Wireless LAN(2)

Mobile Computing

Minho Shin

2012. 9. 13

Review

- Wireless Communication
  - Channel, Multipath interference, Path loss, Shadowing, Microscopic Fading
- Wireless LAN
  - ISM bands, Building Blocks: BSS, DS, ESS
  - MAC
    - PCF/DCF, CSMA/CA, Random Backoff,
    - Hidden/Exposed Terminal Problems, RTS/CTS
  - PHY: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS)

Quiz

- In wireless communication, the original signals can be distorted by distance, obstacles, and time. Explain the three wireless channel distortion models in terrestrial environment and their definitions.
  - Path loss, Shadowing, Microscopic Fading

Quiz

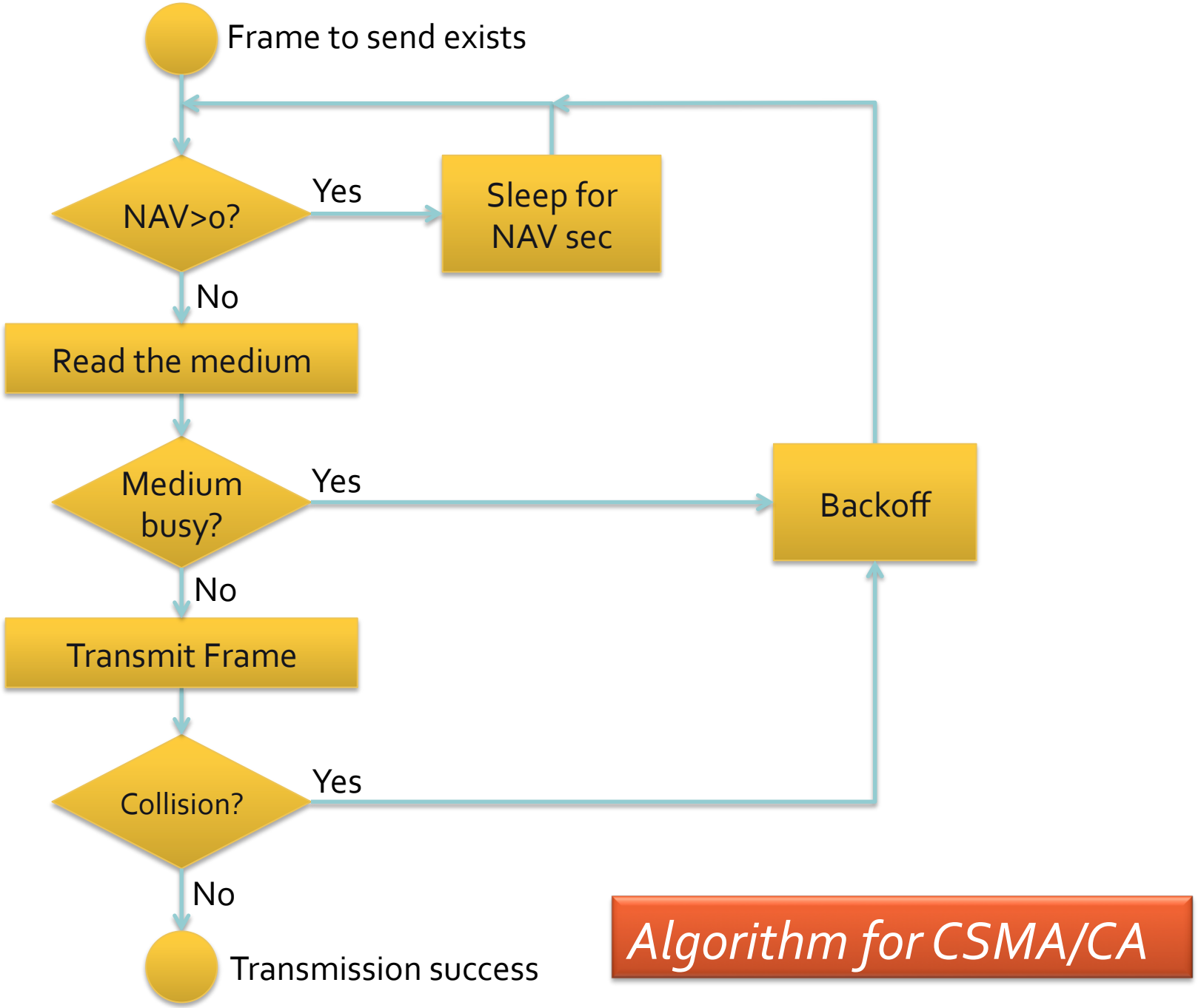
- What were the major challenges, their causes, and resolutions in the design of WLAN?

