May 2009

Q1A) Explain in brief the operation the cellular systems

Ans: The operation of a cellular mobile system can be described as five major functionalities and four additional utilities. All the functions together make a complete mobile cellular system. Mobile unit initialization

a. When mobile unit is turned on, it scans and selects the strongest setup control channel used for system.
b. Cells with different frequency bands repetitively broadcast on different setup channels.
c. The receiver selects the strongest setup channel and monitors that channel.
d. With this the mobile station has automatically selected the BS antenna of the cell within which it will operate.
e. Then handshake takes place b/w the mobile unit and MTSO controlling this cell through the BS in this cell.
f. Handshake is used to identify the user and register its location.
g. As long as the mobile station is on, scanning is repeated periodically to account for the motion of the unit.
h. If the unit enters a new cell, then a new BS is selected. Mobile-originated call

a. A mobile unit originates a call by sending the number (Mobile Identification Number, MIN) of the called unit on the preselected setup channel.
b. The receiver of mobile unit checks if the forward channel (from BS) is idle.
c. If idle the mobile may transmit over the reverse channel(To base station)
d. BS sends request to the MTSO.
Paging
a. MTSO attempts to complete connection
b. MTSO sends a paging message to certain BSs depending on called mobile number.
c. BS sends paging signal on its own assigned setup channel.
Call accepted
a. Called mobile unit recognizes its number on the setup channel being monitored and responds to that BS, which sends the response to the MTSO.
b. MTSO sets up a circuit between calling and called BSs.

c. MTSO selects available traffic channel within each BS's cell and notifies each BS, which in turn notifies its mobile unit (a data message called alert is transmitted over FVC to instruct the mobile to ring).
d. The two mobile units tune to their respective channels.
Rajiv Gandhi Institute Of Technology 60 Ongoing call
a. While connection is maintained, two mobile stations exchange voice or data, through BSs and MTSO.
Handoff
a. If a mobile unit moves from range of one cell to another the traffic channel has to change.
b. System makes this change without either interrupting the call or alerting the user.
Call blocking: If all traffic channels are busy even after multiple attempts a busy tone is returned.
Call termination: When one of the users hangs up, MTSO is informed and the traffic channels
are released
Call drop: during a connection if because of interference or weak signal spots, the BS can't
maintain the minimum required signal strength for a certain period of time the traffic channel is
dropped and MTSO is informed.
Calls to/from fixed and remote mobile subscriber**:** MTSO connects to the public switched
telephone network. Thus it can setup calls b/w mobile user in its area and fixed subscriber via
telephone network, remote MTSO.

Q1.B) List the transmission impairment effecting the wireless transmission. Explain free
space loss? Determine the free space loss at 4 GHz for the shortest path to a geo
synchronous satellite?
Ans: Analog signal consist of varying a voltage with time to represent an information steam. If
the transmission media were perfectly, the receiver could receive exactly the same signal that the

transmitter sent. But communication lines are usually not perfect, so the receive signal is not the
same as the transmitted signal. For digital data this difference can lead to errors. Transmission
lines suffers from three major problems

1. Attenuation
2. Delay distortions
3. Noise

Attenuation:

It is the loss of energy as the signal propagates outward. The amount of energy depends on the
frequency. If the attenuation is too much, the receiver may not be able to detect the signal at all,
or the signal may fall below the noise level. For reliable communication, the attenuation and
delay over the range of frequencies of transmission should be constant.

Distortion:

The second transmission impairment is delay distortion. Communication line have distributed
inductance and capacitance which distort the amplitude of signals and also delay the signals at
different frequencies by different amounts. It is caused by the fact that different Fourier
components travel at different speed.

Noise:

Noise is a third impairment. It can be define as unwanted energy from sources other than the
transmitter. Thermal noise is caused by the random motion of the electrons in a wire and is
unavoidable.

Cross talk:

Similarly cross talk is a noise that is caused by the inductive coupling between two wires that are closed to each other. Sometime when talking on the telephone, you can hear another conversation in the background. That is cross talk

Free space path loss basics The free space path loss, also known as FSPL is the loss in signal strength that occurs when an electromagnetic wave travels over a line of sight path in free space. In these circumstances there are no obstacles that might

cause the signal to be reflected refracted, or that might cause additional attenuation. The free space path loss calculations only look at the loss of the path itself and do not contain any factors relating to the transmitter power, antenna gains or the receiver sensitivity levels. These factors are normally address when calculating a link budget and these will also be used within radio and wireless survey tools and software. To understand the reasons for the free space path loss, it is possible to imagine a signal spreading out from a transmitter. It will move away from the source spreading out in the form of a sphere. As it does so, the surface area of the sphere increases. As this will follow the law of the conservation of energy, as the surface area of the sphere increases, so the intensity of the signal must decrease. As a result of this it is found that the signal decreases in a way that is inversely proportional to the square of the distance from the source of the radio signal. Signal = 1 distance2 The equation for FSPL is Decibel version of free space path loss equation Most RF comparisons and measurements are performed in decibels. This gives an easy and consistent method to compare the signal levels present at various points. Accordingly it is very convenient to express the free space path loss formula, FSPL, in terms of decibels. It is easy to take the basic free space path loss equation and manipulate into a form that can be expressed in a logarithmic format.

FSPL (dB) = 20 log10 (d) + 20 log10 (f) + 32.44

Where:

d is the distance of the receiver from the transmitter (km)

f is the signal frequency (MHz)

Shortest path to a geo synchronous satellite is approximately 35000km .Frequency given is

4GHz i.e. 4000MHz approx.

FSPL(db)=20log 35000+20 log 4000+32.44

= 20*4.54+20*3.6+32.44

=90.8+72+32.44=195.24

Q 2 A) Explain GSM network architecture.

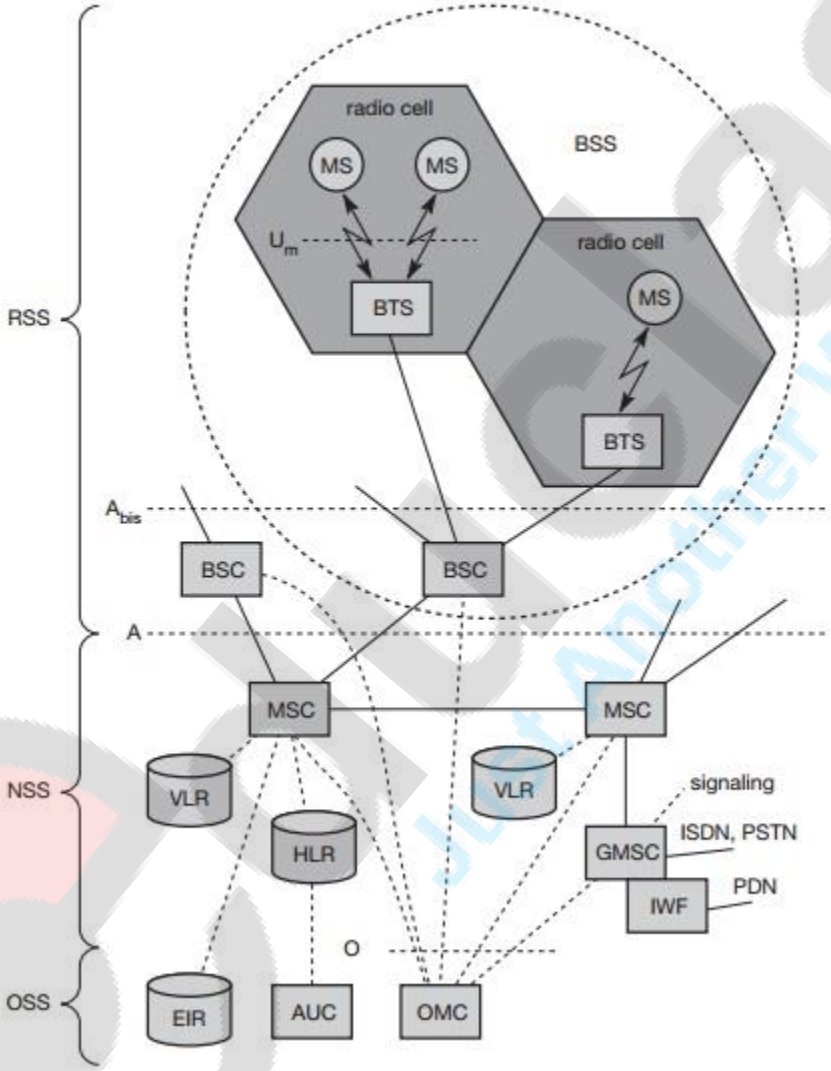
A.

GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms. Figure 4.4 gives a simplified overview of the GSM system as specified in ETSI (1991b). A GSM system consists of three subsystems,

- the radio sub system (RSS),

- the network and switching subsystem (NSS), and
- the operation subsystem (OSS).

Generally, a GSM customer only notices a very small fraction of the whole network – the mobile stations (MS) and some antenna masts of the base transceiver stations (BTS).



Functional architecture of a GSM system

RSS

As the name implies, the radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS). Figure shows the connection between the RSS and the NSS via the A inter face (solid lines) and the connection to the OSS via the O interface (dashed lines).

- **Base station subsystem (BSS):** A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
- **Base transceiver station (BTS):** A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells and is connected to MS via the U_m interface and to the BSC via the A_{bis} interface. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.
- **Base station controller (BSC):** The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS):** The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the subscriber identity module (SIM), which stores all user-specific data that is relevant to GSM. While an MS can be identified via the international mobile equipment identity (IMEI), a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key K_i, and the international mobile subscriber identity (IMSI). The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM.

NSS

The "heart" of the GSM system is formed by the network and switching subsystem (NSS). The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:

- **Mobile services switching center (MSC):** MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A gateway MSC (GMSC) has additional connections to other fixed networks, such as PSTN and ISDN. Using additional interworking functions (IWF), an MSC can also connect to public data networks (PDN) such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs. The standard signaling system No. 7 (SS7) is used for this purpose. SS7 covers all aspects of control signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls). Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.
- **Home location register (HLR):** The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN), subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the international mobile subscriber identity (IMSI). Dynamic information is also needed, e.g., the current location area (LA) of the MS, the mobile subscriber r roaming number (MSRN), the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.

- **Visitor location register (VLR):** The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information. Some VLRs in existence, are capable of managing up to one million customers.

- **Gateway Mobile Switching Centre (GMSC):** The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location. The GMSC is thus in charge of obtaining the MSRN (Mobile Station Roaming Number) from the HLR based on the MSISDN (Mobile Station ISDN number, the "directory number" of a MS) and routing the call to the correct visited MSC. The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to an MSC.

