Specific Instructional Objectives

On completion, the student will be able to:

- Explain the need for a Personal Area Network
- Explain different aspects of Bluetooth
    - Transmission media
    - Topology
    - Medium Access Control

5.8.1 Introduction

Bluetooth wireless technology is a *short-range radio technology*, which is developed for Personal Area Network (PAN). Bluetooth is a standard developed by a group of electronics manufacturers that allows any sort of electronic equipment -- from computers and cell phones to keyboards and headphones -- to make its own connections, without wires, cables or any direct action from a user. It is an ad hoc type network operable over a small area such as a room. Bluetooth wireless technology makes it possible to transmit signals over short distances between telephones, computers and other devices and thereby simplify communication and synchronization between devices. It is a global standard that:

- Eeliminates wires and cables between both stationary and mobile devices
- Facilitates both data and voice communication
- Offers the possibility of ad hoc networks and delivers the ultimate synchronicity between all your personal devices

Bluetooth is a dynamic standard where devices can automatically find each other, establish connections, and discover what they can do for each other on an ad hoc basis. Bluetooth is intended to be a standard that works at two levels:

- It provides agreement at the physical level -- Bluetooth is a radio-frequency standard.
- It also provides agreement at the next level up, where products have to agree on when bits are sent, how many will be sent at a time and how the parties in a conversation can be sure that the message received is the same as the message sent.

It is conceived initially by Ericsson, before being adopted by a myriad of other companies, Bluetooth is a standard for a **small, cheap radio chip to be plugged into computers, printers, mobile phones, etc**. A Bluetooth chip is designed to replace cables by taking the information normally carried by the cable, and transmitting it at a special frequency to a receiver Bluetooth chip, which will then give the information received to the computer, phone whatever.

5.8.2 Topology

There are two types of topology for Bluetooth – Piconet, Scatternet. The Piconet is a small ad hoc network of devices (normally 8 stations) as shown in Fig. 5.8.1. It has the following features:

- One is called **Master** and the others are called **Slaves**
- All slave stations synchronizes their clocks with the master
- Possible communication - One-to-one or one-to-many
- There may be one station in *parked state*
- Each piconet has a **unique hopping pattern/ID**
- Each **master** can connect to **7 simultaneous** or **200+ inactive (parked) slaves** per piconet

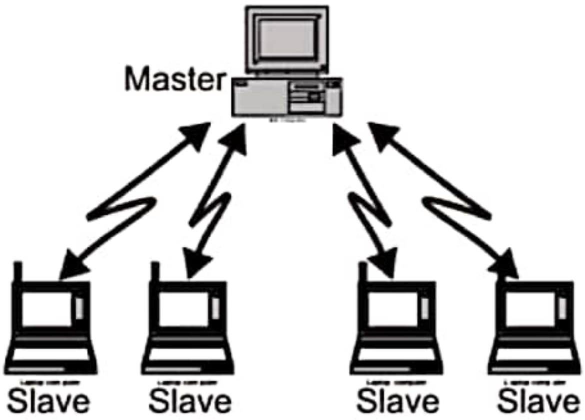

Figure 5.8.1 Piconet topology of Bluetooth

By making one slave as master of another Piconet, Scatternet is formed by combining several Piconets as shown in Fig. 5.8.2. Key features of the scatternet topology are mentioned below:

- A **Scatternet** is the **linking** of multiple **co-located piconets** through the sharing of common master or slave devices.
- A device can be both a **master** and a **slave.**
- Radios are **symmetric** (same radio can be master or slave).
- **High capacity system**, each piconet has maximum capacity (720 Kbps)