802.11 MAC in more detail

- Virtual carrier sense mechanism
- Binary exponential backoff
- Error recovery
- Join/Leave procedures
- Security

Carrier Sense Mechanism

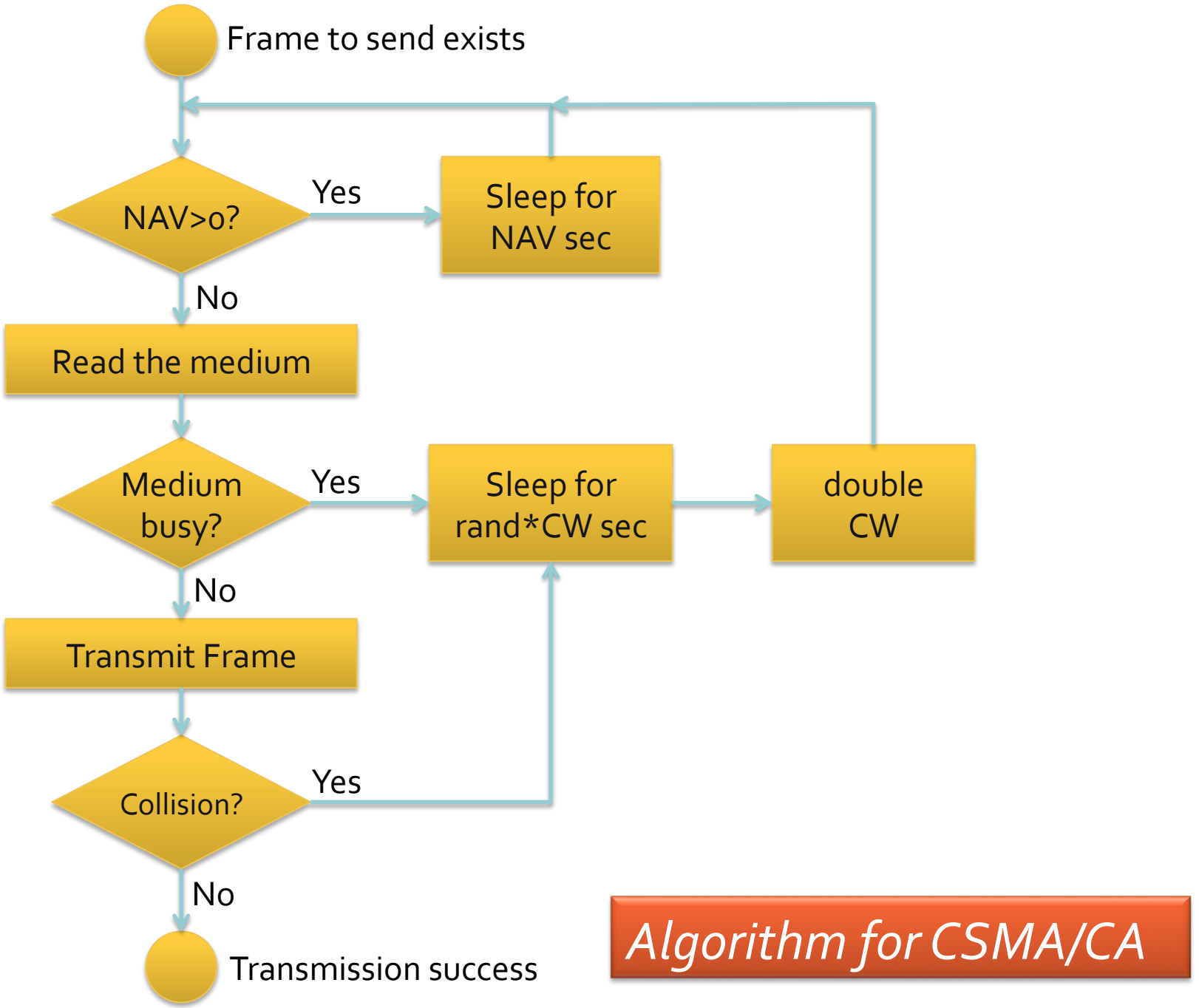
- Physical carrier sense
  - Sense the wireless medium and check if it is busy or not
- Virtual carrier sense
  - Each frame tells others how long it will use the medium in *Duration* field
  - Each STA records that time in NAV (Network Availability Vector), and waits for that reserved time period
  - When NAV expires, the STA does PHY carrier sense