OSS

The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signaling. The following entities have been defined:

- **Operation and maintenance center (OMC):** The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing. OMCs use the concept of telecommunication management network (TMN).
- **Authentication centre (AuC):** As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.
- **Equipment identity register (EIR):** The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs

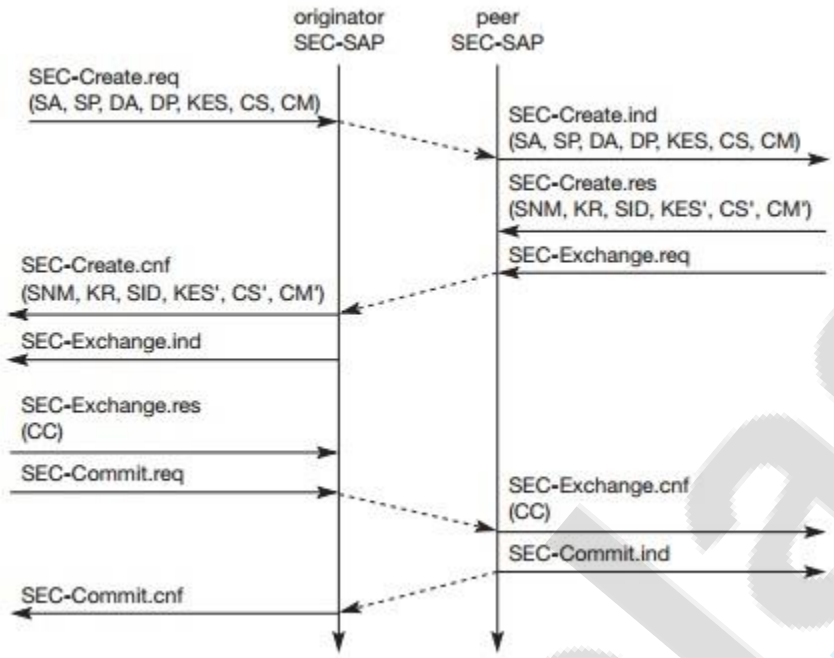
are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible (the reader may speculate as to why this is the case). The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

Q 2 B) How is the security provided in the WAP using wireless transport layer security?

A.

If requested by an application, a security service, the wireless transport layer security (WTLS), can be integrated into the WAP architecture on top of WDP (Wireless Datagram Protocol). WTLS can provide different levels of security (for privacy, data integrity, and authentication) and has been optimized for low bandwidth, high-delay bearer networks. WTLS takes into account the low processing power and very limited memory capacity of the mobile devices for cryptographic algorithms. WTLS supports datagram and connection-oriented transport layer protocols. New compared to, e.g. GSM, is the security relation between two peers and not only between the mobile device and the base station

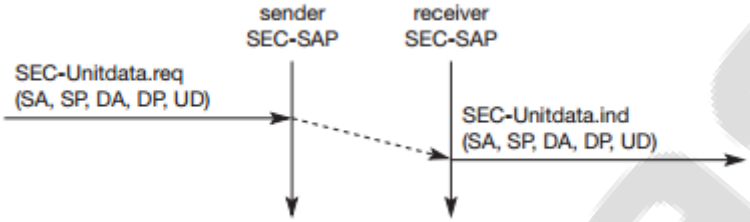
WTLS took over many features and mechanisms from TLS (formerly SSL, secure sockets layer), but it has an optimized handshaking between the peers.



WTLS establishing a secure session

Before data can be exchanged via WTLS, a secure session has to be established. This session establishment consists of several steps: Figure illustrates the sequence of service primitives needed for a so-called 'full handshake' (several optimizations are possible). The originator and the peer of the secure session can both interrupt session establishment any time, e.g., if the parameters proposed are not acceptable.
The first step is to initiate the session with the SEC-Create primitive. Parameters are source address (SA), source port (SP) of the originator, destination n address (DA), destination port (DP) of the peer. The originator proposes a key exchange suite (KES) (e.g., RSA (Rivest, 1978), DH (Diffie, 1976), ECC (Certicom, 2002)), a cipher suite (CS) (e.g., DES, IDEA (Schneier, 1996), and a compression method (CM) (currently not further specified). The peer answers with parameters for the sequence number mode (SNM), the key refresh cycle (KR) (i.e., how often keys are refreshed within this secure session), the session identifier (SID) (which is unique with each peer), and the selected key exchange suite (KES'), cipher suite (CS'), compression method (CM'). The peer also issues a SEC-Exchange primitive. This indicates that the peer wishes to perform public-key authentication with the client, i.e., the peer requests a client certificate (CC) from the originator.
The first step of the secure session creation, the negotiation of the security parameters and suites, is indicated on the originator's side, followed by the request

for a certificate. The originator answers with its certificate and issues a SEC-Commit.req primitive. This primitive indicates that the handshake is completed for the originator's side and that the originator now wants to switch into the newly negotiated connection state. The certificate is delivered to the peer side and the SEC-Commit is indicated. The WTLS layer of the peer sends back a confirmation to the originator. This concludes the full handshake for secure session setup.



WTLS datagram transfer

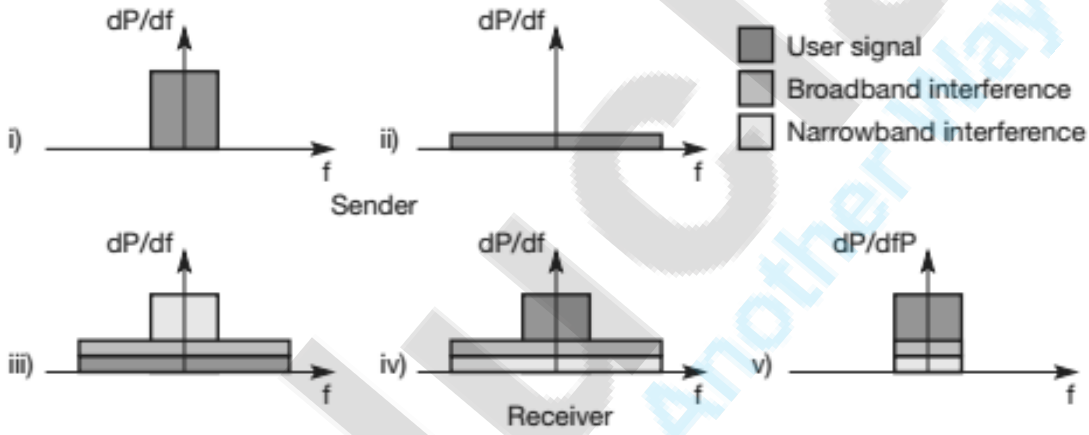
After setting up a secure connection between two peers, user data can be exchanged. This is done using the simple SEC-Unitdata primitive as shown in Figure. SEC-Unitdata has exactly the same function as T-DUnitdata on the WDP layer, namely it transfers a datagram between a sender and a receiver. This
data transfer is still unreliable, but is now secure. This shows that WTLS can be easily plugged into the protocol stack on top of WDP. The higher layers simply use SEC-Unitdata instead of T-DUnitdata. The parameters are the same here: source address (SA), source port (SP), destination address (DA), destination port (DP), and user data (UD).

Although WTLS allows for different encryption mechanisms with different key lengths, it is quite clear that due to computing power on the handheld devices the encryption provided cannot be very strong. If applications require stronger security, it is up to an application or a user to apply stronger encryption on top of the whole protocol stack and use WTLS as a basic security level only. Many programs are available for this purpose. It is important to note that the security association in WTLS exists between the mobile WAP-enabled device and a WAP server or WAP gateway only. If an application accesses another server
via the gateway, additional mechanisms are needed for end-to-end security. If for example a user accesses his or her bank account using WAP, the WTLS security association typically ends at the WAP gateway inside the network operator's domain. The bank and user will want to apply additional security mechanisms in this scenario.

Future work in the WTLS layer comprises consistent support for application level security (e.g. digital signatures) and different implementation classes with different capabilities to select from.

Q.3 (a) What is Spread Spectrum? Explain FHSS and DSSS.

Spread Spectrum:
Spread spectrum techniques involve spreading the bandwidth needed to transmit data – which does not make sense at first sight. Spreading the bandwidth has several advantages. The main advantage is the resistance to narrowband interference.



In Figure 2.32, diagram

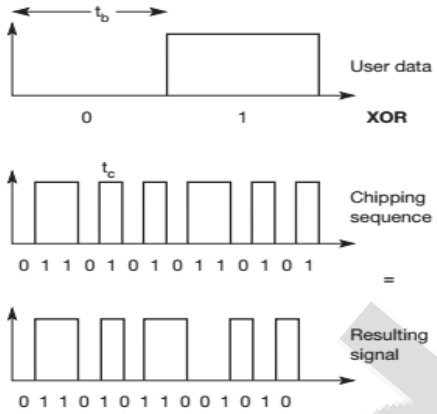
i) shows an idealized narrowband signal from a sender of user data (here power density dP/df versus frequency f).

ii) The sender now spreads the signal in step ii), i.e., converts the narrowband signal into a broadband signal. The energy needed to transmit the signal (the area shown in the diagram) is the same, but it is now spread over a larger frequency range. The power level of the spread signal can be much lower than that of the original narrowband signal without losing data. Depending on the generation and reception of the spread signal, the power level of the user signal can even be as low as the background noise. This makes it difficult to distinguish the user signal from the background noise and thus hard to detect.

iii) During transmission, narrowband and broadband interference add to the signal in step iii). The sum of interference and user signal is received. The receiver now knows how to despread the signal, converting the spread user signal into a narrowband signal again, while spreading the narrowband interference and leaving the broadband interference.

iv) In step v) the receiver applies a bandpass filter to cut off frequencies left and right of the narrowband signal. Finally, the receiver can reconstruct the original data because the power level of the user signal is high enough, i.e., the signal is much stronger than the remaining interference.

Direct sequence spread spectrum:
Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence as shown below.



The example shows that the result is either the sequence 0110101 (if the user bit equals 0) or its complement 1001010 (if the user bit equals 1).

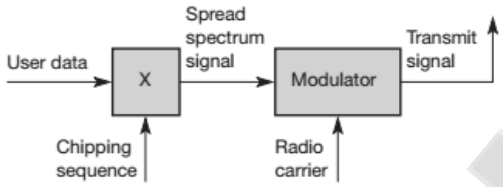
While each user bit has a duration tb, the chipping sequence consists of smaller pulses, called chips, with a duration tc. If the chipping sequence is generated properly it appears as random noise: this sequence is also sometimes called pseudo-noise sequence.

The spreading factor s = tb/tc determines the bandwidth of the resulting signal. If the original signal needs a bandwidth w, the resulting signal needs s·w after spreading. While the spreading factor of the very simple example is only 7 (and the

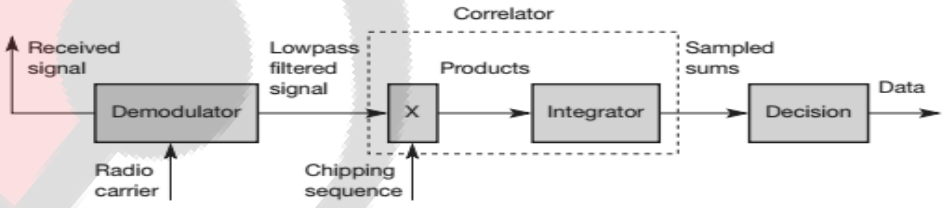
chipping sequence 0110101 is not very random), civil applications use spreading factors between 10 and 100, military applications use factors of up to 10,000.

Wireless LANs complying with the standard IEEE 802.11 (see section 7.3) use, for example, the sequence 10110111000, a so-called Barker code, if implemented using DSSS. Barker codes exhibit a good robustness against interference and insensitivity to multi-path propagation.

