RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Wireless and Mobile Computing**

Subject Code: **IT-602**

Semester: **6th**

Unit 3:

IEEE 802.11: LAN-architecture: The fundamental building block of the 802.11 architecture is the cell, known as the **basic service set (BSS)** in 802.11. A BSS typically contains one or more wireless stations and a central base station, known as an **access point (AP)** in 802.11 terminologies. The stations, which may be either fixed or mobile, and the central base station communicate amongst themselves using the IEEE 802.11 wireless MAC protocol. Multiple APs may be connected together (e.g., using a wired Ethernet or another wireless channel) to form a so-called **distribution system (DS).** The DS appears to upper level protocols (e.g., IP) as a single 802 network, in much the same way that a bridged, wired 802.3 Ethernet network appears as a single 802 network to the upper layer protocols.

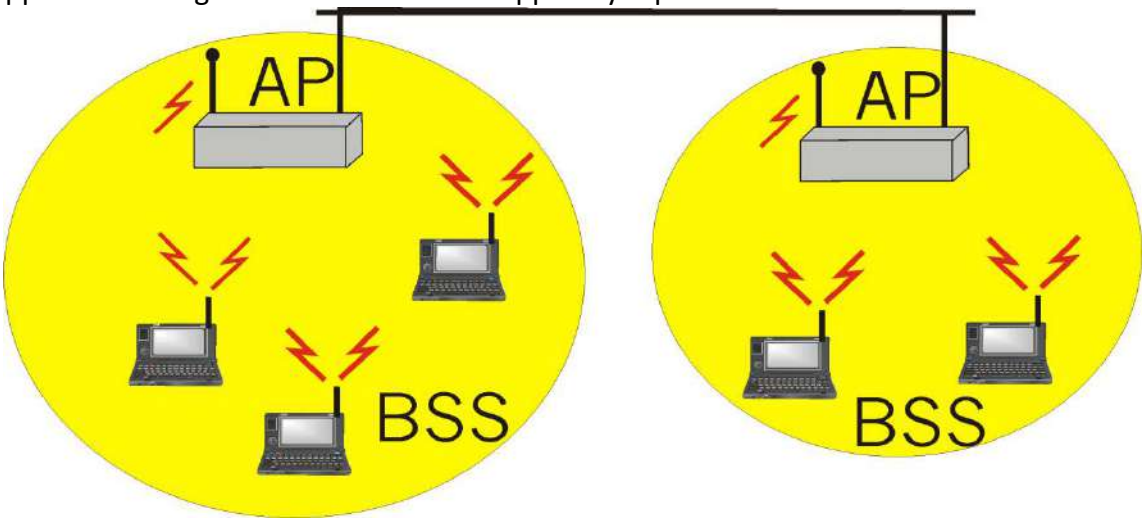

Figure 16: IEEE 802.11 LAN architecture

IEEE 802.11 stations can also group themselves together to form an ad hoc network – a network with no central control and with no connections to the "outside world." Here, the network is formed "on the fly," simply because there happen to be mobile devices that have found themselves in proximity to each other, that have a need to communication, and that find no pre-existing network infrastructure (e.g., a pre-existing 802.11 BSS with an AP) in the location. An ad hoc network might be formed, for example, when people with laptops meet together (e.g., in a conference room, a train, or a car) and want to exchange data in the absence of a centralized AP. There has been a tremendous recent increase in interest in ad hoc networking, as communicating portable devices continue to proliferate.

IEEE 802.11a OFDM

- This method uses Orthogonal Frequency Division Multiplexing (OFDM) for signal generation.
- This method is capable of delivering data up to 18 or 54 Mbps.
- In OFDM all the subbands are used by one source at a given time.
- It uses 5 GHz ISM(*industrial, scientific* and *medical)* band.
- This band is divided into 52 subbands, with 48 subbands for data and 4 subbands for control information.

