Οικονομικό Πανεπιστήμιο Αθηνών
Τμήμα Πληροφορικής

Ευφυή Κινητά Δίκτυα: IEEE 802.11 - Μέρος Β

Γιάννης Θωμάς

Χειμερινό Εξάμηνο 2023-24

(Βασισμένο σε διαφάνειες του Βασίλειου Σύρη)

802.11 MAC

- Three basic access mechanisms have been defined for IEEE 802.11
  - CSMA/CA (mandatory)
  - Optional method avoiding the *hidden terminal problem*
  - A contention-free polling method for time-bounded service
    - access point polls terminals according to a list
- The first two methods are also summarized as **distributed coordination function (DCF)**
- The third method is called **point coordination function (PCF)**
- DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service, but needs an access point to control medium access and to avoid contention.

802.11 MAC (DCF)

- CSMA/CA based
  - Carrier Sense=Listen before you talk
  - Uses exponential backoff
- Robust for error and interference control
  - More efficient to deal with errors at the MAC level than higher layer (such as TCP)
  - MAC layer **ACKnowledgment** for unicast frames
  - MAC level loss recovery through finite **retransmissions**
  - No ACKs for broadcast frames
- Physical carrier sense
  - Sense medium for certain time to ensure channel free
- Optional RTS/CTS offers Virtual Carrier Sensing
  - RTS/CTS include transmission duration (Network Allocation Vector – NAV)
  - Addresses hidden terminal problems

Min Sensing Time

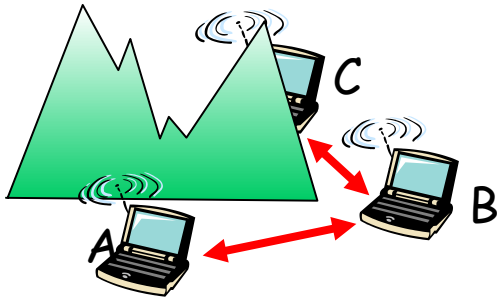
- IFS: minimum time channel must be sensed idle prior to transmission
  - **Short inter-frame spacing (SIFS)**
    - the shortest waiting time for medium access
    - defined for short control messages (e.g., ACK of data packets)
  - **DCF inter-frame spacing (DIFS)**
    - the longest waiting time used for asynchronous data service within a contention period
    - SIFS + two slot times
  - **PCF inter-frame spacing (PIFS)**
    - an access point polling other nodes only has to wait PIFS for medium access (for a time-bounded service)
    - SIFS + one slot time
- Different IFS values allow differential access to wireless channel
- Delay values in slot time
  - slot time=maximum time to detect a transmitting station (20 μsec in 802.11b

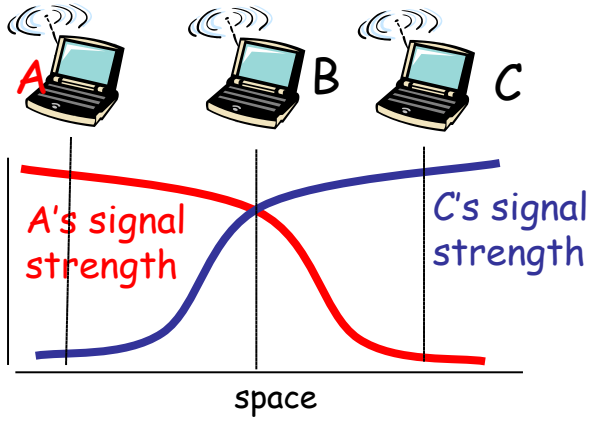
CSMA/CA

- The mandatory access mechanism of IEEE 802.11 is based on Carrier Sense Multiple Access with Collision Avoidance (***CSMA/CA***)
  - random access scheme with carrier sense and collision avoidance through random back-off
- The standard defines also two control frames:
  - RTS: Request To Send
  - CTS: Clear To Send

CSMA/CA: carrier sensing but no collision detection

- avoid collisions: >=2 nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





CSMA/CA

802.11 sender

1. if sense channel idle for **DIFS** then

   transmit entire frame (no CD)