Algorithm for CSMA/CA

Exponential Random Backoff

- Backoff duration(i) = *random()* * $CW(i)$
  - *random()*: picks a random value from (0,1)
  - $CW(i)$: i^{th} collision window, exponentially grows
    - $CW(1) = CW_{min}$
    - $CW(i) = CW(i\text{-}1) * 2$
    - $CW(i) \leq Cw_{max}$



Algorithm for CSMA/CA

Error Recovery

- What if the frame is lost?

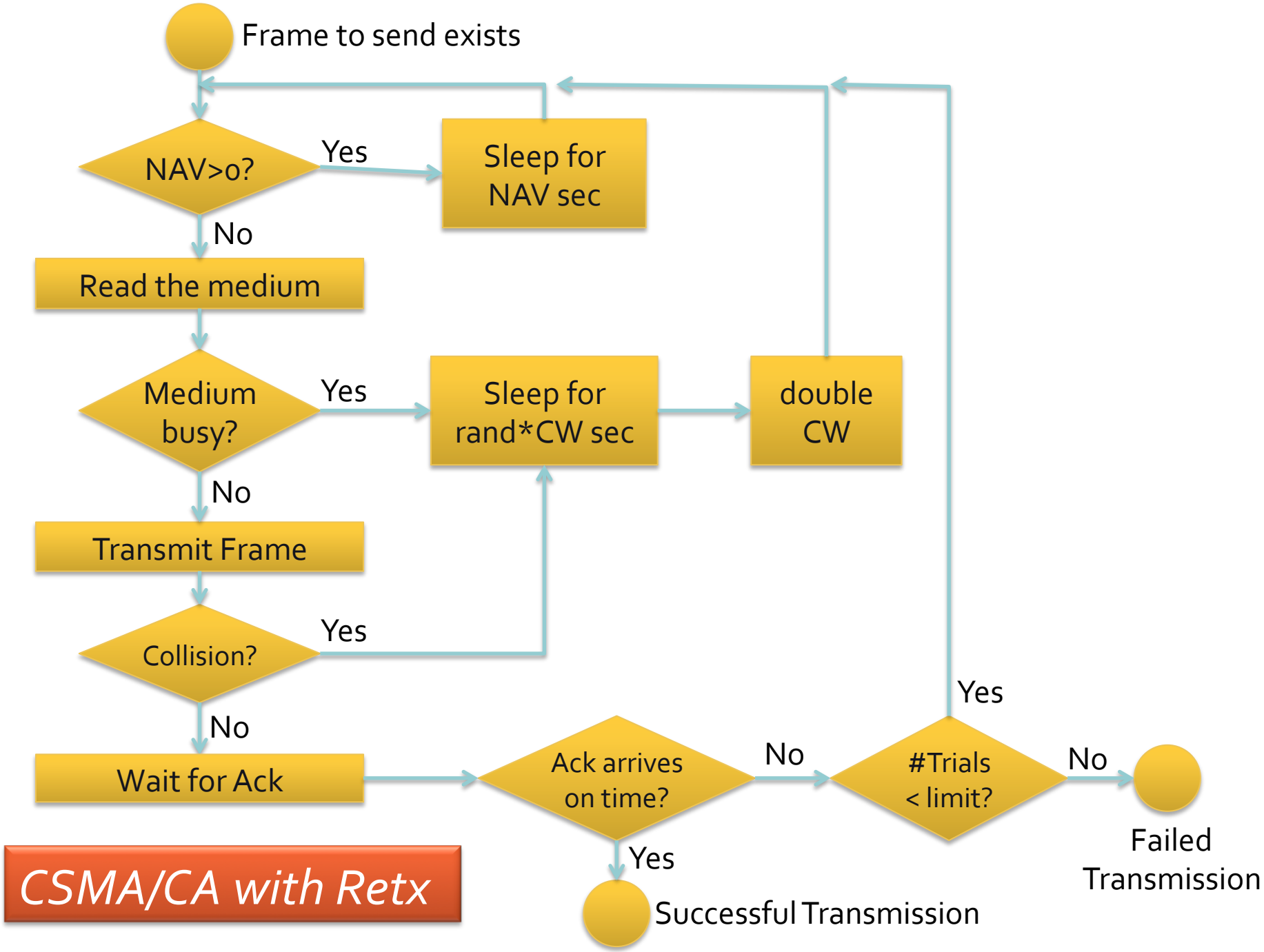
  - Node A is not sure if node B received
  - Solution: *The receiver sends Acknowledgement for every frame*

