Wireless LANs and PANs

Introduction

- Fundamentals of WLANs
- IEEE 802.11
- Bluetooth

Wireless LAN and PAN

- WLAN Wireless Local Area Networks (WLAN), use an industry standard known as 802.11. WLAN's are typically used in confined areas within an organization, such as a warehouse, factory or retail store, and can be considered the wireless extension of the local area network.

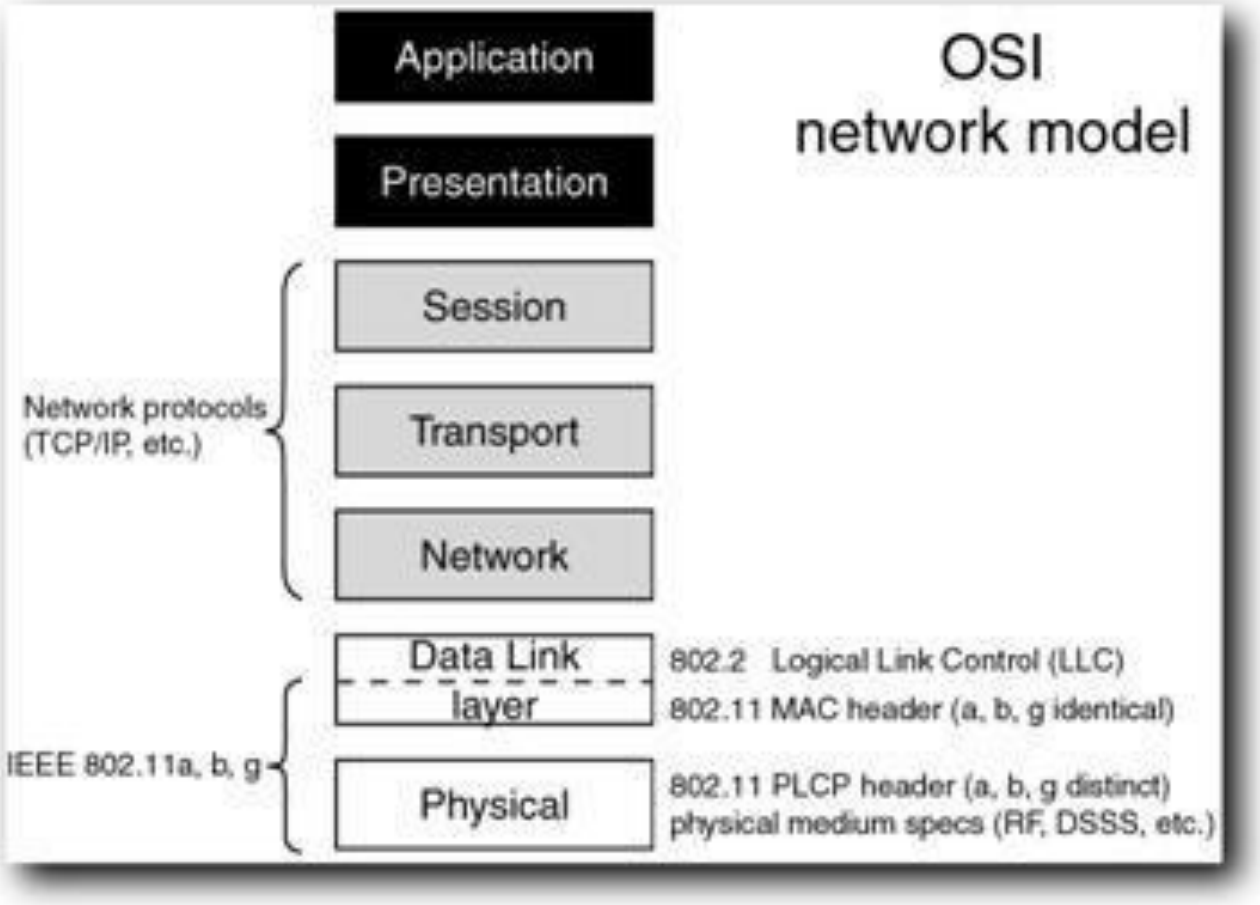
- WPAN: Bluetooth is the most widely used Wireless Personal Area Network (WPAN) standard. Bluetooth allows the transmission of data between Bluetooth-compatible devices such as cellular phones, computers, portable data terminals and bar code printers or scanners. Bluetooth technology may provide a range of up to 100 meters, depending on the radio classification and environmental conditions.

IEEE 802 NETWORKING STANDARD

- The Institute of Electrical and Electronics Engineers (IEEE) has defined several standards for LANs under IEEE 802.
    - 802.1 - internetworking;
    - 802.2 - logical link control;
    - 802.3 - Ethernet or CSMA/CD;
    - 802.4 - token bus LANs;
    - 802.5 - token ring LANs;
    - 802.6 - MANs;
    - 802.7 - broadband LANs;
    - 802.8 - fiber optic LANs and MANs;
    - 802.9 - integrated (voice/data) services LANs and MANs;
    - 802.10 - security in LANs and MANs;
    - 802.11 - wireless LANs;
    - 802.12 - demand priority access LANs;
    - 802.15 - wireless PANs; and
    - 802.16 - broadband wireless MANs.

IEEE 802.11

- The IEEE 802 standard deals with the data link layer and the physical layer of the OSI reference model.
- It defines rules for cabling, signaling, and media access control, which assure interoperability between network products manufactured by different vendors.



Fundamentals of WLANs

- Difference between wireless and wired
  - Address is not equivalent to physical location
  - Dynamic topology and restricted connectivity
  - Medium boundaries are not well-defined
  - Error-prone medium

- Use of WLANs
  - Surf Internet on the move
  - Areas without infrastructure, or affected by earthquakes or disasters WLANs can be set up on the fly
  - Historic buildings may not be wiring

Design Goals

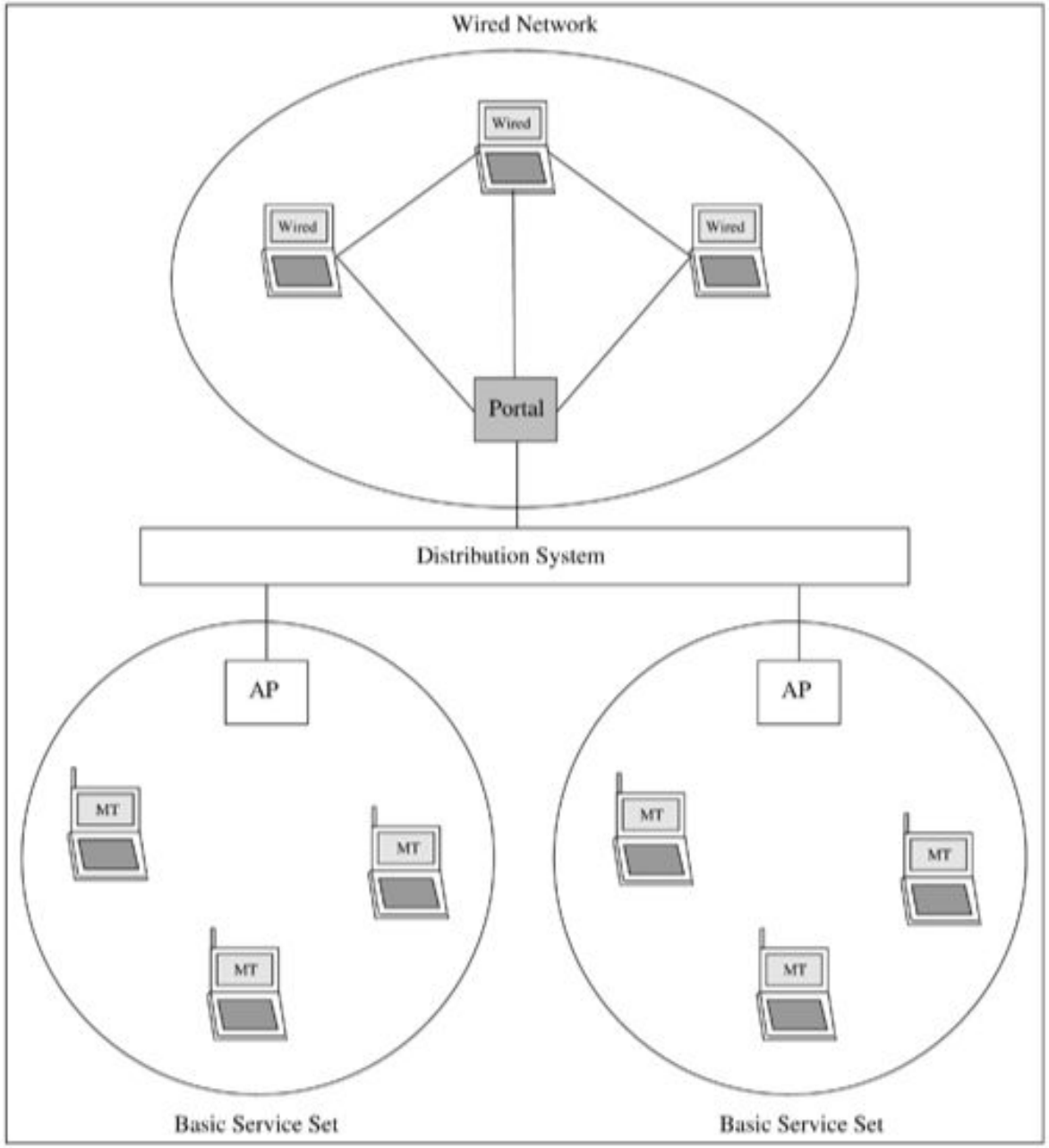
- Design Goals
  - Operational simplicity: Quickly set up n/w and services
  - Power-efficient operation:
  - License-free operation
  - Tolerance to interference
  - Global usability
  - Security: Broadcast Nature
  - Safety requirements: Interference to other devices, Health problem due to increased power level
  - Quality of service requirement
  - Compatibility with other technologies and applications

Network Architecture

- Infrastructure Based vs. Ad Hoc LANs
  - Infrastructure: access points (APs) and mobile stations (STAs or MTs)
  - Ad hoc LANs: do not need fixed infrastructure
- Components in IEEE 802.11 network
  - BSA: coverage of an AP
  - BSS: Basic Service Set
  - DS: Distributed System
  - ESS: Extended Service Set
  - Figure 2.1
- An adhoc LAN has only one BSS and known as independent basic service sets (IBSSs).

