Mobile Networking (MobNet)
Communication Networks III
Winter 2018/2019
Chapter 04: Wireless Local Area Networks
Module 02: IEEE 802.11 Medium Access Control

TECHNISCHE UNIVERSITÄT DARMSTADT

SECURE MOBILE NETWORKING

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

Dr. Gek Hong Sim
allyson.sim@seemoo.de

Outline & Learning Objectives

Chapter 03, Module 02

(1) 802.11 Medium Access Control

(2) Distributed Coordination Function (with and w/o RTS/CTS)

(3) Point Coordination Function

(4) Frame Types

Introduce the core principles for wireless medium access control in the setting of IEEE 802.11

- Be able to explain the basic principles behind the IEEE 802.11 MAC
- Understand the characteristics, pros and cons of the distributed as well as centralized MAC in IEEE 802.11

Chapter 04, Module 02

(1) 802.11 MAC

(2) DCF

(3) PCF

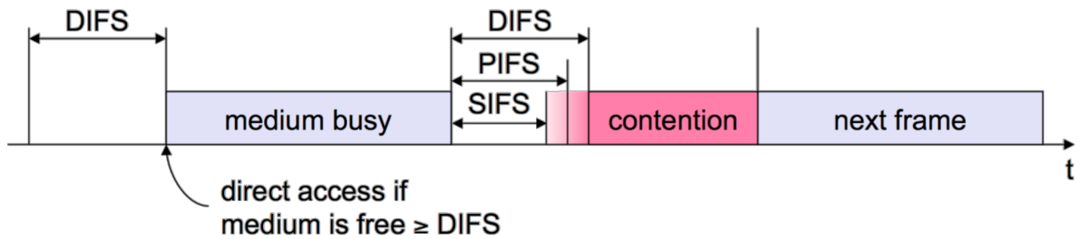
(4) Frame Types

IEEE 802.11 MAC Layer

- Access methods
  - DCF – Distributed Coordination Function
    - CSMA/CA (mandatory)
      - → collision avoidance via randomized "back-off" mechanism
      - → minimum distance between consecutive packets
      - → ACK packet for acknowledgements (not for broadcast)
    - DCF w/ RTS/CTS (optional)
      - → reduces hidden terminal problem
  - PCF – Point Coordination Function (optional)
    - access point polls terminals according to a list
  - HCF – Hybrid Coordination Function
    - EDCA (optional) – Enhanced Distributed Channel Access
      - CSMA/CA with priority levels
    - CCA (optional) – Controlled Channel Access
      - Improved polling

802.11 – MAC Layer (1)

- IFS (Inter frame spacing) is a time interval in which frames cannot be transmitted by stations within a BSS.
- This ensures that the frames do not overlap with each other.
- IFS types:
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
  - PIFS (PCF Inter Frame Spacing)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF Inter Frame Spacing)
    - lowest priority, for asynchronous data service
  - EIFS (Extended Inter Frame Spacing)
    - If a previously received frame contains an error then a station has to defer EIFS duration instead of DIFS before transmitting a frame.



802.11 – MAC Layer (2)

SECURE MOBILE NETWORKING

Timing Intervals

- Timing intervals are defined to control a station's access to the medium/channel
- A slot time (Slot Time)
  - Specific value depends on Physical Medium Dependent (PMD) layer
  - Derived from propagation delay, transmitter delay, etc. ($20\mu s$ for DSSS and $50\mu s$ for FHSS)
  - Basic unit of time for MAC, e.g. backoff time is a multiple of slot time
- Short Inter-Frame Space (SIFS)
  - Shortest interval: SIFS < Slot Time. $10\mu s$ for FHSS
  - Used for highest priority access to the medium, e.g., for ACK and CTS
  - Interval time between DATA-ACK and RTS-CTS

802.11 – MAC Layer (3)