IEEE 802.11b HR-OSSS

- It uses High Rate Direct Sequence Spread Spectrum method for signal generation.
- HR-DSSS is similar to DSSS except for encoding method.
- Here, 4 or 8 bits are encoded into a special symbol called complementary code key (CCK).
- It uses 2.4 GHz ISM band.
- It supports four data rates: 1,2,5.5 and 11 Mbps.
- 1 Mbps and 2 Mbps data rates uses phase shift modulation.
- The 5.5. Mbps version uses BPSK and transmits at 1.375 Mbaud/s with 4-bit CCK encoding.

- The 11 Mbps version uses QPSK and transmits at 1.375 Mbps with 8-bit CCK encoding.

IEEE 802.11g OFDM

- It uses OFDM modulation technique.
- It uses 2.4 GHz ISM band.
- It supports the data rates of 22 or 54 Mbps.
- It is backward compatible with 802.11 b

Protocol Architecture (802.11 Media Access Protocols)

Just as in a wired 802.3 Ethernet network, stations in an IEEE 802.11 wireless LAN must coordinate their access and use of the shared communication media (in this case the radio frequency). Once again, this is the job of the media access control (MAC) protocol. The IEEE 802.11 MAC protocol is a carrier sense multiple access protocol with collision avoidance (**CSMA/CA**). A CSMA protocol first senses the channel to determine if the channel is "busy" with the transmission of a frame from some other station. In the 802.11 specification, the physical layer monitors the energy level on the radio frequency to determine whether or not another station is transmitting and provides this carrier sensing information to the MAC protocol. If the channel is sensed idle for an amount of time equal to or greater than the Distributed Inter Frame Space (DIFS), a station is then allowed to transmit. As with any random access protocol., this frame will be successfully received at the destination station if no other station's transmission has interfered with the frame's transmission.

When a receiving station has correctly and completely received a frame for which it was the addressed recipient, it waits a short period of time (known as the Short Inter Frame Spacing - SIFS) and then sends an explicit acknowledgment frame back to the sender. This data link layer acknowledgment lets the sender know that the receiver has indeed correctly received the sender's data frame. We will see shortly that this explicit acknowledgment is needed because, unlike the case of wired Ethernet, a wireless sender can not itself determine whether or not its frame transmission was successfully received at the destination. The transmission of a frame by a sending station and its subsequent acknowledgment by the destination station is shown in figure.

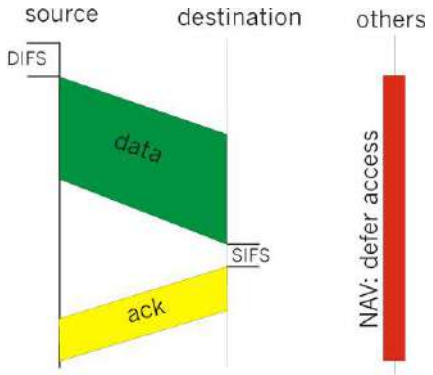

Figure 17: Data transmission and acknowledgment in IEEE 802.11

Figure illustrates the case when the sender senses the channel to be idle. What happens if the sender senses the channel busy? In this case, the station performs a backoff procedure that is similar to that of Ethernet. More specifically, a station that senses the channel busy will defer its access until the channel is later sensed idle. Once the channel is sensed idle for an amount of time equal to DIFS, the station then computes an *additional* random backoff time and counts down this time as the channel is sensed idle. When the random backoff timer reaches zero, the station transmits its frame. As in the case of Ethernet, the random backoff timer serves to avoid having multiple stations immediately begin transmission (and thus collide) after a DIFS idle period. As in the case of Ethernet, the interval over which the backoff timer is randomizes is doubled each time a transmitted frame experiences a collision.

We noted above that unlike the 802.3 Ethernet protocol, the wireless 802.11 MAC protocol does *not* implement collision detection. There are a couple of reasons for this:

- The ability to detect collisions requires the ability to both send (one's own signal) and receive (to determine if another station's transmissions is interfering with one's own transmission) at the same time. This can be costly.
- More importantly, even if one had collision detection and sensed no collision when sending, a collision could still occur at the receiver.