- ESS and IBSS appear identical to the logical link control (LLC)

An example of ESS



Service offered by IEEE 802.11 network

- Association: Knowing STA and giving address to it
- Reassociation: Established association is transferred one AP to another on moving STA
- Diassociation: Termination of existing association
- Distribution: routing
- Integration: if send frames through non-802.11
- Authentication
- Deauthentication
- Privacy
- Data delivery

IEEE 802.11 Standard

- The IEEE 802.11 standard, was brought out in 1997.
- IEEE 802.11b [3], commercially known as Wi-Fi (wireless fidelity)
- The IEEE802.11 working group has challenge of connection management, link reliability management, and power management: none of which was a concern for other standards in IEEE 802.
- In addition, provision for security is to be introduced.
- MTs can operate in two modes:
  - (i) infrastructure mode, in which MTs can communicate with one or more APs which are connected to a WLAN, and
  - (ii) ad hoc mode, in which MTs can communicate directly with each other without using an AP

IEEE 802.11

- Physical Layer: Divided into two parts
  - Physical medium dependent sublayer (PMD)
    - Encoding, decoding and modulation
  - Physical layer convergence protocol (PLCP)
    - Abstracts functionality for MAC
    - Offers service access point (SAP): 1 or 2Mbps
    - Clear channel assessment (CCA): CSMA/CA
  - 3 choices:
    - Frequency Hoping Spread Spectrum (FHSS) in 2.4 GHz ISM band: with Gaussian Frequency Shift Keying (GFSK) 2 Level at 1 Mbps and GFSK 4 level at 2Mbps
    - Direct Sequence Spread Spectrum (DSFF) in ISM band: using differential binary shift keying DBPSK for 1 Mbps and differential quadrature phase shift keying (DQPSK) for 2 Mbps.
    - Infrare: PPM (Pulse position modulation) for 1-2 Mbps

Basic MAC Layer Mechanisms

- Multiplex the transmission requests of various STAs
- MAC is used to access the channel
- Additionally, it offers support for roaming, authentication and power conservation.
- Distributed Foundation Wireless Medium Access Control (DFWMAC)
  - Distributed coordination function (DCF): The primary access method based on CSMA/CA
  - To avoid hidden terminal, RTS/CTS
  - Point coordination function (PCF):Second method fot real time services
  - Inter-Frame Spacing (IFS)
    - SIFS
    - PIFS
    - DIFS
    - EIFS

Inter Frame Spacing (IFS)

- **Short inter-frame spacing (SIFS)** is the shortest of all the IFSs and denotes highest priority to access the medium.
  - Used for short control messages such as acknowledgments and polling responses.
  - The transmission of any packet should begin only after the channel is sensed to be idle for a minimum time period of at least SIFS.
- **PCF inter-frame spacing (PIFS)** is the waiting time whose value lies between SIFS and DIFS. This is used for real-time services.
- **DCF inter-frame spacing (DIFS)** is used by stations that are operating under the DCF mode to transmit packets. This is for asynchronous data transfer within the contention period.
- **Extended inter-frame spacing (EIFS)** is the longest of all the IFSs and denotes the least priority to access the medium. EIFS is used for resynchronization whenever physical layer detects incorrect MAC frame reception.

CSMA/CA Mechanism

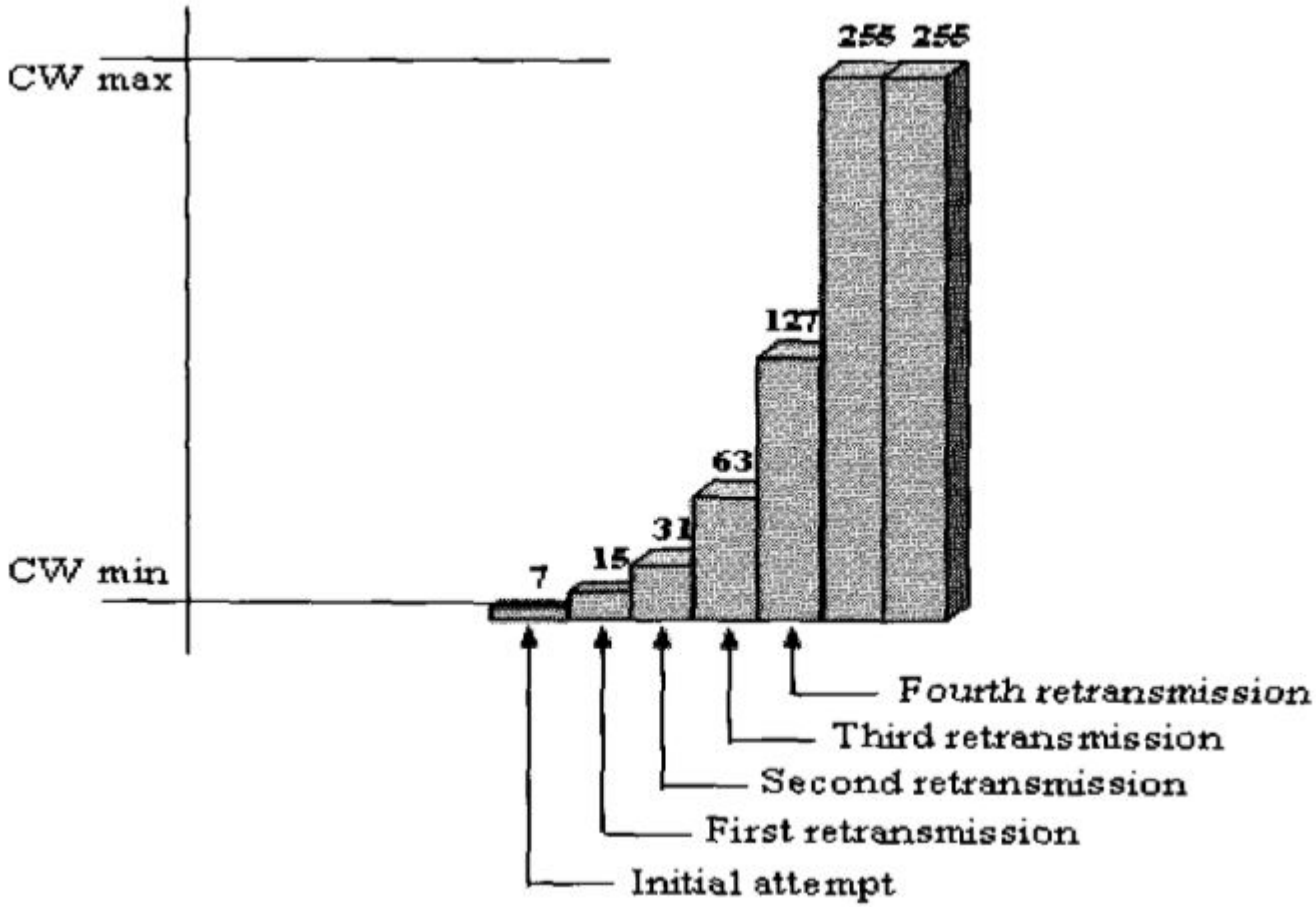
- CSMA/CD is not applicable
- IEEE 802.11 DCF and RTS-CTS

The Distributed Coordination Function (DCF)

- conducts two forms of carrier sensing: physical (by listening to the wireless shared medium) and virtual.
- Virtual carrier sensing uses the duration field which is included in the header of RTS and CTS frames and used to set NAV (Network Allocation Vector)
- Whenever NAV is zero, a station may transmit if the physical sensing allows.

Back off mechanism

- If the medium is found idle for more than a DIFS period, then the frame can be transmitted.
- Otherwise, the transmission is deferred and the station uses an Exponential Random Backoff Mechanism by choosing a random backoff interval from [0, CW], where CW is called contention window.
- When the backoff counter reaches zero, the station attempts to transmit its frame. If collision occurs with some other transmission, the station doubles its CW, chooses a new backoff interval and tries retransmission.
- CW size
  - Unnecessary delay if too large
  - Collision probability increase if too small
  - Binary exponential backoff technique is used


CW max
CW min
255
255
127
63
31
15
7
Fourth retransmission
Third retransmission
Second retransmission
First retransmission
Initial attempt

