# **Pure Aloha**

Saad Aljammaz

435105061

The node immediately transmits its frame completely

If the frame is collided it retransmits the frame again with the probability p.

**Slotted Aloha**

Frames are of the same size

time is divided into equal size slots

**Operation**

* **when node obtains fresh frame**, it transmits in next slot
* **no collision**, node can send new frame in next slot
* **if collision**, node retransmits frame in each subsequent slot with prob. p until success

Lecture 2

Carrier Sense Multiple Access(CSMA)

# Invented to minimize collisions and increase the performance

A node should not send if another node is already sending

# Persistence methods:

1. Non-persistent strategy

2. Persistent strategy

3. P-persistent strategy

CSMA with Collision Detection (CSMA/CD)

There are many collision detection methods!

* detecting voltage level on the line
* detecting power level
* detecting simultaneous transmission & reception

CSMA with Collision Avoidnes (CSMA/CA)

Priorities:

SIFS : highest priority, forACK, CTS, pollingresponse

PIFS : medium priority, for time-bounded service using PCF

DIFS : lowest priority, for asynchronous data service

Random Contention Access

# Slotted contention period:

* Used by all carrier sense variants
* Provides random access to the channel

Contention Window

* Random number selected from [0,cw].
* Small value for cw
* Optimal cw for known number of contenders & know packet size

# 802.11 - CSMA/CA unicast

Sending unicast packets :

* Station has to wait for DIFS before sending data
* Receiver acknowledges at once (after waiting for SIFS ) if the packet was received correctly (CRC)
* Automatic retransmission of data packets incase of transmission errors

Procedure :

* Similar to CSMA but instead of sending packets control frames are exchanged
* RTS = request to send
* CTS = clear to send
* DATA = actual packet
* ACK = acknowledgement

Advantages :

* Small control frames lessen the cost of collisions (when data is large)
* RTS + CTS provide “virtual” carrier sense which protects against hidden terminal collisions (where A can’t hear B)

# 802.11 DCF (CSMA-CA)

* Full exchange with “virtual” carrier sense (called the Network Allocation Vector)

# Carrier Sense Multiple Access (CSMA)

Procedure

* Listen to medium and wait until it is free (no one
* else is talking)
* Wait a random back off time then start talking

Advantages

* Fairly simple to implement
* Functional scheme that works

Disadvantages

* Can not recover from a collision  
  (inefficient waste of medium time)

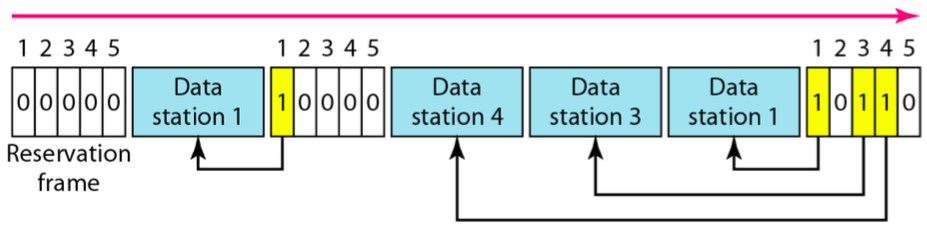
# Virtual Carrier Sense

* Provided by RTS & CTS
* Designed to protect against hidden terminal collisions (when C can’t receive from A and might start transmitting)

