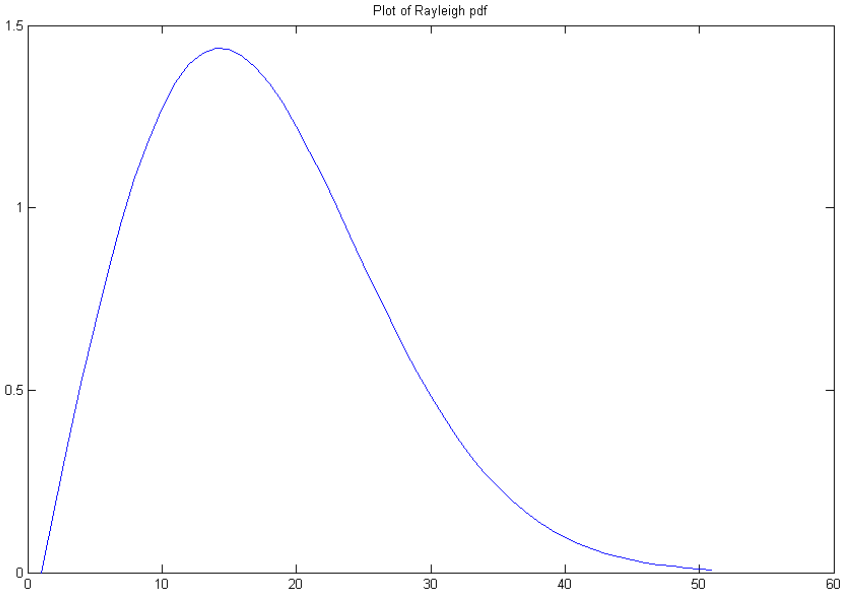
Conclusion:

As α increase , the Spectral occupancy of the Gaussian filter decrease and time dispersion of the applied signal increase.

B] Rayleigh Distribution:

```
clc;
clear all;
r=0:0.1:5;
x = 0.75;
for i=1:length(r)
      p(i)=(r(i)/x^2 )*(exp(-((r(i)*r(i))/2*x*x)));
end
plot(p);
title('Plot of Rayleigh pdf');
```

Simulation Result:



Prac.3	Analyze Shannon's channel capacity Theorem and Bandwidth Efficiency

In 1948, Shanon Demonstrated that by Proper Encoding of the Information, error induced by Noisy Channel can be reduced to any desired level without sacrificing the rate of information transfer. Shannon's Channel capacity Formula is applicable to the AWGN channel and is given by

$$C=B*\log2(1+(P/No*B))$$

Where:

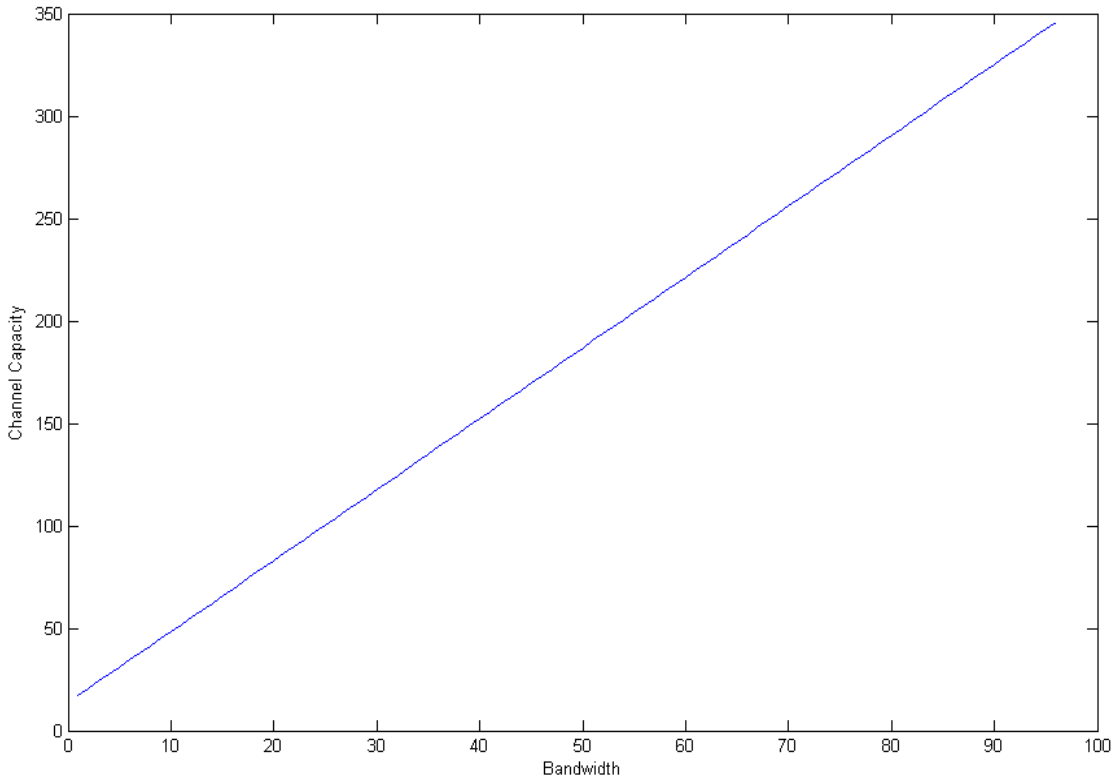
SNR=P/(No*B)

BW Efficiency=C/B=log2(1+SNR)

Code:

```
clc;
s=10;
b=5:100;
for j=1:length(b)
   c(j)=b(j)*log2(1+s);
end
plot(c);
xlabel('Bandwidth');
ylabel('Channel Capacity');
```

Simulation Result:



Conclusion:

Introduction of redundancies bit increases the bandwidth requirement for a fixed source data rate. This reduces the bandwidth efficiency of the link in High SNR condition, but provides excellent BER Performance at low SNR Values

Prac.4	To Study the Effect of AWGN for the sinusoidal signal

Syntax

y = awgn(x, snr)

Description

Adds white Gaussian noise to the vector signal x. The scalar snr specifies the signal-to-noise ratio per sample, in dB. If x is complex, then awgn adds complex noise. This syntax

assumes that the power of x is 0 dBW.