Other known Barker codes are 11, 110, 1110, 11101, 1110010, and 1111100110101 (Stallings, 2002). Up to now only the spreading has been explained. However, transmitters and receivers using DSSS need additional components as shown in the simplified block diagrams in Figure 2.36 and Figure 2.37. The first step in a DSSS transmitter, Figure 2.36 is the spreading of the user data with the chipping sequence (digital modulation).



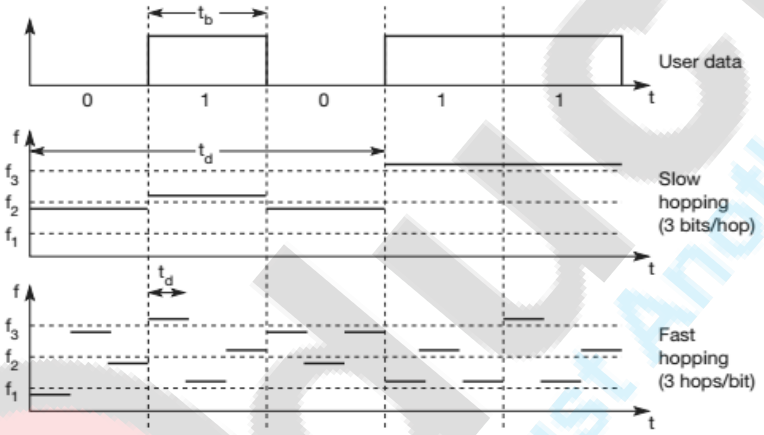
The spread signal is then modulated with a radio carrier as explained in section 2.6 (radio modulation). Assuming for example a user signal with a bandwidth of 1 MHz. Spreading with the above 11-chip Barker code would result in a signal with 11 MHz bandwidth. The radio carrier then shifts this signal to the carrier frequency (e.g., 2.4 GHz in the ISM band). This signal is then transmitted.



The DSSS receiver is more complex than the transmitter. The receiver only has to perform the inverse functions of the two transmitter modulation steps. However,

noise and multi-path propagation require additional mechanisms to reconstruct the original data. The first step in the receiver involves demodulating the received signal. This is achieved using the same carrier as the transmitter reversing the modulation and results in a signal with approximately the same bandwidth as the original spread spectrum signal. Additional filtering can be applied to generate this signal.

Frequency hopping spread spectrum:
For frequency hopping spread spectrum (FHSS) systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels. Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel. This system implements FDM and TDM. The pattern of channel usage is called the hopping sequence, the time spend on a channel with a certain frequency is called the dwell time. FHSS comes in two variants, slow and fast hopping.



In slow hopping, the transmitter uses one frequency for several bit periods.3 Figure 2.38 shows five user bits with a bit period tb. Performing slow hopping, the transmitter uses the frequency f2 for transmitting the first three bits during the dwell time td. Then, the transmitter hops to the next frequency f3. Slow hopping systems are typically cheaper and have relaxed tolerances, but they are not as immune to narrowband interference as fast hopping systems. Slow frequency hopping is an option for GSM (see section 4.1).

For fast hopping systems, the transmitter changes the frequency several times during the transmission of a single bit. In the example of Figure 2.38, the transmitter hops three times during a bit period. Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances to perform hopping at more or less the same points in time. However, these systems are much better at overcoming the effects of narrowband interference and frequency selective fading as they only stick to one frequency for a very short time.

Q.3 (b) Discuss the operation of Mobile IP.

Mobile IP is the standard for mobile access to the Internet. In this article, Bill Stallings describes how this relatively new protocol is changing the face of mobile (or nomadic) computing.

In response to the increasing popularity of palmtop and other mobile computers, Mobile IP was developed to enable computers to maintain Internet connectivity while moving from one Internet attachment point to another. Although Mobile IP can work with wired connections, in which a computer is unplugged from one physical attachment point and plugged into another, it's particularly suited to wireless connections.

The term *mobile* in this context implies that a user is connected to one or more applications across the Internet, that the user's point of attachment changes dynamically, and that all connections are automatically maintained despite the change. This is in contrast to a user, such as a business traveler, with a portable computer of some sort, who arrives at a destination and uses the computer's notebook to dial into an ISP (Internet service provider). In this latter case, the user's Internet connection is terminated each time the user moves, and a new connection is initiated when the user dials back in. Each time an Internet connection is established, software in the point of attachment (typically an ISP) is used to obtain a new, temporarily assigned IP address. For each application-level connection (such as FTP or web connection), this temporary IP address is used by the user's correspondent. A better term for this kind of use is *nomadic*.

Operation of Mobile IP

Routers make use of the IP address in an IP datagram to perform routing. In particular, the *network portion* of an IP address is used by routers to move a datagram from the source computer to the network to which the target computer is attached. Then the final router on the path, which is attached to the same network as the target computer, uses the *host portion* of the IP address to deliver the IP datagram to the destination. Further, this IP address is known to the next-higher layer in the protocol architecture. In particular, most applications over the Internet are supported by TCP connections. When a TCP connection is set up, the TCP entity on each side of the connection knows the IP address of the correspondent host. When a TCP segment is handed down to the IP layer for delivery, TCP provides the IP address. IP creates an IP datagram with that IP address in the IP header and sends the datagram out for routing and delivery. However, with a mobile host, the IP address may change while one or more TCP connections are active.

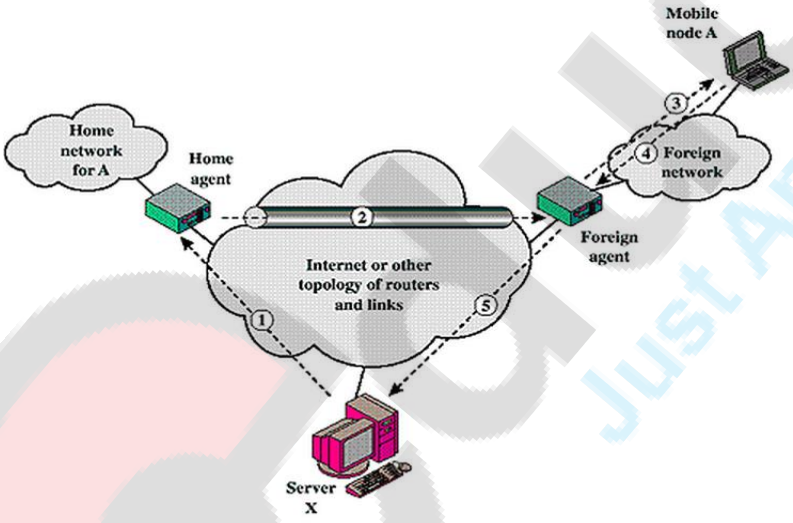


Figure 1 shows in general terms how Mobile IP deals with the problem of dynamic IP addresses. A mobile node is assigned to a particular network, known as its *home network*. Its IP address on that network, known as its *home address*, is static. When the mobile node moves its attachment point to another network, that's considered a *foreign network* for this host. Once the mobile node is reattached, it makes its

presence known by registering with a network node, typically a router, on the foreign network known as a *foreign agent*. The mobile node then communicates with a similar agent on the user's home network, known as a *home agent*, giving the home agent the *care-of address* of the mobile node; the care-of address identifies the foreign agent's location. Typically, one or more routers on a network will implement the roles of both home and foreign agents.

Figure 1 Mobile IP scenario.

When IP datagrams are exchanged over a connection between the mobile node (A) and another host (server X in Figure 1), the following operations occur:

1. Server X transmits an IP datagram destined for mobile node A, with A's home address in the IP header. The IP datagram is routed to A's home network.
2. At the home network, the incoming IP datagram is intercepted by the home agent. The home agent encapsulates the entire datagram inside a new IP datagram that has A's care-of address in the header, and retransmits the datagram. The use of an outer IP datagram with a different destination IP address is known as *tunneling*.
3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network-level protocol data unit or PDU (such as a LAN LLC frame), and delivers the original datagram to A across the foreign network.
4. When A sends IP traffic to X, it uses X's IP address. In our example, this is a fixed address; that is, X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network for routing to X. Typically, this router is also the foreign agent.
5. The IP datagram from A to X travels directly across the Internet to X, using X's IP address.

To support the operations illustrated in Figure 1, Mobile IP includes three basic capabilities:

- **Discovery.** A mobile node uses a discovery procedure to identify prospective home agents and foreign agents.
- **Registration.** A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.
- **Tunneling.** Tunneling is used to forward IP datagrams from a home address to a care-of address.

Q.4 (a) Explain the applications of Wireless LAN.

Answer : Wireless LAN Applications

- There are four application areas for wireless LANs: LAN extension, crossbuilding

interconnect, nomadic access, and ad hoc networks. Let us consider each of these in turn.

❖ **LAN Extension :**

- Early wireless LAN products, introduced in the late 1980s, were marketed as substitutes for traditional wired LANs. A wireless LAN saves the cost of the installation of LAN cabling and eases the task of relocation and other modifications to network structure.
- There is a role for the wireless LAN as an alternative to a wired LAN.

- **For example**, a manufacturing facility typically has an office area that is separate from the factory floor but that must be linked to it for networking purposes. Therefore, typically, a wireless LAN will be linked into a wired LAN on the same premises. Thus, this application area is referred to as LAN extension. Figure 13.1 indicates a simple wireless LAN configuration that is typical of many environments.

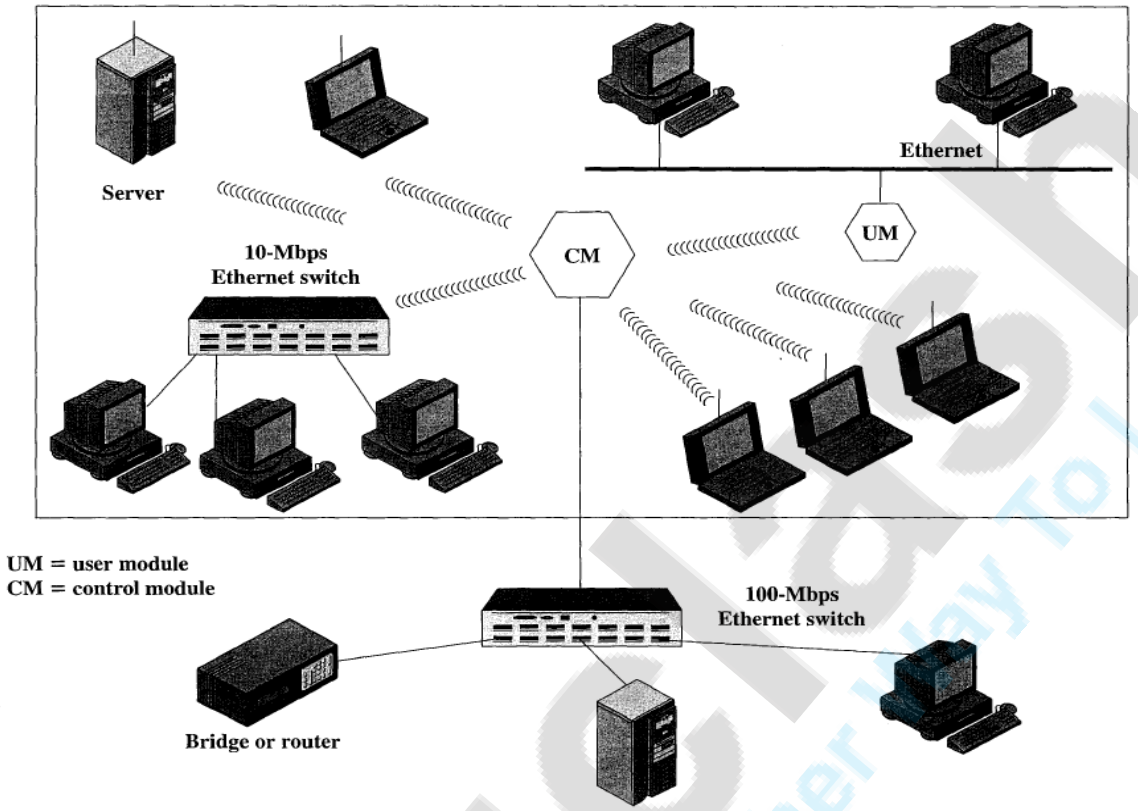


Figure 13.1 Example Single-Cell Wireless LAN Configuration

- There is a backbone wired LAN, such as Ethernet, that supports servers, workstations, and one or more bridges or routers to link with other networks.
- In addition, there is a control module (CM) that acts as an interface to a wireless LAN. The control module includes either bridge or router functionality to link the wireless LAN to the backbone. It includes some sort of access control logic, such as a polling or token-passing scheme, to regulate the access from the end systems.
- Hubs or other user modules (UMs) that control a number of stations off a wired LAN may also be part of the wireless LAN configuration.
- The configuration of Figure 13.1 can be referred to as **a single-cell wireless LAN**; all of the wireless end systems are within range of a single control module.