CSMA/CA Mechanism

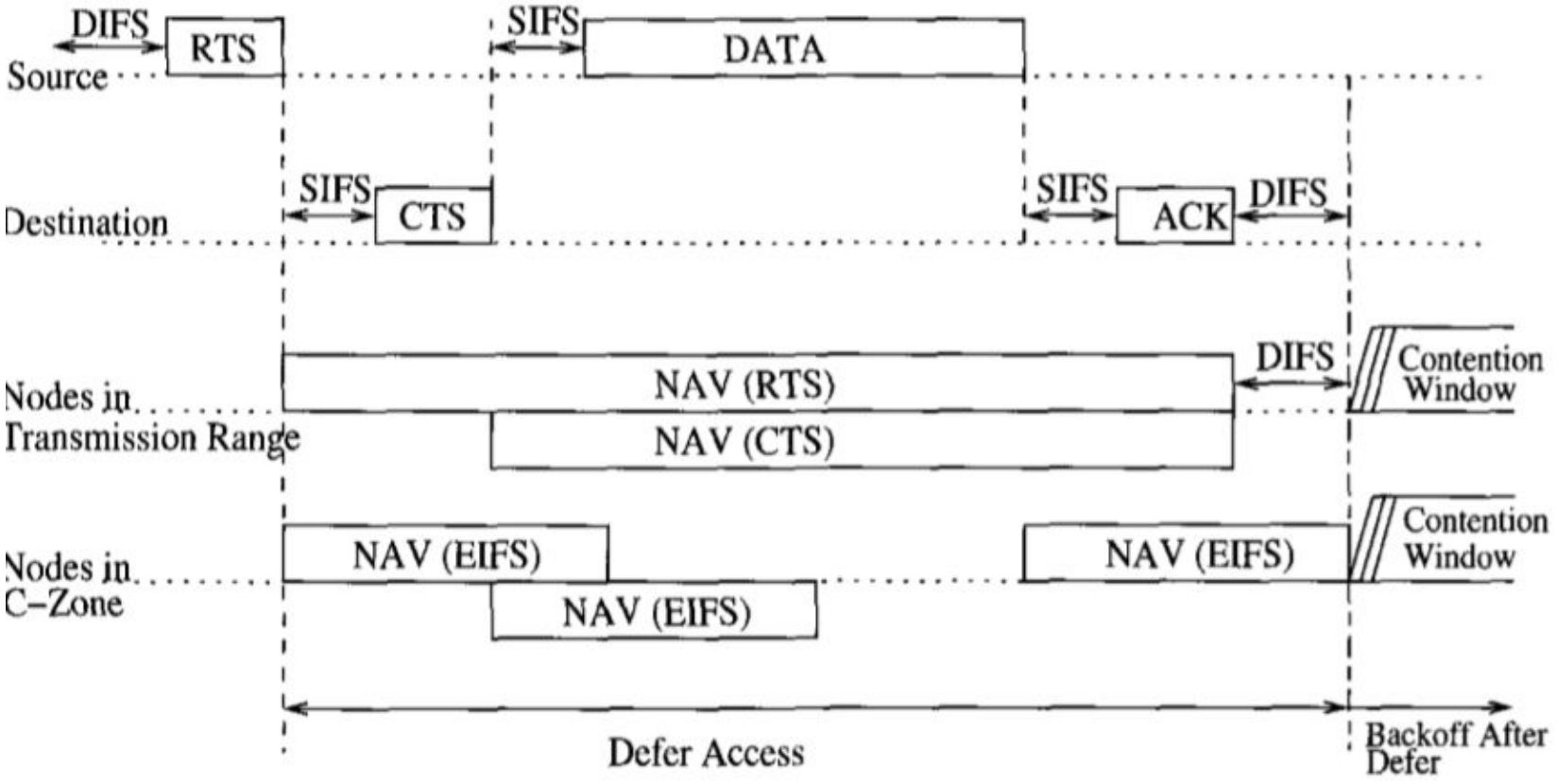


Figure 4.14 – Nodes in the transmission range and C-zone set their NAVs differently

Collision Scenario after RTS/CTS

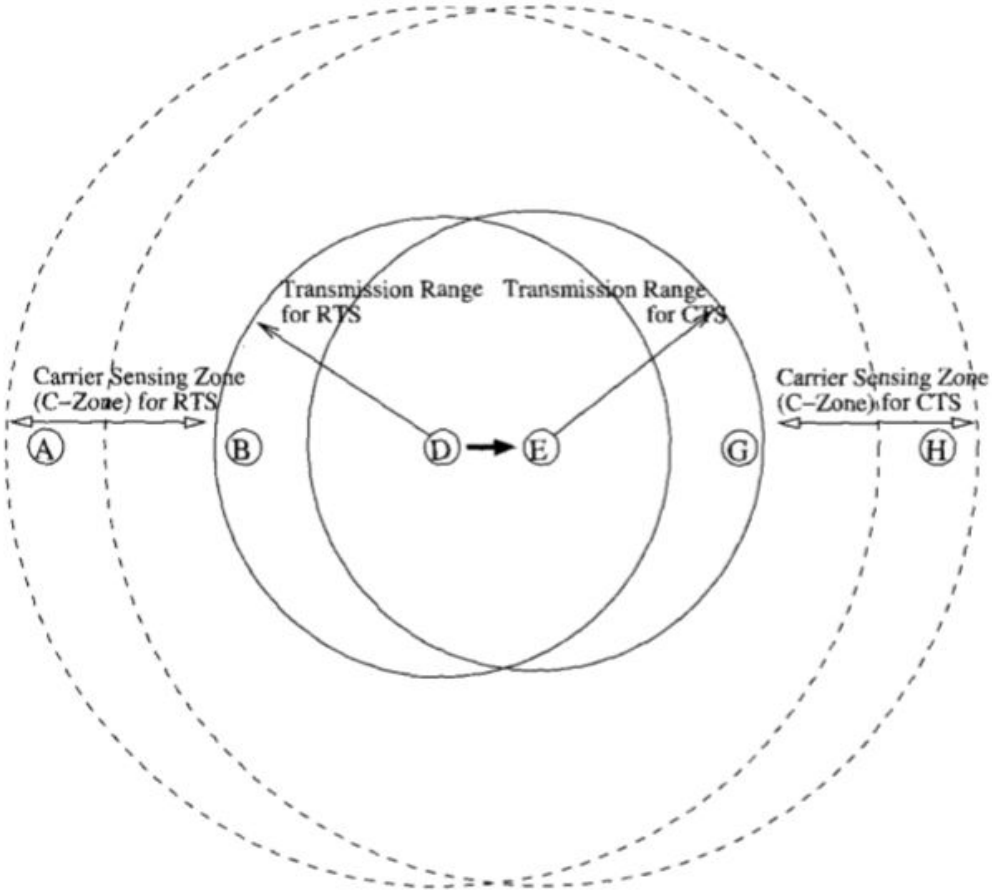


Figure 4.15 – Collisions are not completely avoided in IEEE 802.11

Overhead involved in RTS-CTS

- Non-negligible overhead
- If frame size > RTS_threshold, RTS-CTS is activated, a four-way handshake (I.e. RTS-CTS-DATA-ACK)
- If frame size < RTS_threshold, a two-way handshake (DATA-ACK)

Fragmentation

- Decreasing frame error rate use shorter frames split user data packet into fragments
- RTS/CTS carry duration for current fragment and estimated time for next fragment
- Medium reserved for successive frames

Other MAC Layer Functionalities

- Point Coordination Function
  - Guarantee on maximum access delay, minimum transmission bandwidth and other QoS
  - Centralized scheme, applicable only in networks where AP (Point Coordinator) pool nodes
  - Superframe: contention free periods(CFP)+contention period(CP)

Synchronization

- Timing synchronization function (TSF)
- Required for
  - Power management
  - PCF coordination
  - Frequency hopping spread spectrum (FHSS) hopping sequence synchronization
- Within a BSS
  - Beacon frames transmitted by AP
  - Contains time-stamp for adjusting clock
  - Contains information for power optimization and roaming

Power Management

- Always ready to receive consume more power (as high as 100 mA)
- Must be switched off whenever carrier sensing is not needed
- 2 states: sleep and awake
  - Longer periods in sleep leads to low throughput
  - Shorter periods in sleep leads to high power consumption

Roaming

- Provide uninterrupted service when walk around with a wireless station
- When poor quality of current link, start scanning for another AP
  - Active scanning: send a probe on each channel and wait for response
  - Passive scanning: listen medium to find other networks

Other Issues

- Newer standards
  - 802.11a/11b/g
  - Trademark by Wireless Ethernet Compatibility Alliance (WECA) as Wi-Fi
  - 802.11e: time-sensitive applications, voice/video
  - 802.11f: inter-AP communication to handle roaming
  - 802.11i: advanced encryption for better privacy

Wired Equivalent Privacy (WEP)

- Data integrity
- Access control
- Confidentiality
- Vulnerable if more sophisticated mechanisms are used to crack the key

Wi-Fi

- WiFi stands for Wireless Fidelity. It is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building b
roadband coverage.
- A vast majority of laptops shipped today have a built-in WiFi interface. WiFi interfaces are now also being built into a variety of devices, including personal data assistants (PDAs), cordless phones, cellular phones, cameras, and media players.
- Wi-Fi works by using radio waves operating at frequencies of 2.4 GHz or 5 GHz to transmit and receive data over the air.
- The range and quality of a wireless signal largely depends on the location and environmental conditions that may or may not interfere with the signal.
- Below are rough estimates of maximum WiFi range, concluded from tests done on Teltonika-Networks RUT routers:
- up to 100 meters in LoS (Line of Sight)
- up to 25 meters in buildings

IEEE 802.11 Wi-Fi protocol summary

Protocol	**Frequency**	**Channel Width**	MIMO	**Maximum data rate (theoretical)**
802.11ax	2.4 or 5GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	2.4 Gbps[1]
802.11ac wave2	5 GHz	20, 40, 80, 160MHz	Multi User (MU-MIMO)	1.73 Gbps[2]
802.11ac wave1	5 GHz	20, 40, 80MHz	Single User (SU-MIMO)	866.7 Mbps[2]
802.11n	2.4 or 5 GHz	20, 40MHz	Single User (SU-MIMO)	450 Mbps[3]
802.11g	2.4 GHz	20 MHz	N/A	54 Mbps
802.11a	5 GHz	20 MHz	N/A	54 Mbps
802.11b	2.4 GHz	20 MHz	N/A	11 Mbps
Legacy 802.11	2.4 GHz	20 MHz	N/A	2 Mbps