Syntax

y = awgn(x, snr, 'measured')

Description

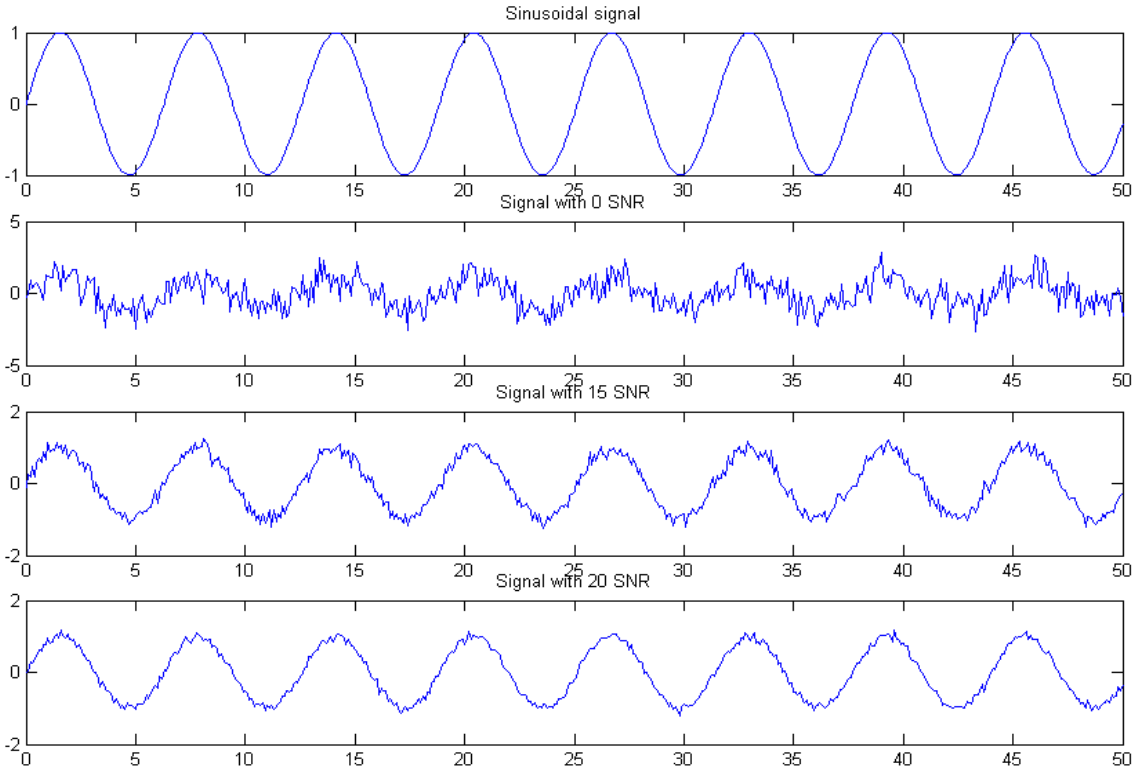
This is the same as y = awgn(x, snr), except that awgn measures the power of x before adding noise.

Code:

```
clc;
close all;
clear all;
t = 0:.1:50;
x = sin(t);
subplot(4,1,1);
plot(t,x);
title('Sinusoidal signal');
a = awgn(x,0,'measured')
subplot(4,1,2);
plot(t,a);
title('Signal with 0 SNR');
c = awgn(x,15,'measured');
subplot(4,1,3);
```

```
plot(t,c);
title('Signal with 15 SNR');

d = awgn(x,20,'measured');
subplot(4,1,4);
plot(t,d);
title('Signal with 20 SNR');
```

Simulation Result:



Conclusion: As the Signal to Noise Ratio increases the effect of Noise reduces.

Prac.5	Estimate Path Loss using Okumura Hata model for a Medium size city using Givan Data .

Given Data:

F = 900 MHz to 1800MHz

Distance = 1 to 30 Km.

Measurement based Propagation Model indicate that average received signal Power decreases logarithmically with distance. The average large-scale path loss for an arbitrary T R separation is expressed as a function of distance by using a path loss Exponent,n

$$PL(dB) = PL(d_0) + 10n\log(d/d_0)$$

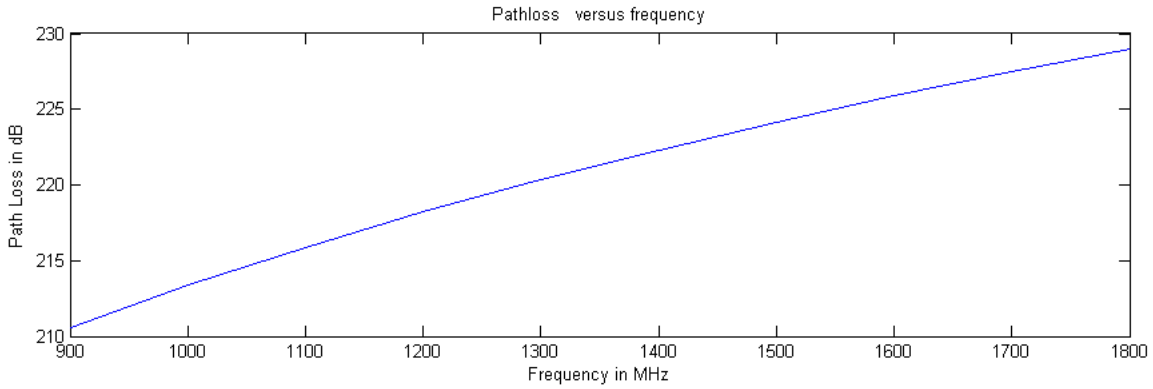
Code:

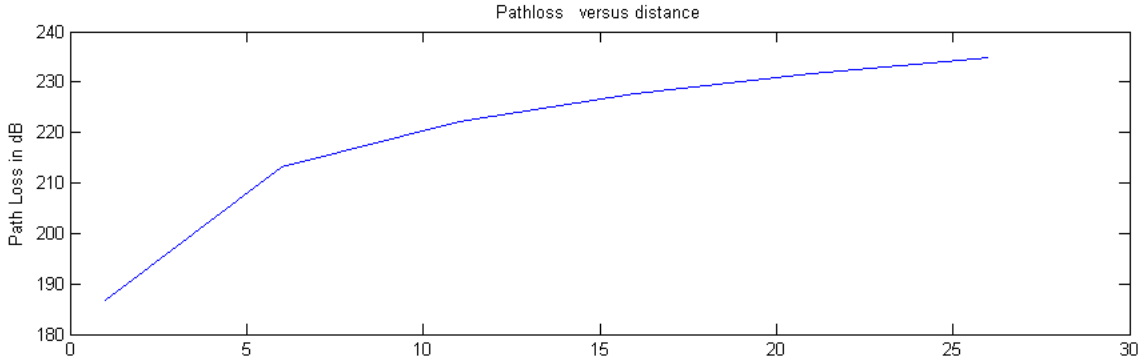
```
clc;
clear all;

d=5;                % distance in Km
ht = 100            % height of transmitting antenna in m
hr = 1              % height of receiving antenna in m

% part (a) for given value of d , f is varied from 900 MHz to 1800 Mhz
f=900:100:1800;
Ahr= (1.1*log(f) -0.7)*hr -(1.56*log(f) -0.8);%  Equation of path loss  using Hata Okumura model
PL =69.55 +26.16*log(f) -13.83*log(ht)-Ahr +(44.9 -6.55*log(ht))*log(d);
disp(PL)
subplot(2,1,1);
plot(f,PL);
title('Pathloss  versus frequency');
```

```
xlabel('Frequency in MHz')
ylabel('Path Loss in dB')
%part(b)  for given value of f=900 Mhz , d is varied from 1Km to 30K m
d=1:5:30;
f=900;
Ahr= (1.1*log(f) -0.7)*hr -(1.56*log(f) -0.8);
PL =69.55 +26.16*log(f) -13.83*log(ht)-Ahr +(44.9 -6.55*log(ht))*log(d);
disp(PL)
 subplot(2,1,2);
plot(d,PL);
title('Pathloss   versus distance')
xlabel('Distance in Km')
ylabel('Path Loss in dB')
%Part(c)
% Calculate received power  f=900 MHz  ;d=36,000 Km ;Gt= 10 ;Gr= 1;Pt= 100 W
f=900
d=36,000
Gt= 10
Gr= 1
Pt= 100
Ptdb  =10*log(Pt)
lemda = 3* 10^8 /(900*10^6)
Pr= (Ptdb * Gt  *Gr * lemda ^2)/(4*pi^2*d^2)
Disp(Pr)
```

Simulation Result:

Pr = 0.0010





Prac.6	For Multipath Propagation Model, write a MATLAB program for Rayleigh Fading at 900 MHz,1800 MHz and 2700MHz.if Receiver replacement rate is 100Km/hr.Assume suitable

```
Clc;
clear all;
freq = [(900*10^60);(1800*10^60);(2700*10^60)];
vel = 100;
c = (3*10^8);
r = 1;
for x = 1:3
    fm(x) = (vel*freq(x)*1000)/(3600*c);   %Maximum Doppler Shift
    Nr(x) = sqrt(2*pi)*fm(x)*r*exp(-r^2); %Fades per second
    FD(x) = exp(-1)/(r*fm(x)*sqrt(2*pi)); %Fade duration
end;
display(fm);
display(Nr);
display(FD);
```

Simulation Result:

```
fm =
    1.0e+056 *
    0.8333    1.6667    2.5000
Nr =
    1.0e+056 *
    0.7684    1.5369    2.3053
FD =
    1.0e-056 *
    0.1761    0.0881    0.0587
```

Prac.7	TO STUDY GSM TRAINER KIT & AT COMMAND CONCERNING MODEM AND SIM CARD HARDWARE.

A] GSM SYSTEM ARCHITECTURE

GSM Frequencies :

The GSM system is a FDMA/ TDMA system; each physical channel is characterized by a carrier frequency & a time slot number. GSM system frequencies includes two bands at 900 MHz and 1800 MHz commonly referred as GSM-900 and DCS-1800.

For the primary band in GSM-900 system, 124 radio carriers have been defined and assigned in two sub-bands of 25 MHz each in the 890-915 MHz and 935-960 MHz ranges,with channel width of 200 KHz.

The GSM system comprises of mobile station (MS), base transceiver station (BTS), base Station controller (BSC), mobile switching center (MSC) and a set of registers (databases) to assist in mobility management & security functions. All signaling between MSC and various registers as well as between MSCs takes place using Signaling System 7(SS7) network.

Mobile Station (MS) :

GSM mobile station is nothing but your handset or subscriber unit. At the time of manufacturing a handset, an international mobile equipment identity (IMEI) is programmed into the terminal. A subscriber identity module (SIM) is required to activate and operate GSM terminal. The SIM may be a removable unit that can be inserted by the user. Any GSM terminal capable of receiving a detachable SIM card can become the user's MS upon plugging into the SIM card.

Base station system (BSS) :

The base station system comprises a base station controller (BSC) and one or more subtending base transceiver stations (BTS).The BSS is responsible for all functions related to the radio resource management.

Mobile switching center (MSC) :

It's a local ISDN switch with additional capabilities to support mobility management functions like location update, terminal registration, and handoff.