- What if the Ack is lost?

  - Node A is not sure why no Ack: the message was lost? or the Ack was lost?
  - Solution: *The sender resends the message until an Ack arrives*

Retransmission

- How long should I wait for an Ack before retransmission?
  - Implementation dependent
  - round-trip-time + SIFS
- How many times should I retry until discarding?
  - MIB:aShortRetryLimit times
    - if frame length < MIB:aRTSThreshold
  - MIB:aLongRetryLimit, otherwise

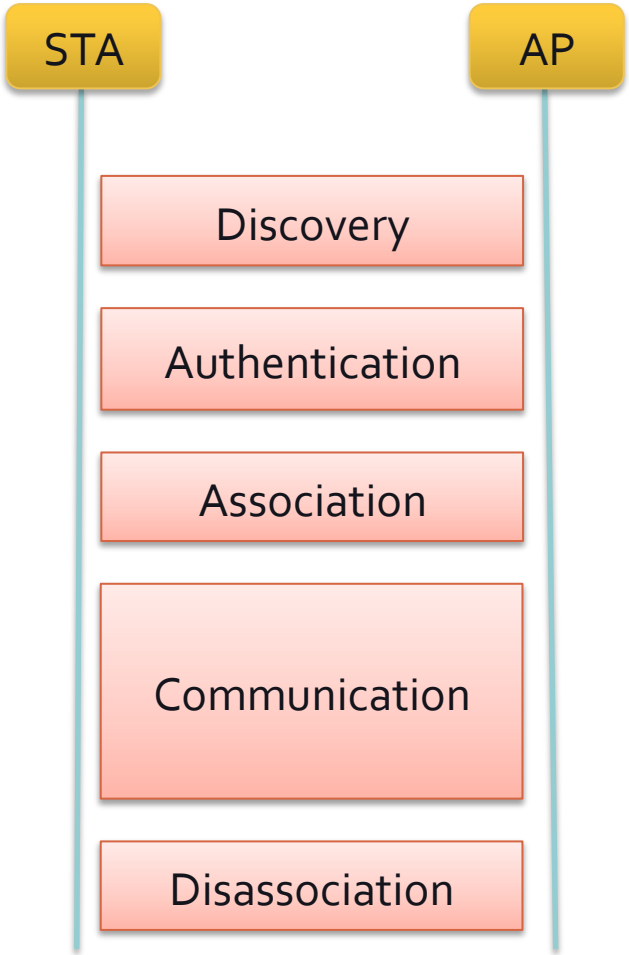

Frame to send exists
NAV>o?
Yes
Sleep for NAV sec
No
Read the medium
Medium busy?
Yes
Sleep for rand*CW sec
double CW
No
Transmit Frame
Collision?
Yes
No
Wait for Ack
Ack arrives on time?
No
#Trials < limit?
No
Yes
Failed Transmission
Yes
Successful Transmission
CSMA/CA with Retx

Network Identity

- Recall
  - BSS (Basic Service Set): a group of stations under the same coordination function
  - IBSS (Independent BSS): BSS without DS connection
  - ESS (Extended Service Set): BSS's + DS
- BSSID: Identity of a BSS. Usually MAC address of the AP
- ESSID = SSID: Identity of an ESS. a string up to 32 octets
- SSID of IBSS: Chosen by the first member

