Advanced Computer Networks
263-3501-00

WLAN, Cellular Networks

Patrick Stuedi
Spring Semester 2013
Last week

- Medium Access
- COPE
- Short Range Wireless Networks: Bluetooth, ZigBee, Sensor Networks

Today

- 802.11, WLAN
- Cellular Networks
Overview of Wireless Networks

- **Wireless Personal Area Networks (WPANs)**
  - IEEE 802.15.1 (Bluetooth), IrDa, Zigbee, sensor networks, etc.

- **Wireless Local Area Networks (WLANs)**
  - IEEE 802.11, a, b, g, etc. (infrastructure and ad hoc)

- **Wireless Metro Area Networks (WMANs)**
  - IEEE 802.16 WiMAX

- **Wireless Wide Area Networks (WWANs)**
  - GSM, UMTS, EDGE, etc.
WLAN – IEEE 802.11
802.11 Architecture: Infrastructure vs. ad hoc networks

- Infrastructure Network
  - Communication through access point

- Ad Hoc Network
  - Direct communication between nodes
802.11 – Architecture of an infrastructure-based WLAN

- **Station (STA)**
  - Terminal with access mechanisms to the wireless medium
- **Basic Service Set (BSS)**
  - Group of stations using the same frequency
- **Access point**
  - Fixed station communicating with the terminals
- **Portal**
  - Bridge to other (wired) networks
- **Distribution System**
  - Interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS
802.11 – Architecture of an infrastructure-less WLAN

- An ad hoc network is built by an 'Independent basic service set' (IBSS)
  - same frequency
- Stations in different IBSSs cannot communicate with each other
802.11 Protocol Architecture

- 802.11 standard only covers physical layer and MAC layer
- 802.11 fits seamlessly into other 802.x networks (wired LAN)
  - Behaves like a slow wired LAN
802.11 Protocol Architecture (2)

- PMD (Physical Medium Dependent Sublayer)
  - Coding, modulation

- PLCP (Physical Layer Convergence Protocol)
  - Carrier sensing, common PHY interface independent of the actual transmission technology

- MAC: medium access, fragmentation

- PHY Management:
  - channel selection

- MAC Management:
  - Synchronization, power

- Station Management:
  - coordination of all management functions

Remember: advantages of layers
802.11 Protocol Architecture (2)

- PMD (Physical Medium Dependent Sublayer)
  - Coding, modulation

- PLCP (Physical Layer Convergence Protocol)
  - Carrier sensing, common PHY interface independent of the actual transmission technology

- MAC: medium access, fragmentation

- PHY Management:
  - channel selection

- MAC Management:
  - Synchronization, power

- Station Management:
  - coordination of all management functions

Remember: advantages of layers
Physical Layer of different 802.11 Generations

- **802.11a**
  - Up to 54 Mbit/s, standard released 1999, 5GHz band
  - PHY: Orthogonal frequency-division multiplexing (OFDM), Modulation (BPSK, QPSK, 16-QAM)

- **802.11b**
  - 1, 2, 5.5, 11 Mbit/s, standard released 1999, 2.4 GHz band
  - PHY: Direct-sequence spread spectrum (DSSS), Differential QPSK (DQPSK)

- **802.11g**
  - Up to 54 Mbit/s, standard released 2003, 2.4 GHz band
  - OFDM, DBPSK, DSSS

- **802.11n**
  - 54 Mbit/s to 600 Mbit/s (in theory), standard released 2009, 2.4GHz and 5GHz band
  - OFDM, Modulation (BPSK, QPSK, 16-QAM, 64-QAM)

- Different generations have different physical layers, but MAC schemes and management functions are common

- 802.11b, g, n most commonly used today
Orthogonal frequency division multiplexing (OFDM)

- Idea: split the high bit rate stream into many lower bit rate streams, each stream sent using an independent carrier frequency
  - If $n$ symbols have to be transmitted, each subcarrier transmits $n/c$ symbols with $c$ being the number of subcarriers
  - One symbol could, for example, represent 2 bits as in QPSK
- Primary advantage: robustness in the case of narrowband interference and frequency-selective fading due to multipath
802.11 Channels

- 802.11b, g: 14 Channels defined (each 22 MHz wide)
  - Most European countries only allow 13 channels to be used