MSC performs the following major functions :

· Call setup, release

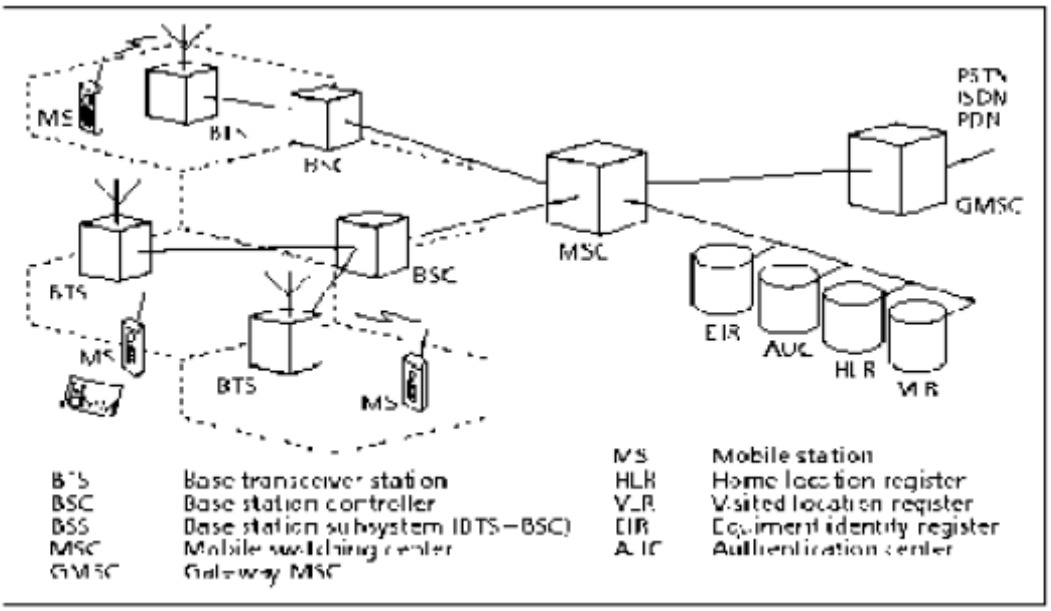
· Call routine

· Billing information

· Paging & altering

· Echo cancellation

· Registration etc.



GSM Network Architecture

Home location register (HLR) :

It is a centralized database that has the permanent data fills about the mobile subscribers in a large service area.

Visiting location register (VLR) :

It represents a temporary data store, and generally there is one VLR per MSC. This register contains information about mobile subscribers who are currently in the service area & which features are activated locally.

Authentication center (AC) :

Generally associated with HLR, contains authentication parameters which are used in initial location registration, location updates etc. It uses authentication & cipher key generation algorithm A3 & A8 respectively.

Equipment identity register (EIR) :

It maintains information to authenticate terminal equipment so that fraud can be identified and denied service.

B] GETTING STARTED

1. GSM antenna and coaxial cable (30cm):

Operating Frequency **:** 900/1800 MHz.

Your modem is actually a low power radio transmitter and receiver. It sends out and receives radio frequency energy. When you use your modem, the cellular system handling your calls controls both the radio frequency and the power level of your cellular modem.

2. RS-232 Serial cable for interfacing to PC.

3. Handsfree kit is all the time connected with serial cable.

4. Adaptor supplied is the only power source for trainer & must be connected when trainer is in use.

5. SIM is must for AT commands related to SIM & making calls.

6. LED continuous on - Modem on but not registered to the network.

LED flashing slowly –Idle mode

LED flashing rapidly – Tx/Rx mode

LED off – Modem off

7. When command **" AT** " is sent to the GSM Trainer ,it every time responses/acknowledges by **"ok" ,**can be use to detect connection.

8. AT+SPEAKER=1, must be the state to use Handsfree kit/ headphones.

9. Use AT&W, to save the present state/status of any command such as speaker, which returns to default each time powered on.

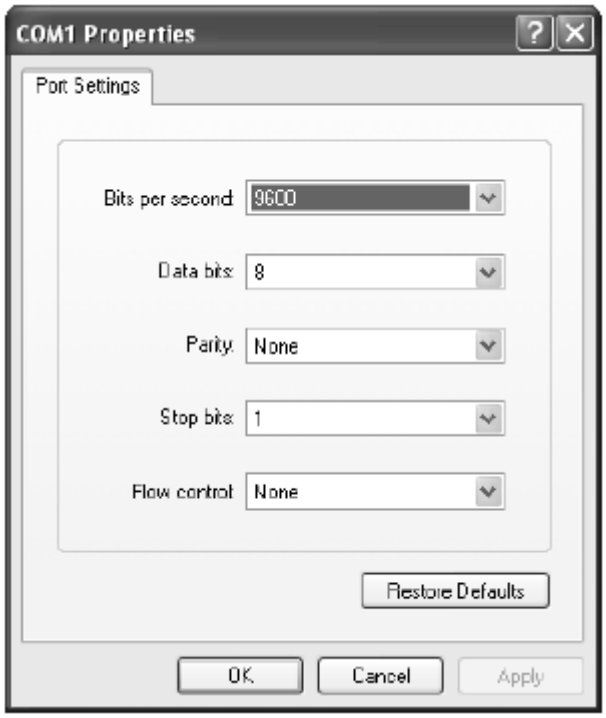
Line settings

How to locate HyperTerminal in windows?

In windows edition, generally it is available in

c:\program files \ accessories \ communication \ Hyper Terminal

A serial link handler is set with the following default values.



Speed 9600 (can be varied)

8 bits data,

No parity,

1 stop bit,

None flow control

Command line

Commands always start with AT (which means AT Attention) and finish with a <CR> character**.**

Information responses and result codes

· If command syntax is incorrect, the “ERROR” string is returned,

· If command syntax is correct but transmitted with wrong parameters, the +CME ERROR: <Err> or +CMS ERROR: <SmsErr> strings is returned with adequate error codes if CMEE was previously set to 1. By default,

CMEE is set to 0, and the error message is only ERROR.