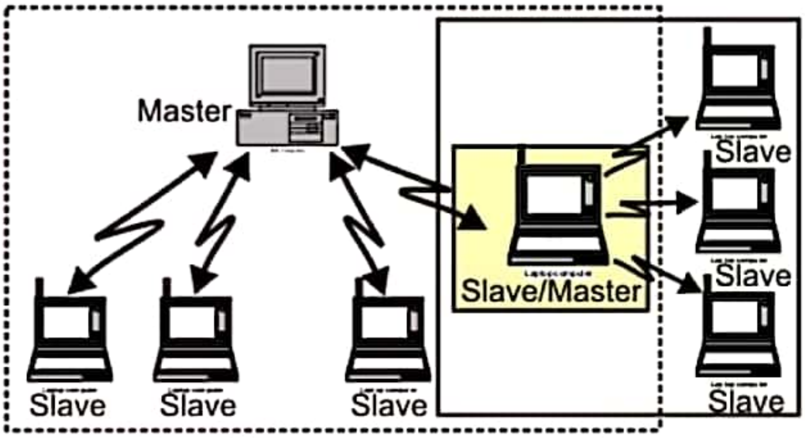

Figure 5.8.2 Scatternet topology

5.8.3 Bluetooth Architecture

The Bluetooth architecture, showing all the major layers in the Bluetooth system, are depicted in the Fig. 5.8.3. The layers below can be considered to be different hurdles in an obstacle course. This is because all the layers function one after the other. One layer comes into play only after the data has been through the previous layer.

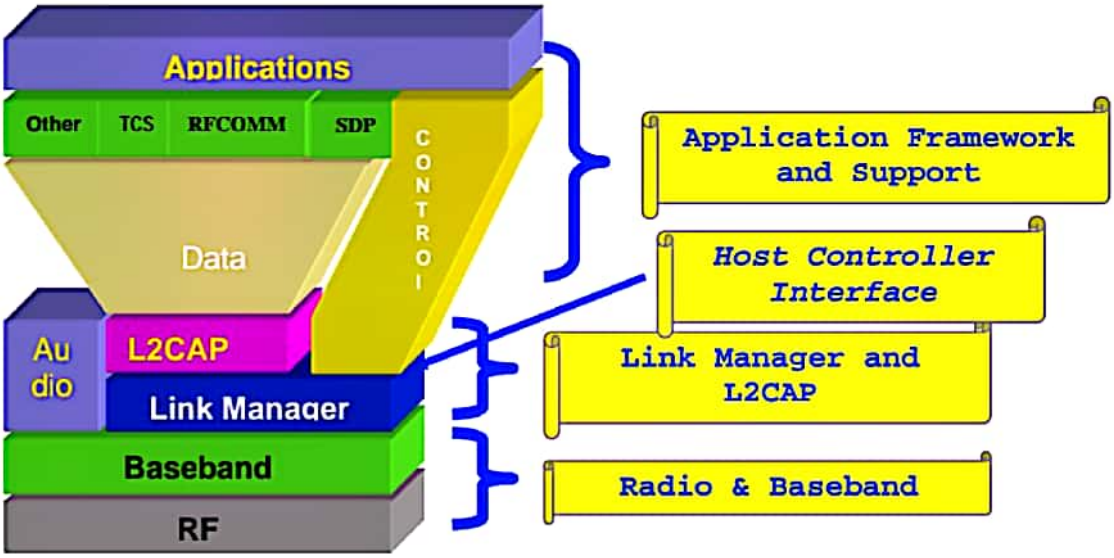

Figure 5.8.3 The Bluetooth architecture

- **Radio:** The **Radio** layer defines the requirements for a Bluetooth transceiver operating in the 2.4 GHz ISM band.

- **Baseband:** The **Baseband** layer describes the specification of the Bluetooth Link Controller (LC), which carries out the baseband protocols and other low-level link routines. It specifies Piconet/Channel definition, "Low-level" packet definition, Channel sharing

- **LMP:** The **Link Manager Protocol** (LMP) is used by the Link Managers (on either side) for link set-up and control.

- **HCI:** The **Host Controller Interface** (HCI) provides a command interface to the Baseband Link Controller and Link Manager, and access to hardware status and control registers.

- **L2CAP: Logical Link Control and Adaptation Protocol** (L2CAP) supports higher level protocol multiplexing, packet segmentation and reassembly, and the conveying of quality of service information.

- **RFCOMM**: The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10.

- **SDP:** The Service Discovery Protocol (SDP) provides a means for applications to discover, which services are provided by or available through a Bluetooth device. It also allows applications to determine the characteristics of those available services.

Now we shall be study each layer in detail (in next few sections) so that we come to know the function of each layer.