2. if sense channel busy then

   start random backoff time

   timer counts down while channel idle

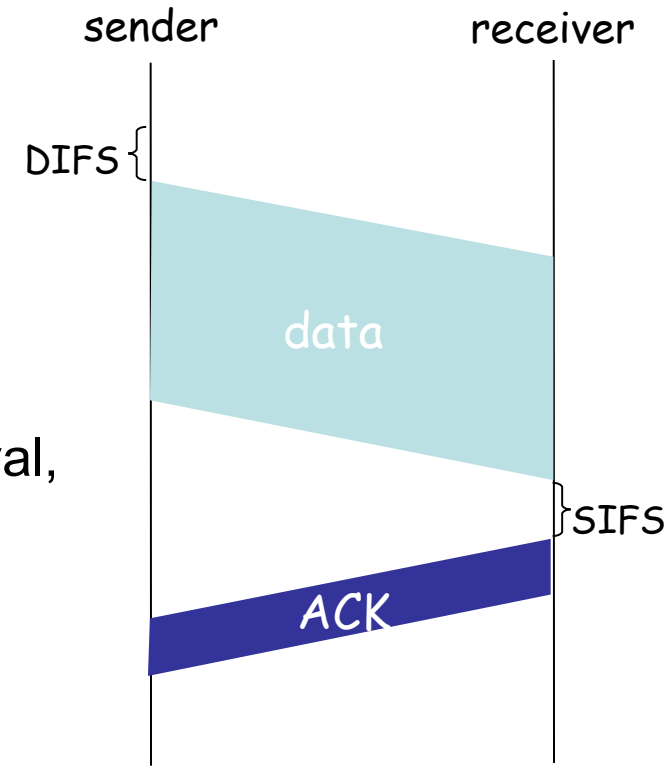
   transmit when timer expires

   if no ACK, increase random backoff interval, repeat 2

802.11 receiver

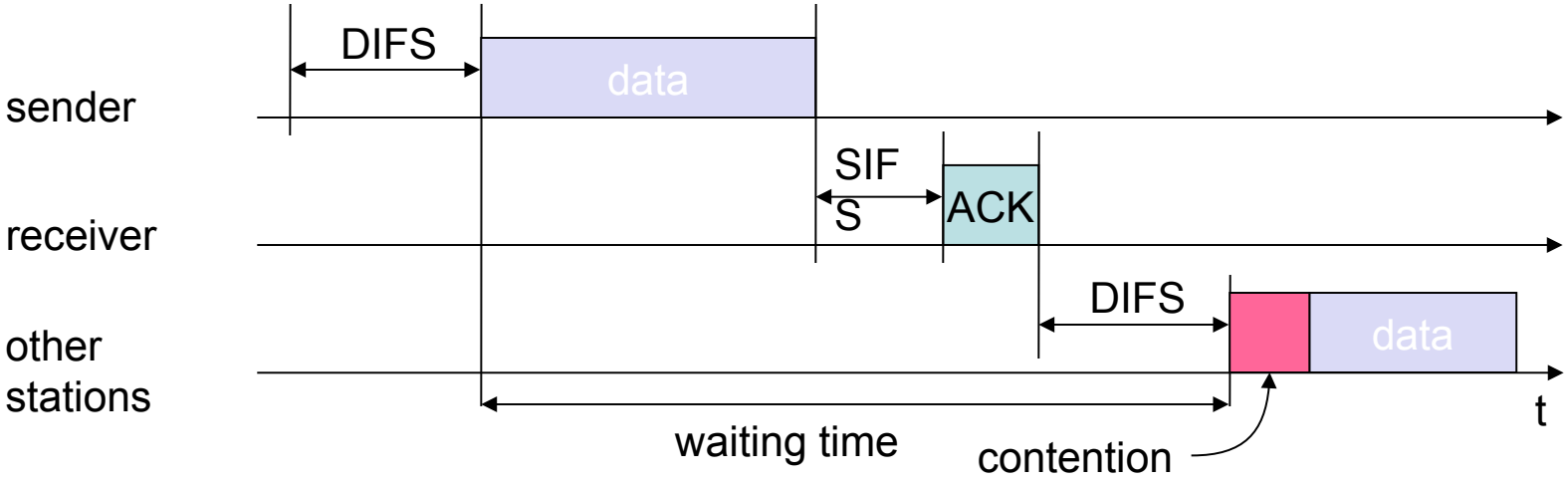
- if frame received OK

  return ACK after **SIFS** (ACK needed due to hidden terminal problem)



CSMA/CA: another view

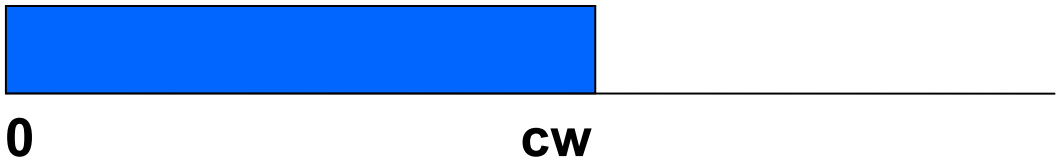
- Unicast data transfer



  - station has to wait for DIFS before sending data
  - receivers acknowledge after waiting for a duration of a Short Inter-Frame Space (SIFS), if the packet was received correctly