Joining & Leaving a WLAN

- Discover a WLAN
  - Find an AP with preferred SSID and strong signal
- Authentication
  - Get permission to connect to the WLAN
- Association
  - Join the WLAN
- Disassociation
  - Leave the WLAN



WLAN Discovery (1)

- Beacon
  - Each AP periodically broadcasts a Beacon frame
    - every MIB:aBeaconPeriod
    - on its channel
  - Containing synchronization information
    - AP's clock
    - Parameters for the coordination function
  - IBSS: every STA beacons

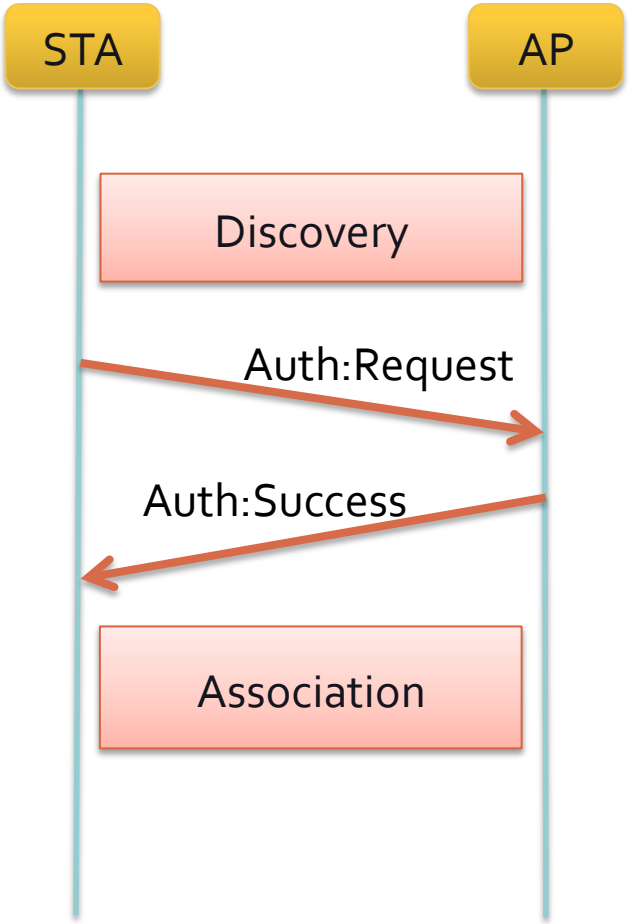
WLAN Discovery (2)

- How an STA finds an AP?
- Passive Scan
  - Collect beacons from all the channels, staying in each channel for MIB:ChannelTime seconds
- Active Scan
  - STA sends a *Probe Request* frame, containing desired SSID
  - AP with the same SSID returns a *Probe Response* frame
  - IBBS: The STA that sent the last Beacon replies
- AP choice
  - STA chooses an AP with the best signal quality

