CMR
INSTITUTE OF
TECHNOLOGY

USN

Internal Assesment Test - III

Sub:	Wireless Communication							Code:	10EC81
Date:	21/ 05 / 2018	Duration:	90 mins	Max Marks:	50	Sem:	8th	Branch:	ECE (A,B)
Answer Any FIVE FULL Questions									

	Marks	OBE CO	OBE RBT
1. Draw and describe frame structure for general and management MAC frame format in 802.11. Also explain the 2 byte control field.	[10]	CO5	L2

Soln:

The IEEE 802.11 standard specifies the format of the MAC frames. Any equipment that is compatible with this standard is able to properly construct frames for transmission and decode frames upon reception. Each MAC frame consists of the following basic components: a MAC header, a variable length frame body, and a frame check sequence (FCS). The MAC header consists of several fields including frame control, duration, address, and sequence control information. The frame body contains information that is specific to the frame type. The FCS contains an IEEE 32-bit cyclic redundancy code (CRC). Figure 9–8 shows the general structure of a MAC frame format and a management MAC frame example. The fields labeled address 2, address 3, sequence control, address 4, and frame body are only present in certain types of frames. Within an individual frame field, there typically exist subfields that are used to provide additional information. 2m

General MAC Frame Format

2 (Bytes)	2	6	6	6	2	2	0–2312 Bytes	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

← MAC Header - 30 Bytes →

Management MAC Frame Format

2 (Bytes)	2	6	6	6	2	0–2312 Bytes	4
Frame Control	Duration	DA	SA	BSSID	Sequence Control	Frame Body	FCS

← MAC Header →

3m

Figure 9–8 Examples of IEEE 802.11 MAC frame formats (Courtesy of IEEE).

2 (Bits)	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

← Frame Control Field (2 Bytes - 16 Bits) →

2m

Figure 9–9 Further details of the frame control field of the MAC frame (Courtesy of IEEE).

Figure 9–9 shows the structure of the frame control field (i.e., the first 2 bytes of the MAC frame). As one can see, further information can be encoded into the control frame subfields that can even consist of 1-bit fields. For further details of the meanings and possible encodings for these fields one should look at the most recent version of the IEEE 802.11 standard. This work will not go into that fine amount of detail.

Returning to the general MAC frame format shown by Figure 9–8, a few comments about the address, sequence, and frame body fields are appropriate here. The four address fields in the MAC frame format are used to indicate the basic service set identifier (BSSID), destination address (DA), source address (SA), receiver address (RA), and transmitter address (TA) (although not all at the same time). Furthermore, some types of MAC frames may not contain some of the address fields just mentioned. Each address field is 48 bits in length and can therefore use 48-bit IEEE 802 MAC addresses to indicate an individual station on the network or a group address. The group address can be one of two types, either a multicast group or a broadcast group (i.e., all of the stations presently active in the wireless LAN). The BSSID field is used to uniquely identify each BSS. For a typical wireless LAN, the value of this field is the MAC address currently in use by the station portion of the AP or APs of the WLAN. The sequence field consists of 16 bits that are composed of two subfields of 4 bits and 12 bits. The 12 bit field provides a sequence number for each MSDU and the 4-bit field provides a MSDU fragment number, if needed. The frame body field has a minimum length of 0 bytes and as shown in the figure can be as long as 2312 bytes. 3m

2. Discuss various coding techniques used in wireless communication. [10] CO4 L2

Soln: Wireless radio channel is most unreliable and random characteristics channels. Hence it is necessary to make the signal more robust before it is transmitting through wireless channels. **At transmitter** increase the transmitted signal's immunity to radio channel noise and other channel impairments like fading and multipath spread. In digitally based systems, techniques correspond to an attempt to realize a reduction in bit errors and frame errors. The best strategy is to employ some form of error detection and correction codes to reduce the required number of requests for retransmission by the system when errors cannot be corrected. Error correction may generally be realized in two different ways:

- Automatic repeat request (ARQ) (sometimes also referred to as backward error correction): This is an error control technique whereby an error detection scheme is combined with requests for retransmission of erroneous data. Every block of data received is checked using the error detection code used, and if the check fails, retransmission of the data is requested – this may be done repeatedly, until the data can be verified.
- Forward error correction (FEC): The sender encodes the data using an error-correcting code (ECC) prior to transmission. The additional information (redundancy) added by the code is used by the receiver to recover the original data. 1m

Different codes are used to enhance the transmission of packet data over wireless systems.