This situation results from the particular characteristics of the wireless channel. Suppose that station A is transmitting to station B. Suppose also that station C is transmitting to station B. With the so-called **hidden terminal problem,** physical obstructions in the environment (e.g. a mountain) may prevent A and C from hearing each others transmissions, even though A's and C's transmissions are indeed interfering at the destination, B. This is shown in Figure. A second scenario that results in undetectable collisions at the receiver results from the **fading** of a signal's strength as propagates through the wireless medium. Figure 5.7-4(b) illustrates the case where A and C are placed such that their signal strengths are not strong enough for them to detect each others' transmissions, and yet their transmissions are strong enough to have interfered with each other at station B.

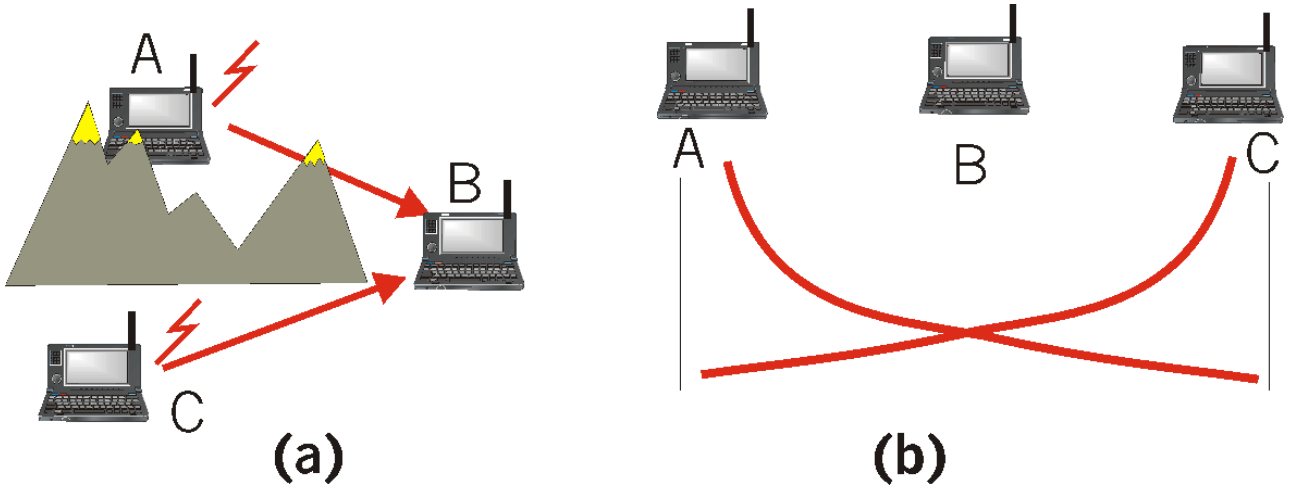

Figure 18: Hidden terminal problem (a) and fading (b)

Given these difficulties with detecting collisions at a wireless receiver, the designers of IEEE 802.11 developed an access protocol which aimed to avoid collisions (hence the name CSMA/CA) , rather than detect and recover from collisions (CSMA/CD). First, the IEEE 802.11 frame contains a duration field in which the sending station explicit indicates the length of time that its frame will be transmitting on the channel. This value allows other stations to determine the minimum amount of time (the so-called network allocation vector, NAV) for which they should defer their access, as shown in figure.

The IEEE 802.11 protocol can also use a short Request To Send (RTS) control frame and a short Clear To Send (CTS) frame to *reserve* access to the channel. When a sender wants to send a frame, it can first send a RTS frame to the receiver, indicating the duration of the data packet and the ACK packet. A receiver that receives an RTS frame responds with a CTS frame, giving the sender explicit permission to send. All other stations hearing the RTS or CTS then know about the pending data transmission and can avoid interfering with those transmissions. The RTS, CTS, DATA and ACK frames are shown in Figure. An IEEE 802.11 sender can operate either using the RTS/CTS control frames, as shown in Figure, or can simply send its data without first using the RTS control frame, as shown in figure.