- Another common configuration, suggested by Figure 13.2, is **a multiple-cell wireless LAN**.

- In this case, there are multiple control modules interconnected by a wired LAN. Each control module supports a number of wireless end systems within its transmission range.

- **For example**, with an infrared LAN, transmission is limited to a single room; therefore, one cell is needed for each room in an office building that requires wireless support.

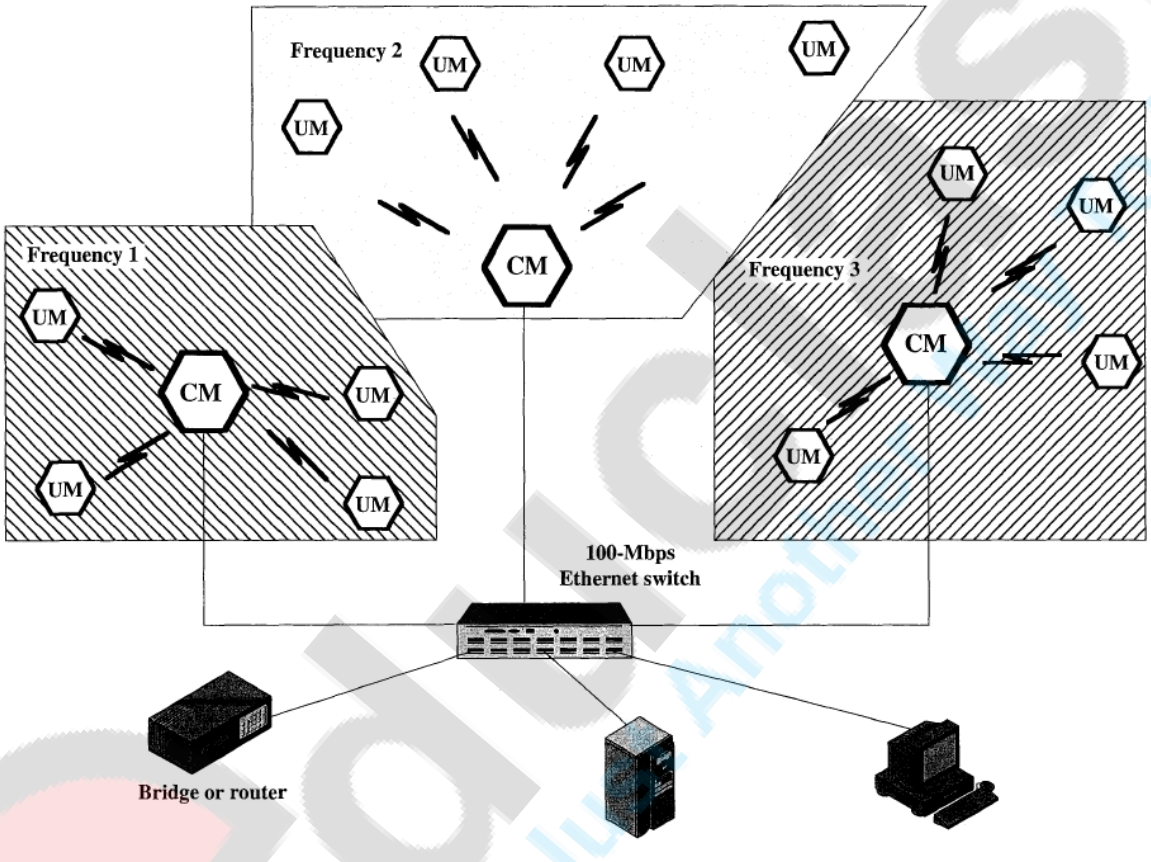


Figure 13.2 Example Multiple-Cell Wireless LAN Configuration

❖ **Cross-Building Interconnect** :

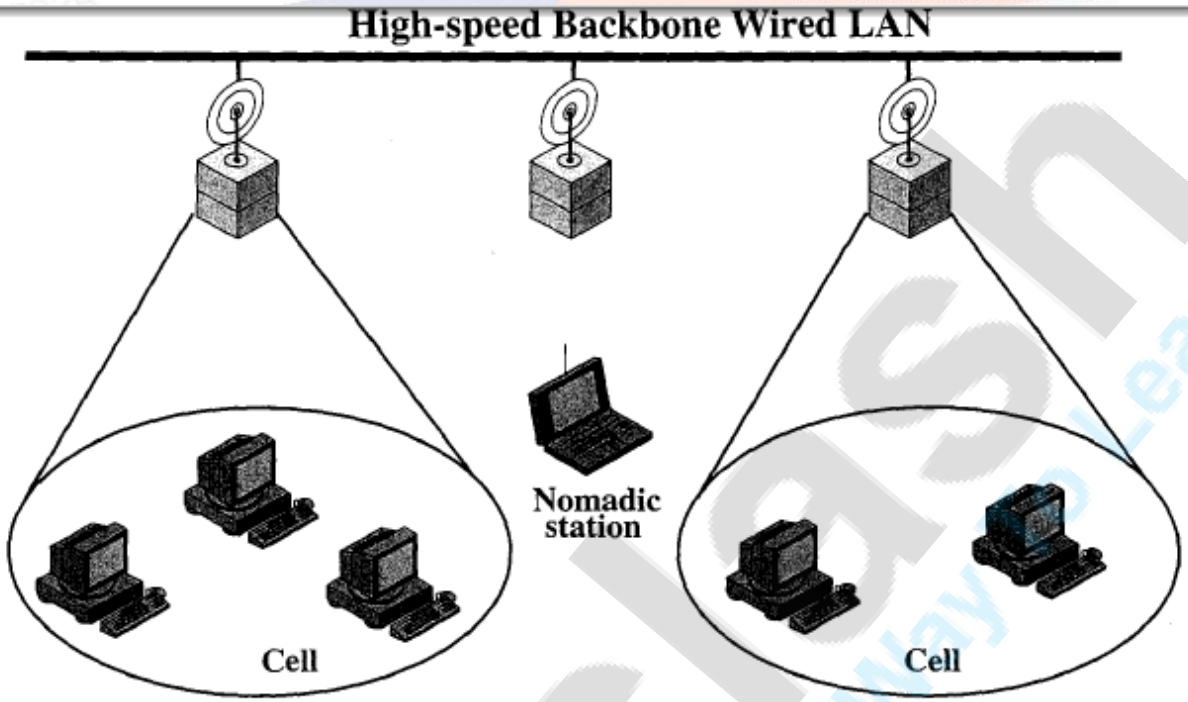
- Another use of wireless LAN technology is to connect LANs in nearby buildings, be they wired or wireless LANs.
- In this case, a point-to-point wireless link is used between two buildings.
- The devices so connected are typically bridges or routers.
- This single point-to-point link is not a LAN per se, but it is usual to include this application under the heading of wireless LAN.

❖ **Nomadic Access** :

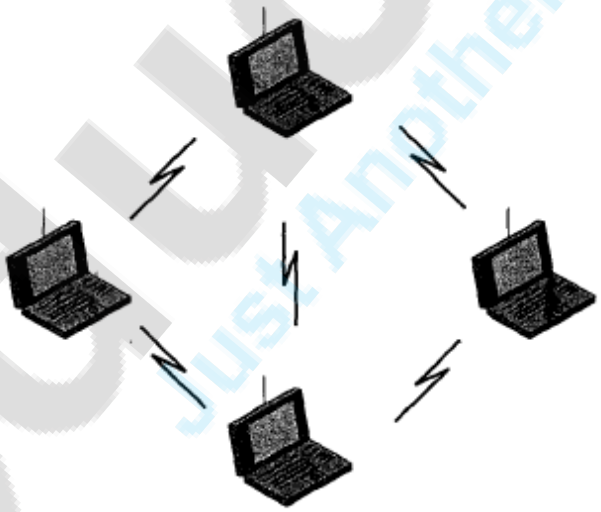
- Nomadic access provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna, such as a laptop computer or notepad computer.
- One example of the utility of such a connection is to enable an employee returning from a trip to transfer data from a personal portable computer to a server in the office.
- Nomadic access is also useful in an extended environment such as a campus or a business operating out of a cluster of buildings.
- In both of these cases, users may move around with their portable computers and may wish access to the servers on a wired LAN from various locations.

❖ **Ad Hoc Networking** :

- An ad hoc network is a peer-to-peer network (no centralized server) set up temporarily to meet some immediate need.
- For example, a group of employees, each with a laptop or palmtop computer, may convene in a conference room for a business or classroom meeting. The employees link their computers in a temporary network just for the duration of the meeting.
- Figure 13.3 suggests the differences between a wireless LAN that supports LAN extension and nomadic access requirements and an ad hoc wireless LAN.
- In the former case, the wireless LAN forms a stationary infrastructure consisting of one or more cells with a control module for each cell. Within a cell, there may be a number of stationary end systems. Nomadic stations can move from one cell to another.
- In contrast, there is no infrastructure for an ad hoc network. Rather, a peer collection of stations within range of each other may dynamically configure themselves into a temporary network.



(a) Infrastructure Wireless LAN



(b) Ad hoc LAN

Figure 13.3 Wireless LAN Configurations

Q4. B) Discuss the Protocol Architecture of Bluetooth.

Answer : Protocol Architecture of Bluetooth

- Bluetooth is defined as a layered protocol architecture (Figme 15.1) consisting of core protocols, cable replacement and telephony control protocol, and adopted protocols.
- The **core protocols** form a five-layer stack consisting of the following elements:

- **Radio:** Specifies details of the air interface, including. requency, the use of frequency hopping, modulation scheme, and transmit power.

- **Baseband:** Concerned with connection establishment within a piconet, addressing, packet format, timing, and power control.

