COMP4310/6310 Wireless Mobile Computing
IEEE 802.11
Review

• Duplexing
  - Full-duplex
  - Half-duplex: FDD, TDD

• MAC protocol design
  - Centralized
    • Widely used in cellular networks
  - Distributed
    • Widely used in wireless LAN (WiFi).
Centralized MAC

- SDMA
- FDMA
- TDMA
- CDMA
Distributed MAC

- ALOHA
- Slotted ALOHA
- CSMA
  - 1-persistent CSMA
  - p-persistent CSMA
- CSMA/CA
  - RTS/CTS
- Today: CSMA/CA based IEEE 802.11 for wireless LAN (WLAN)
Characteristics of wireless LANs

- **Advantages**
  - Very flexible within the reception area
  - Ad-hoc networks without previous planning possible
  - (Almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - More robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

- **Disadvantages**
  - Typically lower bandwidth compared to wired networks (1-108 Mbit/s)
    - Shared among all users.
  - Limited range;
  - Products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions.
Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary
Comparison: infrared vs. radio

• Infrared
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)

• Advantages
  - simple, cheap, available in many mobile devices
  - no licenses needed
  - simple shielding possible

• Disadvantages
  - interference by sunlight, heat sources etc.
  - many things shield or absorb IR light
  - low bandwidth

• Example
  - IrDA (Infrared Data Association) interface available everywhere

• Radio
  - typically using the license free ISM band at 2.4 GHz

• Advantages
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)

• Disadvantages
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices

• Example
  - WaveLAN, HIPERLAN, Bluetooth
**802.11 - Architecture of an infrastructure network**

- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Basic Service Set (BSS)**
  - group of stations using the same radio frequency
- **Access Point**
  - station integrated into the wireless LAN and the distribution system
- **Portal**
  - bridge to other (wired) networks
- **Distribution System**
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS
802.11 - Architecture of an ad-hoc network

- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency
IEEE standard 802.11

mobile terminal

server

fixed terminal

infrastructure network

application

TCP

IP

Logic Link Control (LLC)

802.11 MAC

802.11 PHY

application

TCP

IP

LLC

802.11 MAC

802.3 MAC

802.11 PHY

802.3 PHY

LLC

802.3 MAC

802.3 PHY
### 802.11 - Layers and functions

- **DLC**: Data Link Control Layer
  - **MAC**: access mechanisms, fragmentation, encryption
  - **MAC Management**: synchronization, roaming, MIB, power management

<table>
<thead>
<tr>
<th>DLC</th>
<th>LLC</th>
<th>MAC</th>
<th>MAC Management</th>
<th>Station Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHY</td>
<td>PLCP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHY</td>
<td>PMD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
802.11 - Physical layer

- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- Infrared
- Modulations
  - BPSK, QPSK, 8PSK, 16QAM, 64QAM, 256QAM
- Number of Antennas
  - 1 up to 8 antennas
802.11 MAC

- Logical Link Control
  - Contention-free service
  - Contention service

MAC Layer

Point Coordination Function (PCF)

Distributed Coordination Function (DCF)

<table>
<thead>
<tr>
<th>2.4-Ghz frequency-hopping spread spectrum</th>
<th>2.4-Ghz direct-sequence spread spectrum</th>
<th>Infrared</th>
<th>5-Ghz orthogonal FDM</th>
<th>2.4-Ghz direct sequence spread spectrum</th>
<th>2.4-Ghz DS-SS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>1 Mbps</td>
<td>2 Mbps</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
<td>5.5 Mbps 11 Mbps</td>
<td>6, 9, 12, 18, 24, 36, 48, 54 Mbps</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>2 Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IEEE 802.11 IEEE 802.11a IEEE 802.11b IEEE 802.11g
DCF and PCF

- PCF and DCF can operate concurrently within the same BSS.
- The two access methods alternate, with a contention-free period (CFP) followed by a contention period (CP).