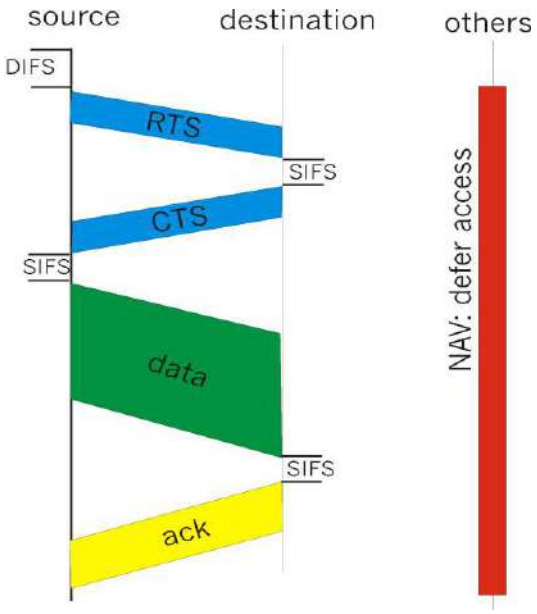

Figure 19: Collision Avoidance using the RTS and CTS frames

The use of the RTS and CTS frames helps avoid collisions in three important ways:

- Because the receiver's transmitted CTS frame will be heard by all stations within the receiver's vicinity, the CTS frame helps avoid both the hidden station problem and the fading problem.
- Because the RTS and CTS frames are short, a collision involving a RTS or CTS frame will only last for the duration of the whole RTS or CTS frame. Note that when the RTS and CTS frames are correctly transmitted, there should be no collisions involving the subsequent DATA and ACK frames.

In our discussion above, we have only highlighted some of the key aspects of the 802.11 protocol. Additional protocol capabilities such as time synchronization, power management, joining and leaving a network (i.e., roaming stations) are covered in the full IEEE 802.11 standard

Physical Layer

The Physical layer of the OSI model is categorized into two sublayers:

Physical Layer Convergence Procedure (PLCP): Contains the data in the form of PLCP Service Data Unit (PSDU), which is equivalent to the MPDU. The PLCP sublayer appends a preamble and PHY header information to the PSDU to make the PPDU. The preamble is additional bits that help in synchronizing the transmitting and receiving 802.11 communications.

Physical Medium Dependent (PMD): Accepts the PPDU from the PLCP sublayer and then modifies and transfers the data frames as bits.

The following figure shows the data moving between the Data-Link and Physical layers.