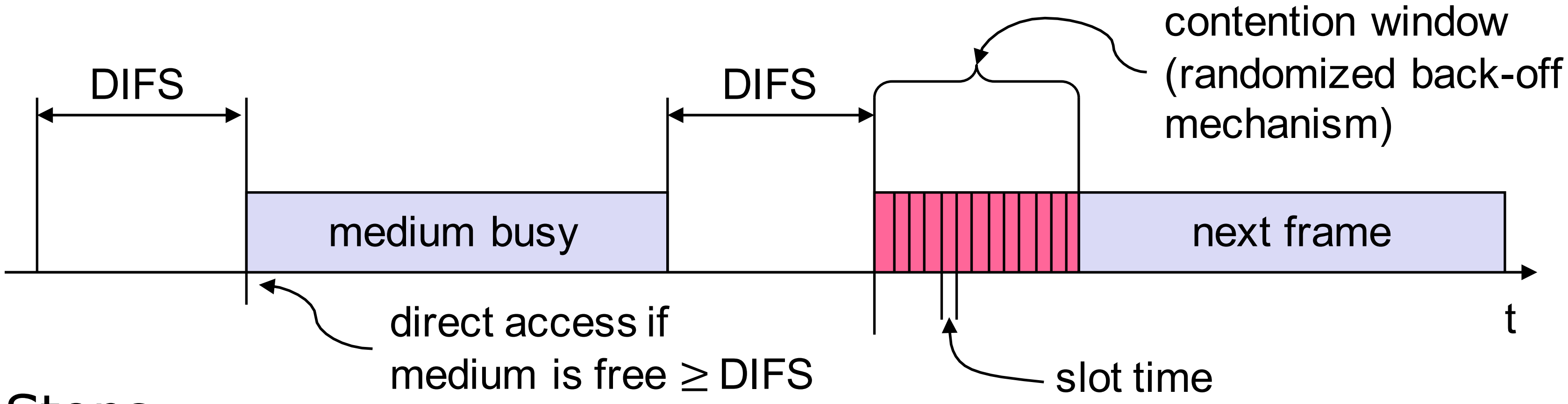
Timing Intervals

- PCF Inter-Frame Space (PIFS)
  - PIFS = SIFS + SlotTime
  - Used for Point Coordination Function (PCF) access to the medium
  - Allows priority based access to the medium after ACKs but before contention based access
- Distributed (DCF) Inter-Frame Space (DIFS)
  - DIFS = SIFS + 2 x SlotTime
  - Used for Distributed Control Function (DCF) access to the medium
  - Results in lower priority access than using SIFS or PIFS
- Summary
  - SIFS < PIFS < DIFS