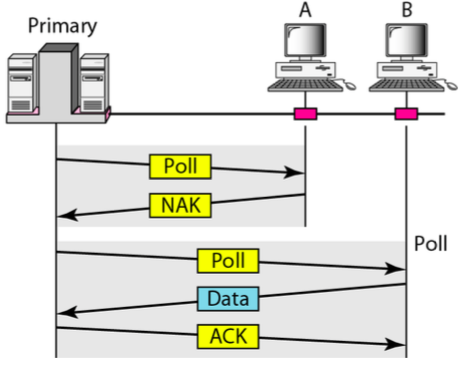
Lecture 2  
Controlled Access Protocols

It means which station has the right to send

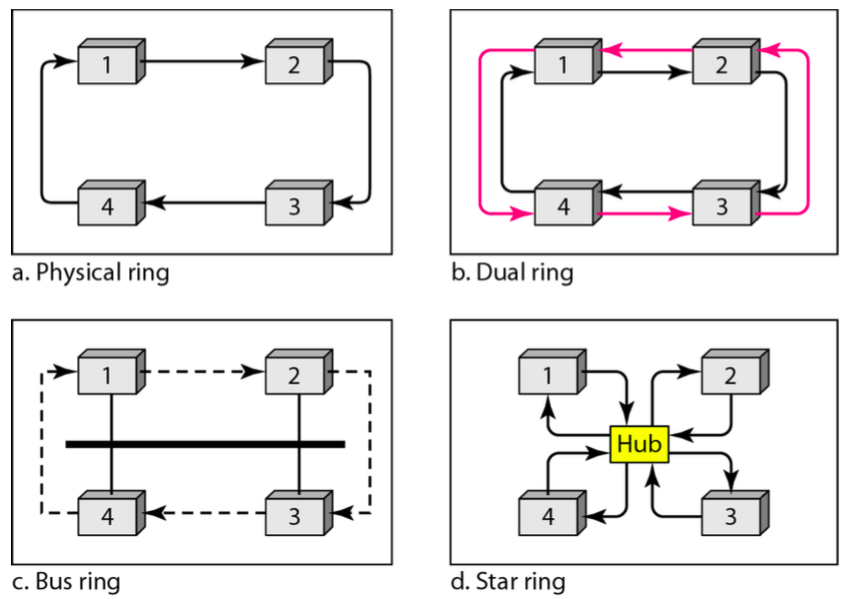
# Reservation



# Polling



# Token passing



Lecture 3

Channelization Protocols

It is multiple-access method in which the available bandwidth of a link is shared in Time , frequency or through code.

# Frequency-division multiple access (FDMA)

# 

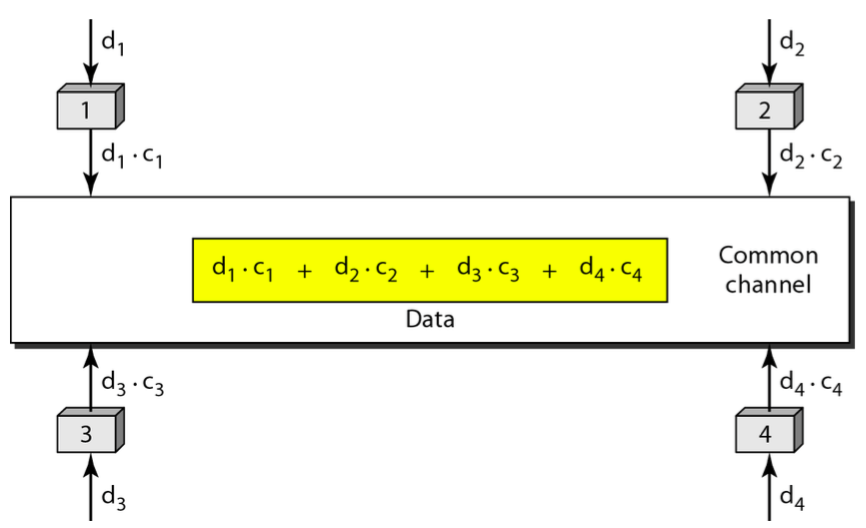
In FDMA, the available bandwidth of the common channel is divided into bands that are separated by guard bands.

# Time-division multiple access (TDMA)

# 

the bandwidth is just one channel that is timeshared between different stations.

Code-Division Multiple Access (CDMA)



In CDMA, one channel carries all transmissions simultaneously.

Lecture 3

Local Area Network  
(Ethernet)

It is the dominant LAN technology.

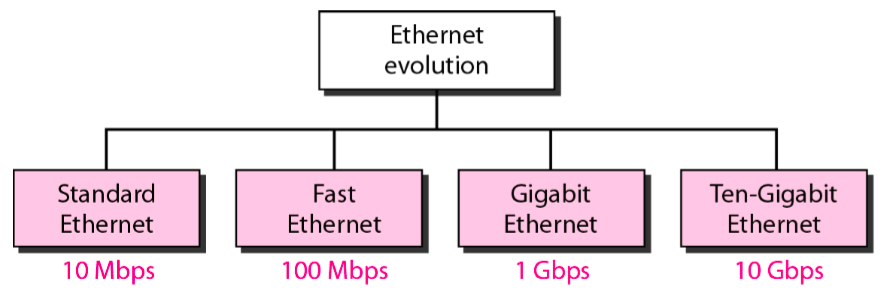
* Cheap
* First widely used LAN technology
* Simpler and cheaper than token LANs
* Kept up with speed race: 10, 100, 1000 Mbps

Physical layer

# Physical layer is dependent on the implementation and type of the physical media used.

* IEEE define detailed specifications for each LAN implementation.

Ethernet evolution



# Ethernet Frame Format

* Sending adapter encapsulates network layer protocol packet such as IP datagram in Ethernet frame

# Preamble:

* 7 bytes with pattern 10101010.
* Used to synchronize receiver, sender clock rates.

# SFD:

* One byte with pattern 10101011 to signal the start of the frame.

# Addresses:

6 bytes, frame is received by all adapters on a LAN and dropped if address does

not match

# Length/Type:

indicates the higher layer protocol or the number of bytes in the data field.

# CRC:

checked at receiver, if error is detected, the frame is simply dropped

# Minimum and Maximum Lengths

Minimum: 64 bytes (512 bits)

Maximum: 1518 bytes (12,144 bits)

# Unicast and multicast addresses

The least significant bit of the first byte defines the type of address. If the bit is 0, the address is unicast; otherwise, it is multicast or broadcast.