Authentication

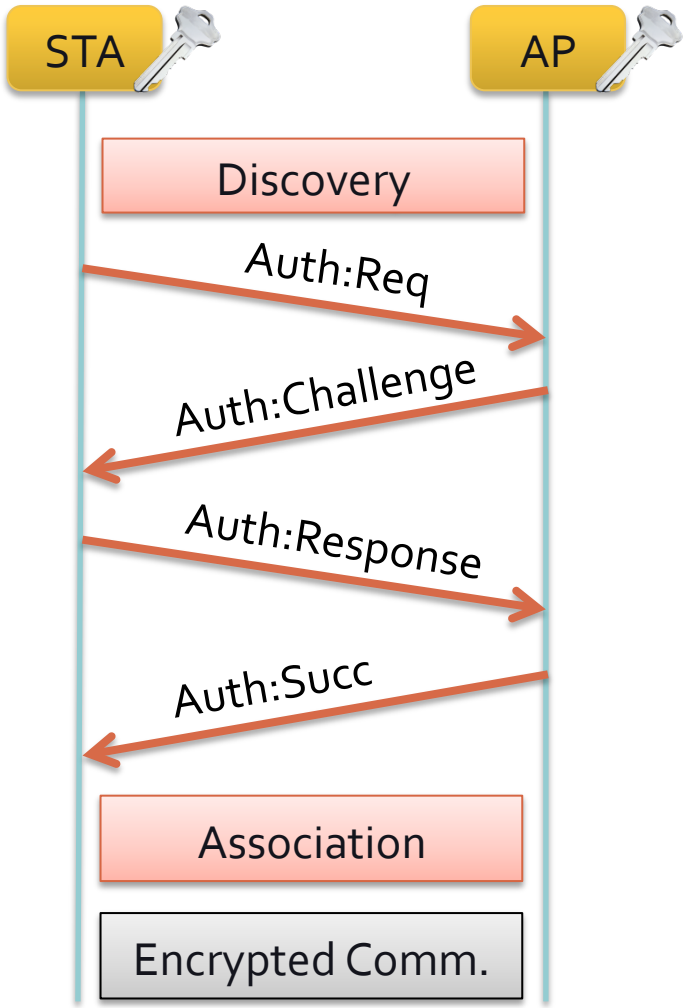
- Open System Authentication
  - Any STA can access the WLAN
- Shared Key Authentication
  - Only STAs that knows the same key with the AP can access the WLAN
  - WEP (Wired Equivalent Privacy)

Open Authentication



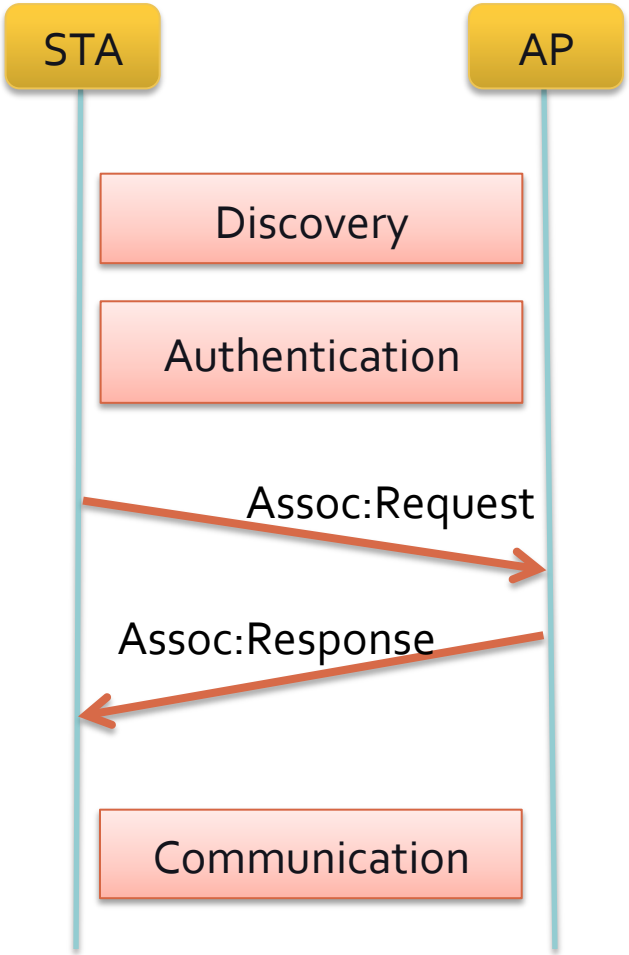
Shared Key Authentication

- WEP
  - STA and AP shares a key
  - STA proves its knowledge by a challenge/ response protocol
  - Auth:Challenge contains a challenge text
  - Auth:Response contains the encryption of the challenge text (128 bits)
  - Authentication is successful if the encryption is correct
  - Subsequent data packets are encrypted



Association

- STA registers itself to the AP so that AP knows the presence of the STA, and handles packets from/to the STA
- Association Request
  - STA's capabilities: supported data rates, WEP support, PHY options, power saving mode
- Association Response
  - Accept/Reject: based on capability, load balancing, security,…
  - Association ID, Supported data rate



Disassociation

- STA notifies the AP of its leaving
- AP notifies the STA of disconnecting
- Reason Code:
  - No reason
  - Authentication invalid
  - Leaving
  - Inactivity
  - Load balancing
  - etc…