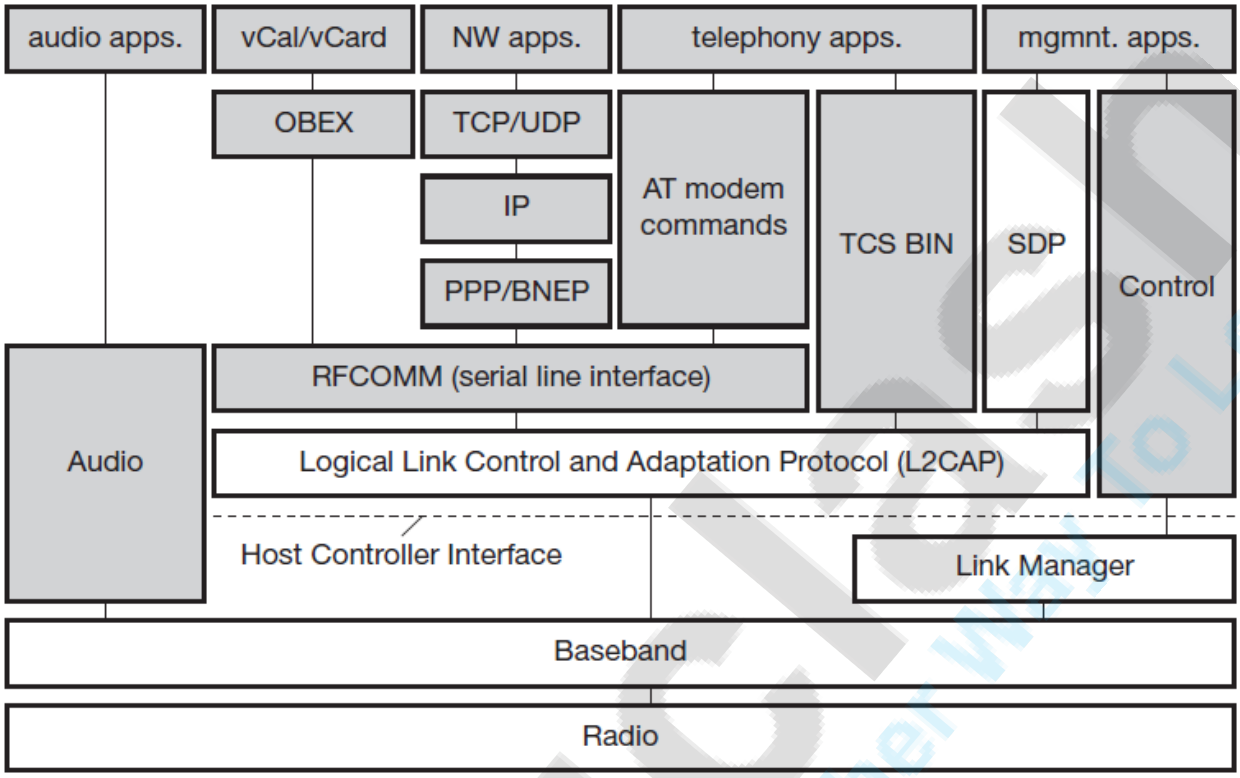
- **Link manager protocol (LMP):** Responsible for link setup between Bluetooth devices and ongoing link management. This includes security aspects such as authentication and encryption, plus the control and negotiation of baseband packet sizes.

- **Logical link control and adaptation protocol (L2CAP):** Adapts upper-layer protocols to the baseband layer. L2CAP provides oth connectionless and connection-oriented services.

- **Service discovery protocol (SDP):** Device information, services, and the characteristics of the services can be queried to enable the establishment of a connection between two or more Bluetooth devices.

- On top of L2CAP is the **cable replacement protocol** RFCOMM that emulates a serial line interface following the EIA-232 (formerly RS-232) standards.
- This allows for a simple replacement of serial line cables and enables many legacy applications and protocols to run over Bluetooth. RFCOMM supports multiple serial ports over a single physical channel.

- The **telephony control protocol specification – binary** (TCS BIN) describes a bit-oriented protocol that defines call control signaling for the establishment of voice and data calls between Bluetooth devices. It also describes mobility and group management functions.
- The **host controller interface** (HCI) between the baseband and L2CAP provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers.
- The HCI can be seen as the hardware/software boundary. Many **protocols** have been **adopted** in the Bluetooth standard. Classical Internet applications can still use the standard TCP/IP stack running over PPP or use the more efficient Bluetooth network encapsulation protocol (BNEP).
- Telephony applications can use the AT modem commands as if they were using a standard modem.
- Calendar and business card objects (vCalendar/vCard) can be exchanged using the object exchange protocol (OBEX) as common with IrDA interfaces.
- A real difference to other protocol stacks is the support of **audio**. Audio applications may directly use the baseband layer after encoding the audio signals.



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Fig : Bluetooth Protocol Stack

Q.5 (a) Explain CDMA technique using an example.

1. Code Division Multiple Access (CDMA) systems use exactly these codes to separate different users in code space and to enable access to a shred medium without interference.

2. One of the basic concepts in data communication is the idea of allowing several transmitters to send information simultaneously over a single communication channel. This allows several users to share a band of frequencies (see bandwidth). This concept is called multiplexing.

3. CDMA employs spread-spectrum technology and a special coding scheme (where each transmitter is assigned a code) to allow multiple users to be multiplexed over the same physical channel. By contrast, time division multiple access (*TDMA*) divides access by time, while frequency-division multiple access (*FDMA*) divides it by frequency.

4. CDMA is a form of spread-spectrum signaling, since the modulated coded signal has a much higher data bandwidth than the data being communicated.

5. An analogy to the problem of multiple access is a room (channel) in which people wish to talk to each other simultaneously. To avoid confusion, people could take turns speaking (time division), speak at different pitches (frequency division), or speak in different languages (code division).

6. CDMA is analogous to the last example where people speaking the same language can understand each other, but other languages are perceived as noise and rejected. Similarly, in radio CDMA, each group of users is given a shared code. Many codes occupy the same channel, but only users associated with a particular code can communicate.

   Example:
   1. Sender A
      a. sends Ad = 1, key Ak = 010011 (assign: „0“= -1, „1“= +1)
      b. sending signal As = Ad * Ak = (-1, +1, -1, -1, +1, +1)

   2. Sender B
      a. sends Bd = 0, key Bk = 110101 (assign: „0“= -1, „1“= +1)
      b. sending signal Bs = Bd * Bk = (-1, -1, +1, -1, +1, -1)

   3. Both signals superimpose in space
      a. interference neglected (noise etc.)
      b. As + Bs = (-2, 0, 0, -2, +2, 0)

   4. Receiver wants to receive signal from sender A
      a. apply key Ak bitwise (inner product)
         i. Ae = (-2, 0, 0, -2, +2, 0) · Ak = 2 + 0 + 0 + 2 + 2 + 0 = 6
         ii. result greater than 0, therefore, original bit was „1“

b. receiving B
   i. Be = (-2, 0, 0, -2, +2, 0) · Bk = -2 + 0 + 0 - 2 - 2 + 0 = -6, i.e. „0“

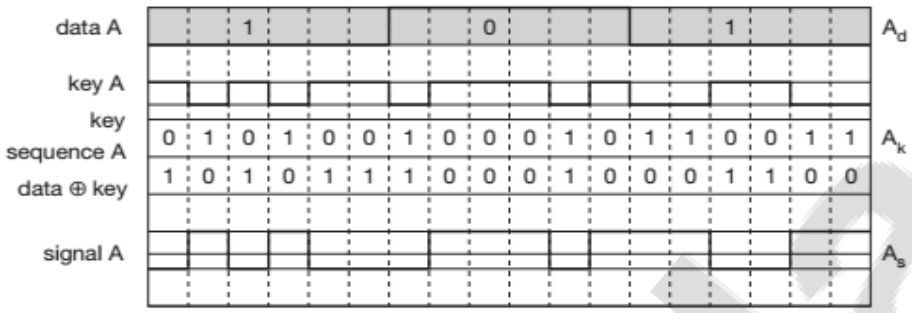


Figure 3.14
Coding and spreading of data from sender A

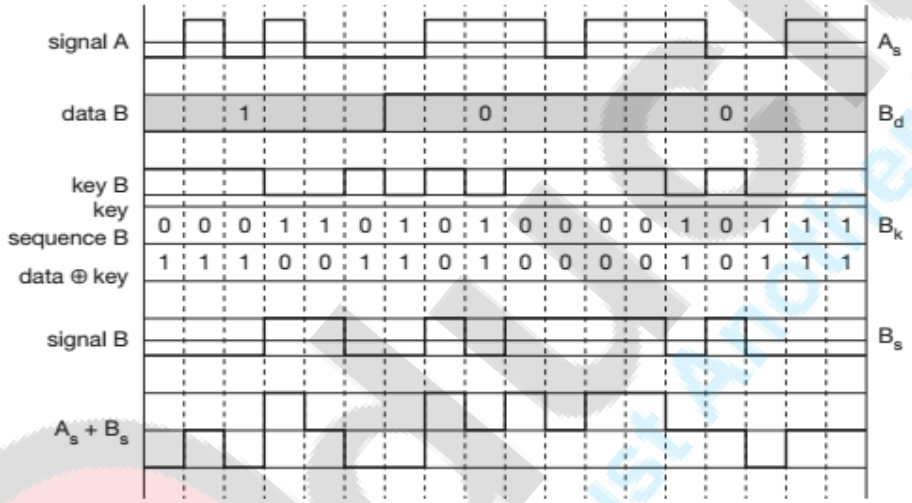


Figure 3.15
Coding and spreading of data from sender B

Q.5 (b) Explain how the capacity of a satellite is allocated using frequency division.

1. Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM).

2. Allocation can either be fixed (as for radio stations or the general planning and regulation of frequencies) or dynamic (i.e., demand driven).

3. Channels can be assigned to the same frequency at all times, i.e., pure FDMA, or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA.

4. Sender and receiver have to agree on a hopping pattern, otherwise the receiver could not tune to the right frequency. Hopping patterns are typically fixed, at least for a longer period. The fact that it is not possible to arbitrarily jump in the frequency space (i.e., the receiver must be able to tune to the right frequency) is one of the main differences between FDM schemes and TDM schemes.

5. Furthermore, FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks. Here the two partners typically establish a duplex channel, i.e., a channel that allows for simultaneous transmission in both directions. The two directions, mobile station to base station and vice versa are now separated using different frequencies. This scheme is then called frequency division duplex (FDD). Again, both partners have to know the frequencies in advance; they cannot just listen into the medium.

6. The two frequencies are also known as uplink, i.e., from mobile station to base station or from ground control to satellite, and as downlink, i.e., from base station to mobile station or from satellite to ground control.

7. As for example FDM and FDD, Figure 3.3 shows the situation in a mobile phone network based on the GSM standard for 900 MHz (see chapter 4). The basic frequency allocation scheme for GSM is fixed and regulated by

national authorities. (Certain variations exist regarding the frequencies mentioned in the examples.)

All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone.

Up- and downlink have a fixed relation. If the uplink frequency is fu = 890 MHz + n·0.2 MHz, the downlink frequency is fd = fu + 45 MHz, i.e., fd = 935 MHz + n·0.2 MHz for a certain channel n. The base station selects the channel.