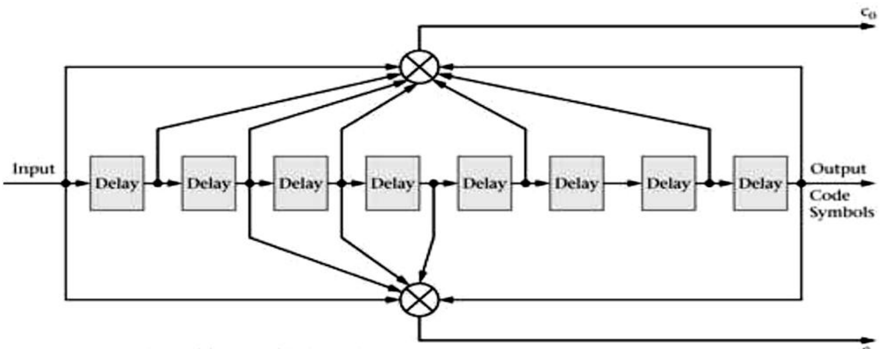
- **Block codes**
- **Convolutional codes**
- **Turbo codes**
- **Speech coders**

Block codes: System takes a block of data bits and encodes them into another block of bits with some additional bits that are used to detect or combat errors. Block codes are processed on a block-by-block basis.

- Using more sophisticated techniques, additional bits may be generated through a matrix or polynomial generator and added to the original block of bits to form a codeword that will be eventually transmitted by the system.
- A codeword generated by a polynomial is a form of cyclic code – codes of this type are known as Cyclic Redundancy Check (CRC) codes.
- Consequently, the block coder is a *memoryless* device
- In block coding, divide message into blocks, each of k bits, called datawords and add 'r' redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called codeword
- Additional bits 'r' may be generated through a matrix or Polynomial generator (eg. CRC code) and added to the original block of bits to form a codeword that will be eventually transmitted by a system. 2m
- Depending upon the type of coding level employed these schemes can both detect and correct limited numbers of errors.

Convolutional codes

- Convolutional codes are applied in applications that require good performance with low implementation complexity.
- They operate on code streams (not in blocks)
- It maps information to code bits sequentially by convolving a sequence of information bits with "generator".
- k & n are very small (usually k=1-3, n=2-6)
- Input depends not only on current set of k input bits, but also on past input.
- In cdma2000 system a convolutional encoder with R=1/3 and K=9 is used.
- In practice, the use of convolutional encoders provides better FEC capabilities than available from block codes.
- Figure shows in block diagram form an implementation of a convolutional encoder (with K=9 and R=1/2) specified for use in cdma2000



Rate 1/2, $K = 9$ Convolutional Encoder

3m

Turbo encoder

- Turbo encoders are a modified form of combined convolutional encoders that can be used to create a new class of enhanced error correction codes.
- It is constructed from two systematic, recursive convolutional encoders connected in parallel with an interleaver preceding the input to the second convolutional encoder.
- The output bit steams of the two convolutional encoders are multiplexed together and repeated to form the final code symbols.
- For cdma2000, Rate 1/2, 1/3, 1/4 and 1/5 turbo encoders are employed instead of convolutional encoders for various higher-bit transfer rates and radio configurations 2m

Speech coders:

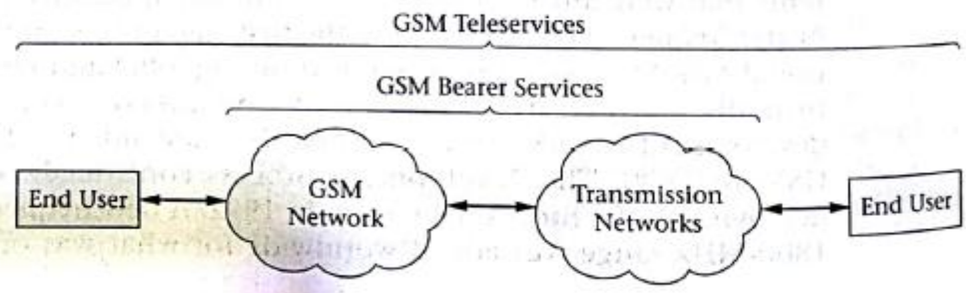
The speech coders used for both GSM and CDMA wireless system. Speech coder take 20-msec segments and process it into lower-bit-rate digitally encoded speech in preparation for its transmission over the air interface

Two broad classifications of speech coders:

1. **Waveform coders**:
   - PCM is a type of coding that is called "waveform" coding because it creates a coded form of the original voice waveform.
   - they do not provide as high a compression ratio as the latter category of speech coders
   - Example PCM at the 64kbps data rate.
2. **Vocoders**:
   - is a category of voice codec that analyzes and synthesizes the human voice signal for audio data compression, multiplexing, voice encryption, voice transformation etc 2m
   - The vocoder examines speech by measuring how its spectral characteristics change over time
   - EX: the Regular Pulse Excitation-Long Term Prediction (RPE-LTP) encoder used in GSM to reduce the amount of data sent between the mobile station (MS) and base transceiver station (BTS).

3. (a) Explain briefly service provided by GSM. [6] CO3 L4

Soln:



2m

Relationship of teleservices and bearer services to the GSM system (Courtesy of ETSI).

Service Category	Service	Additional Details
GSM Teleservices	Telephony Emergency calls Short Message Service Videotext access Teletex, FAX, etc.	Full rate at 13 kbps voice "112" is GSM-wide emergency number Point-to-point (between two users) and cell broadcast types
GSM Bearer Services	Asynchronous data Synchronous data Synchronous packet data Others	300–9600 bps (transparent/nontransparent) 2400–9600 bps transparent
Supplementary Services	Call forwarding Call barring	All calls, when the subscriber is not available Outgoing calls with specifications

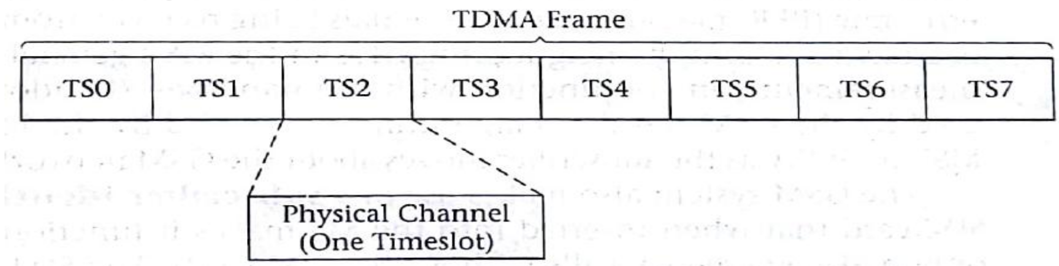
2m

TABLE 5–1 Phase 1 GSM services (Courtesy of ETSI).