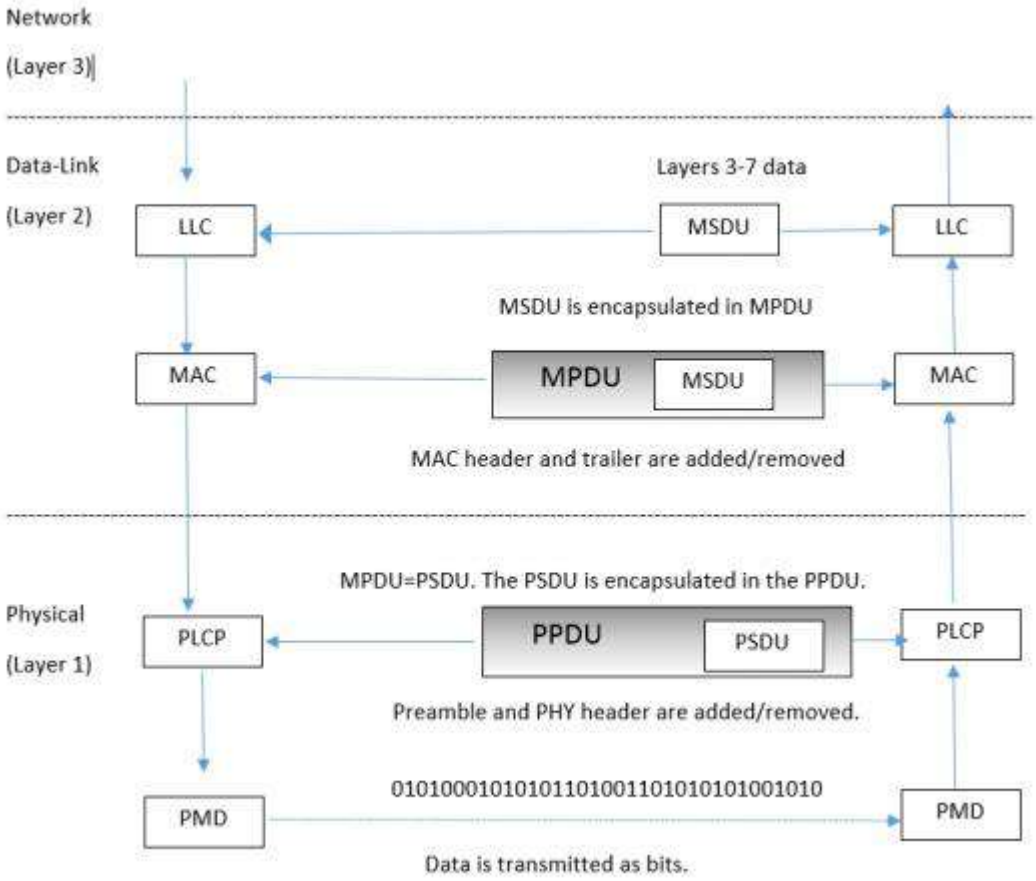

Figure 20: The data moving between the Data-Link and Physical layers

802.11n/High Throughput (HT) MAC Architecture

The 802.11n amendment also defined some new improvements to the MAC sublayer of the Data Link layer for increased throughput and reduced overhead by using the frame aggregation methods. Frame aggregation was introduced after the 802.11n amendment (HT PHY). An analogy for frame aggregation is carpooling that is implemented to reduce traffic and subsequently reduce traffic jams. Similarly, frame aggregation is used to reduce medium contention overhead by combining several service data units (SDUs).

MAC layer:

Media Access Control (MAC): Creates a data frame in the form of MAC Protocol Data Unit (MPDU) after receiving the MSDU. The MAC layer receives the MSDU from the LLC sublayer, and adds the MAC header information to it. This data frame is now called the MPDU. The following figure shows an 802.11 MPDU data frame.

Figure 21: Three main components of the MPDU data frame

MAC Header: Contains information related to frame control, MAC addressing, duration, and sequence control.
Frame body: Contains information related to frame types or subtypes and the MSDU payload that is encrypted (when encryption is used). The frame body can vary in size for different 802.11 frames.
Frame Check Sequence (FCS): Contains a 32-bit cyclic-redundancy check (CRC) to verify the integrity of the MSDU data frames.
Now, the MPDU data frame is sent to the Physical layer from where the data frame is forwarded further to reach at the destination device.