The broadcast destination address is a special case of the multicast address in which all bits are 1s. (FF:FF:FF:FF:FF:FF)

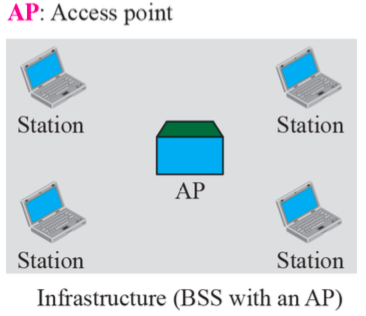
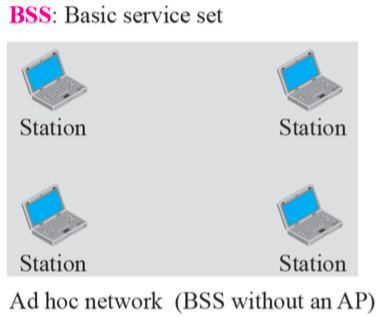
# Slot time

# **Slot time** = round-trip time+ jam sequence time.

**Max Length** = propagation speed \* (slot time/2)

# WIRELESS LANS

# Basic service sets (BSSs)



# Extended service sets (ESSs)

# 

# 802.11 Wireless LAN

A client is always associated with one AP and when the client moves closer to another AP, it associates with the new AP (Hand-Off)

# Wireless LAN Protocols

Wireless has complications compared to wired.

Nodes may have different coverage regions

* Leads to hidden and exposed terminals

Nodes can’t detect collisions, i.e., sense while sending

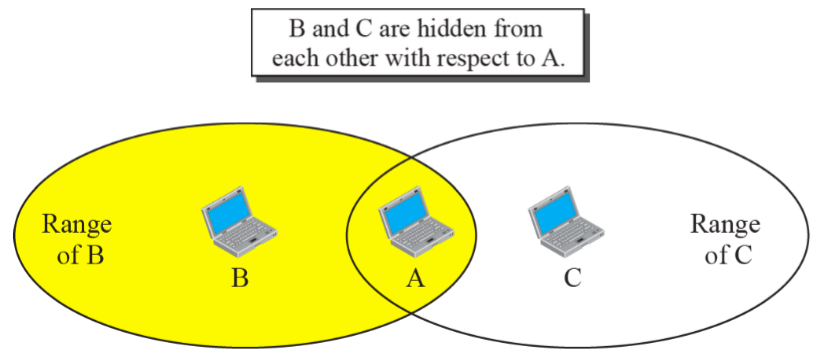
* Makes collisions expensive and to be avoided

# Wireless LANs – Hidden terminals

**Hidden terminals** are senders that cannot sense each other but nonetheless collide at intended receiver

* Want to prevent; loss of efficiency
* S1 and S2 are hidden terminals when sending to R

# Hidden Terminal problem

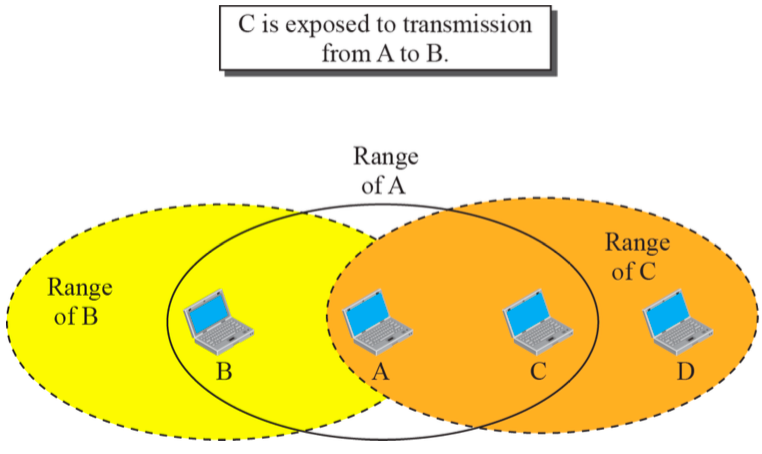


Before every data transmission

* Sender sends a Request to Send (RTS) frame containing the length of the transmission
* Receiver respond with a Clear to Send (CTS) frame
* Sender sends data
* Receiver sends an ACK; now another sender can send data

When sender doesn’t get a CTS back, it assumes collision

# Exposed Terminal problem



Exposed terminals are senders who can sense each other but still transmit safely (to different receivers)

* Desirably concurrency; improves performance
* S1 > R1 and S2 > R2 are exposed terminals

# Wireless LANs – MACA

MACA protocol grants access for A to send to B:

* A sends RTS to B;B replies with CTS.
* A can send with exposed but no hidden terminals