Chapter 04, Module 02

(1) 802.11 MAC
(2) DCF
(3) PCF
(4) Frame Types

802.11 – DCF CSMA/CA

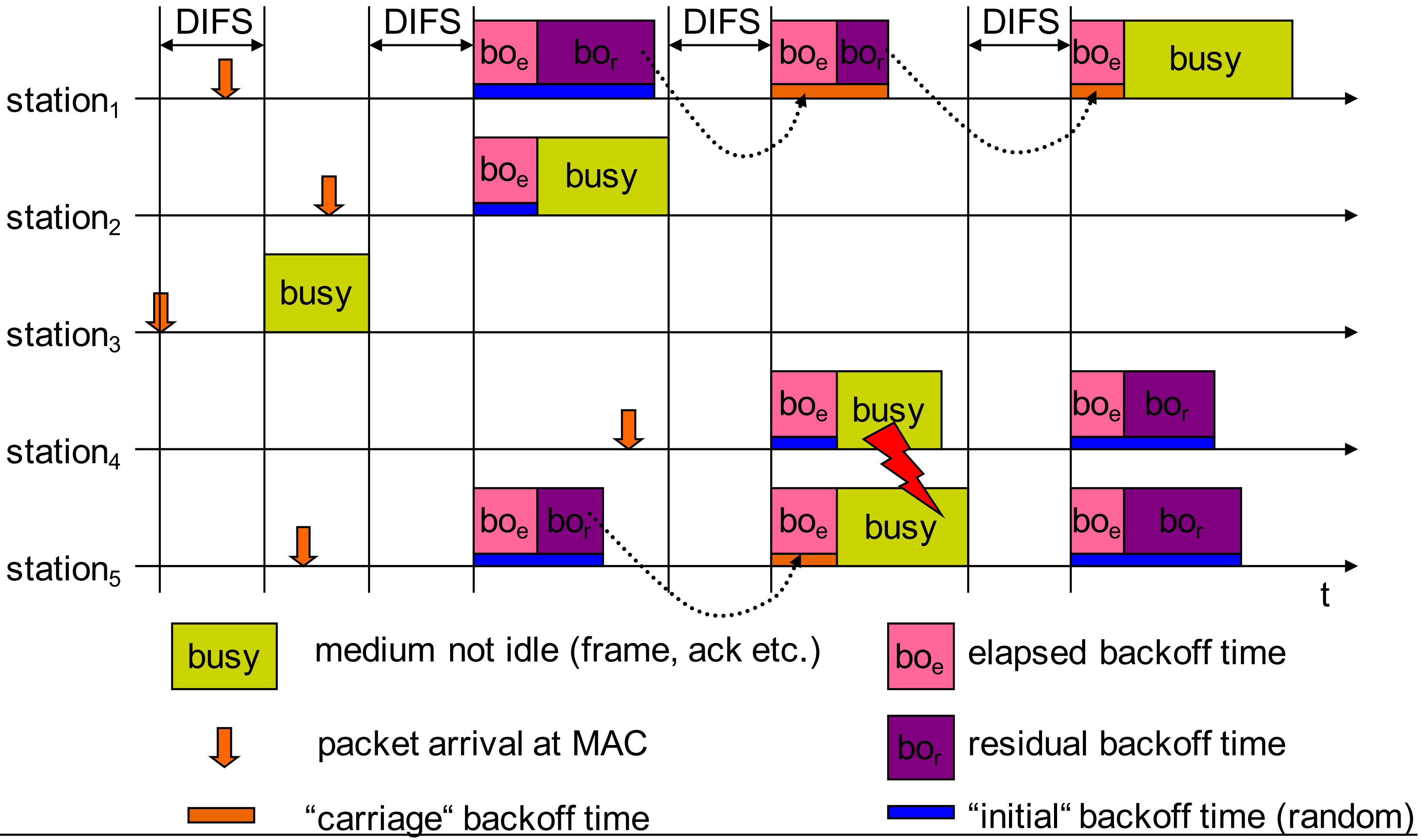


- Steps
  - Station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
  - If the medium is free for the duration of an DCF Inter-Frame Space (DIFS), the station can start sending.
  - If the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
  - If another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

802.11 - Binary Exponential Backoff