· If the command line has been executed successfully, an OK string is returned.

In some cases, such as “AT+CPIN?” or (unsolicited) incoming events, the Product does not return the OK string as a response

C] AT Commands concerning modem and SIM card hardware

1 AT+CGMI
Command gives manufacturer information.

2 AT+CGMM
Command gives GSM model information.

+CGMM MULTIBAND 900E 1800
+CGMM=? OK

3 AT+CGMR

+CGMR <version number>
+CGMR=? OK

4 AT+CGSN
Command gives IMEI information.
+CGSN <IMEI>
+CGSN=? OK

5 AT+CIMI
Command gives IMSI information.

+CIMI <IMSI>
+CIMI=? OK

Prac.8	**TO STUDY AT COMMAND For Call Control and Call setting.**

1 ATD

ATD<number>

Command is used to establish a voice call.

Command Possible responses

ATD<number>; OK If call is established

BUSY If called party is in another call

NO ANSWER If called party does not accept a call

NO CARRIER If there are problems to establish a call

Defined values:

<number>: Telephone number to dial.

Remarks: In case of international number, the local international prefix (usually 00) could be replaced by the '+' character. For phonebook dialling please see phonebook commands section.

2 ATA

Command is used to accept an incoming call.

Command Possible responses

ATA OK If incoming call is a voice call

CONNECT <speed> If incoming call is a data call

Defined values:

<speed> See ATD command.

Remarks: User should use command only if ATS0 equals zero.

3 ATS0

ATS0?

ATS0=<n>

The S0 parameter controls the automatic answering of an incoming call.

Command Possible responses
ATS0=<n> OK

ATS0? <n>

Defined values:

<n>: Automatic answer after <n> rings. A value of 0

disables automatic answering.

4 ATH

Command is used to end a call.

Command Possible responses

ATH OK ERROR

Prac.9	Study of Direct Sequence Spread Spectrum Modulation and Demodulation Process.

Equipments Needed:

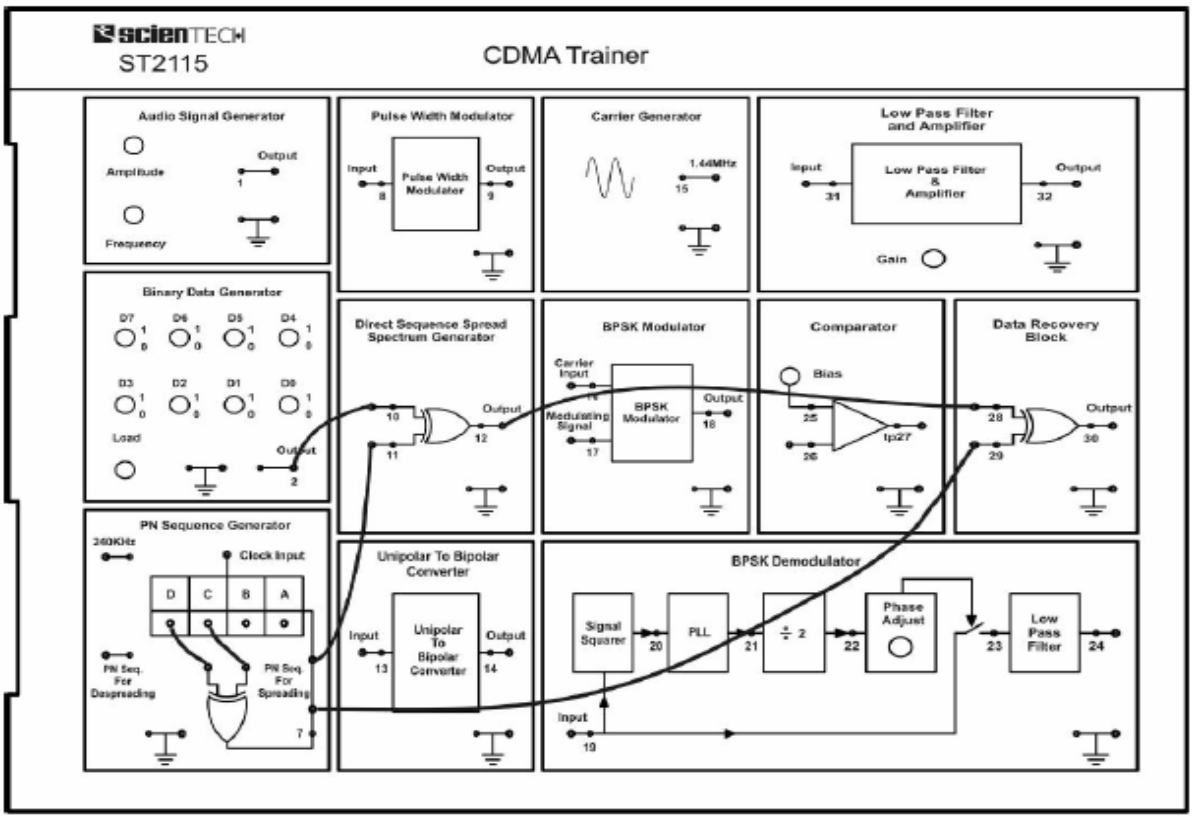
1. ST2115, CDMA Trainer Board,

2. CRO

3. Patch Cords, etc.

Experimental Setup :

Refer to the following diagram to configure experimental setup for the present experiment:



Procedure:

1. Switch data switches to 1 or 0 as per your choice of binary data pattern.

2. Connect any two of the four taps viz. A, B, C or D to the inputs of EX-OR gate of PN Sequence generator. Connect 240 KHz clock signal on board to the clock input of the PN sequence generator.