Service Category	Service	Additional Details
GSM Teleservices	Half-rate speech coder Enhanced full rate	Optional implementation
Supplementary Services	Calling line identification Connected line identification Call waiting Call hold Multiparty communications Closed user group Advice of charge Operator determined call barring	Presentation or restriction of displaying the caller's ID Presentation or restriction of displaying the called ID Incoming call during current conversation Put current call on hold to answer another Up to five ongoing calls can be included in one conversation Restriction of certain features from individual subscribers by operator

TABLE 5–2 Phase 2 GSM services (Courtesy of ETSI). 2m

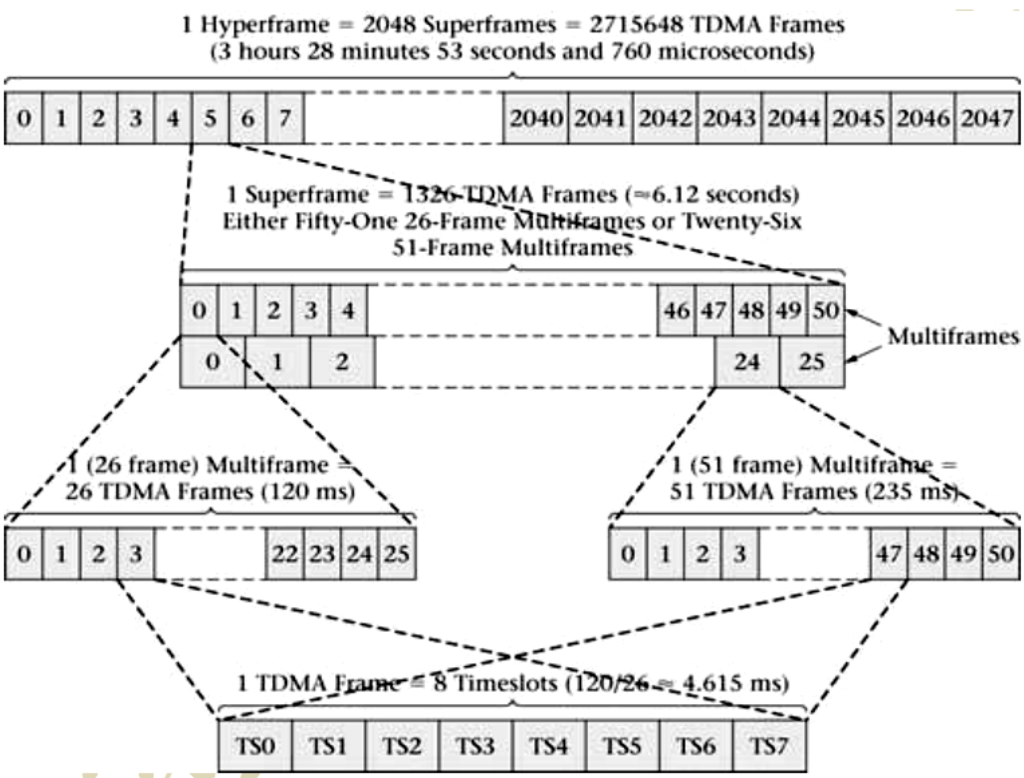
(b) Draw and explain GSM TDMA frame with logical channel. [4] CO3 L4



2m

For a particular carrier frequency , a channel consists of a single timeslot that occurs during a TDMA frame of eight timeslots. (More explanation : Refer Mullet)
Each of these timeslots represents a physical channel 2m

4. Draw and describe the structure of TDMA frame, multiframe, superframe and hyperframe. Specify their time lengths. [10] CO3 L2



5m

- GSM system , both traffic and signaling and control information are transmitted over the physical frequency channel. (More explanation : Refer Mullet) 5m
- To accomplish this time division multiplexing is used.