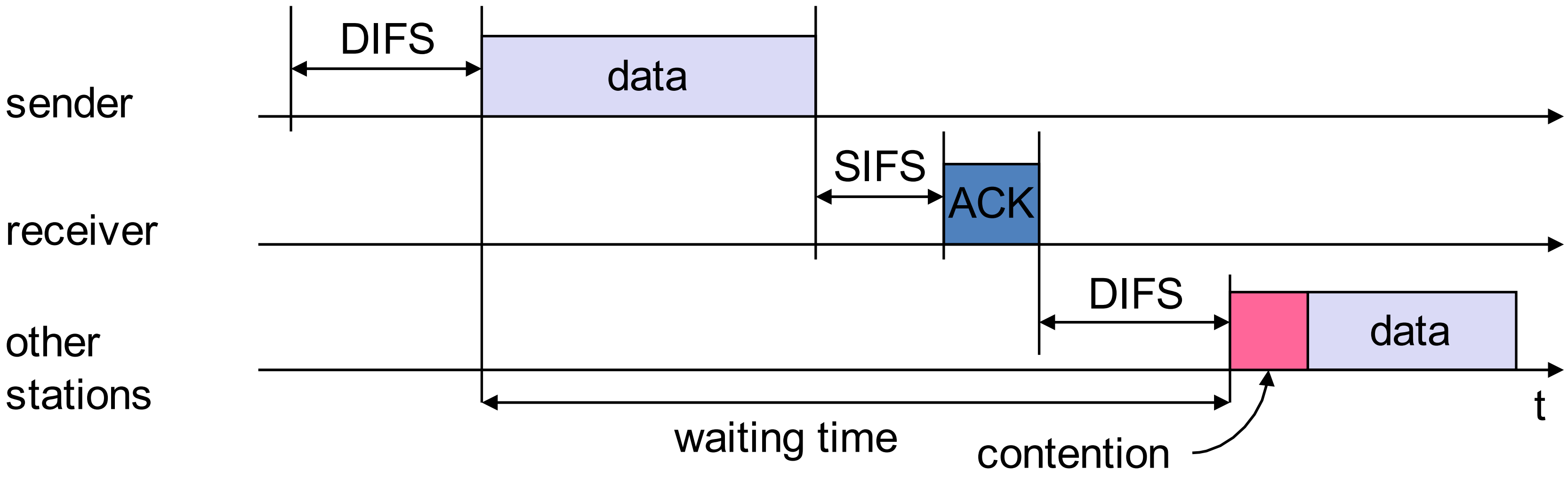
- Stations choose their backoff time randomly from contention window
- Ideal contention window size is trade-off between acceptable load and experienced delay
- Initial contention window size (CWmin) is 7 slots (backoff time between 0 and 7)
- After collision (no ack), contention window is “doubled” until CWmax = 255 is reached:
  7 -> 15 -> 31 -> 63 -> 127 -> 255
- The backoff time is chosen randomly in [0, CW-1], as mentioned by Bianchi.