HIPERLAN/2 Protocol Stack-PHY layer, MAC layer

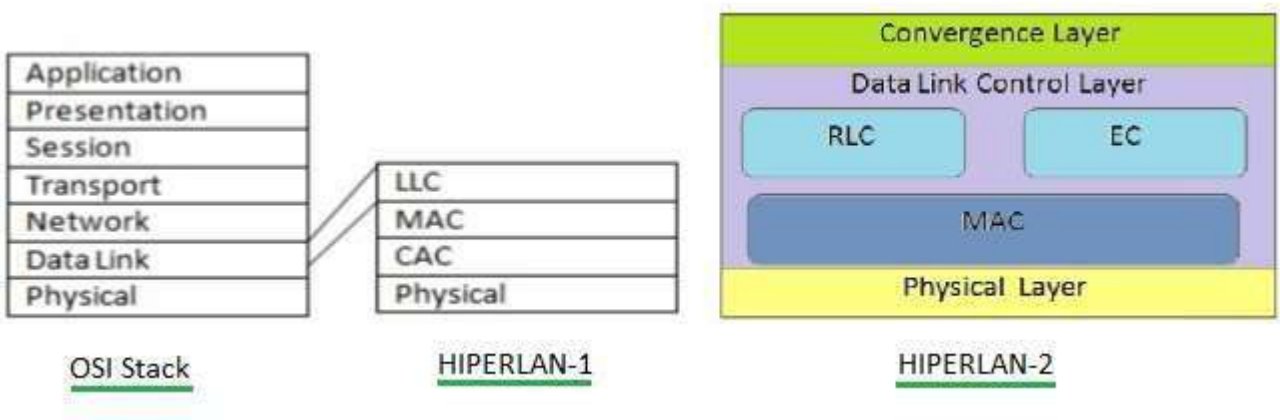

Figure 22: HIPERLAN-1 and HIPERLAN-2 protocol stack

The figure depicts HIPERLAN-1 protocol stack layers. As shown it consists of two layers viz. physical layer and data link layer. Data link layer consists of LLC (Logical Link Control) and MAC (Medium Access Control). There is another sublayer, which exists between PHY and MAC. It is known as CAC (Channel Access and Control Layer).
The figure also depicts HIPERLAN-2 protocol layers viz. Physical Layer, DLC layer and Convergence layer. DLC (Data Link Control) layer is further sub divided into 3 layers viz. MAC, LLC and RLC layers.
PHY layer supports following six modulation/coding rates.

Modulation-code rate	Data rate (Mbps)
BPSK-1/2	6
BPSK-3/4	9
QPSK-1/2	12
QPSK-3/4	18
16QAM-9/16	27
16QAM-3/4	36
64QAM-3/4	54

Table 5: Modulation-code rate

Physical Layer

RF carriers

HiperLAN 1 uses the radio frequency band 5,150 MHz to 5,300 MHz. The following table shows the nominal frequency of each carrier. It is required that all transmissions shall be centered on one of the nominal carrier frequencies, and all HiperLAN 1 equipments shall operate on all 5 channels.

Carrier number	Center Frequency (MHz)
0	5 176,4680
1	5 199,9974
2	5 223,5268
3	5 247,0562
4	5 270,5856

Table 6 : Nominal Carrier center frequencies

The carriers numbered 0, 1 and 2 are designated the "default" carriers.

Access Control Sub-layer

Channel Access and Control (CAC) sublayer, is introduced in the HiperLAN 1 architecture to deal with the channel access signaling and protocol operation required supporting packet priority. A pseudo-hierarchically independent access mechanism achieved via active signaling in a listen-before-talk access protocol. The Elimination-Yield Non-Preemptive Multiple Access (EY-NPMA) mechanism codes priority level selection and contention resolution into a single, variable length radio pulse preceding packet data. EY-NPMA provides good residual collision rate performance for even large numbers of simultaneous channel contenders

The HIPERLAN 1 MAC Sublayer

The HIPERLAN 1 standard was released in 1995 aiming to define a WLAN technology of equal performance to that of traditional wired LANs and capable of supporting isochronous services. Unlike the IEEE 802.11 standard, the HIPERLAN committee was not driven by existing technologies and regulations. A set of requirements was set and the committee started working in order to satisfy them. The standard covers the physical and MAC layers of the OSI model.