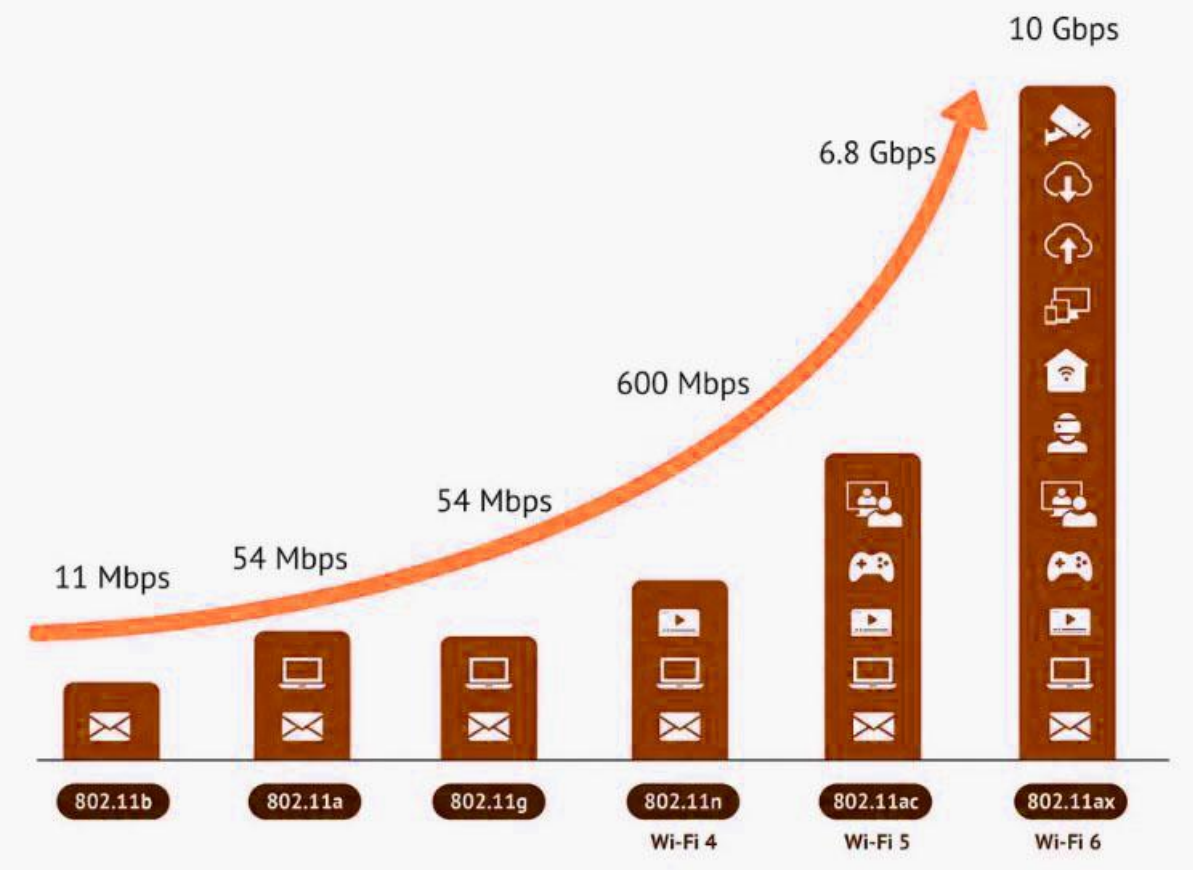
[1] 2 Spatial streams with 1024-QAM modulation.
[2] 2 Spatial streams with 256-QAM modulation.
[3] 3 Spatial streams with 64-QAM modulation.

Evolution of Wi-Fi

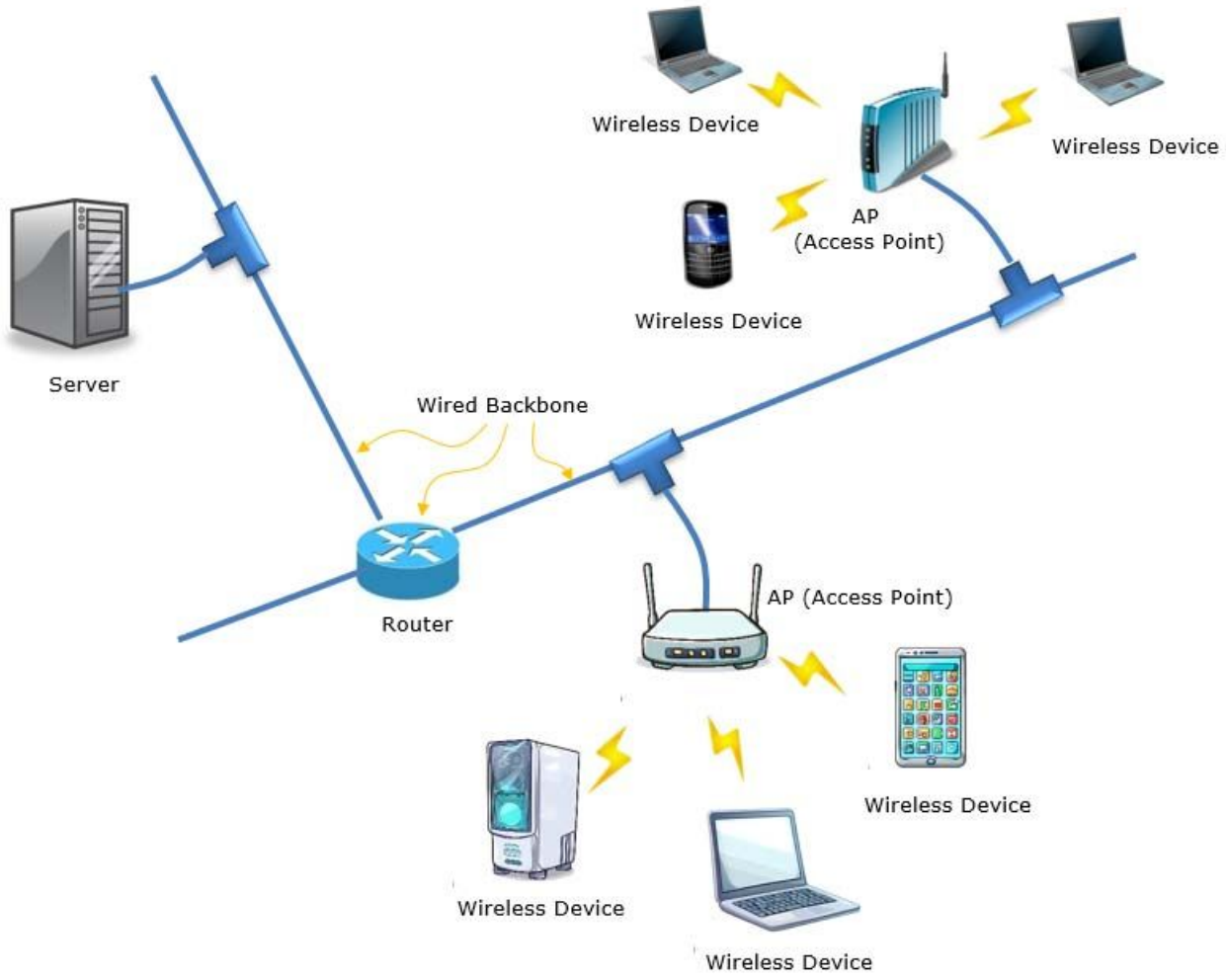
IEEE Protocol	Key Features
802.11	- The original Wi-Fi standard from 1997 operates in the 2.4 GHz band, providing up to 2 Mbps of speed. - This formed the basis for Wi-Fi wireless networks.
802.11b (Wi-Fi 1)	- Released in 1999, it also operated at the 2.4 GHz band but incorporated modulation techniques like DSSS/CCK to reduce interference and achieve higher speeds of up to 11 Mbps. - Enabled wireless usage at distances of 140m outdoors.
802.11a (Wi-Fi 2)	- Introduced in 1999 as a successor to 802.11b. - First Wi-Fi standard to use OFDM modulation to support high data rates up to 54 Mbps in a 5 GHz band.
802.11g (Wi-Fi 3)	- Released in 2003, it allows speeds up to 54 Mbps in the 2.4 GHz band through OFDM. - Appealing to the mass market due to the lower cost of 2.4 GHz devices.
802.11n (Wi-Fi 4)	- Introduced in 2009, supporting 2.4 and 5 GHz bands. - Delivered up to 600 Mbps speeds using multiple channels and other features. Enabled replacement of wired networks.
802.11ac (Wi-Fi 5)	- Released in 2013, it supports 3.5 Gbps speeds with greater bandwidth, channels, and better modulation. - The first standard to use Multiple Input Multiple Output (MIMO) allows multiple antennas on devices.
802.11ax (Wi-Fi 6)	- Latest standard from 2021. The focus is on improving performance in dense deployments through mechanisms like multi-user and scheduling transmissions. - It enhances video streaming and cloud access.
802.11ay (Wi-Fi 6E)	- is an upgraded version of WiFi 6, operates in the 6 GHz band, offering significant bandwidth for high speeds. - Reduces interference with existing 2.4/5 GHz devices for a better experience.
P802.11be (Wi-Fi 7)	- The next evolution under development is aiming for 4x faster speeds up to 40 Gbps. - Will support more devices efficiently with lower latency. Expected completion in 2024.

Evolution of Wi-Fi

- Future standards will also focus on new use cases like **battery-free IoT devices** using ambient energy harvesting, extremely high throughput for **AR/VR,** and **leveraging AI/ML** to improve Wi-Fi performance.



Components and Working Principles of Wi-Fi



Components and Working Principles of Wi-Fi

- The working principle and key components involved in Wi-Fi communication are:
- **Access point**: This device creates the wireless network and broadcasts the network name or **SSID**.
  - The access point hardware has a wireless transmitter, receiver, router and an ethernet port to connect to the internet via a **modem or LAN.**
- **Wireless device**: The device like a smartphone has an **inbuilt Wi-Fi antenna** and **transceiver.** This allows the device to detect wireless networks in the area and connect to them.
- **Router**: This connects the access point to the internet. Both access point and router functions can be in the same hardware device.
- **Frequency band**: The Wi-Fi frequencies like **2.4 GHz** and **5 GHz** have multiple channels. Data transmission happens on these channels avoiding interference.
- **2.4 GHz and 5 GHz:** 2.4 GHz provides a longer range while 5 GHz can deliver faster speeds with less interference.
  - Wi-Fi routers typically transmit on both bands to utilise their complementary strengths and support different types of devices and use cases.
  - **Older Wi-Fi standards** relied more on **2.4 GHz** while **newer standards** focus on **5 GHz** for performance.
- **Data transmission**: When a wireless device connects to the network, radio waves transmit data on the wireless channel.
  - The data is encoded into **binary format** and then **electromagnetic waves** in the channel carry this data.
- **Security encryption**: To secure the wireless transmissions, data is encrypted using protocols like **WPA2**.
  - Only authorised devices with the correct encryption passwords can connect and transmit data.
- **Internet**: The router connects the Wi-Fi network to the Internet. This allows the wireless devices to access the internet via the access point. The modem connects the router to the ISP.