5.8.4 Bluetooth Layers

5.8.4.1 Layer 1: Radio Layer

This is the lowest layer in the Bluetooth protocol stack. Bluetooth uses a technique called frequency hopping, as explained in the context of wireless LANs, in establishing radio links with other Bluetooth devices. Suppose we have a data packet then the whole packet is never transmitted at the same frequency. It is always split into different parts and transmitted at different frequencies. This is the frequency hopping technique (already discussed previously in Wireless LAN lesson). This partly gives the necessary protection to the transmitted data and avoids tampering. Standard hop values are 79 hops, which are spaced at an interval of 1 MHz. In some countries like France, due to government regulations 23 hops are used.

Transmitter characteristics: Each device is classified into 3 power classes, Power Class **1**, **2** & **3**.

- **Power Class 1**: is designed for long range (~100m) devices, with a max output power of 20 dBm,
- **Power Class 2**: for ordinary range devices (~10m) devices, with a max output power of 4 dBm,

- **Power Class 3**: for short range devices (~10cm) devices, with a max output power of 0 dBm.

The Bluetooth radio interface is based on a nominal antenna power of 0dBm. Each device can optionally vary its transmitted power. Equipment with power control capability optimizes the output power in a link with LMP commands (see Link Manager Protocol). It is done by measuring RSSI and reporting it back, if the power is required to be increased or decreased.

Modulation Characteristics: The Bluetooth radio module uses GFSK (Gaussian Frequency Shift Keying) where a binary one is represented by a positive frequency deviation and a binary zero by a negative frequency deviation. BT is set to 0.5 and the modulation index must be between 0.28 and 0.35.

Radio Frequency Tolerance: The transmitted initial center frequency accuracy must be ±75 kHz from Fc. The initial frequency accuracy is defined as being the frequency accuracy before any information is transmitted. Note that the frequency drift requirement is not included in the ±75 kHz.

Receiver Characteristics: The receiver must have a sensitivity level for which the bit error rate (BER) 0.1% is met. For Bluetooth this means an actual sensitivity level of 70dBm or better.

5.8.4.2 Layer 2: Baseband Layer

The baseband is the digital engine of a Bluetooth system. It is responsible for constructing and decoding packets, encoding and managing error correction, encrypting and decrypting for secure communications, calculating radio transmission frequency patterns, maintaining synchronization, controlling the radio, and all of the other low level details necessary to realize Bluetooth communications.

Bluetooth operates in the **2.4 GHz ISM band**. In the US and Europe, a band of 83.5 MHz width is available; in this band, 79 RF channels spaced 1 MHz apart are defined. In France, a smaller band is available; in this band, 23 RF channels spaced 1 MHz part are defined.

The channel is represented by a **pseudo-random hopping sequence** hopping through the 79 or 23 RF channels. Two or more Bluetooth devices using the same channel form a **piconet**. The hopping sequence is unique for the piconet and is determined by the Bluetooth device address (BD_ADDR) of the master; the phase in the hopping sequence is determined by the Bluetooth clock of the master. The channel is divided into time slots where each slot corresponds to an RF hop frequency. Consecutive hops correspond to different RF hop frequencies. Figure 5.8.4 shows the communication between the master and a slave. In this case, the master uses even numbered slots and the slave communicates in the odd numbered slots in a half-duplex mode.