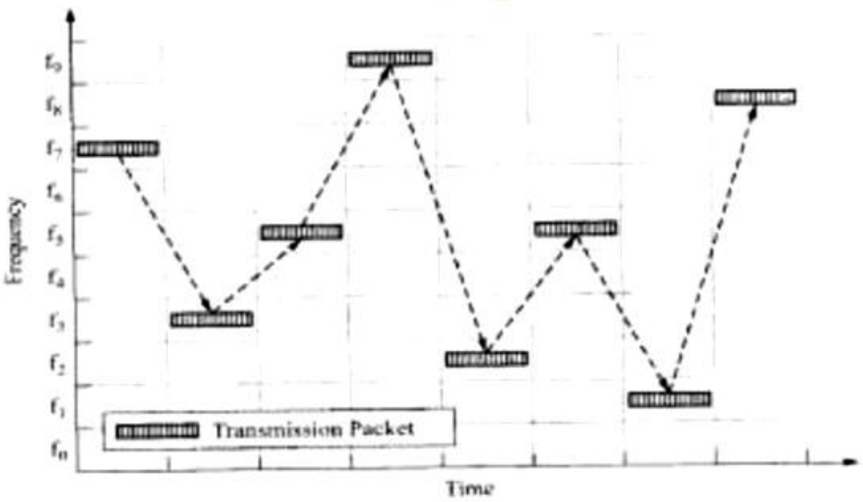
5. Briefly explain the spread spectrum modulation techniques: FHSS and DSSS. [10] CO4 L4

There are two basic ways of implementing spread spectrum transmission:

- 1. Frequency Hopping Spread Spectrum (FHSS)
- 2. Direct Sequence Spread Spectrum (DSSS).

Frequency-hopping spread spectrum (FHSS) transmission is the repeated switching of frequencies during radio transmission to reduce interference and avoid interception. It is useful to counter eavesdropping, or to obstruct jamming of telecommunications. It can minimize the effects of unintentional interference. It consists of a system that changes the center frequency of transmission on a periodic basis with a pseudorandom sequence.

Here data are transmitted through number of different carrier frequencies hops. All the carrier frequencies hop independent from one another. For the system to work both the transmitter and receiver must have prior knowledge of the hopping sequence. In a frequency-hopping spread spectrum (FHSS) system, the transmitted signal is spread across multiple channels. Ex: The full bandwidth is divided into 8 channels, centered at f_0 through f_9. The signal "hops" between them in the following sequence: f_7, f_3, f_5, f_9, f_2, f_5, f_1, f_8. 3m



Frequency hopping spread spectrum example. 3m

- Direct Sequence Spread Spectrum (DSSS) is a spread spectrum technique whereby the original data signal is multiplied with a pseudo random noise spreading code.
- This spreading code has a higher chip rate (this the bit rate of the code), which results in a wideband time continuous scrambled signal.
- DSSS significantly improves protection against interfering (or jamming) signals, especially narrowband and makes the signal less noticeable. 4m
- It also provides security of transmission if the code is not known to the public.
- These reasons make DSSS very popular by the military. In fact, DSSS was first used in the 1940s by the military

6. Explain working of BSS, DS and ESS network with neat diagrams. [10] CO5 L4

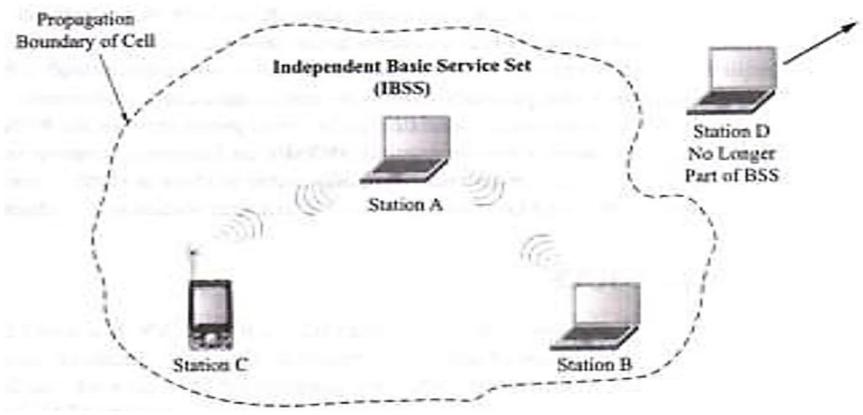


Figure 9–2 A typical independent basic service set.