WiFi vs Cellular Networks

Parameters	WiFi	Cellular
Standards	802.11 protocols	3G, 4G, 5G standards
Frequency bands	2.4 GHz, 5 GHz	700 MHz to 2.5 GHz
Typical range	<100 meters indoors	Multiple km outdoors
Maximum speed	1-10 Gbps	10-100 Mbps
Architecture	Wireless LAN	Cell towers, core networks
Scalability	Limited	Excellent
Security	WPA2 encryption	Encryption, network-level measures
Mobility	Medium	High
Power	High	Low
Latency	Very low <20 ms	Medium 50-500 ms

Bluetooth vs Wi-Fi

Parameter	Bluetooth	WiFi
Range	Up to 10 meters	Up to 100 meters indoors
Speed	1-3 Mbps	Up to 1300 Mbps (WiFi 6)
Frequency	2.4 GHz	2.4 GHz / 5 GHz
Devices	Headsets, speakers, smartphones, IoT devices	Computers, smartphones, tablets, printers
Power	Very low	Higher power consumption
Security	Encryption available	Stronger security like WPA3

Challenges and Issues with Wi-Fi Technology

- Despite the convenience of Wi-Fi networks, they come with some challenges and limitations, such as:-
- **Range limitations:** Consumer Wi-Fi networks indoors typically have a range of 100-150 feet, and outdoors up to 300 feet.
  - However, obstacles can further reduce the range.
- **Speed variability:** Actual Wi-Fi speeds are often lower than the maximum advertised speeds due to factors such as distance from the access point and interference.
- **Congestion:** In areas with a high density of Wi-Fi networks, such as apartments, interference and congestion can degrade performance.
- **Power consumption**: Wi-Fi communication consumes more power on mobile devices compared to low-power Bluetooth, which reduces battery life.
- **Interoperability issues:** There is a varying level of support for new Wi-Fi generations across device types and operating systems.
- **Security vulnerabilities:** Public Wi-Fi networks can pose privacy and security concerns.
- **Set-up complexity:** Correct installation and configuration require some technical skill beyond just plug and play.

Impact of Wi-Fi in India

- Wi-Fi Technology has greatly influenced wireless internet access, mobility, and connectivity across India. Some pertinent points regarding Wi-Fi in India are:
- **Universal coverage**: Wi-Fi is now present everywhere in India, with over 800 million mobile internet subscribers.
  - The majority of devices are Wi-Fi-enabled.
- **Public hotspots growth**: Public Wi-Fi hotspots have seen steady growth, with over 36,000 installed across India as of 2022.
- **The key for Smart Governance:** Wi-Fi is a centrepiece of Digital India initiatives like **Smart Cities,** facilitating **e-governance** and **public service delivery.**
- **Institutional adoption**: Educational institutes, offices, malls, and hotels have extensively deployed Wi-Fi networks.
  - It has transformed internet access.
- **Work/Study from home:** During the pandemic, Wi-Fi enabled critical work/study-from-home capabilities.
- **Emerging applications:** Wi-Fi has opened up new applications in IoT, industrial automation, retail analytics using captive portals, location-based services, etc.

Government Initiatives

- **RailWire Wi-Fi**: Indian Railways has installed 6108 free public Wi-Fi networks at railway stations across India through its RailWire initiative.
- **Smart Cities mission**: Under the Smart Cities mission, over 5000 Wi-Fi hotspots are being deployed across 100 smart cities by 2022.
- **BharatNet**: BharatNet project aims to expand broadband penetration to gram panchayats through Wi-Fi and wireless mesh networks.
- **PM-WANI**: The Prime Minister's **Wi-Fi Access Network Interface** initiative aims to proliferate Wi-Fi hotspots through public data offices.
- **Wi-Fi in schools**: **National Digital Communications Policy 2018** outlined setting up Wi-Fi networks in all secondary and higher secondary schools.

ZigBee Network

- The name ZigBee originates from the zig-zag waggle dance of Honey bees. ZigBee is based on IEEE 802.15.4 standard for Low Rate Wireless Personal Area Network (LR-WPAN).
- ZigBee uses radio frequency (RF) for communication and operated on one of the three different radio bands: 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in world wide.

IEEE 802.15.4 and ZigBee

IEEE 802.15.4	**ZigBee**
It was created by the Institute of Electrical and Electronics Engineers (IEEE),for low rate personal area network.	It was created by the ZigBee Alliance.
IEEE 802.15.4 focuses on lower two layers(physical and data link layer) of OSI.	ZigBee Alliance aims to provide the upper layers (from network to the application layer) of OSI based on IEEE 802.15.4.
Its main purpose is the communication between two devices.	Its main purpose is to create a network topology and add features such as security, encryption, association and in the upper layer application services.

ZigBee vs. Bluetooth

ZigBee	Bluetooth
ZigBee is a low-cost, low-power, wireless mesh network.	Bluetooth was designed for low power consumption with short range communications.
The operational range of ZigBee is 10-75m.	The operational range of Bluetooth is 10m.
It allows up to 254 nodes.	It allows up to 8 slave nodes in a basic master-slave piconet set-up.
Battery life is 100-1000 days.	Battery life is 1-7 days.

Features & Characteristic of ZigBee Technology

- ZigBee network connect several units and control through one button.
- ZigBee network is controlled by a remote control device at a specific range and as the control device is present centrally, it reduces manpower.
- ZigBee devices are reliable because they are designed on low-power frequency.
- ZigBee technology supports 3 different types of devices. They are coordinator, router and end-user devices.
- Coordinators are the primary devices to help in activation of the system by collecting the data in form of memory.
- Routers are the secondary devices that function by sending information to the destination.
- End-user devices are basically receivers that are not able to send information itself.

Application of ZigBee Technology

- ZigBee technology is programmed in a chip form and that chip is used in many devices to function automatically. For example controlling and monitoring a whole factory unit while sitting in one cabin is possible by using ZigBee technology.
- Building automation
- Consumer electronics
- Automatic meter reading
- Home automation
- Managing health care system
- Retail management
- Telecommunications

Component of IEEE 802.15.4 LR-WPAN

- **Coordinator :** Coordinator controls and monitor the established network. Based on their operation scope two different kinds of coordinators are present. The PAN-Coordinator, which acts as a coordinator for the entire PAN and the ordinary coordinator, which function within the scope of a cluster.
- **Cluster :** A cluster is a small section of a bigger network, which has its own coordinator. Groups of clusters communicate with a central PAN-Coordinator to form the PAN in a mesh topology.
- **Device/End Node :** A device is either a reduced/full function device, these are the end devices(leaf of a tree structure). Any device that is not a co-ordinator is an end node (device).
- **Personal Operating Space(POS) :** It is the operating range of a node in all directions, and is a constant irrespective of being in motion or stationary.

Component of IEEE 802.15.4 LR-WPAN

- There are 14 PHY and 35 MAC Primitives defined by the IEEE 802.15.4 standard. The LR-WPAN supports two types of devices called the Full Function Device and the Reduced Function Device.
- **Full Function Device(FFD) :** It is a device which supports all the 49 primitives supported by the technology. It acts as a PAN coordinator, a Coordinator, or just as an end node (device). Also an FFD can function as a routing device in certain network topologies where data transfer among FFD is allowed (EX: peer-to-peer communication).
- **Reduced Function Device(RFD) :** It is a device with reduced functionality which can only function as an end device or node. It can only communicate with the coordinator. Their functionality is extremely low. So these devices are intended for simple applications like a light switch, etc. They merely send information to the coordinator at regular intervals about the status of the device it is monitoring. It can only support a maximum of 38 primitives .

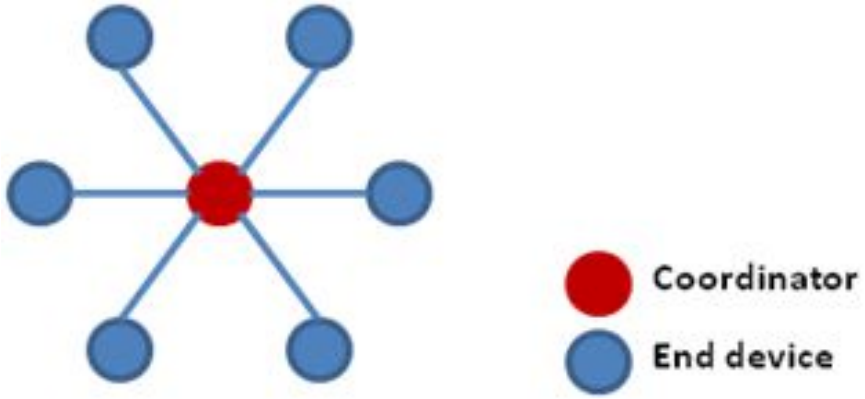
Network Topologies

A Low rate WPAN supports three different types of topologies

- Star Topology
- Peer-to-Peer Topology
- Cluster Tree/Mesh Topology

Star Topology

In the star topology, the PAN coordinator have the primary control. In this topology devices monitor their application and report it to the coordinator. The Figure-01 shows star topology.



Network Topologies

Peer-to-Peer Topology

The peer-to peer topology has a PAN coordinator and any device can communicate with any other device. This topology allows more complex network formations. Figure-02 shows peer-to-peer topology.