3. Now switch 'On' the power supply and observe the output of Binary Data generator and PN sequence generator. Since the data generator frequency used here is 30 KHz and that of PN Sequence Generator is 240 KHz, and hence there are 8 PN sequence bits per Data bits for spreading the binary signal.

4. Change the positions of taps for feedback in the PN Sequence Generator block to obtain deferent patterns of the PN sequences. Switch 'Off' and then 'On' the power supply to reload the changes, if changes do not appear in the output on changing the tap positions.

5. Connect output of binary data generator to one of the inputs of Direct sequence spread spectrum generator input.

6. Connect output of PN sequence generator to the other input of DSSS Ex-OR gate.

7. Now turn 'On' power supply and observe the output of DSSS generator block. This is our DSSS signal.

8. Now connect output of this DSSS bock to the one of the input of Ex-OR gate of Data Recovery block. Connect the same output of PN sequence generator, which we have taken for spreading to the other input of this recovery gate for dispreading. Note that the PN sequence used for dispreading is taken from the same output pin where from the PN sequence is taken for spreading the signal. This is because of the fact that there is complete synchronization between the spreaded signal and PN sequence. In other words there is not any significant delay involved in spreading process.

9. Observe the output of this data recovery block. This is recovered output without almost any error.

10. Now change the tape positions of shift registers (A, B, C or D) to get a new PN Sequence and repeat the above process again. Thus you will observe that with each different sequence we are quit able to recover the original data. Also with different PN sequences, the modulated (Spreaded) data looks different

i.e. we can recover the data if and only if we are using the same PN sequence for both modulation and demodulation. This is the reason that this DSSS technique has a large

potential for being a multiple access technique. This multiple access technique is known as “Code Division Multiple Access”

Observation :

We can observe that same bit Pattern received ,that was transmitted without any Phase difference.

Prac.10	To Study of Wi-Fi Networks.

The term Wi-Fi suggests Wireless Fidelity. Wi-Fi is a term for certain types of wireless local area network (WLAN) that use specifications in the 802.11 family. The term Wi-Fi was created by an organization called the Wi-Fi Alliance, which oversees tests that certify product interoperability. Wi-Fi uses both single carrier direct-sequence spread spectrum radio technology (part of the larger family of spread spectrum systems) and multi-carrier OFDM (Orthogonal Frequency Division Multiplexing) radio technology.

Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks. These locations are known as hot spots. An interconnected area of hot spots and network access points is known as a hot zone.

Uses:

A Wi-Fi enabled device such as a PC, game console, mobile phone, MP3 player or PDA can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more interconnected access points — called a hotspot — can comprise an area as small as a single room with wireless-opaque walls or as large as many square miles covered by overlapping access points. Wi-Fi technology has served to set up mesh networks, for example, in London. Both architectures can operate in community networks.

A Wi-Fi antenna

A roof mounted Wi-Fi antenna

In addition to restricted use in homes and offices, Wi-Fi can make access publicly available at Wi-Fi hotspots provided either free of charge or to subscribers to various providers. Organizations and businesses such as airports, hotels and restaurants often provide free hotspots to attract or assist clients. Enthusiasts or authorities who wish to provide services or even to promote business in a given area sometimes provide free Wi-Fi access. There are already more than 300 metropolitan-wide Wi-Fi (Muni-Fi) projects in progress. There were 879 Wi-Fi based Wireless Internet service providers in the Czech Republic as of May 2008.

A municipal wireless antenna in Minneapolis

A keychain size Wi-Fi detector

Wi-Fi also allows connectivity in peer-to-peer (wireless ad-hoc network) mode, which enables devices to connect directly with each other. This connectivity mode can prove useful in consumer electronics and gaming applications.

Operational advantages:

Wi-Fi allows local area networks (LANs) to be deployed without wires for client devices, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.

Wireless network adapters are now built into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices. Wi-Fi has become widespread in corporate infrastructures.

Limitations:

Spectrum assignments and operational limitations are not consistent worldwide. Wi-Fi networks have limited range. A typical Wi-Fi home router using 802.11b or 802.11g with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors. The new IEEE 802.11n however, can exceed that range by more than double. Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block. Outdoor range with improved (directional) antennas can be several kilometers or more with line-of-sight. In general, the maximum amount of power that a Wi-Fi device can transmit is limited by local regulations. Wi-Fi performance decreases roughly quadratically as distance increases at constant radiation levels.

Threats to security:

The most common wireless encryption standard, Wired Equivalent Privacy or WEP, has been shown to be easily breakable even when correctly configured. Wi-Fi Protected Access (WPA and WPA2), which began shipping in 2003, aims to solve this problem and is now available on most products. Wi-Fi Access Points typically default to an "open" (encryption-free) mode. Novice users' benefit from a zero-configuration device that works out of the box, but this default is without any wireless security enabled, providing open wireless access to their LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). Wi-Fi networks that are open (unencrypted) can be monitored and used to read and copy data (including personal information) transmitted over the network, unless another security method is used to secure the data, such as a VPN or a secure web page.

Population:

Many 2.4 GHz 802.11b and 802.11g access points default to the same channel on initial startup, contributing to congestion on certain channels. To change the channel of operation for an access point requires the user to configure the device.

Channel pollution:

Standardization is a process driven by market forces. Interoperability issues between non-Wi-Fi brands or proprietary deviations from the standard can still disrupt connections or lower throughput speeds on all user's devices that are within range, to

include the non-Wi-Fi or proprietary product. Moreover, the usage of the ISM band in the 2.45 GHz range is also common to Bluetooth, WPAN-CSS, ZigBee and any new system will take its share.