2m

The **Basic Service Set** (BSS) is the simplest and most fundamental structure of an IEEE 802.11x WLAN.

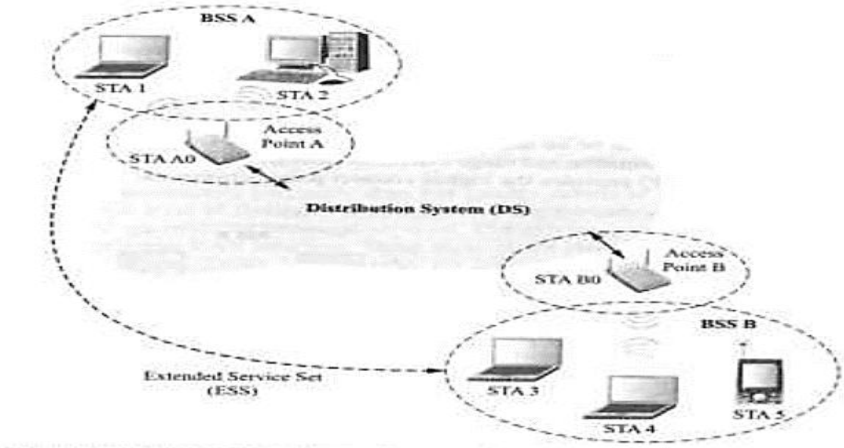
Architecture description:

There is no backbone infrastructure and the network consists of at least two wireless stations. BSS structure is referred to as a peer-to-peer or ad hoc wireless network. The propagation boundary will exist but its exact extent and shape are subject to many variables. Simulation software exists that can provide some reasonable estimates of RSS for typical multi-floor architectural layouts and various building materials. It is also possible to have two or more of these IBSSs in existence and operational within the same general area but not in communication with one another. An STA may be turned on or off or come into or go out of range of the BSS an unlimited number of times. The STA becomes a member of the BSS structure when it becomes associated with the BSS. 1m

Distribution System (DS)

It provides an extended wireless network consisting of multiple BSSs.To provide flexibility to the WLAN architecture, IEEE 802.11 logically separates the wireless medium (WM) from the Distribution System Medium (DSM). The function of the DS is enable mobile device support. It provides seamless integration of multiple BSSs. This function is physically performed by a device known as an access point (AP). The AP provides access in the DS by providing DS services and at the same time performing the STA function within the BSS. 1m

Data transfers occur between stations within a BSS and the DS via an AP.
All the APs are also stations and as such have addresses. However, the address used by an AP for data communications on the WM side and the one used on the DSM side are not necessarily one and the same. This DS structure gives rise to the use of APs as bridges to extend the reach of a network.