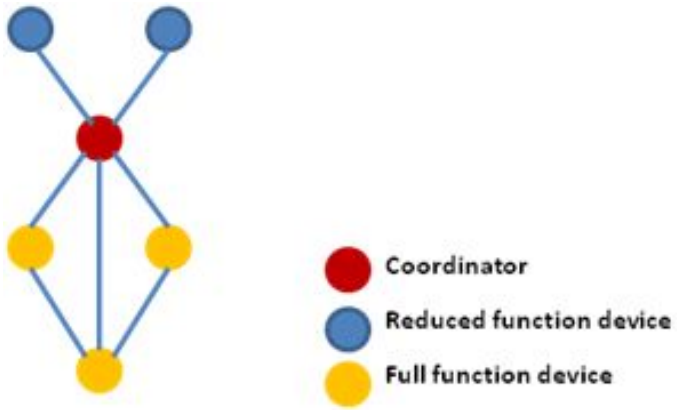


Figure-02: Peer-to-peer topology

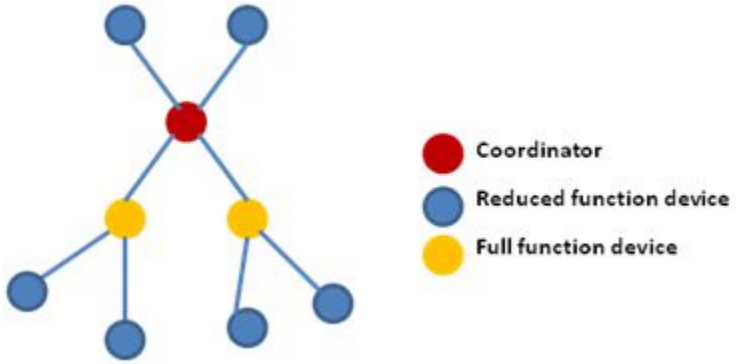


Figure-03: Cluster-tree topology

Cluster-Tree Topology

In cluster tree topology several small clusters are present and are able to communicate peer-to-peer and can be controlled with a PAN coordinator. Each cluster can have its own coordinator and the coordinators can communicate with the PAN Coordinator. We can choose a PAN coordinator among several existing clusters.Figure-03 shows cluster-tree topology.

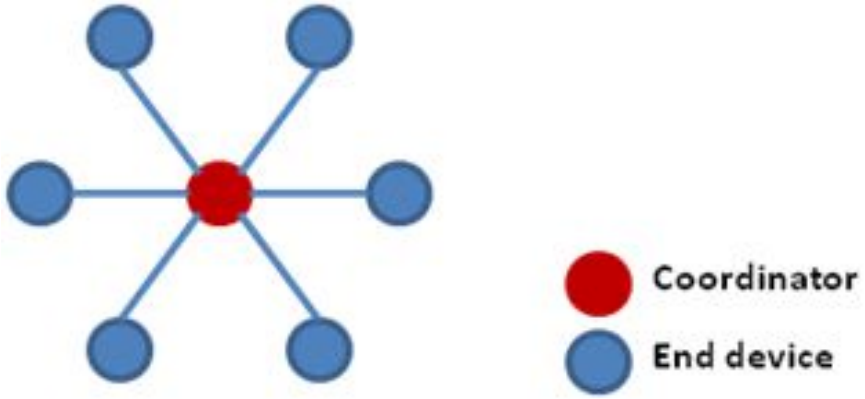
Network Topologies

A Low rate WPAN supports three different types of topologies

- Star Topology
- Peer-to-Peer Topology
- Cluster Tree/Mesh Topology

Star Topology

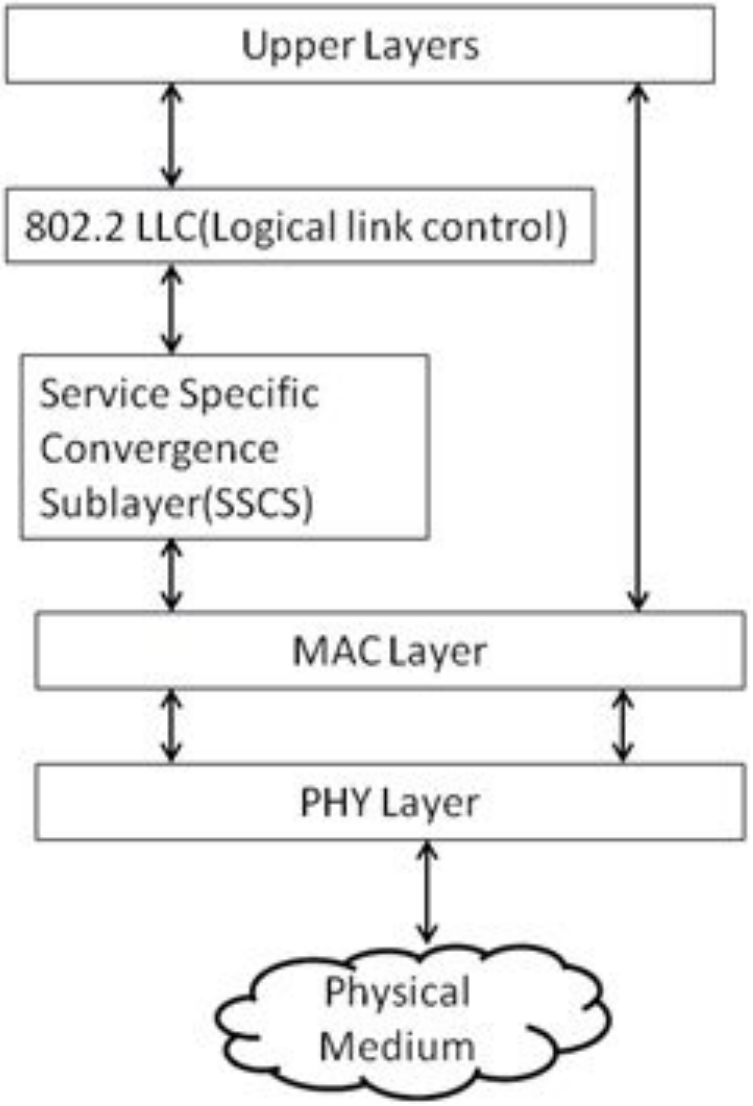
In the star topology, the PAN coordinator have the primary control. In this topology devices monitore their application and report it to the coordinator.The Figure-01 shows star topology.



ZigBee Architecture

- IEEE 802.15.4 consists of PHY and the MAC layers. The upper layers are left for application developers.

- The PHY layer is responsible for activation and deactivation of the radio transceiver, ED, LQI, channel selection, clear channel assessment (CCA), and transmitting as well as receiving packets across the physical medium. Similarly, the MAC layer is responsible for beacon management, channel access, guaranteed time slots (GTS) management, frame validation, acknowledged frame delivery, association, and disassociation.

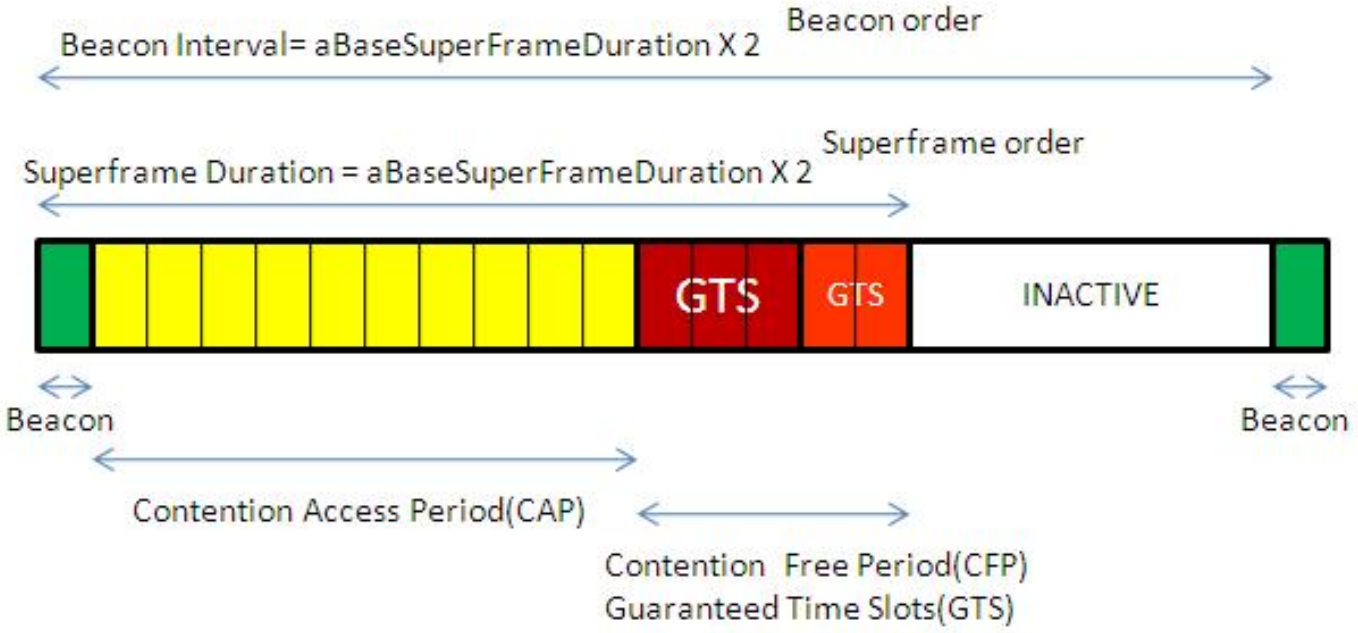


The Superframe structure

The superframe structur is determined by the coordinator. IEEE 802.15.4 networks are able to operate in two different modes of operation

- **Beacon mode or**
- **Non beacon mode**

In beacon mode, the coordinator sends out periodic packets or beacons. The purpose of this is to enable all nodes to sleep between beacons and wake up when the beacon timer expires, ready to receive the beacon from the coordinator. The superframe structure is only applicable in beacon mode networks. In non beacon networks the superframe structure is disabled and nodes contend for channel access by CSMA/CA.



The Superframe structure

Contention Access Period: It is the time duration in symbols during which the devices can compete with each other to access the channel using CSMA-CA and transmit the data.

Contention Free Period/Guaranteed Time Slots: Certain low-latency application devices are given exclusive rights over the channel to start transmission directly. There can as many as 7 slots assigned for GTS transmissions. These transmissions start immediately after the contention access period.

Inactive Period: It is the time period during which the coordinator would not interact with the PAN. Therefore, there will be no beacon transmissions. So the devices go to sleep mode in this duration.

Superframe Duration: The total time duration of the CAP, CFP (GTS) and a Beacon. The superframe duration doesn't include the inactive period.

Beacon Interval: It is the time duration between two successive beacons.

The beacon and superframe orders can range from 1 to 15 inclusive but the superframe order must be less than or equal to the beacon order. When the beacon and superframe order are equal there is no inactive period between beacons, when the superframe order is less than the beacon order there is an inactive period and setting them both to 15 disables beacon mode.