Collision Avoidance

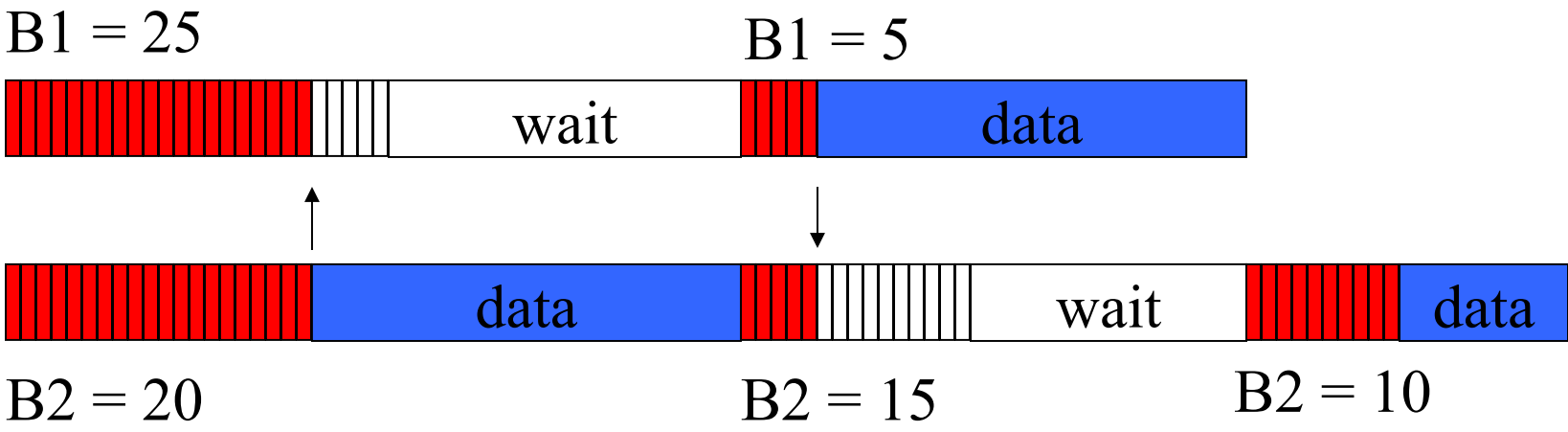
- Collision avoidance mechanism: When transmitting a packet, choose a backoff interval in the range [0,cw]
  - cw is contention window



- Count down the backoff interval **when medium is idle**
- When backoff interval reaches 0, transmit

Collision Avoidance: Example

Timer decremented only in RED periods



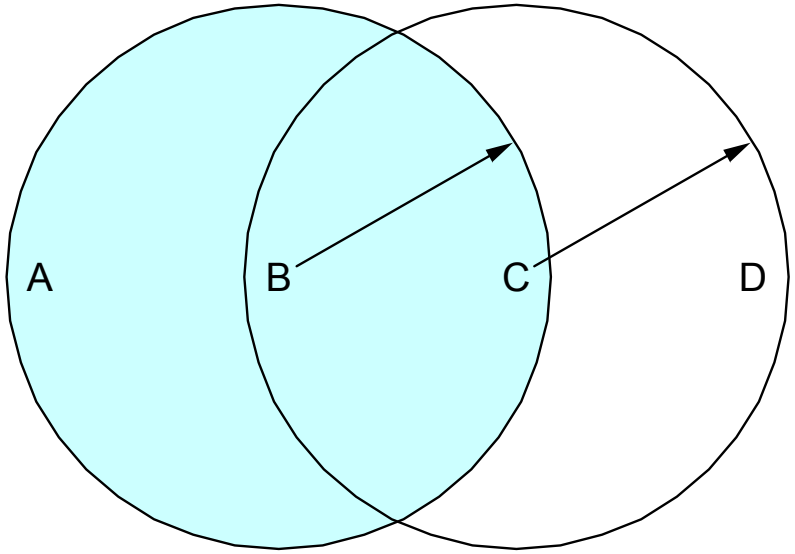
cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

Collision Avoidance: **Exponential Backoff**

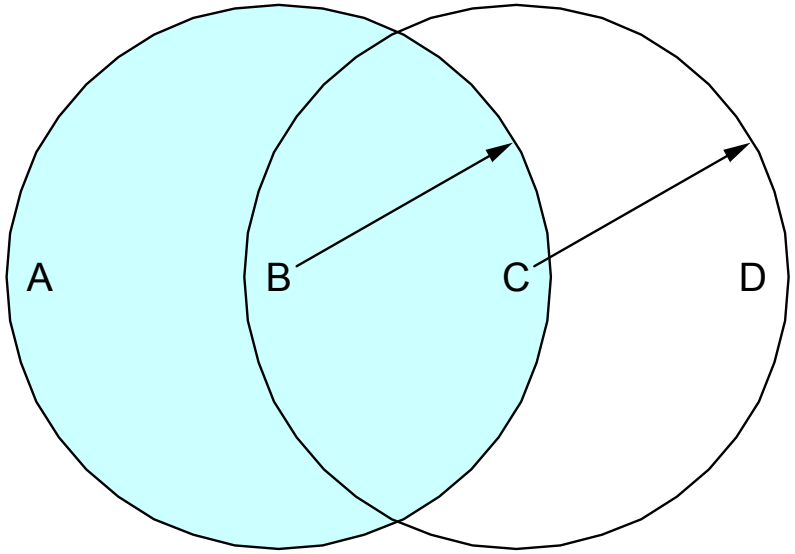
- Initial value of CW is CWmin
- For each collision, double the contention window CW
- Maximum value of CW is CWmax
- After successful transmission set contention window to CWmin

Hidden Node Problem



- A and C want to communicate with B
- Signal from A cannot reach C and vice-versa
- **Carrier sensing does not work!**