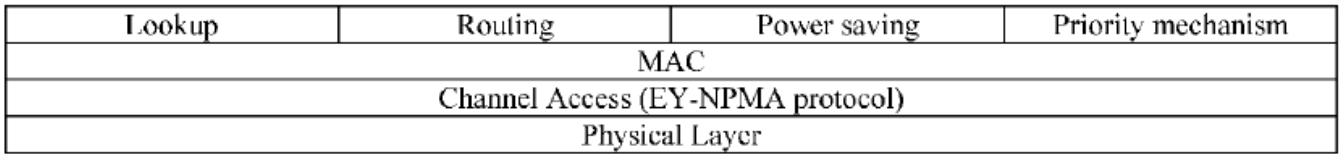

Figure 23: HIPERLAN 1 system architecture

The HIPERLAN 1 has defined the system architecture shown in figure. It divides the functions of the Medium Access Control (MAC) into two subparts, which it refers to as Channel Access and Control (CAC) and MAC sublayers. The CAC layer defines how a given channel access attempt will be made depending on whether the channel is busy or idle, and at what priority level the attempt will be made, if contention is necessary. The HIPERLAN MAC sublayer defines the various protocols which provide the HIPERLAN features of power conservation, lookup, security, and multihop routing, as well as the data transfer service to the upper layers of protocols. The routing mechanism supports the ability of HIPERLAN nodes to forward packets to stations out of their range with the help of intermediate forwarding stations. The lookup functionality enables collocated operation of more than one HIPERLAN network. Finally, the standard supports priorities, power conservation and support for encryption

The Priority Mechanism and QoS Support

HIPERLAN 1 dynamically assigns channel access priorities to packets by taking into account the packet's lifetime and its MAC priority. The MAC priority of a packet can be either normal or high, with normal being the default value. Every packet is generated with a specific lifetime ranging from 0 to 32767 ms, with the default value set at 500 ms. Packets that cannot be delivered within the allocated lifetime are dropped. Therefore, as time expires, the channel priority of each packet increases. Channel priority values range from 1 to 5, with 1 is the highest priority.

The HIPERLAN 1 MAC Protocol

In HIPERLAN 1, a station can immediately commence transmission after sensing an idle medium for duration of 1700 high rate bit times. When a station senses the medium busy, it waits until it becomes idle and then the Elimination Yield-Non-Preemptive Priority Multiple Access (EY-NPMA) protocol is applied. After the end of the detected transmission, all stations that want to transmit wait for another 256-bit period, which called a synchronization slot. Then, the EY-NPMA protocol applied.

Multihop Routing

HIPERLAN 1 supports both infrastructure and ad hoc topologies. Furthermore, the standard supports multihop configurations, where a station can transmit a packet to another station, which is out of its radio range without the need for additional infrastructure. This achieved with the help of intermediate stations that can forward packets destined for other stations. This means that a forwarder needs to know the network topology, maintain, and dynamically update routing databases.

Furthermore, maintenance of routing databases at a forwarder demands periodic exchange of information with its neighbors, a fact that limits the useful bandwidth of the channel.

Power Saving

The HIPERLAN 1 standard supports power saving by using both hardware-specific and protocol-based techniques. using two transmission speeds. As mentioned, the header of each packet is transmitted at the lower 1.47 Mbps rate. A node that hears a packet destined for another station can shut down the error correction, channel equalization and other receiver circuits until it receives a packet destined for itself.

Bluetooth

"Bluetooth" was the nickname of Harald Blåtland II, king of Denmark from 940 to 981, who united all of Denmark and part of Norway under his rule. Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. The Bluetooth technology aims at so-called ad-hoc piconets, which are local area networks with a very limited coverage and without the need for an infrastructure.

User scenarios

Many different user scenarios can be imagined for wireless piconets or WPANs:

Connection of peripheral devices: Today, most devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers). This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, wires block office space. In a wireless network, no wires are needed for data transmission. However, batteries now have to replace the power supply, as the wires not only transfer data but also supply the peripheral devices with power.

Support of ad-hoc networking: Imagine several people coming together, discussing issues, exchanging data (schedules, sales figures etc.). For instance, students might join a lecture, with the teacher distributing data to their personal digital assistants (PDAs). Wireless networks can support this type of interaction; small devices might not have WLAN adapters following the IEEE 802.11 standard, but cheaper Bluetooth chips built in.

Bridging of networks: Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip. The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network.