802.11 – Competing Stations (Simple Version)



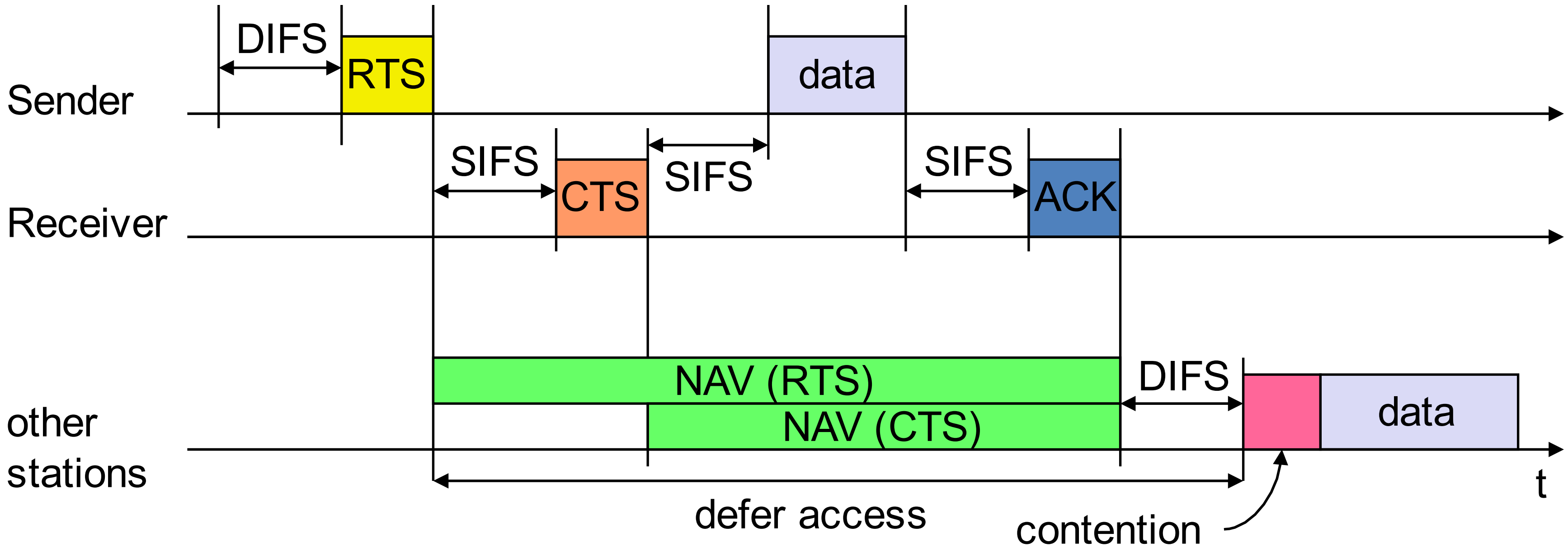
802.11 – DCF CSMA/CA

- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors



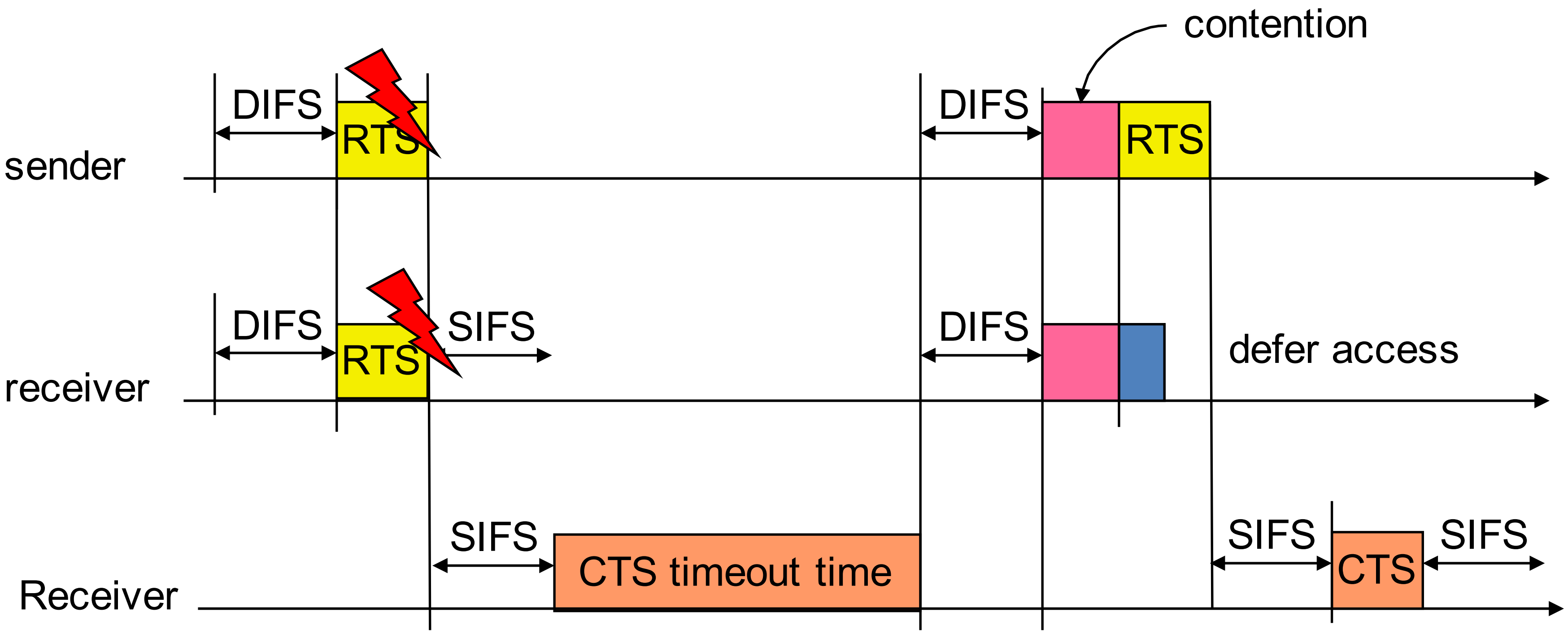
802.11 – DCF with RTS/CTS

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



802.11 - Colliding RTS

- When multiple RTS collides
  - The transmitting node only realize upon failure in receiving the CTS frame, which is called CTS timeout time.
  - CTS timeout time is equivalent to $300\mu s$ according to Bianchi's paper



Chapter 04, Module 02

(1) 802.11 MAC
(2) DCF
(3) PCF
(4) Control Types

802.11 - PCF (1)

- In PCF the base-station polls the other stations, asking them if they have anything to send
- It sends a beacon frame once every 10 or 100 ms.
  - This frame carries information on frequencies and such, and invites stations to sign up for transmission.
- To save battery, a base station can also direct a mobile station to go into sleep state
  - incoming messages will be buffered until it wakes up
- When base station transmits, ideally there can be no hidden terminals.
- PCF and DCF can coexist together
  - it works by carefully defining the interframe time interval.
  - first the base station can poll the other stations
  - if nobody replies, any station can acquire the channel