Exposed Node Problem

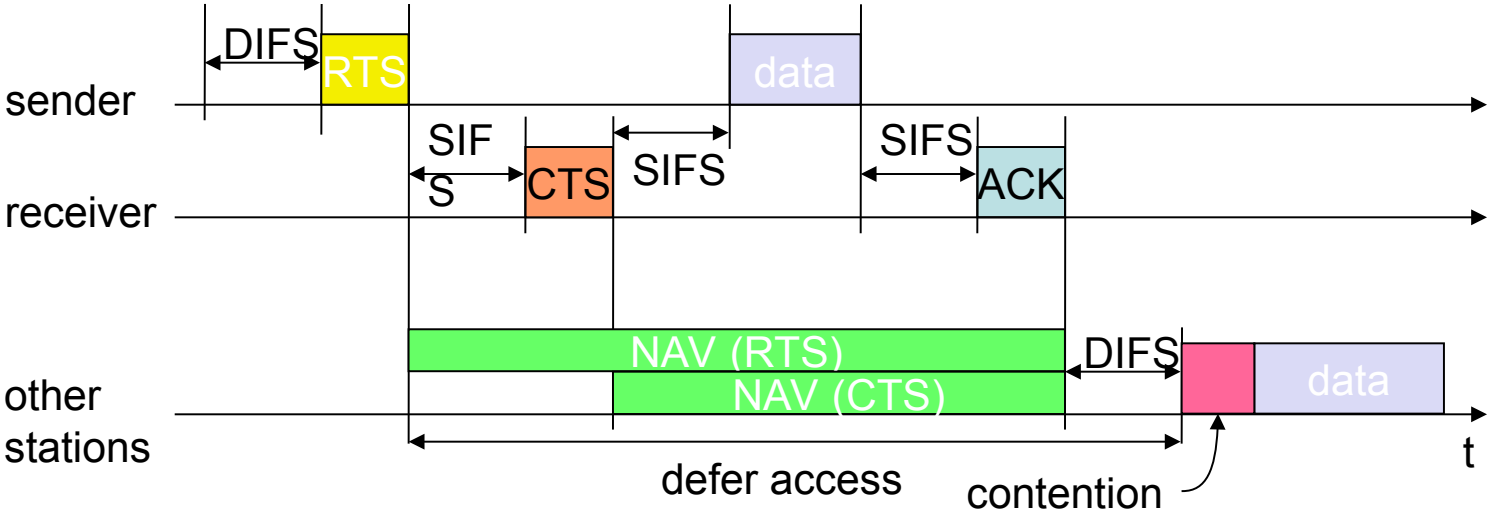


- B wants to send to A & C wants to send to D
- C senses B's transmission, hence doesn't transmit
- But, B->A and C->D both possible !
- Carrier sensing does not work!

