IEEE802.11

Guevara Noubir

Textbook:
Jochen Schiller, Mobile Communications, Addison-Wesley
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
 LLC
 802.11 MAC
 802.11 PHY

application
 TCP
 IP
 LLC
 802.11 MAC
 802.11 PHY

application
 TCP
 IP
 LLC
 802.3 MAC
 802.3 PHY
### 802.11 - Layers and functions

- **MAC**
  - access mechanisms, fragmentation, encryption
- **MAC Management**
  - synchronization, roaming, MIB, power management
- **PLCP** Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- **PMD** Physical Medium Dependent
  - modulation, coding
- **PHY Management**
  - channel selection, MIB
- **Station Management**
  - coordination of all management functions

<table>
<thead>
<tr>
<th>DLC</th>
<th>LLC</th>
<th>MAC</th>
<th>MAC Management</th>
<th>PHY</th>
<th>PLCP</th>
<th>PHY Management</th>
<th>PMD</th>
<th>Station Management</th>
</tr>
</thead>
</table>

IEEE802.11
Figure 14.5  IEEE 802.11 Protocol Architecture
802.11 - Physical layer

- 5 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum) 2.4 GHz
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum) 2.4GHz
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
  - chipping sequence: +1, -1, +1, -1, +1, -1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- Infrared
  - 850-950 nm, diffuse light, typ. 10 m range
  - carrier detection, energy detection, synchronization
IEEE 802.11abgn

- IEEE 802.11a
  - Makes use of 5-GHz band
  - Provides rates of 6, 9, 12, 18, 24, 36, 48, 54 Mbps
  - Uses orthogonal frequency division multiplexing (OFDM)
  - Subcarrier modulated using BPSK, QPSK, 16-QAM or 64-QAM

- IEEE 802.11b
  - Provides data rates of 5.5 and 11 Mbps
  - Complementary code keying (CCK) modulation scheme

- IEEE 802.11g
  - Mix of a & b on 2.4Ghz

- IEEE802.11n
  - Multiple Input Multiple Output

- Higher rates are not achieved for free
  - There are assumptions about range, channel, power
FHSS PHY packet format