Each channel (uplink and downlink) has a bandwidth of 200 kHz. This illustrates the use of FDM for multiple access (124 channels per direction are available at 900 MHz) and duplex according to a predetermined scheme.

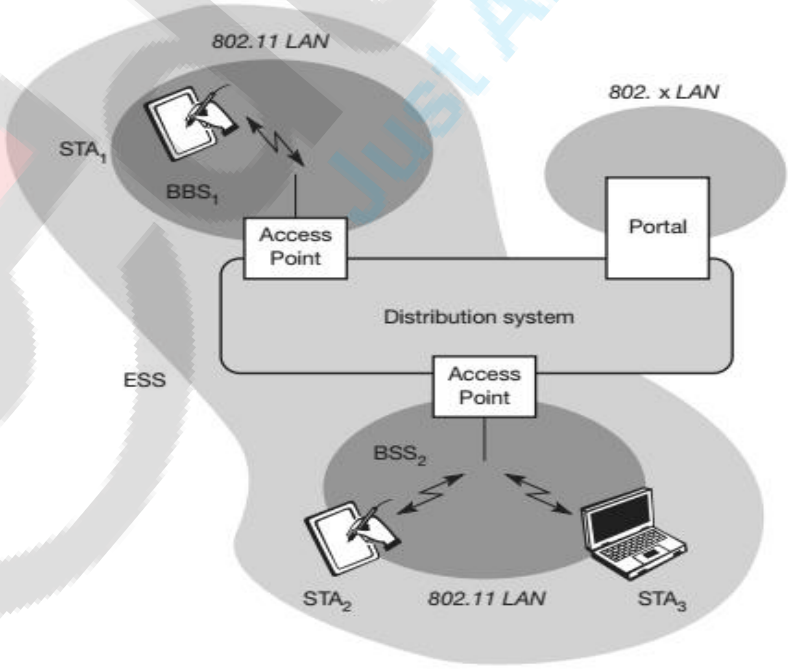
Q.6 (a) Discuss the architecture and the services provided by IEEE802.11

The IEEE standard 802.11 (IEEE, 1999) specifies the most famous family of WLANs in which many products are available. As the standard's number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. This means that the standard specifies the physical and medium access layer adapted to the special requirements of wireless LANs, but offers the same interface as the others to higher layers to maintain interoperability.

The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic. Candidates for physical layers were infrared and spread spectrum radio transmission techniques.

SYSTEM ARCHITECTURE

Wireless networks can exhibit two different basic system architectures as shown in section 7.2: infrastructure-based or ad-hoc. Figure 7.3 shows the components of an infrastructure and a wireless part as specified for IEEE 802.11.



Several nodes, called stations (STAi), are connected to access points (AP). Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. The stations and the AP which are within the same radio coverage form a basic service set (BSSi).

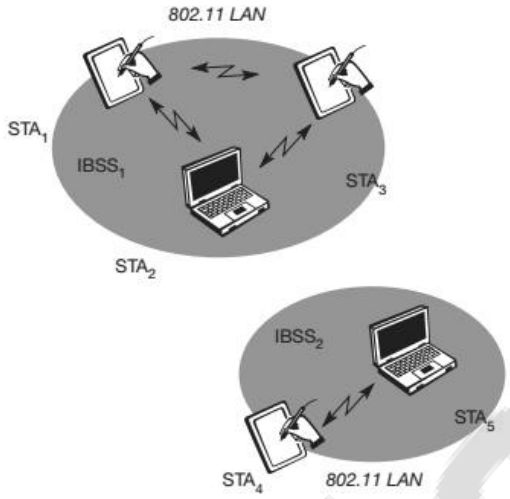
The example shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system. A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. This network is now called an extended service set (ESS) and has its own identifier, the ESSID.

The ESSID is the 'name' of a network and is used to separate different networks. Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN. The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.

The architecture of the distribution system is not specified further in IEEE 802.11. It could consist of bridged IEEE LANs, wireless links, or any other networks. However, distribution system services are defined in the standard (although, many products today cannot interoperate and needs the additional standard IEEE 802.11f to specify an inter access point protocol, see section 7.3.8).

Stations can select an AP and associate with it. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs. APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service. These and further functions are explained in the following sections.

In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) as shown in Figure 7.4. In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2.



Q6B)
What are convolutional codes? Describe the (2,1,3) convolutional code?

Convolution Codes:
Block codes are one of the two widely used categories of error correcting codes for wireless transmission; the other is convolutional codes. An *(n, k)* block code process data in blocks of *k* bits at a time, producing a block of *n* bits *(n > k)* as output for every block of *k* bits as input.

If data are transmitted and received in a more or less continuous stream, a block code, particularly one with a large value of *n*, may not be as convenient as a code that generates redundant bits continuously so that error checking and correcting are carried out continuously.

This is the function of convolution codes. A convolutional code is defined by three parameters: *n, k,* and *K.* An *(n, k, K)* code processes input data *k* bits at a time and produces an output of *n* bits for each incoming *k* bits. So far this is the same as the block code. In the case of a convolutional code, nand *k* are generally quite small numbers.

The difference is that convolutional codes have memory, which is characterized by the *constraint factor K.* In essence, the current *n-bit* output of an *(n, k, K)* code depends not only on the value of the current block of *k* input bits but also on the previous *K* – 1 blocks of *k* input bits. Hence, the current output of *n* bits is a function of the last *K* X *k* input bits.

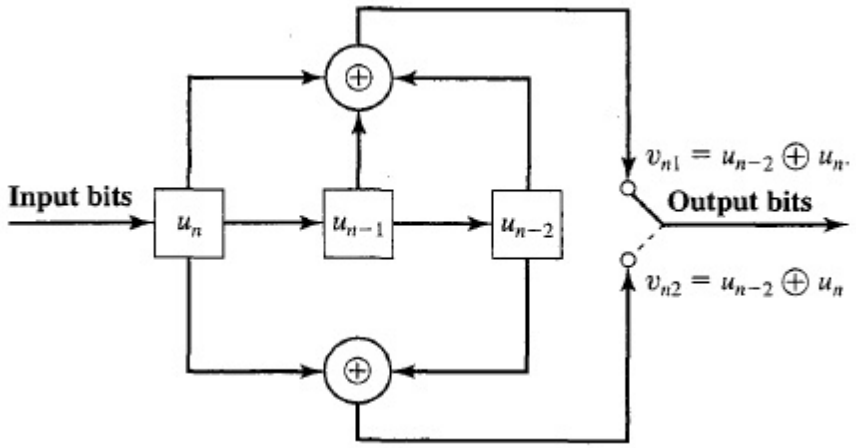
Convolutional codes are best understood by looking at a specific example For an *(n, k, K)* code, the shift register contains the most recent *K* X *k* input bits; the register is initialized to all zeros.6
The encoder produces *n* output bits, after which the oldest *k* bits from the register are discarded and *k* new bits are shifted in. Thus, although the output of *n* bits depends on *K* X *k* input bits, the rate of encoding is *n* output bits per *k* input bits. As in a block code, the code rate is therefore *kin.* The most commonly used binary encoders have *k* = 1 and hence a shift register length of *K.* Our example is of a (2, 1,3) code (Figure 8.9a).

In this example, the encoder converts an input bit *Un* into two output bits *Vnl* and *Vn2,*using the three most recent bits. The first output bit produced is from the upper logic circuit *(Vnl = Un* E9 *Un-l* E9 *Un -2),* and the second output bit from the lower logic circuit *(Vn2 = Un* Rajiv Gandhi Institute Of Technology 10 E9 *Un - 2).*

For any given input of *k* bits, there are *2k(K-l)* different functions that map the *k* input bits into *n* output bits. Which function is used depends on the history of the last *(K* - 1) input blocks of *k* bits each. We can therefore represent a convolutional code using a finite-state machine. The machine has *2k(K-l)* states, and the transition from one state to another is determined by the most recent *k* bits of inputs and produces *n* output bits.

The initial state of the machine corresponds to the all-zeros state. For our example (Figure 8.9b) there are 4 states, one for each possible pair of values for the last two bits. The next input bit causes a transition and produces an output of two bits. For example, if the last two bits were 10 *(Un-l* = 1, *Un -2* = 0) and the next bit is 1 *(Un* = 1), then the current state is state b (10) and the next state is d (11).

The output is *Vnl = Un -2* EB *Un-l* EB *Un* = 0 EB 1 EB 1 = 0 *Vn2* = 0 EB 1 = 1



Q 7

Infrared LAN

IR wireless is the use of wireless technology in devices or systems that convey data through infrared (IR) radiation.

IR wireless is the use of wireless technology in devices or systems that convey data through infrared (IR) radiation. Infrared is electromagnetic energy at a wavelength or wavelengths somewhat longer than those of red light. The shortest-wavelength IR borders visible red in the electromagnetic radiation spectrum; the longest-wavelength IR borders radio waves.

Some engineers consider IR technology to be a sub-specialty of optical technology. The hardware is similar, and the two forms of energy behave in much the same way. But strictly speaking, "optical" refers to *visible* electromagnetic radiation, while "infrared" is *invisible* to the unaided eye. To compound the confusion, IR is sometimes called "infrared light."

IR wireless is used for short- and medium-range communications and control. Some systems operate in *line-of-sight mode*; this means that there must be a visually unobstructed straight line through space between the transmitter(source) and receiver (destination). Other systems operate in *diffuse mode*, also called *scatter mode*. This type of system can function when the source and destination are not directly visible to each other. An example is a television remote-control box. The box does not have to be pointed directly at the set, although the box must be in the same room as the set, or just outside the room with the door open.

IR wireless technology is used in intrusion detectors; home-entertainment control units; robot control systems; medium-range, line-of-sight laser communications; cordless microphones, headsets, modems, and printers and other peripherals. Unlike radio-frequency (RF) wireless links, IR wireless cannot pass through walls. Therefore, IR communications or control is generally not possible between different rooms in a house, or between different houses in a neighbourhood (unless they have facing windows). This might seem like a disadvantage, but IR wireless is more private than RF wireless. Some IR wireless schemes offer a level of security comparable to that of hard-wired systems. It is difficult, for example, to eavesdrop on a well-engineered, line-of-sight, IR laser communications link.

There are three media that can be used for transmission over wireless LANs. Infrared, radio frequency and microwave. In 1985 the United States released the industrial, scientific, and medical (ISM) frequency bands. These bands are 902 - 928MHz, 2.4 - 2.4853 GHz, and 5.725 - 5.85 GHz and do not require licensing by the Federal Communications Commission (FCC). This prompted most of the wireless LAN products to operate within ISM bands. The FCC did put restrictions on the ISM bands however. In the U.S. radio frequency (RF) systems must implement spread spectrum technology. RF systems must confine the emitted spectrum to a band. RF is also limited to one watt of power. Microwave systems are considered very low power systems and must operate at 500 milli watts or less.
Infrared
Infrared systems are simple in design and therefore inexpensive. They use the same signal frequencies used on fiber optic links. IR systems detect only the amplitude of the signal and so interference is greatly reduced. These systems are not bandwidth limited and thus can achieve transmission speeds greater than the other systems. Infrared transmission operates in the light spectrum and does not require a license from the FCC to operate, another attractive feature. There are two conventional ways to set up an IR LAN. The infrared transmissions can be aimed. This gives a good range of a couple of kilometre and can be used outdoors. It also offers the highest bandwidth and throughput. The other way is to transmit Omni-directionally and bounce the signals off of everything in every direction. This reduces coverage to 30 - 60 feet, but it is an area coverage. IR technology was initially very popular because it delivered high data rates and relatively cheap price. The drawbacks to IR systems are that the transmission spectrum is shared with the sun and other things such as fluorescent lights. If there is enough interference from other sources it can render the LAN useless. IR systems require

an unobstructed line of sight (LOS). IR signals cannot penetrate opaque objects. This means that walls, dividers, curtains, or even fog can obstruct the signal. Infra LAN is an example of wireless LANs using infrared technology.