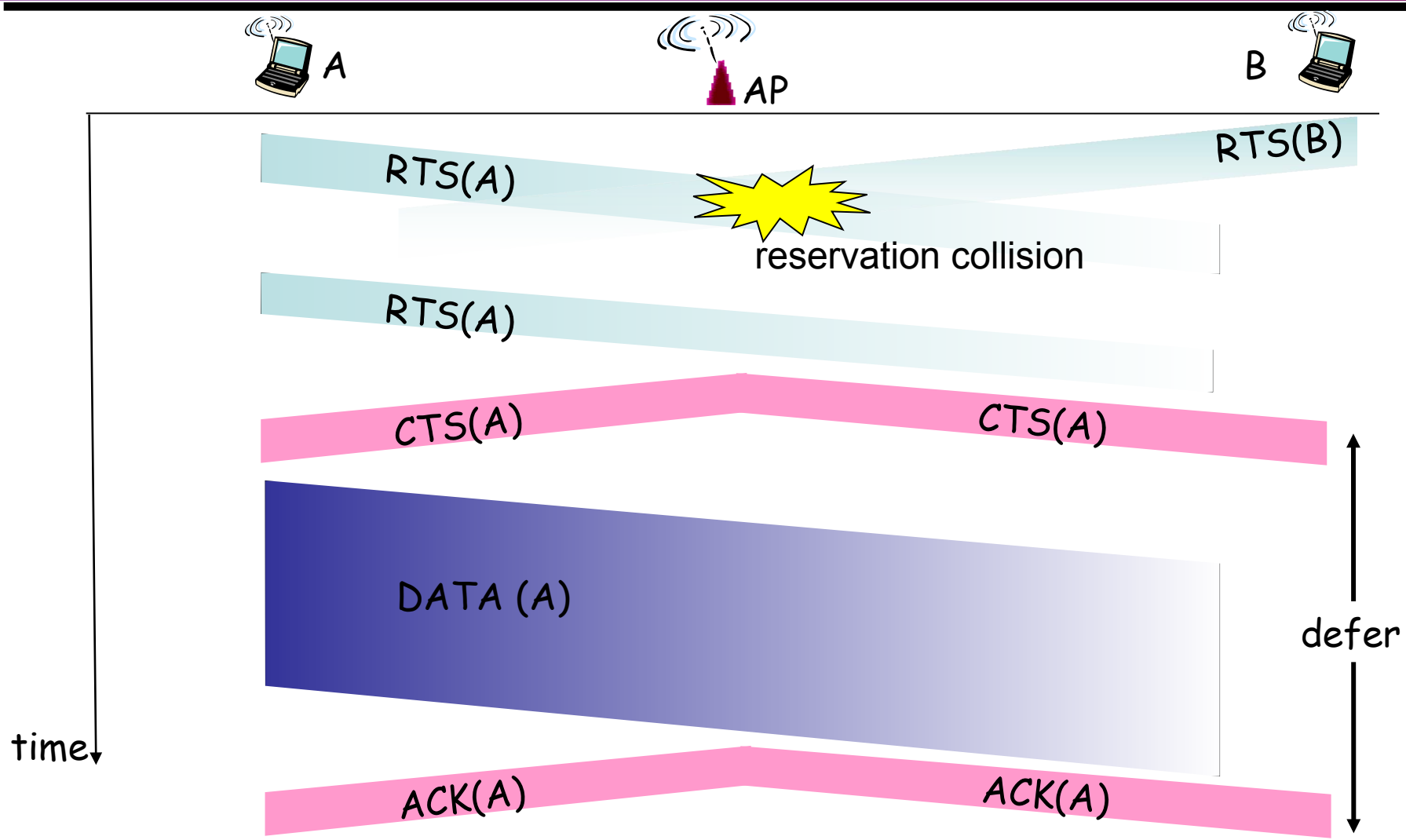
4-way handshake using RTS/CTS

- Sender “reserves” channel prior to transmitting data frames
  - First transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

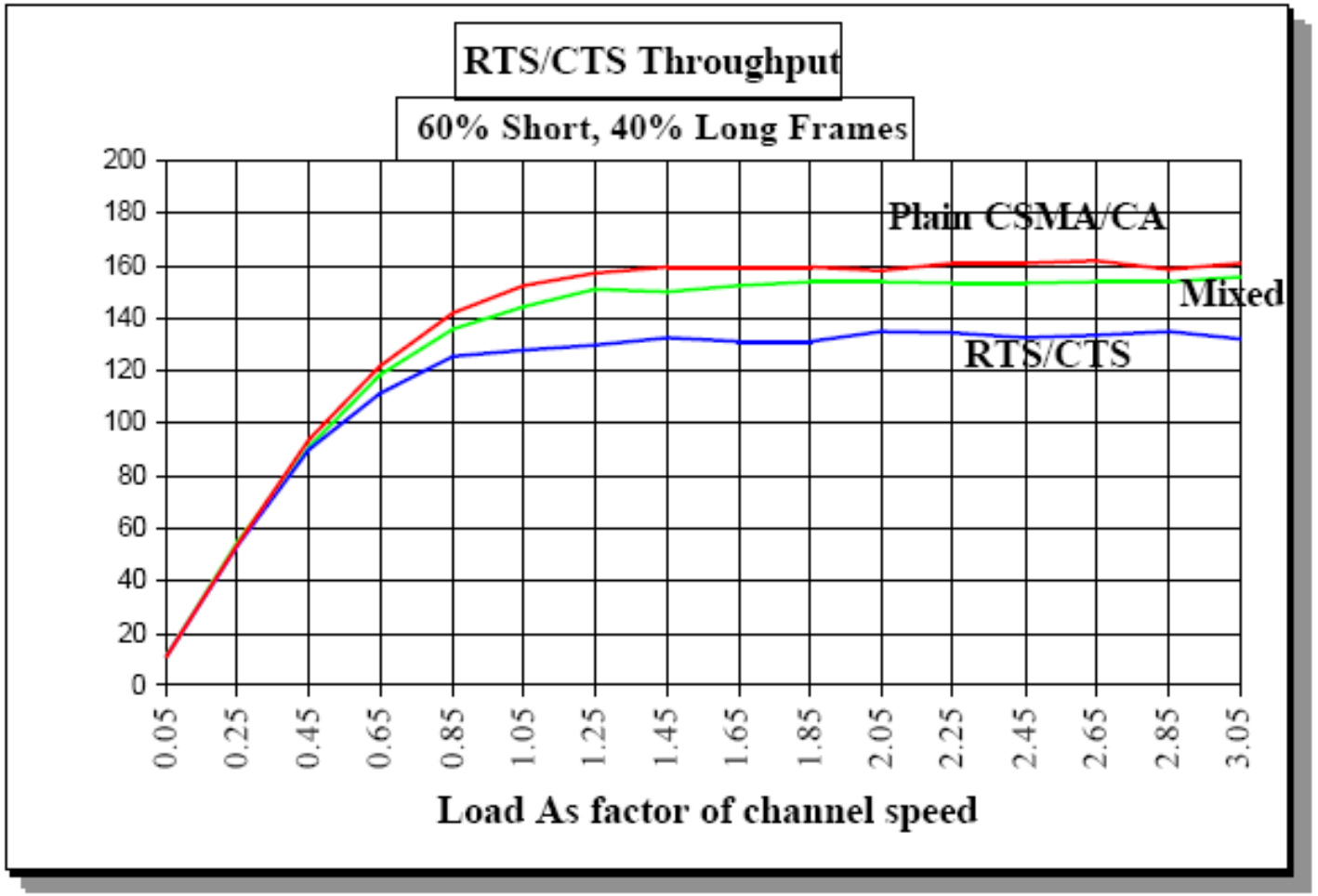
- Sending unicast packets with RTS/CTS control frames