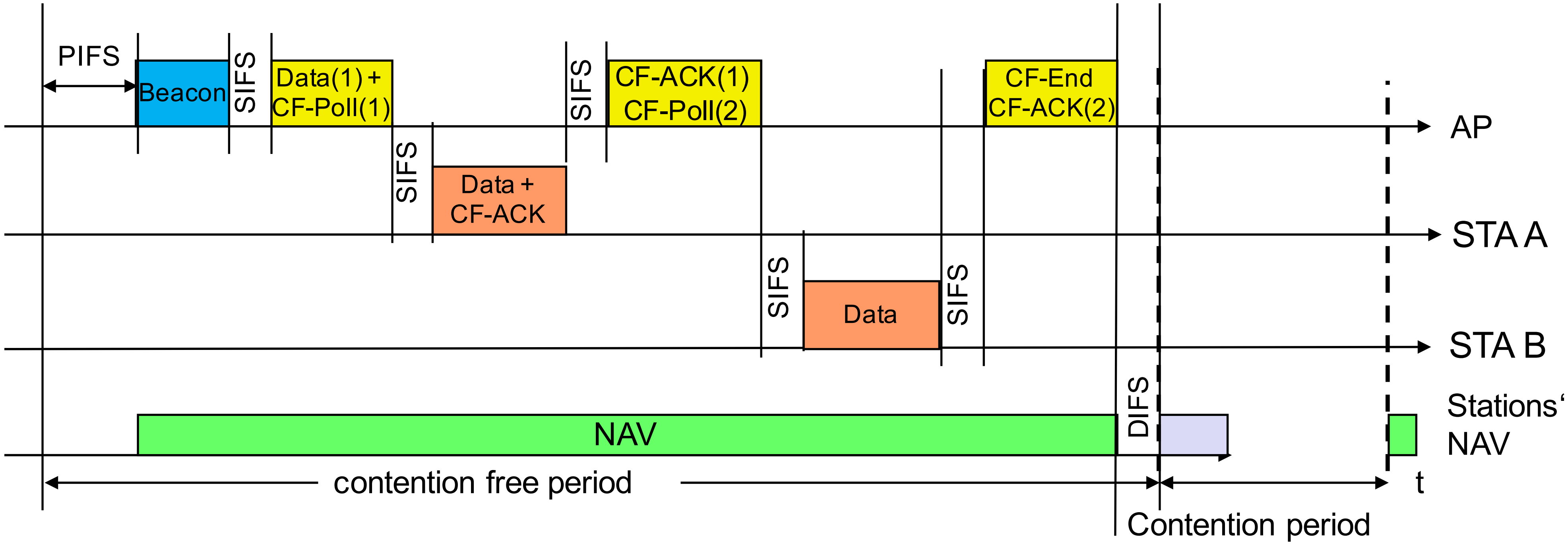
802.11 – PCF (2)

- Periodic "Super Frames"
  - contention-free period (CFP) and contention period (CP)

1. Start of CFP
2. Point coordinator (e.g., AP) sends beacon frame to all stations in basic service area after the channel is free for PIFS time.
3. Point coordinator polls the first station with
   - DATA+CF-poll frame, or
   - CF-poll frame only
4. After SIFS, a station replies with
   - DATA + CF-ACK or
     - After SIFS, AP replies with
       - DATA + CF-ACK + CF-Poll frame
       - CF-ACK + CF-Poll
   - NULL (No data) + CF-ACK
     - Station has no data to send, AP proceed to poll another station after SIFS time

802.11 – PCF (3)

- The AP continues to poll each station until it reaches the maximum duration of the CFP OR
- The AP can terminate the CFP by sending a CF-End frame
- Large overhead if few stations have data to send



Chapter 04, Module 02

(1) 802.11 MAC
(2) DCF
(3) PCF
(4) Frame Types

802.11 MAC Frame Format

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

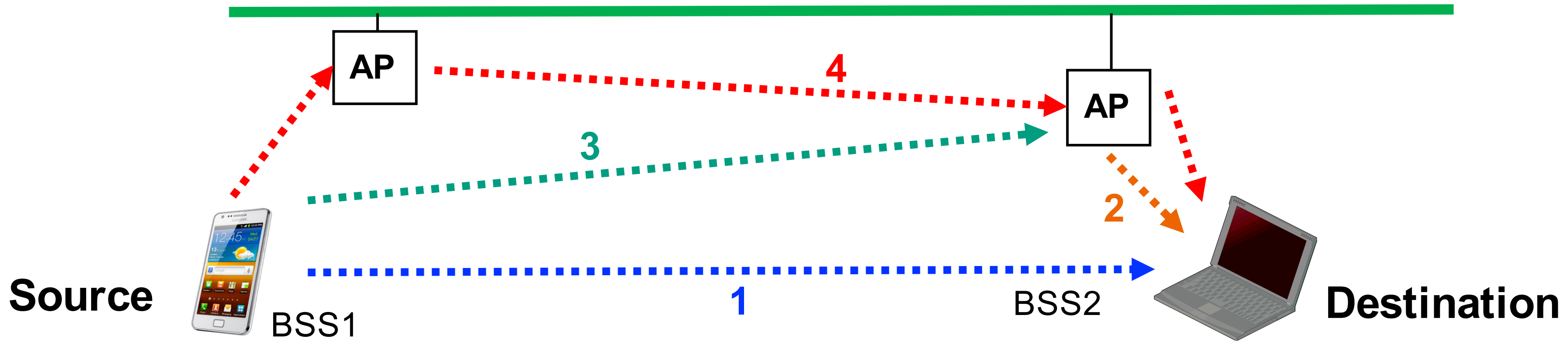
bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	WEP	Order