Wi-Fi pollution, or an excessive number of access points in the area, especially on the same or neighboring channel, can prevent access and interfere with the use of other access points by others, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased signal-to-noise ratio (SNR) between access points. This can be a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. Additionally, other devices use the 2.4 GHz band: microwave ovens, security cameras, and Bluetooth devices and (in some countries) Amateur radio, video senders, cordless phones and baby monitors, all of which can cause significant additional interference. General guidance to those who suffer these forms of interference or network crowding is to migrate to a Wi-Fi 5 GHz product, (802.11a, or the newer 802.11n if it has 5 GHz support) because the 5 GHz band is relatively unused, and there are many more channels available. This also requires users to set up the 5 GHz band to be the preferred network in the client and to configure each network band to a different name (SSID). It is also an issue when municipalities, or other large entities such as universities, seek to provide large area coverage. This openness is also important to the success and widespread use of 2.4 GHz Wi-Fi.

Hardware:

Standard devices:

An embedded Router Board 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) in the Czech Republic.

OSBRiDGE 3GN - 802.11n Access Point and UMTS/GSM Gateway in one device.

USB wireless adapter

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point is similar to a network hub, relaying data between connected wireless devices in addition to a (usually) single connected wired device, most often an ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC card. Most new laptop computers are equipped with internal adapters. Internal cards are generally more difficult to install.

Wireless routers integrate a Wireless Access Point, ethernet switch, and internal Router firmware application that provide IP Routing, NAT, and DNS forwarding through an integrated WAN interface. A wireless router allows wired and wireless ethernet LAN devices to connect to a (usually) single WAN device such as cable modem or DSL modem. A wireless router allows all three devices (mainly the access point and router) to be configured through one central utility. This utility is most usually an integrated web server which serves web pages to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a desktop computer such as Apple's AirPort.

Wireless network bridges connect a wired network to a wireless network. This is different from an access point in the sense that an access point connects wireless devices to a wired network at the data-link layer. Two wireless bridges may be used to connect two wired networks over a wireless link, useful in situations where a wired connection may be unavailable, such as between two separate homes.

Wireless range extenders or wireless repeaters can extend the range of an existing wireless network. Range extenders can be strategically placed to elongate a signal area or allow for the signal area to reach around barriers such as those created in L-shaped

corridors. Wireless devices connected through repeaters will suffer from an increased latency for each hop. Additionally, a wireless device connected to any of the repeaters in the chain will have a throughput that is limited by the weakest link between the two nodes in the chain from which the connection originates to where the connection ends.

Network security:

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as ethernet. With wired networking it is necessary to either gain access to a building, physically connecting into the internal network, or break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Thus being able to get wireless reception provides an attack vector, if encryption is not used or can be defeated.

Attackers who have gained access to a Wi-Fi network can use DNS spoofing attacks very effectively against any other user of the network, because they can see the DNS requests made, and often respond with a spoofed answer before the queried DNS server has a chance to reply.

Securing methods:

A common but unproductive measure to deter unauthorized users is to suppress the AP's SSID broadcast, "hiding" it. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known MAC addresses to join the network. MAC addresses are easily spoofed. If the eavesdropper has the ability to change his MAC address, then he may join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping, but is now considered completely broken. Tools such as AirSnort or aircrack can quickly recover WEP encryption keys. Once it has seen 5-10 million encrypted packets, AirSnort can determine the encryption password in under a second; newer tools such as aircrack-ptw can use Klein's attack to crack a WEP key with a 50% success rate using only 40,000 packets.

To counteract this in 2002, the Wi-Fi Alliance blessed Wi-Fi Protected Access (WPA) which uses TKIP as a stopgap solution for legacy equipment. Though more secure than WEP, it has outlived its designed lifetime, has known attack vectors and is no longer recommended.

In 2004 the full IEEE 802.11i (WPA2) encryption standards were released. If used with a 802.1X server or in pre-shared key mode with a strong and uncommon passphrase WPA2 is still considered secure, as of 2009

Prac.11	Study of Bluetooth Architecture.

Bluetooth architecture overview

Any Bluetooth implementation consists of:

• Application Software

• Protocol Software that runs the lower level Bluetooth protocols on the Bluetooth hardware itself

• Baseband and Radio Frequency Semiconductor Integrated circuit

The Bluetooth hardware architecture is a typical wireless system, consisting of an RF block, a digital Baseband logic block (typically ASIC or DSP), a microcontroller with ROM or flash memory to hold the software. Typically initial implementation will consist of three or four chips in addition of a few passive components that have insignificant cost. Nevertheless, volume application of Bluetooth will require lower cost, which in turn requires a very tight integration of semiconductors to drive towards the single chip implementation.

Cambridge Silicon Radio has achieved this goal with their last BlueCore 02 Bluetooth Chip. The design is optimized to require very few external RF components to facilitate rapid design of the motherboard, and therefore the fastest possible time to market and lowest overall cost.

Bluetooth protocol

The complete Bluetooth protocol stack comprises both protocols that are specific to the Bluetooth technology, e.g. LMP, and those that can be used with many other platforms, like WAP, UDP and OBEX. These existing protocols were reused to speed up the development of the Bluetooth protocol at the higher layers at the same time to facilitate adaptation of legacy applications with work with Bluetooth devices and help to ensure interoperability of these devices' applications. The Bluetooth protocol stack consists of four layers [2]. The layers and the protocols that fit into them are summarized in Table 1.