- station can send RTS with reservation parameter after waiting for DIFS
  - (reservation determines amount of time the data packet needs the medium and the ACK related to it).
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- Other stations store medium reservations distributed via RTS and CTS
- sender can now send data at once, acknowledgement via ACK


A
AP
B
RTS(A)
RTS(B)
reservation collision
RTS(A)
CTS(A)
CTS(A)
DATA (A)
defer
time
ACK(A)
ACK(A)

RTS/CTS overhead impact



802.11 Point Coordination Function (PCF)

- AP coordinates network communication
- AP waits for PIFS
  - PIFS<DIFS → AP has priority
- AP polls stations
  - Sends CF-Poll frame to station to permit transmission
  - Polled station responds with data or null frame
- Only one AP should operate PCF periods in each channel
- PCF periods alternate with DCF periods

- Solves hidden/exposed node problems?

802.11 MAC management

Synchronization

- Finding and staying with a WLAN
  - Uses TSF timers and beacons
    - TSF: Time Synchronization Function

Power Management

- Sleeping without missing any messages
  - Periodic sleep, frame buffering, traffic indication map

Association and Reassociation

- Joining a network
- Roaming, moving from one AP to another
- Scanning

Synchronization

- **Timing Synchronization Function (TSF)**
  - Enables synchronous waking/sleeping
  - Enables switching from DCF to PCF
  - Enables frequency hopping in Frequency-hopping spread spectrum (FHSS) PHY
    - Transmitter and receiver has identical dwell interval at each center frequency
- **Achieving TSF**
  - All stations maintain a local timer.
  - AP periodically broadcasts beacons containing timestamps, management info, roaming info, etc.
    - Not necessary to hear every beacon
  - Beacon synchronizes entire BSS
    - Applicable in infrastructure mode ONLY
  - Distributed TSF (for Independent BSS) more difficult – why?

802.11 power management

- Station-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this station
  - Station wakes up before next beacon frame
- Beacon frame: contains list of stations with packets **waiting in AP buffer**
  - station stays awake as long as AP has frames to send it; otherwise sleeps again until next beacon frame
  - if AP has packets for it, station polls AP
- Broadcast packets can also be buffered

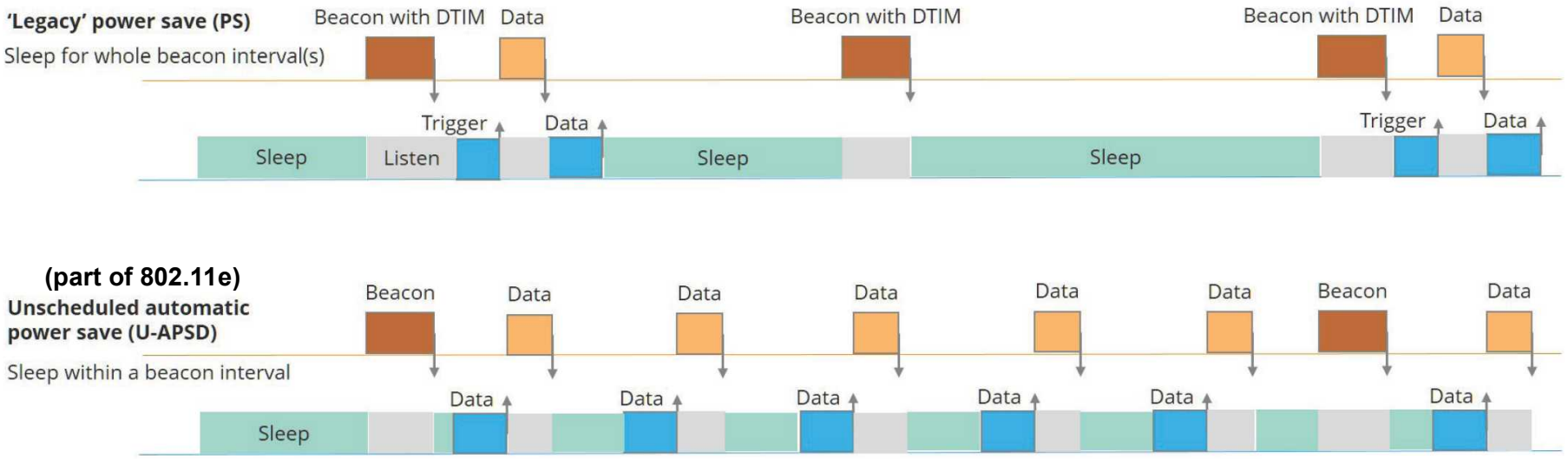
802.11 power management (cont.)