- **Synchronization**
  - synch with 010101... pattern
- **SFD (Start Frame Delimiter)**
  - 0000110010111101 start pattern
- **PLW (PLCP_PDU Length Word)**
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- **PSF (PLCP Signaling Field)**
  - data rate of payload (1 or 2 Mbit/s)
- **HEC (Header Error Check)**
  - CRC with $x^{16}+x^{12}+x^5+1$

```
80  16  12  4  16  variable  bits

<table>
<thead>
<tr>
<th></th>
<th>SFD</th>
<th>PLW</th>
<th>PSF</th>
<th>HEC</th>
<th>payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLCP preamble</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PLCP header</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

IEEE802.11
### DSSS PHY packet format

- **Synchronization**
  - synch., gain setting, energy detection, frequency offset compensation
- **SFD (Start Frame Delimiter)**
  - 11100111010000
- **Signal**
  - data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- **Service Length**
  - future use, 00: 802.11 compliant
  - length of the payload
- **HEC (Header Error Check)**
  - protection of signal, service and length, $x^{16}+x^{12}+x^5+1$

<table>
<thead>
<tr>
<th>bits</th>
<th>fixed</th>
<th>variable</th>
</tr>
</thead>
<tbody>
<tr>
<td>128</td>
<td>SFD</td>
<td>signal</td>
</tr>
<tr>
<td>16</td>
<td>service</td>
<td>length</td>
</tr>
<tr>
<td>16</td>
<td>HEC</td>
<td>payload</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PLCP preamble

IEEE802.11
802.11 - MAC layer I – DFWMAC
Distributed Foundation Wireless MAC

• Traffic services
  – Asynchronous Data Service (mandatory)
    • exchange of data packets based on “best-effort”
    • support of broadcast and multicast
  – Time-Bounded Service (optional)
    • implemented using PCF (Point Coordination Function)

• Access methods
  – DFWMAC-DCF CSMA/CA (mandatory)
    • collision avoidance via randomized “back-off” mechanism
    • minimum distance between consecutive packets
    • ACK packet for acknowledgements (not for broadcasts)
  – DFWMAC-DCF w/ RTS/CTS (optional)
    • Distributed Foundation Wireless MAC
    • avoids hidden terminal problem
  – DFWMAC- PCF (optional)
    • access point polls terminals according to a list
802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
  - PIFS (PCF IFS)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF, Distributed Coordination Function IFS)
    - lowest priority, for asynchronous data service
IFS Timing

- $\text{aSIFSTime} = \text{aRxRFDelay} + \text{aRxPLCPDelay} + \text{aMACProcessingDelay} + \text{aRxTxTurnaroundTime}.$
- $\text{aSlotTime} = \text{aCCATime} + \text{aRxTxTurnaroundTime} + \text{aAirPropagationTime} + \text{aMACProcessingDelay}.$
- $\text{PIFS} = \text{aSIFSTime} + \text{aSlotTime}$
- $\text{DIFS} = \text{aSIFSTime} + 2 \times \text{aSlotTime}$
- $\text{EIFS} = \text{aSIFSTime} + (8 \times \text{ACKSize}) + \text{aPreambleLength} + \text{aPLCPHeaderLength} + \text{DIFS}$
- For Direct Sequence Spread Spectrum physical layer:
  - $\text{aSlotTime}$ 20 $\mu$s
  - $\text{aSIFSTime}$ 10 $\mu$s
  - $\text{aCCATime}$ < 15 $\mu$s
  - $\text{aRxTxTurnaroundTime}$ <5 $\mu$s
802.11 - CSMA/CA access method I

- 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 Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- 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)
IEEE802.11 - competing stations - simple version

- **DIFS**: Inter-Frame Space
- **bo**: Backoff
- **bo_e**: Elapsed backoff time
- **bo_r**: Residual backoff time
- **busy**: Medium not idle (frame, ack etc.)
- **t**: Time

Packet arrival at MAC

Diagram with stations and backoff states.
802.11 - CSMA/CA access method

II

• 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 - DFWMAC

- 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
Fragmentation
DFWMAC-PCF I

IEEE802.11
DFWMAC-PCF II

IEEE802.11

7.20.1
802.11 - Frame format

- **Types**
  - control frames, management frames, data frames
- **Sequence numbers**
  - important against duplicated frames due to lost ACKs
- **Addresses**
  - receiver, transmitter (physical), BSS identifier, sender (logical)
- **Miscellaneous**
  - sending time, checksum, frame control, data

<table>
<thead>
<tr>
<th>bytes</th>
<th>2</th>
<th>2</th>
<th>6</th>
<th>6</th>
<th>6</th>
<th>2</th>
<th>6</th>
<th>0-2312</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Frame Control</td>
<td>Duration ID</td>
<td>Address 1</td>
<td>Address 2</td>
<td>Address 3</td>
<td>Sequence Control</td>
<td>Address 4</td>
<td>Data</td>
<td>CRC</td>
</tr>
</tbody>
</table>

Version, Type, Subtype, To DS, From DS, More Fragments, Retry, Power Management, More Data, Wired Equivalent Privacy (WEP), and Order
MAC address format

<table>
<thead>
<tr>
<th>scenario</th>
<th>to DS</th>
<th>from DS</th>
<th>address 1</th>
<th>address 2</th>
<th>address 3</th>
<th>address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad-hoc network</td>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, from AP</td>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, to AP</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, within DS</td>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

DS: Distribution System
AP: Access Point
DA: Destination Address (final recipient)
SA: Source Address (initiator)
BSSID: Basic Service Set Identifier
RA: Receiver Address (immediate recipient)
TA: Transmitter Address (immediate sender)
802.11 - MAC management

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

- **Power management**
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements

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

- **MIB - Management Information Base**
  - managing, read, write
Synchronization using a Beacon (infrastructure)
Synchronization using a Beacon (ad hoc)
Power management

• Idea: switch the transceiver off if not needed
• States of a station: sleep and awake
• Timing Synchronization Function (TSF)
  – stations wake up at the same time
• Infrastructure
  – Traffic Indication Map (TIM)
    • list of unicast receivers transmitted by AP
  – Delivery Traffic Indication Map (DTIM)
    • list of broadcast/multicast receivers transmitted by AP
• Ad hoc
  – Ad hoc Traffic Indication Map (ATIM)
    • announcement of receivers by stations buffering frames
    • more complicated - no central AP
    • collision of ATIMs possible (scalability?)
Power saving with wake-up patterns (infrastructure)

- **TIM interval**: Time Interval Message
- **DTIM interval**: Distributed Token Bucket Interval Message
- **access point**: The device that manages the network
- **medium**: The communication medium
- **station**: A device that communicates with the access point
- **D**: TIM
- **B**: DTIM
- **T**: busy
- **D**: busy
- **T**: busy
- **D**: busy
- **P**: PS poll
- **D**: data transmission to/from the station
- **B**: broadcast/multicast
- **awake**: The state when the device is active

IEEE802.11
Power saving with wake-up patterns (ad hoc)

- **ATIM window**
- **Beacon interval**

Station 1:
- \[B_1\] beacon frame
- \[\text{random delay}\]
- \[A\] transmit ATIM
- \[D\] transmit data

Station 2:
- \[B_2\] beacon frame
- \[\text{random delay}\]
- \[B_2\] transmit ATIM
- \[a\] acknowledge ATIM
- \[d\] acknowledge data

IEEE 802.11
802.11 - Roaming

- No or bad connection? Then perform:
  - Scanning
    - scan the environment, i.e., listen into the medium for beacon signals (passive) or send probes (active) 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