- **Type**: Control, management, or data
- **Sub-Type**: Association, disassociation, re-association, probe, authentication, de-authentication, CTS, RTS, Ack, ...
- Retry/retransmission
- Going to **Power Save mode**
  - More buffered data at AP for a station in power save mode
- Wireless Equivalent Privacy (**Security**) info in this frame
- **Strict ordering**

MAC Frame Fields

- **Duration/Connection ID**:
  - If used as duration field, indicates time (in seconds) channel will be allocated for successful transmission of MAC frame. Includes time until the end of ACK
  - In some control frames, contains association or connection identifier
- **Sequence Control**:
  - 4-bit fragment number subfield
    - For fragmentation and reassembly
  - 12-bit sequence number
  - Number frames between given transmitter and receiver

802.11 Frame Address Fields



	To Distribution System	From Distribution System	Address 1	Address 2	Address 3	Address 4
1 Ad-hoc network	0	0	Destination Address	Source Address	BSS ID	-
2 Infrastructure network, from AP	0	1	Destination Address	BSS ID	Source Address	-
3 Infrastructure network, to AP	1	0	BSS ID	Source Address	Destination Address	-
4 Infrastructure network, within DS	1	1	Receiver Address	Transmitter Address	Destination Address	Source Address

Management Frames

- ***Management frames*** are used to manage access to wireless networks and to move associations from one access point to another within an extended service set (ESS).

Management Frame Types and Subtype Field Values

Frame Subtype	Subtype Field Value
Association request	0000
Association response	0001
Reassociation request	0010
Reassociation response	0011
Probe request	0100
Probe response	0101
Beacon	1000
Announcement Traffic Indication Message (ATIM)	1001
Disassociation	1010
Authentication	1011
Deauthentication	1100
Action (added with 802.11i amendment)	1101
Block ACK Request (added with 802.11i amendment)	1000
Block ACK (added with 802.11i amendment)	1001
Power Save Poll (PS-Poll)	1010
Request to Send (RTS)	1011
Clear to Send (CTS)	1100
Acknowledgment (ACK)	1101
Contention-Free (CF)-End	1110
CF-End + CF-ACK	1111

Control Frames, Data Frames

SECURE MOBILE NETWORKING

- ***Control frames*** are used to assist with the delivery of data frames and must be able to be interpreted by all stations participating in a BSS.
  - This means that they must be transmitted using a modulation technique and at a data rate compatible with all hardware participating in the BSS.
  - Power Save(PS) Poll, Request to Send (RTS), Clear to send (CTS), Acknowledgement(ACK), Contention-Free(CF)-End (PCF only), CF-End+CF-ACK (PCF only), Black-ACK(HCF), Black Ack Request(HCF)
- ***Data frames*** are the actual carriers of application-level data.
  - Data, Data+CF-Ack (PCF only), Data+CF-Poll (PCF only), Data+CF-Ack+CF-Poll (PCF only), Null data (no data transmitted), CF-Ack (no data transmitted) (PCF only), CF-Poll (no data transmitted) (PCF only), Data+CF-Ack+CF-Poll (PCF only), Qos Data (HCF), Qos Null (No Data) (HCF), Qos Data+CF-Ack (HCF), Qos Data+CF-Poll (HCF), Qos Data+CF-Ack+CF-Poll (HCF), Qos Cf-Poll(HCF), Qos CF-ACK+CF-Poll (HCF)

Control Frames: ACK, RTS, CTS

- Acknowledgement

ACK

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

- Request To Send

RTS

bytes	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	CRC

- Clear To Send

CTS

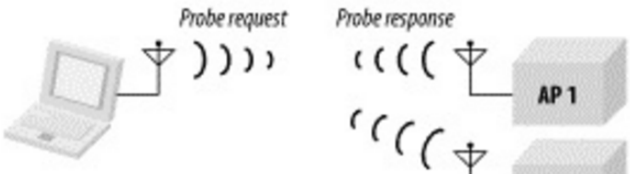
bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