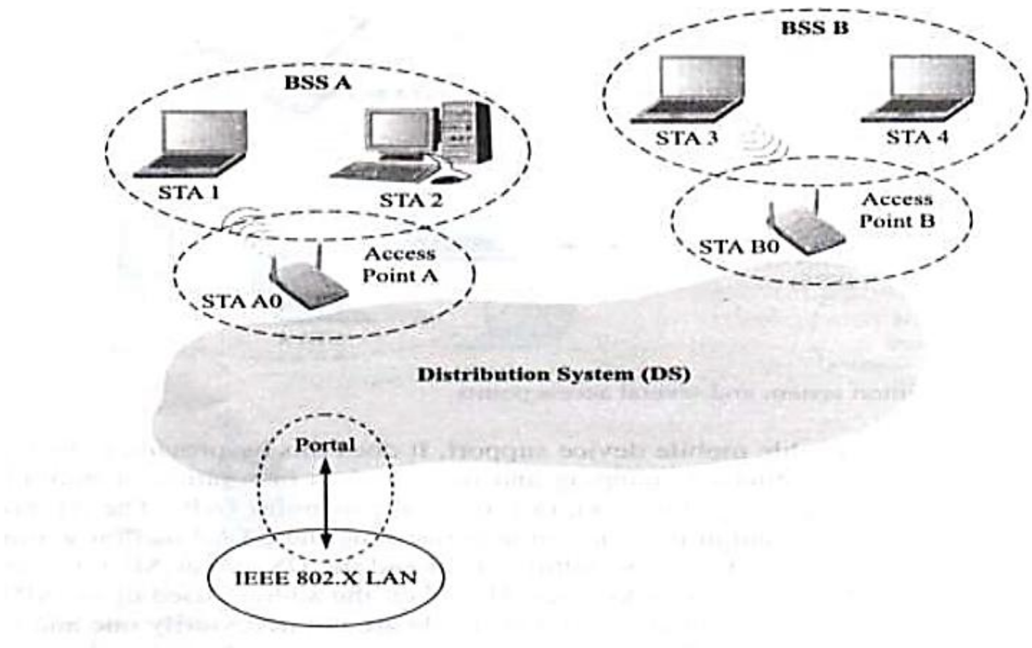


A typical distribution system and several access points.]

2m

Extended Service Set (ESS)

The IEEE 802.11 standard provides for the use of multiple BSSs and a DS to create a wireless network of arbitrary size and complexity networks are known as extended service set (ESS) networks. ESS networks provide advantages, so that stations within an ESS network may communicate with one another and mobile stations may move transparently from one BSS to another as long as they are all part of the same ESS network. The most basic BSS consists of one AP and one STA.



A wireless LAN with a connection to an IEEE 802.x wired LAN.

Due to use of an ESS network the following situations may occur: 4m

- BSSs may overlap to provide continuous coverage areas or BSSs can be physically separate entities
- BSSs may be physically collocated for redundancy reasons, and one or more ESS networks may be physically located in the same area.
- The above situation can commonly occur when separate organizations set up their own WLANs in close proximity to one another.

7. Describe Bluetooth protocol stack with relevant figures. [10] CO5 L3

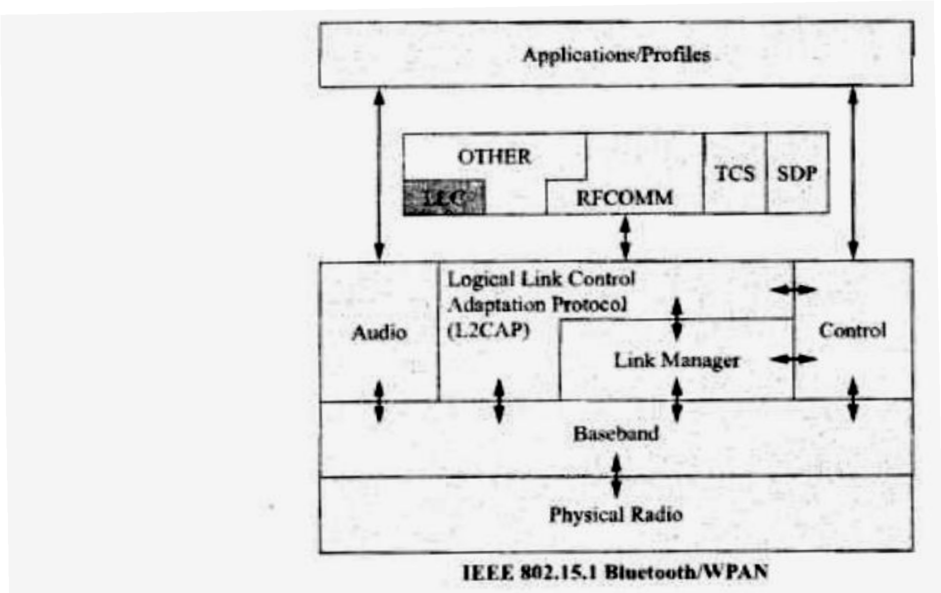


Figure 10–7 The Bluetooth protocol stack (Courtesy of IEEE).