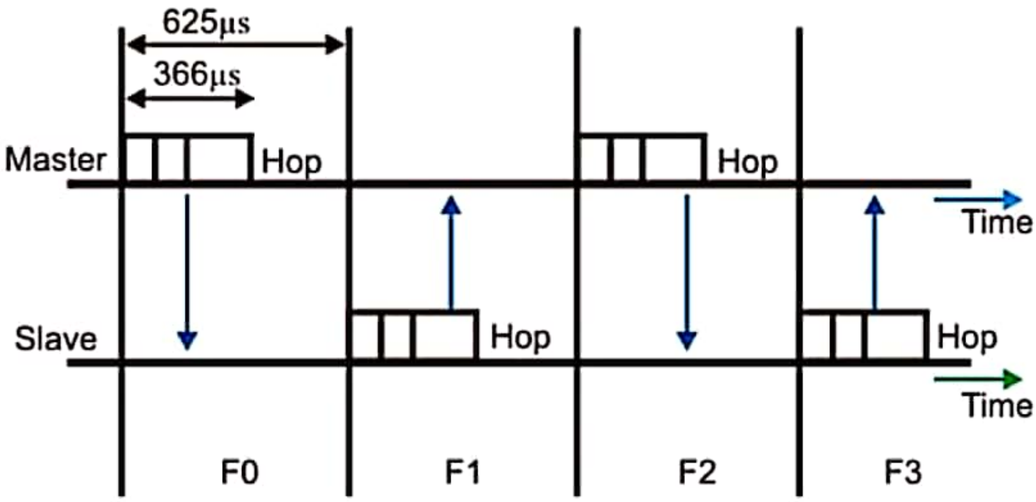

Figure 5.8.4 Master-slave communication

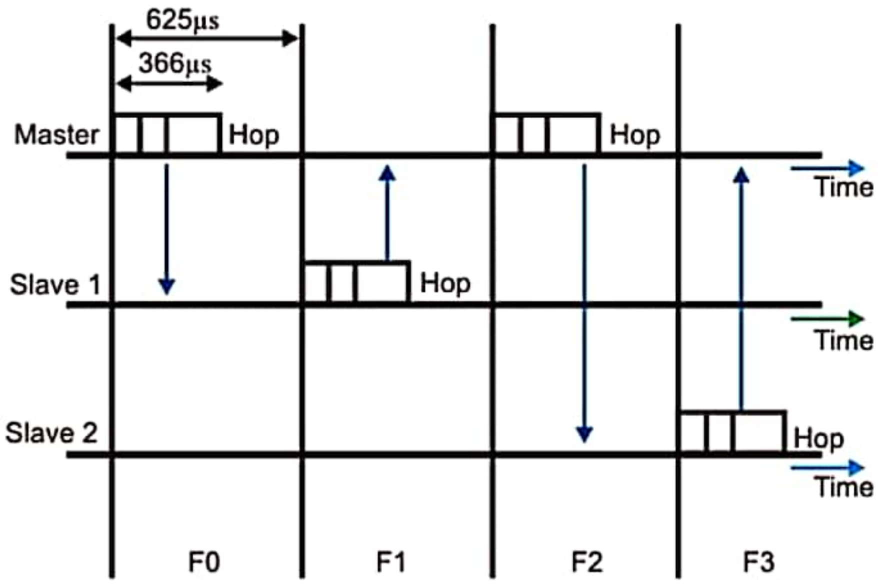

Figure 5.8.5 Master and multi-slave communication

The data exchange takes place with every clock tick. The clock synchronization is with respect to that of the master. Transmission takes place by way of TIME DIVISION DUPLEXING (TDD). The channel is divided into time slots, each 625 µs in length. The time slots are numbered according to the Bluetooth clock of the piconet master. A TDD scheme is used where master and slave alternatively transmit. The master shall start its transmission in even-numbered time slots only, and the slave shall start its transmission in odd-numbered time slots only. The packet start shall be aligned with the slot start.

Always remember that the 'slave has to adjust itself to the whims of its master'. If a slave is to establish a connection with the master, then the slave has to synchronize its own clock according to that of the master. In the multiple-slave scenario, the slave uses even numbered slots, but only one slave communicates in the next odd-numbered slot if the packet in the previous slot was addressed to it. This is shown in Fig. 5.8.5.

The Baseband handles three types of links:

- **SCO (Synchronous Connection-Oriented):** The SCO link is a symmetric point-to-point link between a master and a single slave in the piconet. The master maintains the SCO link by using reserved slots at regular intervals (circuit switched type). The SCO link mainly carries voice information. The master can support up to three simultaneous SCO links while slaves can support two or three SCO links. SCO packets are never retransmitted. SCO packets are used for 64 kB/s speech transmission.
- **Polling-based (TDD) packet transmissions**: In this link type one slot is of 0.625msec (max 1600 slots/sec) and master/slave slots (even-/odd-numbered slots)
- **ACL (Asynchronous Connection-Less) link**: The ACL link is a point-to-multipoint link between the master and all the slaves participating on the piconet. In the slots not reserved for the SCO links, the master can establish an ACL link on a per-slot basis to any slave, including the slave already engaged in an SCO link (packet switched type). Only a single ACL link can exist. For most ACL packets, packet retransmission is applied.

Device Addressing: Four possible types of addresses can be assigned to bluetooth units.