Bluetooth Protocols Layer	Members of the Protocol Stack
Bluetooth Core Protocols	1.Baseband 2. Link Management Protocol(LMP) 3.Logical Link Control and Adaptation Layer(L2CAP) 4. Service Discovery Protocol(SDP)
Cable Replacement Protocol	Radio Frequency Communication(RFCOMM)
Telephony Control Protocols	1.Telephony Control Specification Binary(TCSBIN) 2.AT-Commands
Adopted Protocols	1.Point to Point Protocol(PPP) 2.User Datagram Protocol(UDP) Transmission control Protocol(TCS)/Internet Protocol(IP) 3.Object Exchange Protocol(OBEX) 4.Wireless Application Protocol(WAP) 5.vCard and vCalendar 6.Infrared Mobile Communications(IrMC) 7.Wireless Application Environment(WAE)

Bluetooth Protocol Stack

The core protocols are specific to Bluetooth wireless technology, developed by the Bluetooth SIG. RFCOMM and the TCS BIN protocol were also developed by the Bluetooth SIG based on existing standards, i.e. the ETSI TS07.10 and the ITU Q.931, respectively. In addition, the Bluetooth specification also defines a Host Controller Interface (HCI), which provide a command interface to the Baseband controller, link manager and access to hardware status and control registers. The core protocols and the Bluetooth radio are required by all the Bluetooth devices, while the rest of the protocols are used only when needed. The Cable replacement layer, the Telephony Control layer and the adopted layer form application-oriented protocols, which enable applications to run over the Bluetooth Core protocols. With the Open Systems Interconnection reference Model of the Bluetooth Specifications, additional protocols can be accommodated in an interoperable specification or on top of the application-oriented protocols.

Bluetooth profiles

Beside the protocols, the Bluetooth SIG has defined a number of profiles. These profiles have been developed to specify how applications and devices shall be mapped onto the Bluetooth concept by detailing a selection of messages and procedures from the Bluetooth specification and give an unambiguous description of the air interface for specific services and use cases.

The profile concept is used to decrease the risk of interoperability problems between different manufacturers' products. It defines options in each protocol that are mandatory for the profile as well as parameters ranges for each protocol. Hence the profile is a vertical slice through the protocol stacks. There are four general profiles and their functionalities are defined as follows:

1. Generic Access Profile (GAP) defines how two Bluetooth units discover and establish a connection with each other.
2. Serial Port Profile (SPP) defines the investigation of services available to a Bluetooth unit.
3. Service Discovery Application Profile (SDAP) defines how to set-up virtual serial ports on two devices and connecting these with Bluetooth.
4. Generic Object Exchange Profile (GOEP) defines the set of protocols and procedures to be used by application handling object exchanges.

The Bluetooth air interface

Since the ISM band is open to anyone, radio systems operating in this band have to cope with many unforeseeable sources of interference, such as cordless phone, microwave ovens, automatic gate opening systems and even toys. The interference can be suppressed by spreading the radio spectrum. In addition, radios operating in the U.S. are obliged to employ spectrum-spreading techniques if their transmitted power levels exceed 0 dBm.

Bluetooth technology makes use of Frequency Hopping Spread Spectrum (FHSS) to achieve low cost, low power radio implementation. Frequency hop systems divide the frequency band into many channels, radio transceiver hop from one channel to another in a pseudo-random manner. This results in very narrow-band data transceiving with maximum immunity to interference with a nominal hop rate of 1,600 hops/second. The frequency hop channel is determined by a frequency hopping sequence broadcast by the master unit's systems clock. All the slave units have to offset its own native clock to re-create the master clock. The channel makes use of several equally spaced 1 MHz hops. With Gaussian Frequency Shift Keying (GFSK) modulation, a transceiving rate of 1 Mbit/s can be achieved. The channel is further divided into 625ms slots, where a different hop frequency is used for each slot. In each slot, a packet with a fixed format can be exchanged between the master and the slave unit. Each packet starts with a 72-bit access code, follow by a 54 bits packet header and 0 to 2745 bits of payload. Every packet exchanged on the channel is preceded by the access code, which is very robust to

interference. All the control information is in the header, such as the Media Access Control (MAC) address, packet type, flow control bits and a Header Error Check (HEC) code.

To support multimedia applications that contain both data and voice features, two type of physical links have been defied:

1. Synchronous Connection Oriented (SCO) link
2. Asynchronous Connection-less (ACL) link

The SCO links support symmetrical, circuit-switched, point to point connections, which is typically used by voice transmission. A robust voice encoding scheme is employed. The scheme is based on Continuous Variable Slope Delta (CVSD) modulation, which is very resistant to bit error, as the modulation intensifies as bit error increase. Whereas, the ACL links support all the packet-switched, asymmetrical or asymmetrical, point to multipoint connections needed by the data transmission.

Application of Bluetooth technology

Bluetooth technology can be used to make wireless data connections to conventional local areas networks (LANs) via an access point equipped with a Bluetooth radio transceiver that is wired to the LAN. Once a wireless connection is established with one of these access points, a mobile device can access any of the resources on that LAN, including printers, database servers and the Internet. The user can tap out an e-mail reply on a PDA, tell it to make an Internet connection through a mobile phone and print a copy of the web page on a printer nearby, while walking down from his/her office to a meeting room.

There are many usages of Bluetooth Technology and more users scenarios are emerged everyday by the Bluetooth SIG.

1. All in one phone - use the same phone everywhere. In the office, the phone works as an intercom with no telephony charges and it function as a corporate phone to make business call with airtime charge to the company. At home it function as a cordless phone with fixed line charges. It function as a cellular phone with cellular charge, when the user is on the move.
2. Internet Bridge - Surf the Internet regardless of the connection. Use portable computing devices (i.e. Notebook, PDA or Portable PC) to surf the Internet anywhere, through a mobile phone or through a wired connection.

3. Automatic Synchronization of the address list, calendar, and all the modified documents of your desktop computer, Portable PC, PDA and mobile phone, as soon as those devices come within the range of their radio transceivers.

4. Interactive conference. In meeting and conferences, the user can share information instantly with other participants.

5. The cordless headset. Connect a headset to the mobile phone or mobile PC wirelessly to free your hand for more important tasks at office or in the car.

6. Wireless Personal Area Network. The user will be able to access documents in the portable PC while it is still in the briefcase and print the document through his hand phone at the nearby printer. In addition, two mobile devices could also exchange information (e.g. electronics name card) when needed.

7. Intelligent Commerce. Anybody will be able to access to gas station, local supermarket or department store consumer information through his mobile phone or PDA when she/he is near to the premises. Special promotion, on-going event, new products information as well as frequent buyer account information will be available through the mobile information devices.