An alternative approach to radio-based wireless L ANs is infrared communications. Infrared networking uses electromagnetic radiation with wavelengths of 820 to 890 Nano meters, corresponding to a frequency of about 350,000 GHz. The advantages of IR include no need for licenses, no safety issues, huge potential capacity and good control of interference. IR does not penetrate walls, so infrared LANs must be contained in a room. Note that IR LANs generally do not operate in outdoor areas where there is sunlight. IR transmitters and receivers can be designed either for directional use or for diffuse use, where signals bounce off walls and other objects to reach the receiver. In fact, IR is specified as one of the physical layer options in the new IEEE 802.11 standard.
Though it is a promising technology, there are relatively few IR LAN products available today. But one type of infrared technology that has been broadly deployed is the use of IR for short point-to-point connections following standards specified by the Infrared Data Association.

Piconets and Scatternets

Definition - What does *Piconet* mean?

A piconet is a network of devices connected using Bluetooth technology. The network ranges from two to eight connected devices. When a network is established, one device takes the role of the master while all the other devices act as slaves.

Piconet gets its name from the word "pico", which means very small. This very small network is so called because the number is limited to seven devices, plus the master, which limits network and data sharing capability. Data transfer rates vary from 200 to 2,100 kbps at the application.

A piconet is sometimes called a personal area network (PAN) because the range of optimal operation for Bluetooth is 10 meters, about the size of a living room.

Piconet

A piconet is usually implemented with small mobile devices or home devices that need to communicate with each other.

A good example of a piconet is the Playstation 3 (PS3) console gaming system. Instead of having wired controllers, the PS3 implements Bluetooth technology to connect up to four controllers at the same time. The main console acts as the master and the controllers act as slaves. Newer home appliances are also able to communicate through Bluetooth.

Definition - What does *Scatternet* mean?

A scatternet is a type of network that is formed between two or more Bluetooth-enabled devices, such as smartphones and newer home appliances. A scatternet is made up of at least two piconets.

Bluetooth devices are peer units that act as slaves or masters. Scatternets are formed when a device in a piconet, whether a master or a slave, decides to participate as a slave to the master of another piconet. This device then becomes the bridge between the two piconets, connecting both networks.

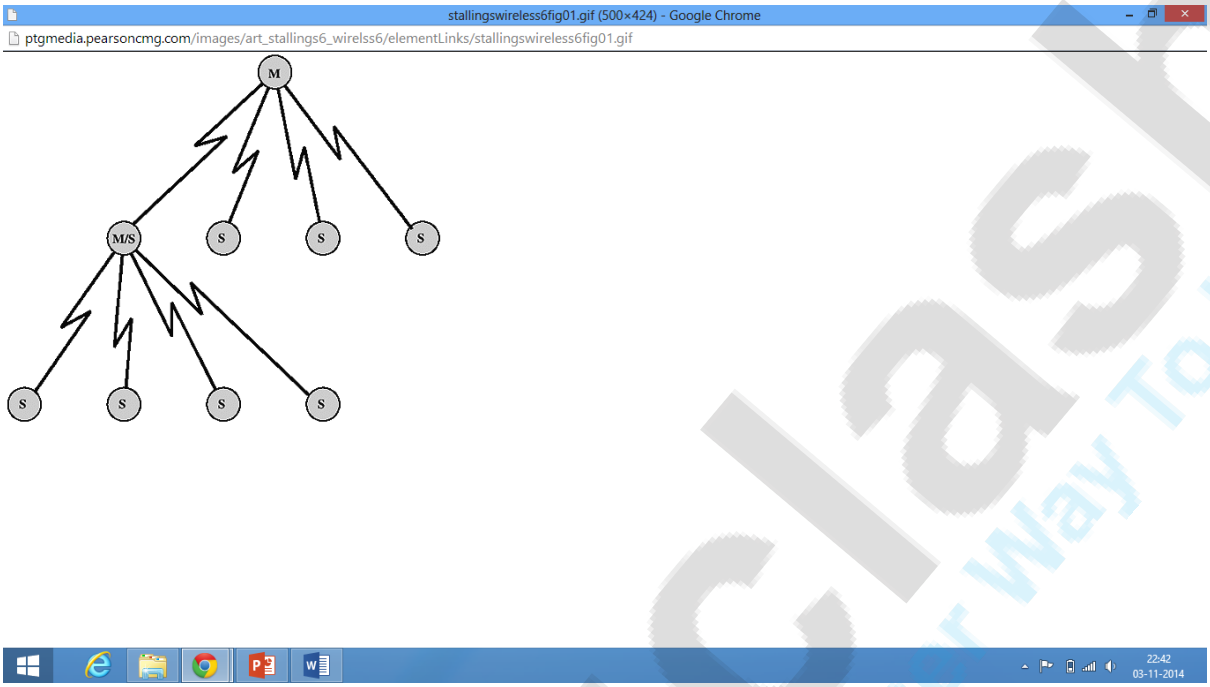
Scatternet

In order for a scatternet to form, one Bluetooth unit must submit as a slave to another piconet to become a bridge for both networks. If the master of a piconet is the bridge to another piconet, it functions as a slave in the other piconet, even though it is a master of its own piconet. The device participating in both piconets can relay data between members of both networks.

However, basic Bluetooth protocol does not support this type of relay, so the host software of each device needs to manage it. Using this approach, it is possible to join together numerous piconets into a large scatternet, and to expand the physical size of the network beyond Bluetooth's limited range. A scatternet can thus support communication between more than eight devices, which is the limit for a piconet.

The value of scatternets is still being discovered, but a valuable function could be communication between small robots. The robots could connect to each other, with one acting as the master and the others as slaves. Different teams of piconets could

form larger scatternets for more thorough coverage of an area. This type of scatternet could have potential uses in bomb disposal and search and rescue.



As mentioned earlier, the basic unit of networking in Bluetooth is a piconet, consisting of a master and from one to seven active slave devices. The radio designated as the master makes the determination of the channel (frequency-hopping sequence) and phase (timing offset—that is, when to transmit) that will be used by all devices on this piconet. The radio designated as master makes this determination using its own device address as a parameter, while the slave devices must tune to the same channel and phase. A slave may only communicate with the master and may only communicate when granted permission by the master. A device in one piconet may also exist as part of another piconet and may function as either a slave or master in each piconet (see Figure 1). This form of overlapping is called a *scatternet*. Figure 2 contrasts the piconet-scatternet architecture with other forms of wireless networks.

Figure 1 Master/slave relationships.

Figure 2 Wireless network configurations.

The advantage of the piconet/scatternet scheme is that it allows many devices to share the same physical area and make efficient use of the bandwidth. A Bluetooth system uses a frequency-hopping scheme with a carrier spacing of 1 MHz. Typically, up to 80 different frequencies are used, for a total bandwidth of 80 MHz. If frequency hopping isn't used, a single channel would correspond to a single 1 MHz band. With frequency hopping, a logical channel is defined by the frequency-hopping sequence. At any given time, the bandwidth available is 1 MHz, with a maximum of eight devices sharing the bandwidth. Different logical channels (different hopping sequences) can simultaneously share the same 80 MHz bandwidth. Collisions will occur when devices in different piconets, on different logical channels, happen to use the same hop frequency at the same time. As the number of piconets in an area increases, the number of collisions increases, and performance degrades. In summary, the physical area and total bandwidth are shared by the scatternet. The logical channel and data transfer are shared by a piconet.

Antenna

An antenna (or aerial) is an electrical device which converts electric power into radio waves, and vice versa.[1] It is usually used with a radio transmitter or radio receiver. In transmission, a radio transmitter supplies an electric current oscillating at radio frequency (i.e. a high frequency alternating current (AC)) to the antenna's terminals, and the antenna radiates the energy from the current aselectromagnetic waves (radio waves). In reception, an antenna intercepts some of the power of an electromagnetic wave in order to produce a tiny voltage at its terminals, that is applied to a receiver to be amplified.
Antennas are essential components of all equipment that uses radio. They are used in systems such as radio broadcasting,broadcast television, two-way radio, communications receivers, radar, cell phones, and satellite communications, as well as other devices such as garage door openers, wireless microphones, Bluetooth-enabled devices, wireless computer networks, baby monitors, and RFID tags on merchandise.
Typically an antenna consists of an arrangement of metallic conductors (elements), electrically connected (often through atransmission line) to the receiver or transmitter. An oscillating current of electrons forced through the antenna by a

transmitter will create an oscillating magnetic field around the antenna elements, while the charge of the electrons also creates an oscillating electric field along the elements. These time-varying fields radiate away from the antenna into space as a moving transverse electromagnetic field wave. Conversely, during reception, the oscillating electric and magnetic fields of an incoming radio wave exert force on the electrons in the antenna elements, causing them to move back and forth, creating oscillating currents in the antenna.

Antennas can be designed to transmit and receive radio waves in all horizontal directions equally (omnidirectional antennas), or preferentially in a particular direction (directional or high gain antennas). In the latter case, an antenna may also include additional elements or surfaces with no electrical connection to the transmitter or receiver, such as parasitic elements, parabolic reflectors or horns, which serve to direct the radio waves into a beam or other desired radiation pattern.

According to their applications and technology available, antennas generally fall in one of two categories:

1. Omnidirectional or only weakly directional antennas which receive or radiate more or less in all directions. These are employed when the relative position of the other station is unknown or arbitrary. They are also used at lower frequencies where a directional antenna would be too large, or simply to cut costs in applications where a directional antenna isn't required.
2. Directional or *beam* antennas which are intended to preferentially radiate or receive in a particular direction or directional pattern.

In common usage "omnidirectional" usually refers to all horizontal directions, typically with reduced performance in the direction of the sky or the ground (a truly isotropic radiator is not even possible). A "directional" antenna usually is intended to maximize its coupling to the electromagnetic field in the direction of the other station, or sometimes to cover a particular sector such as a 120° horizontal fan pattern in the case of a panel antenna at a cell site.