2.5 Bluetooth

- Logically partitioned into 3 layers:
  - Transport protocol group
    - Radio layer
    - Baseband layer
    - Link manager layer
    - Logical link control
    - Adaptation layer
    - Host controller interface
  - Middleware protocol group
    - RFCOMM, SDP, IrDA
  - Application group
    - Application profiles

Fig 2.7 Bluetooth protocol stack

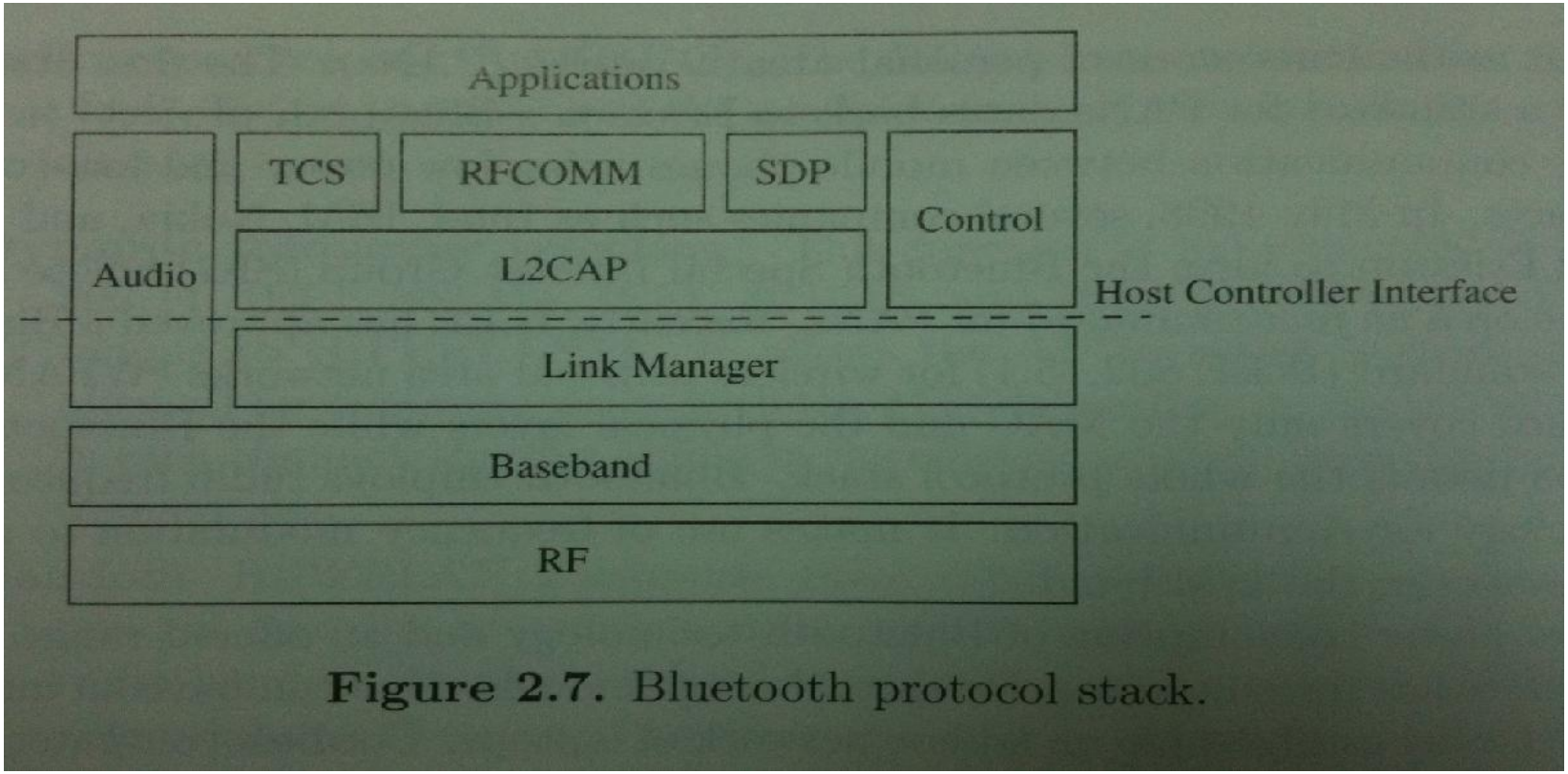


Figure 2.7. Bluetooth protocol stack.

本圖取自 "Ad Hoc Wireless Networks", by C. Siva Ram Murthy and B. S. Manoj, published by Prentice Hall, 2004

Radio (Physical) Layer

- GFSK
- 64Kbps voice channels and asynchronous data channels with peak rate of 1Mbps
- Data channel: asymmetric or symmetric
- 79 channels, 79 hops
- Typical link range: up to 10 m, can be extended to 100m by increasing power

Baseband Layer

- Piconet (Fig 2.8)
- 48-bit address

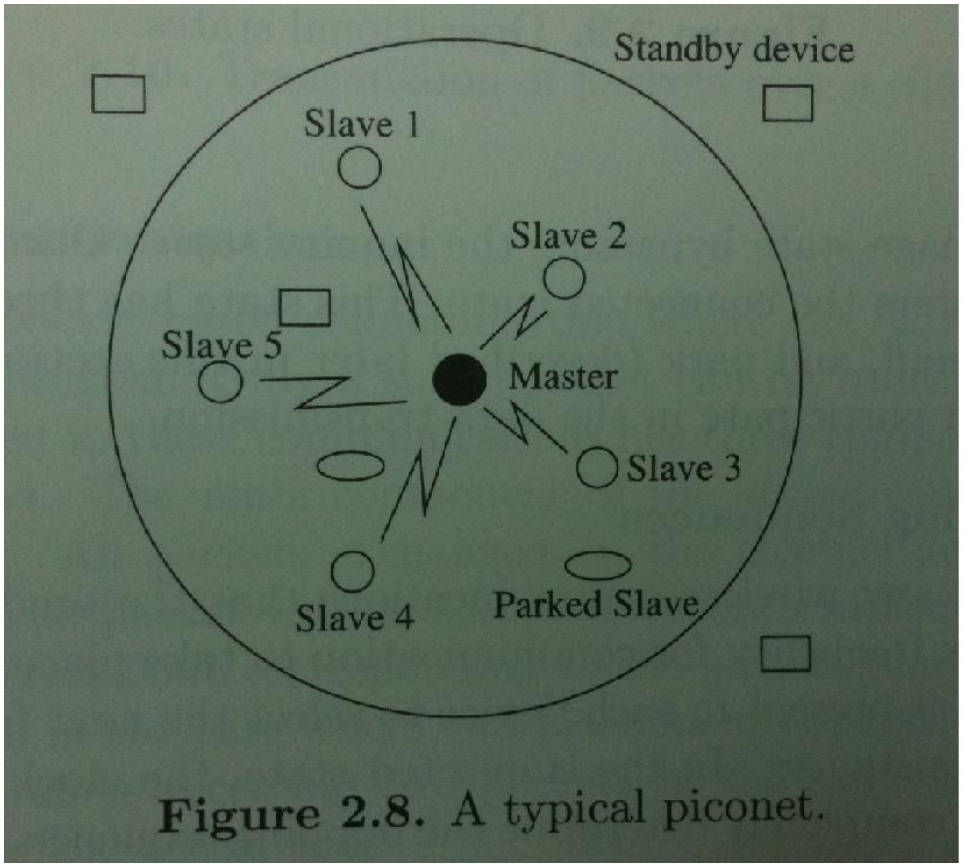


Figure 2.8. A typical piconet.

本圖取自 "Ad Hoc Wireless Networks", by C. Siva Ram Murthy and B. S. Manoj, published by Prentice Hall, 2004

Piconet

- Master + up to 7 active slaves

Fig 2.9 Operational States

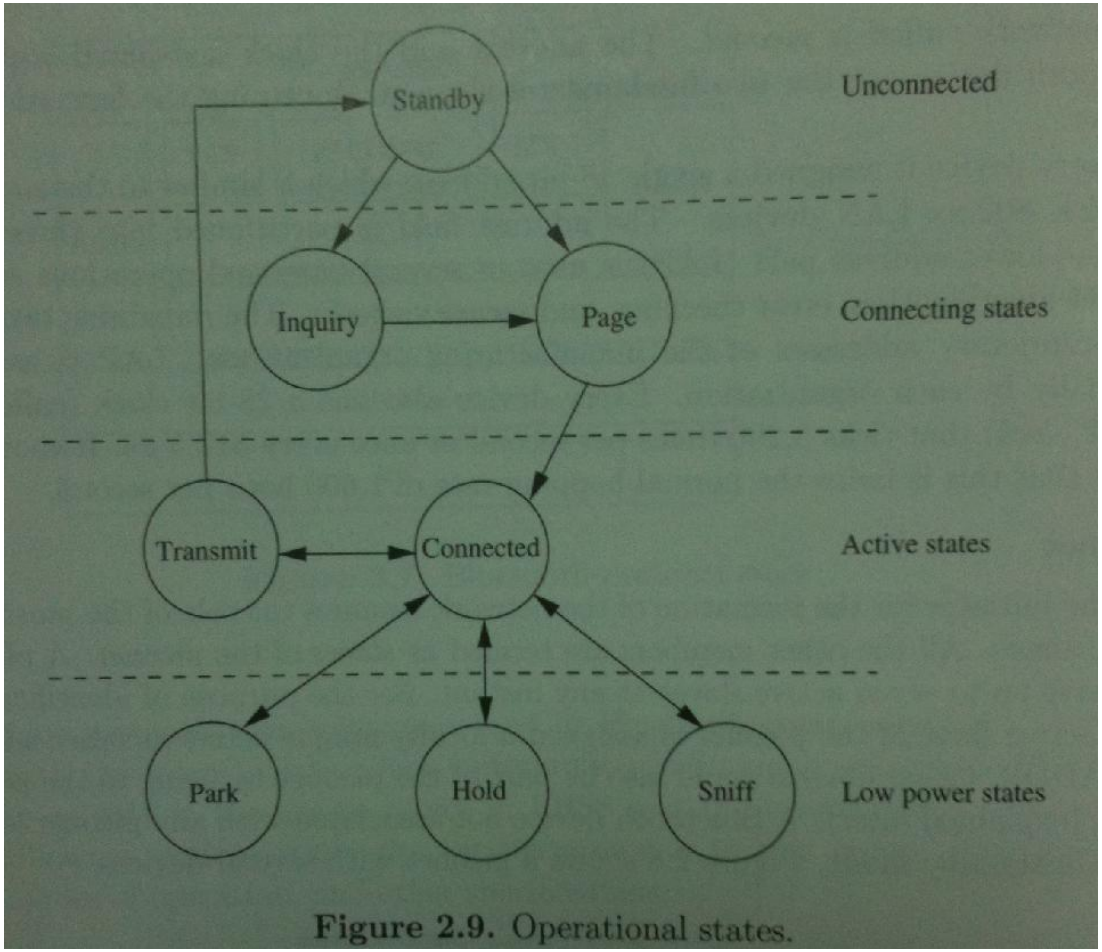


Figure 2.9. Operational states.