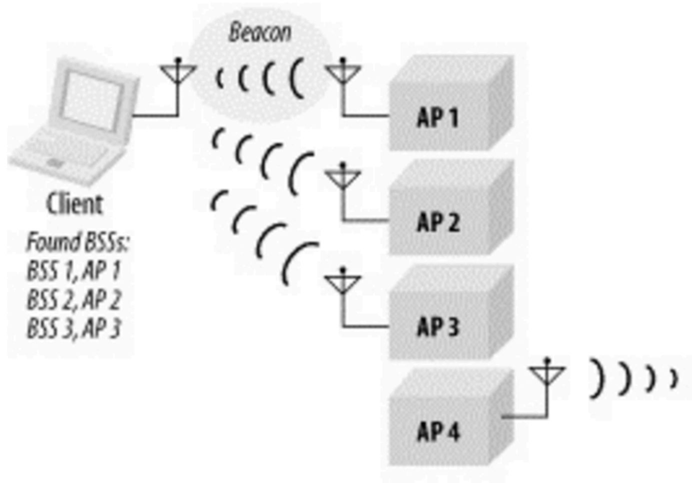
Beacon Management Frame

SECURE MOBILE NETWORKING

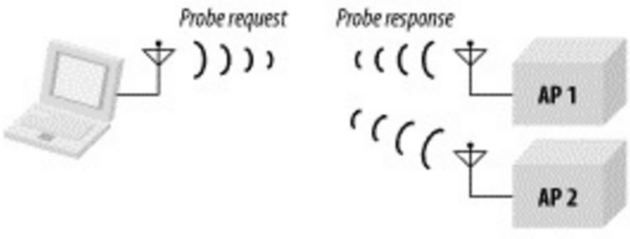
- Beacon frames can be used by client stations seeking wireless network to join, or these client stations may use other frames known as *probe request* and *probe response* frames.
- ***Active scanning*** uses probe request and probe response frames instead of the beacon frame to find a WLAN to join.
  - Station finds out network rather than waiting for network to announce its availability to all the stations.
- The ***passive scanning:*** the client station listens (receives) in order to find the access points. This is done by receiving beacon frames and using them to find the access point for the BSS to be joined.

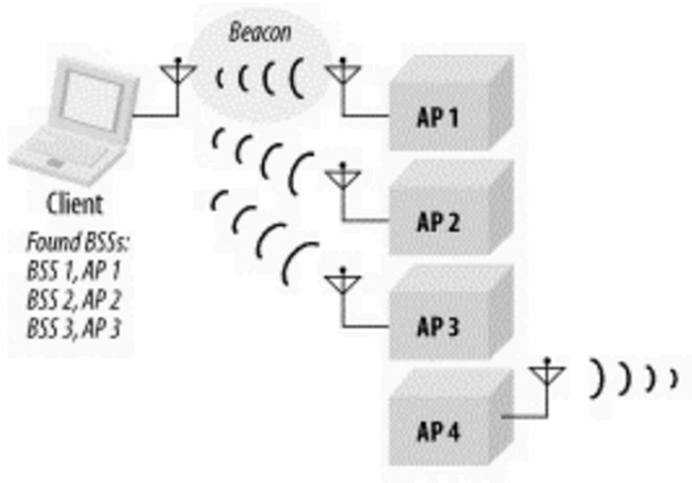
Active or Passive Scanning?





Active or Passive Scanning?





Active Scanning **Passive Scanning**

Acknowledgements & Additional Readings

- Some of the slides in this chapter have been adopted from
  - Duncan Kitchin @ Intel Corporation, Wireless Networking Group
  - Prof. Jochen Schiller @ FU Berlin, Prof. Schmitt @ U Kaiserslautern

- Additional Readings
  - [Schiller2003] gives an overview
  - Standards and web resources
    - http://grouper.ieee.org/groups/802/11/
      - → IEEE 802.11 committee
    - http://standards.ieee.org/getieee802/
      - → Download of selected specifications (see also download area on our course webpage)
    - http://www.wi-fi.org (Wi-Fi Alliance)
    - http://www.wifiplanet.com

Copyright Notice