6m

The Bluetooth standard call for a set of communication protocols and a set of interoperable application that are used to support the usages address in the specifications. The link manager protocol (LMP) and the Logical Link Control And Adaptation(L2CAP) layer protocol are Bluetooth specific whereas the protocols within the "Other" box are not. Some of these other protocols are the point-to-point protocol (PPP) and wireless application protocol (WAP).

Physical radio layer: It is for Tx and Rx data and voice.

Baseband layer: It enables RF link between Bluetooth devices.

Link manager: It is the protocol that handles link establishment b/w Bluetooth devices which include authentication and encryptions. 4m

LLC and L2CAP: It is connection based communication protocol that implements multiplexing. No flow control. But provide reliable base band link.

Audio profile: It responsible for managing connection for Tx /Rx data from audio devices.

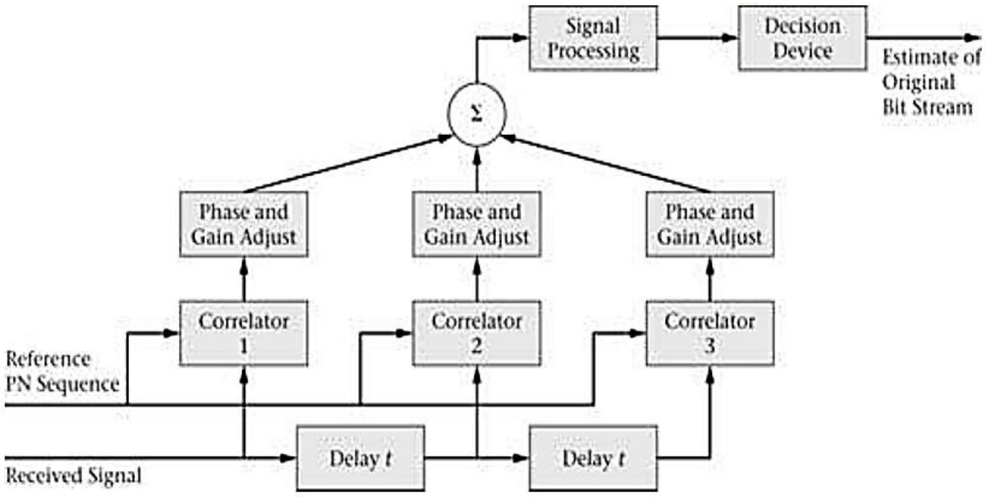
Control: For control signal generations for various activities.

Other LLC: Link controller for optional device, fax, headsets like cordless phone etc.

8. Explain RAKE receiver with a neat block diagram. [10] CO4 L4

A rake receiver is a radio receiver designed to counter the effects of multipath fading. It does this by using several "sub-receivers" called fingers, that is, several correlators each assigned to a different multipath component. Each finger independently decodes a single multipath component; at a later stage the contribution of all fingers are **combined** in order to make the most use of the different transmission characteristics of each transmission path. This could very well result in higher signal-to-noise ratio (or Eb/N0) in a multipath environment than in a "clean" environment.

Since each component contains the original information, if the magnitude and time-of-arrival (phase) of each component is computed at the receiver (through a process called channel estimation), then all the components can be added. The outputs of each correlator are weighted to provide better estimate of the transmitted signal than is provided by a single component. Demodulation and bit decisions are then based on the weighted outputs of the *M* correlators. 5m



5m

Figure 7.10: RAKE receiver block diagram

- Each correlator detects a time-shifted version of the original CDMA transmission, and each finger of the RAKE correlates to a portion of the signal, which is delayed by at least one chip in time from the other fingers.
- Assume M correlators are used in a CDMA receiver to capture M strongest multipath components.
- A weighting network is used to provide a linear combination of the correlator output for bit decision.
- Correlator 1 is synchronized to the strongest multipath m1.
- Multipath component m2 arrived t1 later than m1 but has low correlation with m1