本圖取自 "Ad Hoc Wireless Networks", by C. Siva Ram Murthy and B. S. Manoj, published by Prentice Hall, 2004

Fig 2.10 Transmission over a channel

- ACL: asynchronous connectionless link
- SCO: synchronous connection oriented link

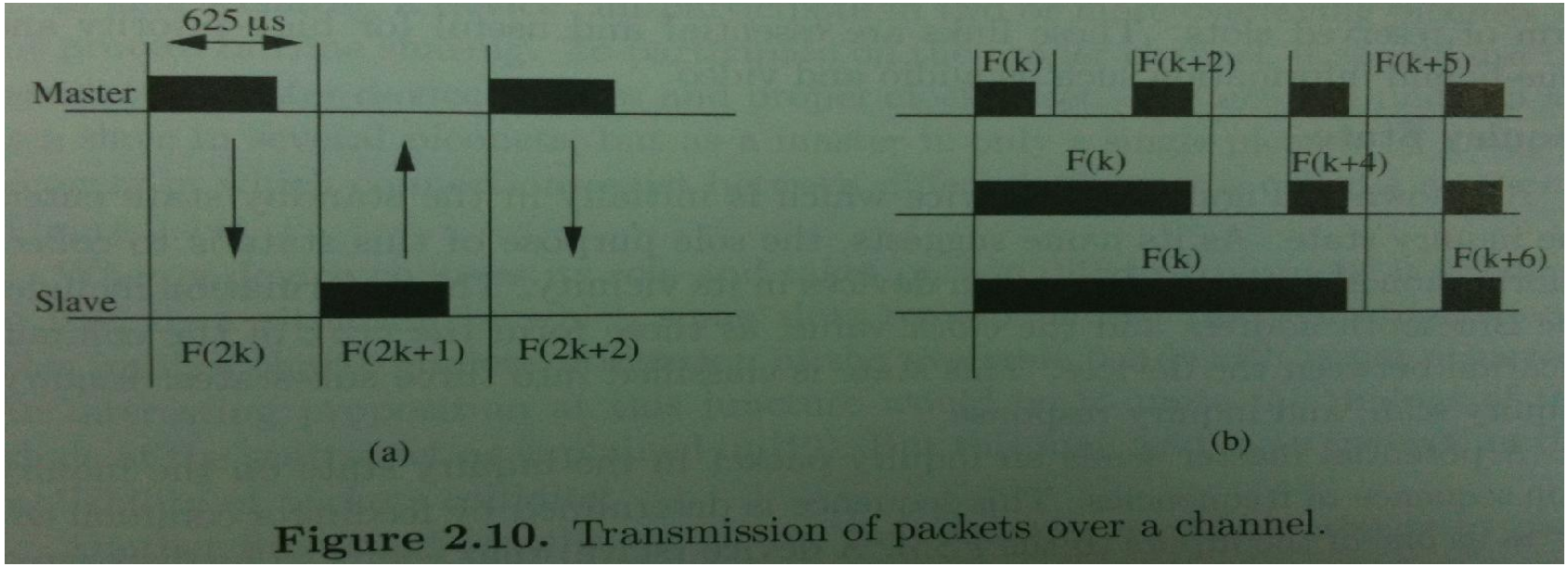


Figure 2.10. Transmission of packets over a channel.

本圖取自 "Ad Hoc Wireless Networks", by C. Siva Ram Murthy and B. S. Manoj, published by Prentice Hall, 2004

Inquiry State

- A potential master sends inquiry packet on inquiry hop sequence of frequencies
- A slave periodically enter inquiry scan state and listen for inquiry packets
- When received, send response packet containing hopping sequence and device address

Page State

- Master estimate slave's clock to determine hop sequence, and send page message
- Slaves listen in page scan mode
- On receiving page message, slave enter page response sub-state, send page response containing its device access code (DAC)
- Master enter page response state (after receiving slave's response), inform slaves its clock and address for determining hopping sequence and synchronization

Scatternets and Issues

- Piconet may overlap both spatially and temporally
- Each piconet is characterized by a unique master and hop independently
- As more piconets added, more probability of collisions
- Device can participate in 2 or more piconets by time sharing (as a slave in several piconets, but as a master in only a single piconet)
- A group of piconets □scatternet (Fig2.11)

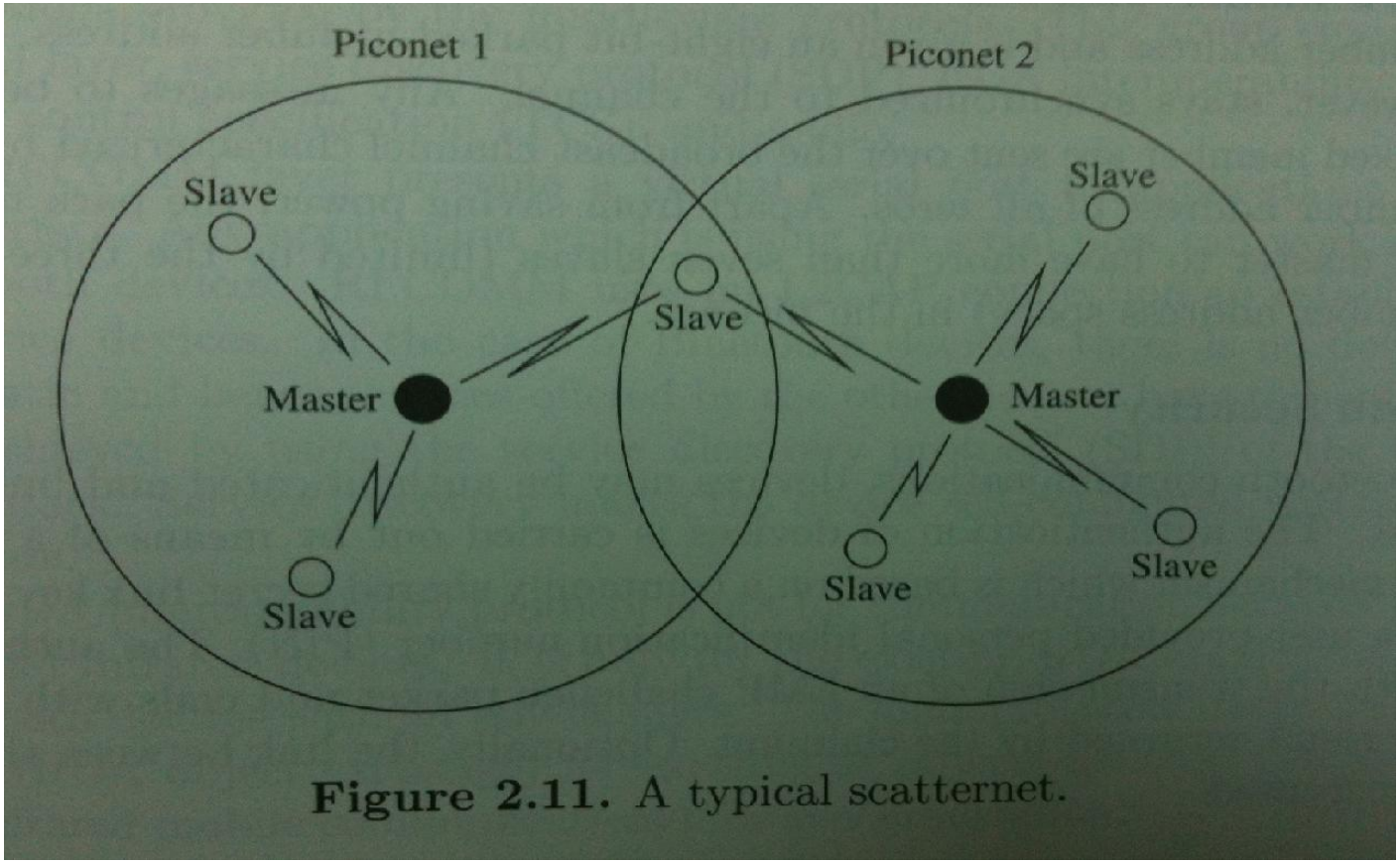


Figure 2.11. A typical scatternet.

本圖取自 "Ad Hoc Wireless Networks", by C. Siva Ram Murthy and B. S. Manoj, published by Prentice Hall, 2004

- Issues:
  - Gateway nodes: bound back-and-forth, hard to achieve full utilization
  - Timing may miss:

Link Manager Protocol

- Power Management
  - Active mode: active slaves are polled by master
  - Sniff mode: master issues a command to slave to enter sniff mode
  - Hold mode: temporarily not support ACL packets, performing scanning, paging, inquiring, or attending another piconet
  - Park mode: slave gives up its active member adress
- Security Management
- Minimal QoS support by allowing control over parameters such delay and jitter

2.5.4 Bluetooth Profiles

- Promote interoperability among many implementations of bluetooth protocol stack
- Provide a clear and transparent standard that can be used to implement a specific user end function
- 4 categories
  - Generic profiles
  - Telephony profiles
  - Networking profiles
  - Serial and object exchange profiles