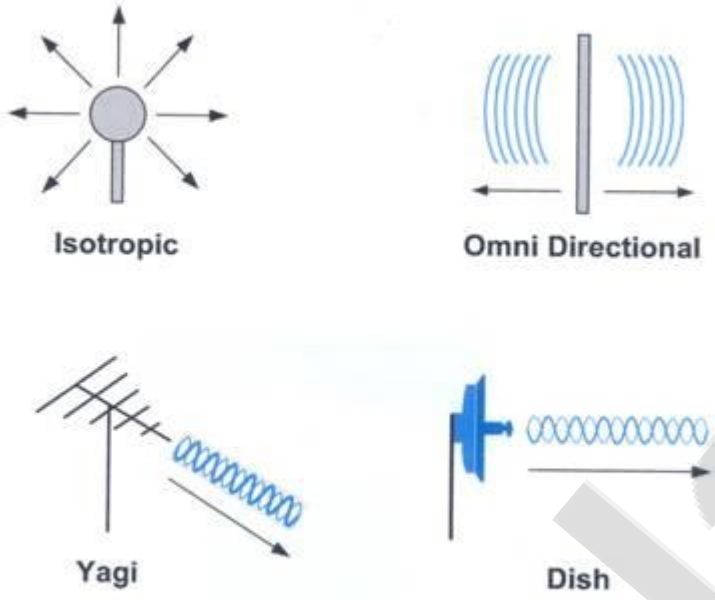


Figure 3 – WiFi Antenna Types

Time-division duplexing

Definition - What does *Time Division Duplex (TDD)* mean?

Time division duplex (TDD) refers to duplex communication links where uplink is separated from downlink by the allocation of different time slots in the samefrequency band. It is a transmission scheme that allows asymmetric flow for uplink and downlink data transmission. Users are allocated time slots for uplink and downlink transmission.

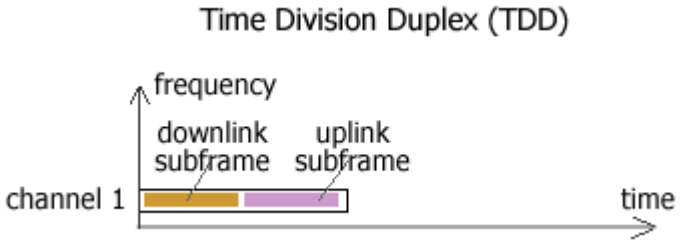
Time division multiplexing separates uplink and downlink signals by matching full duplex communication over a half-duplex communication link. This method is highly advantageous in case there is an asymmetry of uplink and downlink data rates. TDD divides a data stream into frames and assigns different time slots to forward and reverse transmissions, thereby allowing both types of transmissions to share the same transmission medium.

Time Division Duplex (TDD)

When data over uplink increases, more communication capacity is allocated. This is taken away when the traffic load becomes lighter. It operates by toggling transmission directions over a time interval, which occurs rapidly and is barely visible to the user. TDD supports voice and symmetrical as well as asymmetric data services. It also handles a dynamic mix of both traffic types. The capacities of downlinks and uplinks are altered in favor of one direction over another by providing greater time allocation through time slots to downstream transmission intervals than to upstream ones.

Well known examples of TDD are:

- Half-duplex packet mode networks based on carrier sense multiple access
- IEEE 802.16 WiMAX
- PACTOR
- Digital enhanced cordless telecommunications (DECT) wireless telephony
- Universal Mobile Telecommunications System 3G supplementary air interfaces
- TD-CDMA for indoor mobile telecommunications
- TD-SCDMA 3G mobile telephony air interface



Time-division duplexing (TDD) is the application of time-division multiplexing to separate outward and return signals. It emulates full duplex communication over a half duplex communication link.

Time-division duplexing has a strong advantage in the case where there is asymmetry of the uplink and downlink data rates. As the amount of uplink data increases, more communication capacity can be dynamically allocated, and as the traffic load becomes lighter, capacity can be taken away. The same applies in the downlink direction.

For radio systems that aren't moving quickly, another advantage is that the uplink and downlink radio paths are likely to be very similar. This means that techniques such asbeamforming work well with TDD systems.

Examples of time-division duplexing systems are:

- UMTS 3G supplementary air interfaces TD-CDMA for indoor mobile telecommunications.
- The Chinese TD-LTE 4-G, TD-SCDMA 3-G mobile communications air interface.
- DECT wireless telephony
- Half-duplex packet switched networks based on carrier sense multiple access, for example 2-wire or hubbed Ethernet, Wireless local area networks and Bluetooth, can be considered as Time Division Duplexing systems, albeit not TDMA with fixed frame-lengths.
- IEEE 802.16 WiMAX
- PACTOR
- ISDN BRI U interface, variants using the Time Compression Multiplex (TCM) line system
- G.fast, a digital subscriber line (DSL) standard under development by the ITU-T

Time Division Duplex

TDD uses a single frequency band for both transmit and receive. Then it shares that band by assigning alternating time slots to transmit and receive operations *(Fig. 3)*. The information to be transmitted—whether it's voice, video, or computer data—is in serial binary format. Each time slot may be 1 byte long or could be a frame of multiple bytes.

TDD alternates the transmission and reception of station data over time. Time slots may be variable in length.

Because of the high-speed nature of the data, the communicating parties cannot tell that the transmissions are intermittent. The transmissions are concurrent rather than simultaneous. For digital voice converted back to analog, no one can tell it isn't full duplex.

In some TDD systems, the alternating time slots are of the same duration or have equal DL and UL times. However, the system doesn't have to be 50/50 symmetrical. The system can be asymmetrical as required.

For instance, in Internet access, download times are usually much longer than upload times so more or fewer frame time slots are assigned as needed. Some TDD formats offer dynamic bandwidth allocation where time-slot numbers or durations are changed on the fly as required.

The real advantage of TDD is that it only needs a single channel of frequency spectrum. Furthermore, no spectrum-wasteful guard bands or channel separations are needed. The downside is that successful implementation of TDD needs a very precise timing and synchronization system at both the transmitter and receiver to make sure time slots don't overlap or otherwise interfere with one another.

Timing is often synched to precise GPS-derived atomic clock standards. Guard times are also needed between time slots to prevent overlap. This time is generally equal to the send-receive turnaround time (transmit-receive switching time) and any transmission delays (latency) over the communications path.

Application Examples

Most cell-phone systems use FDD. The newer LTE and 4G systems use FDD. Cable TV systems are fully FDD.

Most wireless data transmissions are TDD. WiMAX and Wi-Fi use TDD. So does Bluetooth when piconets are deployed. ZigBee is TDD. Most digital cordless

telephones use TDD. Because of the spectrum shortage and expense, TDD is also being adopted in some cellular systems, such as China's TD-SCDMA and TD-LTE systems. Other TD-LTE cellular systems are expected to be deployed where spectrum shortages occur.

Conclusion

TDD appears to be the better overall choice, but FDD is far more widely implemented because of prior frequency spectrum assignments and earlier technologies. FDD will continue to dominate the cellular business for now. Yet as spectrum becomes more costly and scarce, TDD will become more widely adopted as spectrum is reallocated and repurposed.

Fading

In wireless communications, fading is deviation of the attenuation affecting a signal over certain propagation media. The fading may vary with time, geographical position or radio frequency, and is often modeled as a random process. A fading channel is a communication channel comprising fading. In wireless systems, fading may either be due to multipath propagation, referred to as multipath induced fading, or due to shadowing from obstacles affecting the wave propagation, sometimes referred to as shadow fading.

Slow versus fast fading

The terms *slow* and *fast* fading refer to the rate at which the magnitude and phase change imposed by the channel on the signal changes. The coherence time is a measure of the minimum time required for the magnitude change or phase change of the channel to become uncorrelated from its previous value.

Slow fading arises when the coherence time of the channel is large relative to the delay constraint of the channel. In this regime, the amplitude and phase change imposed by the channel can be considered roughly constant over the period of use. Slow fading can be caused by events such as shadowing, where a large obstruction such as a hill or large building obscures the main signal path between the transmitter and the receiver. The received power change caused by shadowing is often modeled using a log-normal distribution with a standard deviation according to the log-distance path loss model.

Fast fading occurs when the coherence time of the channel is small relative to the delay constraint of the channel. In this regime, the amplitude and phase change imposed by the channel varies considerably over the period of use.

In a fast-fading channel, the transmitter may take advantage of the variations in the channel conditions using time diversity to help increase robustness of the communication to a temporary deep fade. Although a deep fade may temporarily erase some of the information transmitted, use of an error-correcting code coupled with successfully transmitted bits during other time instances (interleaving) can allow for the erased bits to be recovered. In a slow-fading channel, it is not possible to use time diversity because the transmitter sees only a single realization of the channel within its delay constraint. A deep fade therefore lasts the entire duration of transmission and cannot be mitigated using coding.

The coherence time of the channel is related to a quantity known as the Doppler spread of the channel. When a user (or reflectors in its environment) is moving, the

user's velocity causes a shift in the frequency of the signal transmitted along each signal path. This phenomenon is known as the Doppler shift. Signals traveling along different paths can have different Doppler shifts, corresponding to different rates of change in phase. The difference in Doppler shifts between different signal components contributing to a single fading channel tap is known as the Doppler spread. Channels with a large Doppler spread have signal components that are each changing independently in phase over time. Since fading depends on whether signal components add constructively or destructively, such channels have a very short coherence time.

In general, coherence time is inversely related to Doppler spread, typically expressed as $T_c \approx \frac{1}{D_s}$ where T_c is the coherence time, D_s is the Doppler spread. This equation is just an approximation,[1] to be exact, see Coherence time.Block fading

Block fading is where the fading process is approximately constant for a number of symbol intervals. [2] A channel can be 'doubly block-fading' when it is block fading in both the time and frequency domains.[3]

Selective fading

Selective fading or frequency selective fading is a radio propagation anomaly caused by partial cancellation of a radio signal by itself — the signal arrives at the receiver by two different paths, and at least one of the paths is changing (lengthening or shortening). This typically happens in the early evening or early morning as the various layers in the ionosphere move, separate, and combine. The two paths can both be sky wave or one be ground wave.

Selective fading manifests as a slow, cyclic disturbance; the cancellation effect, or "null", is deepest at one particular frequency, which changes constantly, sweeping through the received audio.

As the carrier frequency of a signal is varied, the magnitude of the change in amplitude will vary. The coherence bandwidth measures the separation in frequency after which two signals will experience uncorrelated fading.

- In flat fading, the coherence bandwidth of the channel is larger than the bandwidth of the signal. Therefore, all frequency components of the signal will experience the same magnitude of fading.

- In frequency-selective fading, the coherence bandwidth of the channel is smaller than the bandwidth of the signal. Different frequency components of the signal therefore experience uncorrelated fading.

Since different frequency components of the signal are affected independently, it is highly unlikely that all parts of the signal will be simultaneously affected by a deep fade. Certain modulation schemes such as orthogonal frequency-division multiplexing (OFDM) and code division multiple access (CDMA) are well-suited to employing frequency diversity to provide robustness to fading. OFDM divides the wideband signal into many slowly modulated narrowband subcarriers, each exposed to flat fading rather than frequency selective fading. This can be combated by means of error coding, simple equalization or adaptive bit loading. Inter-symbol interference is avoided by introducing a guard interval between the symbols. CDMA uses the rake receiver to deal with each echo separately.
Frequency-selective fading channels are also *dispersive*, in that the signal energy associated with each symbol is spread out in time. This causes transmitted symbols that are adjacent in time to interfere with each other. Equalizers are often deployed in such channels to compensate for the effects of the intersymbol interference.

The echoes may also be exposed to Doppler shift, resulting in a time varying channel model.
The effect can be counteracted by applying some diversity scheme, for example OFDM (with subcarrier interleaving and forward error correction), or by using two receivers with separate antennas spaced a quarter-wavelength apart, or a specially designed diversity receiver with two antennas. Such a receiver continuously compares the signals arriving at the two antennas and presents the better signal.