- **Battery powered devices require power efficiency**
  - LAN protocols assume idle nodes are always ON and thus ready to receive.
  - Idle-receive state key source of power wastage
- **Devices need to power off during idle periods**
  - Yet maintain an active session – tradeoff power Vs throughput
- **Achieving power conservation**
  - Allow idle stations to go to sleep periodically
  - APs buffer packets for sleeping stations
  - AP announces which stations have frames buffered when all stations are awake – called **Traffic Indication Map (TIM)**
    - TIM is a bitmap
    - TSF assures AP and Power Save stations are synchronized
    - TSF timer keeps running when stations are sleeping

Unscheduled Automatic Power Save Delivery (U-APSD)

- Part of the 802.11e (2005)
  - Wi-Fi extension for delay-sensitive applications
- if a network card doesn't have to transmit anything, it will go in stand-bye mode.
- As soon as it has anything to transmit to the AP, the network card will wake up and will transmit the packets.
- At the same time, the network card will check if the AP has anything to transmit back.
- In case of no traffic, the network card will wake up randomly every 100-200ms to check if there is anything that might come from the Aps.
- fine for instant messaging, web browsing or mails. Why?
  - Voice call?

802.11ax power save mode TWT (Target Wait Time)



- Legacy 802.11: Clients can sleep between AP beacons (or multiples of beacons), waking when they have data to transmit and for beacons containing the delivery traffic information map (DTIM)
- 802.11ax: allows more flexible, long-term, multi-client sleeping arrangements
  - A negotiation between the client and AP sets up an agreed schedule for client to wake and communicate.
  - Schedule is often periodic, with a long, multi-beacon interval (minutes, perhaps hours or days) between activities

802.11 association and roaming

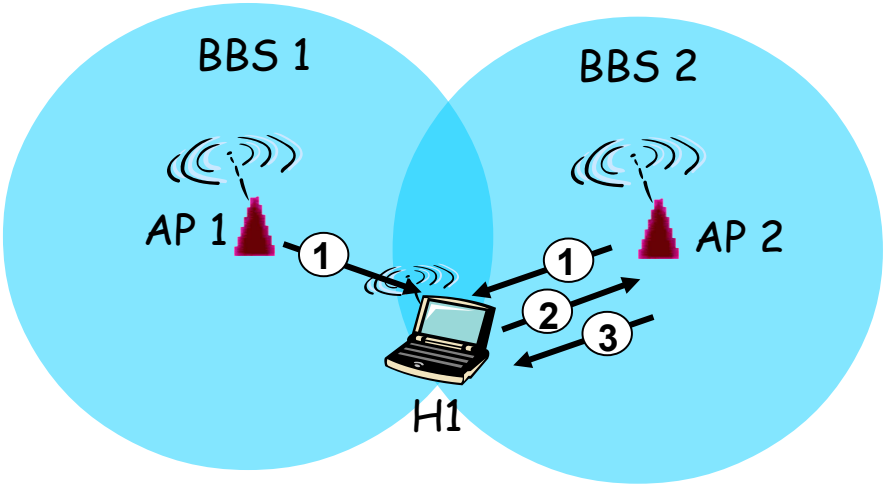
Questions

- How does station find AP?
- How does station associate with AP?
- How does station roam to another AP?

802.11 channels and association

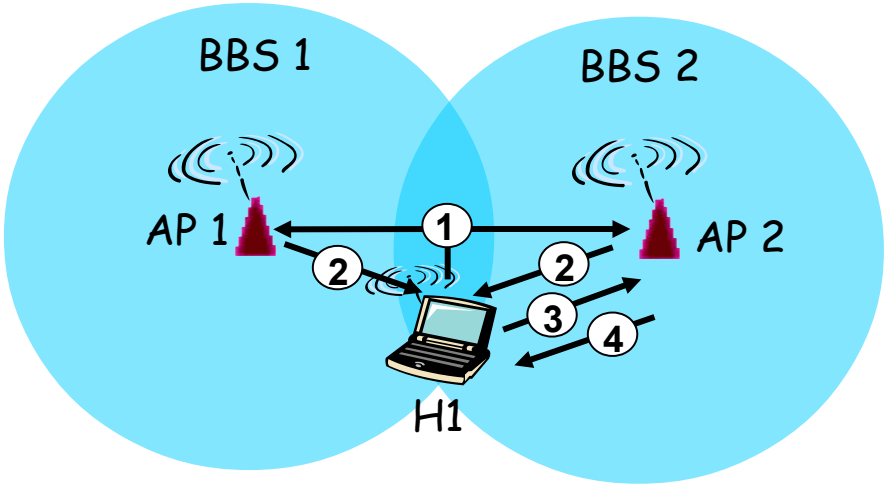
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses AP channel
  - interference possible: channel can be same as that chosen by neighboring AP!
- Stations association with an AP
  - scans channels, listening for ***beacon frames*** containing AP's name (SSID) and MAC addr. (BSSID)
  - selects AP to associate with
    - based on beacon signal strength
  - may perform authentication
  - will typically run DHCP to get IP address in AP's subnet

Passive vs. active scanning



Passive Scanning:

(1) beacon frames sent by APs
(2) association Request frame sent by H1 to selected AP
(3) association Response frame sent by selected AP to H1



Active Scanning:

(1) Probe Request frame broadcasted from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent from H1 to selected AP
(4) Association Response frame sent from selected AP to H1

Authentication and association

- Three 802.11 connection states
  - No authentication and no association
  - Authenticated but not associated
  - Authenticated and associated
- Original 802.11 authentication occurred before association
  - 802.1X/802.11i authentication follows
- Association allows the AP/router to record each mobile device so frames are properly delivered
  - Association involved agreeing on **bit rates** and **security** params (for 802.1X/802.11i authentication)
  - After successful association, AP sends station an **Association ID** used

802.11 roaming

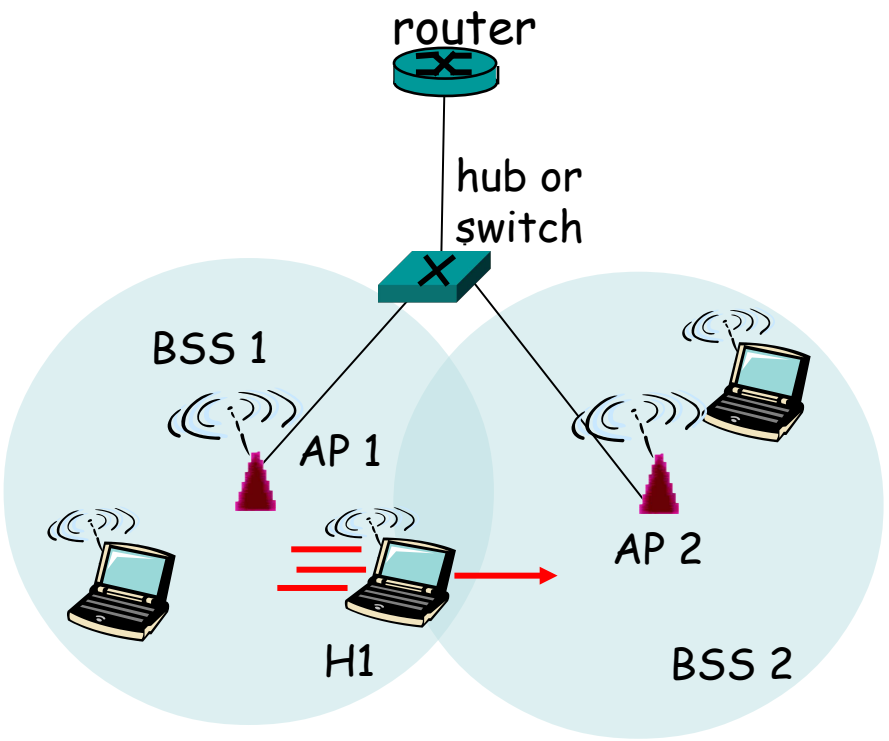
- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources
- Roaming supports robustness/redundancy and mobility

802.11 roaming (cont)

- L2 handover
  - If handover from one AP to another belonging to the same subnet, then handover is completed at L2
- L3 handover
  - If new AP is in another domain, then the handover must be completed at L3, due to the assignment of an IP belonging to the new domain – hence routing to the new IP.
    - Mobile IP deals with these issues – more later

802.11 roaming (cont)

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and “remember” which switch port can be used to reach H1

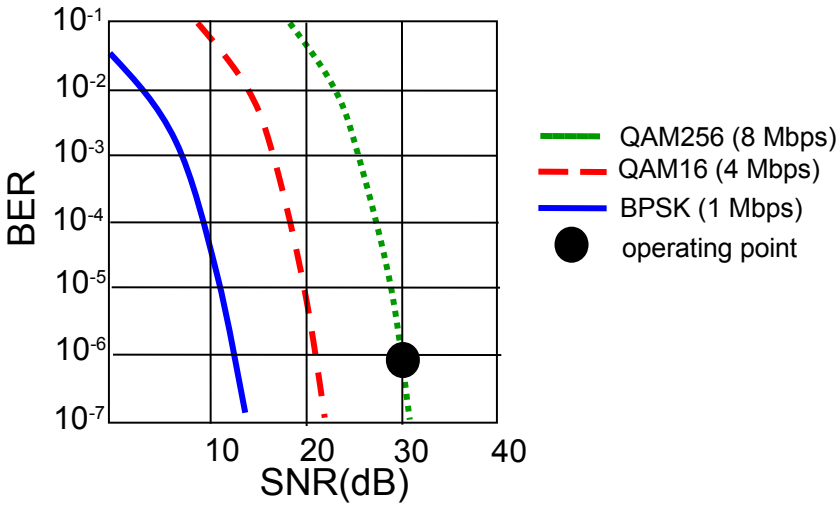


Roaming: Reactive Vs. Proactive

- Reactive: scan when connection lost
- Proactive: periodically scan for **better** AP
  - higher performance but higher overhead
- not standardized by 802.11
  - vendor/implementation specific

802.11 rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique)
- Key questions:
  - **what** to measure
  - **when** to change rate
  - what **rate** to change to



1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER