Wireless networks
Overview

- Wireless networks basics
- IEEE 802.11 (Wi-Fi) a/b/g/n
- ad Hoc MAC protocols
- ad Hoc routing DSR AODV
Wireless Networks

• Autonomous systems of mobile hosts connected by wireless links
• Nodes are autonomous and independent
  – mobile, battery powered
  – communicate mainly via radio frequencies
• Two modes of operations
  – *wireless networking with a base station*:
    • wired access points
  – *ad hoc networking*:
    • no centralized coordinators
Wireless networking with a BS

Diagram: A base station connects to multiple wireless nodes, and the network is linked to a wired network.
Wireless networking with a BS (2)

Base station

To wired network

Intracell communication
Wireless networking with a BS (3)
Ad hoc networking
Ad hoc networking (2)
Ad hoc networking (3)
Ad hoc networking (4)

Multihop communication
Wireless networks: challenges

• Limited knowledge
  – a terminal cannot head all the others
  – multipath fading effects

• Mobility/Failure of terminals
  – terminals move in the range of different BS
  – terminals move away from each other

• Limited terminals
  – battery life, memory, processing and transmission range

• Privacy
  – eavesdropping of ongoing communications
Wireless networks: some problems

• Access to a shared wireless channel
  – CSMA/CD cannot be used
  – hidden-exposed terminal problem

• Hand-off
  – moving a terminal into the range of a different BS

• Routing
  – deciding a path from source to destination in multi hop networks
  – dealing with arbitrary changes in neighborhood
## Wireless networks: protocol stack

<table>
<thead>
<tr>
<th>Layer</th>
<th>Protocols/Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application layer</td>
<td>App1, App2, App3</td>
</tr>
<tr>
<td>Transport layer</td>
<td>TCP, UDP</td>
</tr>
<tr>
<td>Network layer</td>
<td>Routing: AODV, DSR</td>
</tr>
<tr>
<td>Data link layer</td>
<td>MAC: CSMA/CA</td>
</tr>
<tr>
<td>Physical layer</td>
<td>RF, Infrared</td>
</tr>
</tbody>
</table>
Wired networks MAC protocols

• **Basic assumptions:**
  – a single channel is available for all communications
  – all stations can transmit on it and receive from it
  – if frames are send simultaneously on the channel the resulting signal is garbles (a *collision*)
  – all stations can detect collisions

• **Different protocols**
  – ALOHA, slotted ALOHA, CSMA, CSMA/CD
CSMA/CD

- Carries Sense Multiple Accesses with *Collision Detection*

- Basic idea of CSMA:
  - When a station has a frame to send listens to the channel to see if anyone else is transmitting
  - *if the channel is busy*, the station waits until it becomes idle
  - when channel is idle, the station transmits the frame
  - if a collision occurs the station waits a random amount of time and repeats the procedure.
CSMA/CD (2)

- **CSMA with Collision Detection**
  - a station aborts its transmission as soon as it detects a collision
    - if two stations sense the channel idle simultaneously and start transmitting, they quickly abort the frame as soon as collision is detected
  - it is widely used on LANs in MAC sub-layer
  - IEEE 802.3 Ethernet
CSMA/CD (3)

- CSMA/CD behavior

Frame □ □ □ □ Frame □ □ □ □ Frame □ □ □ □

- transmission period
- contention period
- contention slot (2*T)
- idle period
Binary Exponential Backoff

- Used in IEEE 802.3

- Time after a collision is divided in contention slots
  - length of a contention slot is equal to worst case round propagation time (2T if T is the time to reach the most distant stations)

- After the first collision
  - each station waits 0 or 1 slot before trying again
Binary Exponential Backoff (2)

• After collision $i$
  – chooses $x$ at random in $0, 1, 2, \ldots, 2^i - 1$
  – skips $x$ slots before retrying

• After 10 collisions:
  – the randomization interval is frozen at $0..1023$

• After 16 collisions
  – failure is reported back to upper levels
Wireless networks: MAC

• **Hidden terminal problem**
  – what matters is interference at the receiver *not* at the sender
The hidden terminal problem

Radio range
The hidden terminal problem (2)

A is sending to B
A is sending to B
C senses the medium: it will NOT hear A, out of range
A Hidden terminal problem (4)

A is sending to B

C senses the medium: it will NOT hear A, out of range

C starts to sent to B -- COLLISION OCCURS at B
Wireless networks: MAC

- **Hidden terminal problem**
  - what matters is interference at the receiver *not* at the sender
  - in the example: C is not able to detect a potential competitor because it is out of range and collision happens at B (the receiver)

- **Exposed terminal problem**
  - a station can hear a transmission and be able to transmit without interfere with it
The exposed terminal problem

1. B is transmitting to A, C wants to transmit to D
1. B is transmitting to A, C wants to transmit to D
2. C senses the medium, hears B and concludes: cannot transmit to D
The exposed terminal problem (3)

1. B is transmitting to A, C wants to transmit to D
2. C senses the medium, concludes: cannot transmit to D
3. The two transmissions can actually happen in parallel.
Wireless networks: MAC (2)

- what matters is interference at the receiver *not* at the sender
  - this cannot be established *sensing the carrier at the sender*

- Multiple transmissions can occur simultaneously if destinations are out of range of each other
  - a station can hear a transmission and be able to transmit without interfere with it

- Need different MAC protocols from wired LANs
The MACA protocol

- **Multiple Accesses with Collision Avoidance**
- **Basic idea:**
  - stimulate the receiver into transmitting a short frame
  - then transmitting a (long) data frame
  - stations hearing the short frame **refrain from transmitting** during the transmission of the subsequent data frame
The MACA protocol

C is within range of A but not within range of B and D
D is within range of B but not within range of A and C
E is within range of both A and B
The MACA protocol (2)

1. A wants to transmit to B, sends a Request To Send to B
1. A wants to transmit to B, sends a Request To Send to B
RTS is a short frame including the length of the data frame
that will eventually follow
The MACA protocol (3)

1. A wants to transmit to B, sends an RTS to B
The MACA protocol (4)

1. A wants to transmit to B, sends an RTS to B
2. If B wants to receive the message replies with a Clear To Send
   CTS is a short frame with data length copied from RTS
1. A wants to transmit to B, sends an **RTS** to B
2. If B wants to receive the message replies with a **CTS**
The MACA protocol (6)

1. A wants to transmit to B, sends an **RTS** to B
2. If B wants to receive the message replies with a **CTS**
3. Upon receipt of the CTS frame, A transmits the data frame
The MACA protocol (7)

C hears RTS, but not CTS
it is free to transmit after A has received the CTS from B
The MACA protocol (8)

D hears CTS, but not RTS
it should stay silent until data frame transmission completes
D hears CTS and RTS
it should stay silent until data frame transmission completes
The MACA protocol: collisions

C and B send RTS simultaneously to A
C and B send RTS simultaneously to A
The two messages collide
No CTS is generated
The MACA protocol: collisions (3)

C and B use *Binary Exponential Backoff* (same as Ethernet) to retry RTS
MACAW: MACA for Wireless

- Fine tunes MACA to improve performance
  - introduces an ACK frame to acknowledge a successful data frame
  - added Carrier Sensing to keep a station from transmitting RTS when a nearby station is also doing so to the same destination
  - exponential backoff is run for each separate pair source/destination and not for the single station
  - mechanisms to exchange information among stations and recognize temporary congestion problems
  - CSMA/CA used in IEEE 802.11 is based on MACAW
IEEE 802.11 family

- IEEE 802.11 (Legacy mode)
  - First released in 1997 and clarified in 1999
  - rarely used today
  - 1-2 Mbps data rate implemented via
    - infrared (IR) signals,
    - radio frequencies in the 2.4GHz band (ISM -- Industrial Scientific Medical Frequency band)
  - many degrees of freedom: interoperability was challenging among different products
  - rapidly supplemented (and popularized) by 802.11b
  - most used today 802.11a/b/g emerging 802.11n
IEEE 802.11 family (2)

- **IEEE 802.11b**
  - Released 1999
  - Operating frequency: 2.4GHz band (ISM band)
    - potential interference with other appliances: cordless telephones, microwave ovens etc
  - Throughput (typ): 4.3 Mbps
  - Data rate (max): 11 Mbps
  - Modulation technique: DSSS
IEEE 802.11a

- Released 1999
- Operating frequency: 5 GHz band (Unlicensed National Information Infrastructure U-NII band)
- Throughput (typ): 23 Mbps
- Data rate (max): 54 Mbps
- Modulation technique: OFDM
IEEE 802.11 family (4)

• **IEEE 802.11g**
  – Released 2003
  – Operating frequency: 2.4GHz band (ISM band)
  – Throughput (typ): 19 Mbps
  – Data rate (max): 54 Mbps
  – Modulation technique: OFDM
IEEE 802.11 family (5)

- **IEEE 802.11n**
  - To be released 2009
  - Operating frequency: 2.4GHz band and 5GHz band
  - Throughput (typ): 74 Mbps
  - Data rate (max): 248 Mbps
  - Modulation technique: MIMO using multiple antennas
IEEE 802.11: protocol stack

Upper Layers

Logical Link Control

MAC Sublayer

802.11 legacy
802.11n MIMO
802.11a OFDM
802.11b HR-DSSS
802.11g OFDM

Data link layer

Physical layer
IEEE 802.11: Architecture

- A group of stations operating under a given coordination function
  - may use or not a base station (Access Point)
  - is using APs a station communicates with another channeling all the traffic through a centralized AP
  - AP can provide connectivity with other APs and other groups of stations via fixed infrastructure
IEEE 802.11: Architecture (2)

• Supports ad hoc networks

the IEEE 802.11 view

*a group of stations that are under the direct control of a single coordination function without the aid of an infrastructure network*

– a station can communicate directly with another without channeling all the traffic through AP
The physical layer

- All techniques make it possible to deliver a MAC frame from one station to another
- Technology used and speed differ
- We give a short list of keyword
The physical layer: IR

- **Features:**
  - Diffused transmission at 0.85-0.95 microns
  - Two speeds: 1Mbps 2Mbps
  - encoding *gray code*
    - at 1Mbps: 4 bits on 16 bits containing fifteen 0s and a single 1
    - at 2Mbps: 2 bits on 4 bits 0001, 0010, 0100, 1000
  - cannot penetrate walls, swamped by sun
  - not very popular
The physical layer: FHSS

- Frequency Hopping Spread Spectrum
  - 79 channels, 1MHz wide each starting at the low end of the 2.4 GHz
  - bandwidth: 1MBps
  - Frequency hopping
    - pseudo-random generator drives hopping
    - same seed on all stations, synchronization
    - dwell time (time spent in each frequency) less than 400msec
    - makes eavesdropping harder
    - solves multipath fading over long distances
The physical layer: DSSS

- Discrete Sequence Spread Spectrum
  - bandwidth: 1-2MBps
  - ?????
IEEE 802.11: MAC Sublayer

- Two modes of operations:
  - DCF: Distributed Coordination Function
    - completely decentralized
    - thought for best effort asynchronous traffic
  - PCF: Point Coordination Function
    - uses base station to control all activity in its cell
    - thought for delay-sensitive traffic
    - BS polls stations to ask for transmissions
    - based on DCF

- **DCF must be implemented by all stations**
- **DCF and PCF can be active at the same time in the same cell**
IEEE 208.11 MAC architecture

Distributed Coordination Function (DCF)

Used for contention services
IEEE 208.11 MAC architecture (2)

Used for contention free services and based on DCF

Point Coordination Function (PCF)

Distributed Coordination Function (DCF)
IEEE 802.1: DCF

- Must be implemented by all stations
- Completely decentralized
- Best effort asynchronous traffic
- Stations must contend for the channel for each frame
  - using CSMA/CA
IEEE 802.1: DCF (2)

• Carrier sensing is performed at two levels:
  – physical CS
    • detects the presence of other IEEE 802.11 WLAN users by analyzing all the detected packets
    • detects any activity in the channel due to other sources
  – virtual CS
    • performed sending duration information in the header of an RTS, CTS and data frame
    • duration information is used to adjust station’s NAV (network allocation vector) that indicates channel busy and the time that must elapse before sampling again the channel for idle status
  – A channel is marked busy if either the physical or the virtual CS indicate busy
**IEEE 802.1: DCF (3)**

- Priority access to the medium is controlled through the use of interframe space (IFS) time intervals
  - IFS: mandatory periods of idle time on the transmission medium

- **Three IFS specified by the standard:**
  - short IFS (SIFS)
  - point coordination function IFS (PIFS)
  - DCF-IFS (DIFS)
  - SIFS < PIFS < DIFS
  - stations only required to wait a SIFS have the highest priority
DCF basic access method

source

Senses channel idle and waits for DIFS

destination

other
DCF basic access method (2)

source

If idle starts transmitting data

destination

other
DCF basic access method (3)

First bytes in frame specify duration (data + ACK)
DCF basic access method (3)

First bytes in frame specify duration (data + ACK)

Hearing duration sets NAV for virtual CS
DCF basic access method (4)

source

Waits SIFS before ack successful transmission

destination

other

NAV
Stations must again wait DIFS before transmitting.
DCF basic access method: collision

When collision occurs stations continue to transmit the entire frame.

Band wasted for large data frames.
DCF basic access method: collision (2)
DCF RTS/CTS

- **Source**
  - DIFS
  - RTS (20 bytes)
  - SIFS
  - CTS
  - SIFS
  - NAV/CTS
  - NAV/data

- **Destination**
  - SIFS
  - Data (14 bytes)
  - SIFS
  - ACK

- **Other**
  - NAV/RTS
  - NAV/CTS
  - NAV/data
DCF: RTS/CTS

- never use RTS/CTS: lightly loaded medium
- use RTS/CTS for long messages: when length exceeds \texttt{RTS\_Threshold}
- always use RTS/CTS
DCF: Fragmentation

• Fragmentation of large data frames may improve reliability:
  – performed only if data is larger than Fragmentation_Theshold (size of each fragment except last)
  – all fragments are sent in sequence
  – channel is not released until the complete data has been transmitted or the source station fails to receive an acknowledgement for the transmitted fragment
DCF Fragmentation (2)

source

| SIFS | Frag0 | SIFS | Frag1 | SIFS | ACK0 | SIFS | ACK1 |

destination

| NAV/RTS/CTS | NAV/Frag0 | NAV/Frag1 |
DCF: Fragmentation (3)

- When an ACK is not received in time, the source station re-contents the channel
- after getting the channel again it starts from the last unacknowledged fragment

- if RTS/CTS is used the duration in RTS/CTS account only for the transmission of the first fragment

- the subsequent duration information are extracted in the duration information of each fragment
More on random backoff

• Time is slotted
  – slots of $\text{Slot\_time}$ different for each PHY layer used

• To get a channel after a collision
  – a station senses the channel if the channel is not busy it waits until the channel is idle for a DIFS period
  – after DIFS idle it computes a random backoff time
    • randomly chooses a number $x$ of slots to be waited (init. 0--7)
    • decrements $x$ until channel becomes busy or $x$ reaches 0
      – if $x==0$, the station sends the frame
      – if $x>0$ and channel becomes busy the station freezes the timer, and starts to decrement it after it becomes idle again for DIFS
More on random backoff (2)

• To get a channel after a collision (contd.)
  – if two stations reach 0 at the same time a new collision occurs
  
  – after the $i$ collisions, $x$ is chosen in range
    
    $0 \ldots \lfloor 2^{(2+i)} \times \text{ranf}() \rfloor$
    
    where $\text{ranf}()$ is a uniform random var. in $(0,1)$

  – The idle period after a DIFS idle period is called 
    contention window (CW)
IEEE 802.11: Frames

• Three types of frames:
  – **management**: station association/disassociation with the AP, synchronization, authentication
  – **control**: handshaking and acknowledgement
  – **data**: data transmission, can be combined with polling and ACK in PCF
IEEE 802.11: Frame format

Version: more than one protocol can coexist in the same cell
IEEE 802.11: Frame format (2)

Type of the frame: management, control, data

Subtype of the frame: eg. RTS, CTS, ACK
IEEE 802.11: Frame format (3)

Is the frame going to or coming from the intercell distribution system?

eg. To/From Ethernet interconnecting AS
### IEEE 802.11: Frame format (4)

<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 conn ID</td>
<td>Addr</td>
<td>Addr</td>
<td>Addr</td>
<td>Seq</td>
<td>Addr</td>
<td>Data</td>
<td>CRC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bits</th>
<th>2</th>
<th>2</th>
<th>4</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prot. Vers.</td>
<td>Type</td>
<td>Sub-type</td>
<td>To DS</td>
<td>From DS</td>
<td>More Frag</td>
<td>Retry</td>
<td>Power mgt</td>
<td>More data</td>
<td>W</td>
<td>O</td>
<td></td>
</tr>
</tbody>
</table>

- **More fragments will follow?**
- **Marks retransmission of a frame sent earlier**
IEEE 802.11: Frame format (5)

Frame control
- Duration
- ID
- Addr
- Addr
- Addr
- Seq
- Addr
- Data
- CRC

Prot. Vers.
- Type
- Sub-type
- To DS
- From DS
- More Frag
- Retry
- Power mgt
- More data
- W
- O

Used to put the receiver into sleep or take out from sleep

Sender has additional frames for the receiver
IEEE 802.11: Frame format (6)

Has the frame been encrypted using WEP?

Order: a sequence of frames with this bit on must be processed in order.
IEEE 802.11: Frame format (7)

Time (microsecs): how long the frame/fragment and its acknowledgement will occupy the channel
IEEE 802.11: Frame format (8)

<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>Frame ctrl</td>
<td>Duration conn ID</td>
<td>Addr</td>
<td>Addr</td>
<td>Addr</td>
<td>Seq</td>
<td>Addr</td>
<td>Data</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

Standard IEEE 48-bit MAC addresses:
source, destination, source and destination AP for inter-cell traffic
**IEEE 802.11: Frame format (9)**

**Sequence:** allows fragments to be numbered. 12 bits identify the frame and 4 identify fragments.

<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>Frame ctrl</td>
<td>Duration conn ID</td>
<td>Addr</td>
<td>Addr</td>
<td>Addr</td>
<td>Seq</td>
<td>Addr</td>
<td>Data</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

- **Frame ctrl**: contains control information like the frame type and duration.
- **Duration conn ID**: indicates the duration and connection ID.
- **Addr**: addresses, typically MAC addresses.
- **Seq**: sequence number for fragments.
- **Addr**: addresses, typically MAC addresses.
- **Data**: the payload data.
- **CRC**: cyclic redundancy check for error detection.
## IEEE 802.11: Frame format (10)

<table>
<thead>
<tr>
<th>Frame ctrl</th>
<th>Duration conn ID</th>
<th>Addr</th>
<th>Addr</th>
<th>Addr</th>
<th>Seq</th>
<th>Addr</th>
<th>Data</th>
<th>CRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>6</td>
<td>0--2312</td>
<td>4</td>
</tr>
</tbody>
</table>

Payload + (optional) bytes encryption/decryption for WEP (Wired Equivalent Privacy) protocol
IEEE 802.11: Frame format (11)

<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>Frame control</td>
<td>Duration conn ID</td>
<td>Addr</td>
<td>Addr</td>
<td>Addr</td>
<td>Seq</td>
<td>Addr</td>
<td>Data</td>
<td>CRC</td>
<td></td>
</tr>
</tbody>
</table>

**Cyclic Redundancy Check:**
32 bit hash code of the data for transmission error detection (NOT recovery)
IEEE 802.11: PCF

- **Optional capability:**
  - connection oriented
  - provides contention-free frame transfer
  - acts under the control of the point coordinator (PC) that performs polling and enables stations to transmit without contending for the channel
  - the method by which polling tables are maintained and polling sequence is determined is left to the implementor
  - it is required to coexist with DCS
• **Starting contention-free period**
  – AP sends a Beacon Frame (BF)
  – stations synchronize using BF

• **PCF occurs periodically**
  – $\text{CFP\_rate}$ specifies the repetition interval
  – in each repetition interval a portion of the time is allotted for contention-free traffic and the remaining for contention based traffic
  – $\text{CFP\_rate}$ corresponds to an integral number of BF
IEEE 802.11: PCF (3)

- **Length of PCF period**
  - CFP\_Max\_Duration determines the maximum size of a contention free period
  - AP decides the actual length, can be smaller if PCF traffic is light or DCF traffic is heavy
Coexistence of PCF and DCF

At the beginning of each period all stations update their NAV to the maximum length of PCF (CFP_max_duration)
Coexistence of PCF and DCF (2)

During PCF stations can only respond to a poll from the PC or for transmission of an ACK in the SIFS after receiving a data frame.
Coexistence of PCF and DCF (3)

PCF repetition interval

CF Period

PCF is always closed by PC sending a Contention Free End frame (CFE)

All stations
Running PCF

PC senses the medium. If idle for PIFS (SIFS < PIFS < DIFS) it sends the beacon frame

PC

PIFS BF

NAV-PCF

All stations
Running PCF (2)

Then waits for SIFS and sends a data and/or CF-poll frame

PIFS  BF  SIFS  D1+poll

PC

NAV-PCF

All stations
After SIFS, the destination can send a CF-ACK or data+CF-ACK frame.
After SIFS, the PC can send a CF-ACK or data or CF-poll frame.
Running PCF (5)

When polled a station can send data directly to another station

PC

NAV-PCF

All stations
Running PCF (6)

PC waits PIFS following and ACK frame to be sure transmission is finished before polling again.
Running PCF (7)

• With this model
  – PC can decide to send to a non-PCF aware station (one that only has DCF)
    • interaction works well as this station will respond with an ACK
  – messages can be fragmented as in DCF