- **BD_ADDR: Bluetooth Device Address :** Each Bluetooth transceiver is allocated a unique 48-bit device address. It is divided into a 24-bit LAP field, a 16-bit NAP field and a 8-bit UAP field.
- **AM_ADDR: Active Member Address:** It is a 3-bit number. It is only valid as long as the slave is active on the channel. It is also sometimes called the MAC address of a Bluetooth unit.
- **PM_ADDR: Parked Member Address:** It is a 8-bit member (master-local) address that separates the parked slaves. The PM_ADDR is only valid as long as the slave is parked.
- **AR_ADDR: Access Request Address :** This is used by the parked slave to determine the slave-to master half slot in the access window it is allowed to send access request messages in. It is only valid as long as the slave is parked and is not necessarily unique.

5.8.4.3 Layer 3: Link Manager Protocol

The Link Manager is responsible for managing the physical details for Bluetooth connections. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure. The link manager is implemented in a mix of hardware and software.

The Link Manager carries out link setup, authentication, link configuration and other protocols. It discovers other remote LM's and communicates with them via the Link Manager Protocol (LMP). To perform its service provider role, the LM uses the services of the underlying Link Controller (LC).

The Link Manager Protocol essentially consists of a number of PDU (protocol Data Units), which are sent from one device to another, determined by the AM_ADDR in the packet header.

5.8.4.4 Layer 4: Host Controller Interface

This is the layer of the stack that contains the firmware i.e. the software that actually controls all the activities happening in the Baseband and Radio layers. It provides a common interface between the Bluetooth host and a Bluetooth module. It manages the hardware links with the scatternets. It also contains the drivers for the hardware devices used in the connection. Basically the BIOS is loaded in the HCI Layer.

5.8.4.5 Logical Link Control and Adaptation Protocol

The Logical Link Control and Adaptation Layer Protocol (L2CAP) is layered over the Baseband Protocol and resides in the data link layer.

The L2CAP is the big picture brains of a Bluetooth system. It manages the high level aspects of each connection (who is connected to who, whether to use encryption or not, what level of performance is required, etc.). In addition it is responsible for converting the format of data as necessary between the APIs and the lower level Bluetooth protocols. The L2CAP is implemented in software and can execute either on the host system processor or on a local processor in the Bluetooth system. L2CAP provides connection oriented and connectionless data services to upper layer protocols with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions. L2CAP permits higher-level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

Two link types are supported for the Baseband layer: Synchronous Connection-Oriented (SCO) links and Asynchronous Connection-Less (ACL) links. SCO links support real-time voice traffic using reserved bandwidth. ACL links support best effort traffic. The L2CAP Specification is defined for only ACL links and no support for SCO links is planned.

5.8.4.6 Layer 6: Radio Frequency Communication (RFCOMM)

This is the most important layer in the Bluetooth architecture. RFCOMM takes care of the communication channel between two devices or between a master and a slave. It connects the serial ports of all the devices according to the requirement.

RFCOMM basically has to accommodate two kinds of devices:

1. Communication end-points such as computers or printers.
2. Devices that are a part of communication channel such as Modems.

RFCOMM protocol is not aware of the distinction between these two kinds of devices. Hence to prevent any loss of data, it passes on all the information to both the devices. The devices in turn distinguish between the data and filter it out.

5.8.4.7 Layer 7: Service Discovery Protocol

The service discovery protocol (SDP) provides a means for applications to discover which services are available and to determine the characteristics of those available services.

A specific Service Discovery protocol is needed in the Bluetooth environment, as the set of services that are available changes dynamically based on the RF proximity of devices in motion, qualitatively different from service discovery in traditional network-based environments. The service discovery protocol defined in the Bluetooth specification is intended to address the unique characteristics of the Bluetooth environment.

Bluetooth is basically a universal protocol. Manufacturers may embed Bluetooth ports in their devices. SDP is very important when devices from different companies and from different parts of the world are brought together. The devices try to recognize each other through SDP.

5.6.4.8 Telephony Control Protocol Spec (TCS)

Basic function of this layer is call control (setup & release) and group management for gateway serving multiple devices.

5.6.4.9 Application Program Interface (API) libraries

These are software modules which connect the host application program to the Bluetooth communications system. As such they reside and execute on the same processing resource as the host system application.