Physical layer: Bluetooth physical layer consists of baseband and radio specifications as defined in IEEE 802.15.1.
Bluetooth network is composed of one master and one to seven slave devices. This small region is referred as piconet. Once master device selects channel with frequency hopping sequence and time to transmit, other devices also in the same piconet use the same. One bluetooth device of piconet can also exist and function as either master or slave in the other nearby biconet, this overlapping region is referred as *scatternet.*

Frequency hopping

It serves two purposes, one is that it helps provide resistance to multipath interference. Second, one is that it provides multiple accesses to devices in different piconets co-located.

Bluetooth system uses frequency hopping scheme with about 80 different frequencies,with a carrier spacing of about 1MHz.With frequency hopping enabled, a logical channel is defined by hopping sequence. At any time 1 MHz bandwidth is shared by max. 8 devices. Different logical channels can utilize same 80 MHz BW at the same time. Collisions occur when two bluetooth devices use same hopping frequency simultaneously evenif they are on different piconets and different logical channels. The hopping rate is 1600 hops per second, hence physical channel exists for only 0.625ms.

Bluetooth radio uses TDD topology in which data transmission occur in one direction at one time and it alternates in two directions one after the other. The access is TDMA, as piconet medium is shared among two devices. Hence piconet access is referred as FH-TDD-TDMA.

Physical links

There are two ways link can be established between master and slave devices.

- SCO referred as Synchronous connection oriented. In this type, fixed bandwidth is allocated for point to point connection between master and slave. The basic reservation is 2 consecutive slots. The master supports 3 SCO links and slave supports 2 or 3 links.
- ACL referred as Asynchronous connectionless. This is used for point to multipoint link between master and slaves. Only one ACL link exists and for more retransmission of packet is required. In the cases when slots are not reserved in SCO links, master device can exchange packets with any of the slave device on a per time slot.

Baseband packet formats

Bluetooth Packet Format = Access Code(72 bits) + Header(54 bits) + Payload (0 to 2745 bits)

- Access code consists of preamble(4bits),sync word(64bits) and trailer field(4 bits).
- Header field consists of AM_ADDR(3 bits), type(4 bits),flow(1 bit),ARQN(1 bit),SEQN(1 bit) and HEC(8 bits).

Access code in bluetooth packet is used for timing synchronization and other offset compensations. Access code is also used for paging requests, paging responses and inquiry purposes.
Header is used for identification of packet type and will carry protocol control information.
Payload field will carry user voice or data.
Channel Access code identifies a piconet, Device Access Code used for paging REQ/RES, Inquiry Access Code is used for inquiry purposes.

MAC layer: Bluetooth MAC layer consists of Link Manager Protocol(LMP) and Logical Link Control and Adaptation Protocol(L2CAP).

Logical channels

Bluetooth standard defines five different types of logical data channels based on different payload traffic carried by them. They are link control, link manager, user asynchronous, user isochronous and user synchronous. Link Control channel carry information such as ARQ, flow control and payload characterization.

Control Channels

Bluetooth modes of operation

During the connection state Bluetooth device can be in one of the four modes, which include active mode, sniff mode, hold mode and park mode.

- In the Active mode, Bluetooth device actively participates in the channel.
- In the Sniff mode, Bluetooth slave device will not listen on all the received slots but listen only specified slots for messages meant for it.
- In the Hold mode, the Bluetooth device does not transmit data for long time.
- In the Park mode, the Bluetooth device will have little activity to be performed and hence will consume very low power.

Link Manager Protocol (LMP)

LMP protocol is used to establish the link and to control the link. Link Control (LC) provides the reliability to Link Manager Protocol. LM PDUs are sent in single slot packets.

PDU = Opcode(7bits), transaction ID(1bit), information contents

Logical Link Control and Adaptation Protocol(L2CAP)

This L2CAP protocol like LLC takes care of link layer protocol services between the entities. It provides services to upper layers and rely on lower layer for flow control as well as error control.L2CAP makes use of ACL links and does not use SCO links.

L2CAP provides two type of services connectionless and connection mode services. Connectionless type provide reliable datagram delivery service. Connection mode type provide service using HDLC protocol.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in