DCF: fundamental access method of IEEE 802.11 MAC, implemented in all STAs.
- known as CSMA/CA
PCF

- Coordinated by Point Coordinator (PC), typically collocated with the AP.
  - Beacon frame is a management frame that maintains the synchronization of the timers in the stations and delivers protocol related parameters.
- Polling stations one by one (centralized operation)
  - Like TDMA
- PCF has higher priority than the DCF.
- Limited use
DCF MAC Requirements

- No centralized coordinators: fully distributed operations
- No clock synchronization: asynchronous operations
- Widely-used today

- To avoid interference among simultaneous transmissions
  - But enable as many non-interfering transmission as possible
  - Maintain fairness among transmissions
CSMA/CA in DCF

- DCF is based on CSMA/CA
  - if station has frame to send it listens to medium
  - if medium idle, station may transmit
  - else waits until current transmission completes, then back off (called exponential backoff).
IEEE 802.11 MAC Logic

IFS: inter-frame space:
- DIFS: DCF IFS
- SIFS: Short IFS
- ...
Basic Example DCF

DIFS: DCF inter-frame space
SIFS: short inter-frame space (SIFS < DIFS)
How to transmit ACK

- Question: The receiver should send an ACK back to the transmitter, should the receiver do the same process of CSMA/CA to send the ACK?
Example

should B send the ACK immediately or sense the channel first?

802.11 DCF specifies ACK must be sent immediately, and guarantees there will be no collision.
Guaranteed Delivery of ACK

The length of ACK is SIFS < DIFS
Binary Exponential Backoff

Backoff Interval (measured by number of time slots)
When channel is busy, choose a backoff interval randomly from the range $[0, cw-1]$.
- $cw$ is called the contention window
Count down the backoff interval when medium becomes idle.
Count down is suspended if medium becomes busy again.
When backoff interval reaches 0, transmit
If the transmission does not succeed, double $cw$ next time
- Next time, the transmission may wait even longer.
- That’s the reason it is called (binary) exponential backoff
- Q: Why binary exponential backoff is useful?
Transmission with RTS/CTS, also called virtual carrier sensing

Network Allocation Vector (NAV): when a node receives RTS or CTS, it knows someone will use the channel.
IEEE 802.11 DCF (1)

- CSMA/CA
  - Contention-based random access
  - Collision detection not possible while transmitting
- Uses RTS/CTS exchange to avoid hidden terminal problem
  - Any node overhearing a CTS cannot transmit for the duration of the transfer.
  - Any node overhearing an RTS cannot transmit for the duration of the transfer (to avoid collision with ACK)
- Uses ACK to achieve reliability
IEEE 802.11 DCF (2)

- Carrier sense in 802.11
  - Physical carrier sense
  - Virtual carrier sense using Network Allocation Vector (NAV)
    - RTS/CTS specify duration of subsequent DATA/ACK
    - NAV is updated based on overheard RTS/CTS /DATA

- Collision avoidance
  - Nodes stay silent when carrier sensed busy (physical/virtual)
  - Backoff intervals are used to reduce collision probability
Disadvantages of IEEE 802.11 DCF

• High power consumption
• Hidden terminal problem not totally solved
• Exposed terminal problem not solved
• Fairness problem among different transmitting nodes
• Only providing best-effort service
Summary of IEEE 802.11 MAC Timing Basic Access Method

(a) Basic Access Method
802.11 - MAC management

- **Synchronization**
  - try to find a LAN, try to stay within a LAN
  - timer etc.

- **Association/Reassociation**
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
Synchronization using a Beacon (infrastructure)

- beacon interval
- access point
- medium
- busy
- value of the timestamp
- B beacon frame
Synchronization using a Beacon (ad-hoc)

- beacon interval
- station_1: B_1, busy
- station_2: B_2, busy
- medium: busy, busy, busy, busy
- value of the timestamp
- beacon frame
- random delay
Active Scanning Example

Steps to Association:
Station sends Probe.

Initial connection to an Access Point

Access Point A
Access Point C
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.

Initial connection to an Access Point
Steps to Association:

1. Station sends Probe.
2. APs send Probe Response.
3. Station selects best AP.
4. Station sends Association Request to selected AP.
5. AP sends Association Response.

Initial connection to an Access Point
Active Scanning Example

Steps to Association:

Station sends Probe.

APs send Probe Response.

Station selects best AP.

Station sends Association Request to selected AP.

AP sends Association Response.

Initial connection to an Access Point
- ReAssociation follows a similar process