- 802.11n: Additional 40MHz wide channels in the 5GHz band
- Typically an 802.11 access point chooses one particular channel to operate on
  - All mobile devices connected to the access point have to transmit on the channel of the access point
Multi-rate

- Most 802.11 PHY standards allow support different data rates
  - 802.11b supports 4 rates between 1-11Mbits
  - 802.11g supports 11 rates between 1-54Mbits
- Bit-error rate (BER) depends on channel conditions (e.g. SINR) and data-rate
- Idea: sender chooses data rate dependent on channel conditions for optimal BER

put algorithm
802.11 Preambles

- Two different preamble formats
  - Long: original, 144bits mandatory
  - Short preamble: new, better for short packets and realtime traffic, 72bits, optional

- Different parts of a packet are sent with different data rates

- Problem if stations with short preamble support and stations without short preamble support are mixed up in a BSS
  - Why?
802.11 MAC

- Access methods:
  - Distributed Coordination Function (DCF)
    - mandatory
    - CSMA/CA (carrier sense and backoff algorithm)
  - DCF + RTS/CTS
    - optional
    - Avoids hidden/exposed terminal problem
  - Point coordination function (PCF)
    - optional
    - Access point polls terminals according to a list

- DCF works in infrastructure and ad hoc mode, PCF only in infrastructure mode
Inter-frame intervals (IFS)

Three inter-frame intervals used by stations to access the medium (access priorities)

- SIFS (Short Inter Frame Spacing)
  - Highest priority: waittime used before short control messages (ACKs, polling response) in DCF mode
- PIFS (PCF inter-frame spacing)
  - Medium priority, used in PCF mode
- DIFS: lowest priority, waittime used before data packet in DCF mode
802.11 – CSMA/CA

- Station ready to send starts sensing the medium
- If the medium is free for the duration of DIFS, the station can start sending
- If the medium is busy, the station has to wait for a free DIFS, then the station must additionally wait a random back-off time (multiple of slot-time)
- If another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)
How to detect collision?

- **station\_1**
  - DIFS
  - bo\_e
  - bo\_r

- **station\_2**
  - DIFS
  - bo\_e
  - busy

- **station\_3**
  - busy

- **station\_4**
  - DIFS
  - bo\_e
  - busy
  - bo\_e
  - bo\_r

- **station\_5**
  - DIFS
  - bo\_e
  - bo\_r
  - bo\_e
  - bo\_r

- **t**

**Legend:**
- **busy**: medium not idle (frame, ack etc.)
- **bo\_e**: elapsed backoff time
- **bo\_r**: residual backoff time
- **↓**: packet arrival at MAC
When do packets collide in CSMA/CA?

- If they two stations happen to choose the same backoff timer
  - Like stations 4 and 5
- Hidden terminal
CSMA/CA (2)

- Sending unicast packets
  - A station has to wait for DIFS before sending data
  - Receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly
  - Automatic retransmission of data packets in case of transmission errors (max. number of retransmissions limited)
How Collisions Get Detected in CSMA/CA?

- **CSMA/CA** = Collision Avoidance not Collision Detection
- Unicast packets
  - Detection via missing ACK
- Broadcast packets
  - No mechanism
  - Typically have a much higher loss rate
DCF with RTS/CTS

- After DIFS waittime, stations can send RTS with reservation parameter (specifies the amount of time the data packet needs the medium)
- Receiver sends ACK after SIFS, sender sends data after SIFS
- Other nodes store medium reservations in network allocation vector (NAV), earliest time to access medium again
NAV Vector in PCF Mode

- Access point splits time into super frame periods consisting of contention and contention-free periods.
- Contention period uses CSMA/CA.
- Contention-free period uses polling, PIFS < DIFS.
- Access points communicate superframe time boundaries to stations (t0-t3).
- Stations set their NAV vector accordingly so that they don’t issue DCF packets during contention-free period.
- Start of contention-free period gets shifted to t1 because of ongoing DCF traffic.
- Contention free period ends early (t2) so AP signals CF-end.
Power Management in 802.11

- Stations synchronized: time divided into TIMs and DTIMs
- 'T' packet (every TIM) announces transmission of unicast packet, 'D' packet (every DTIM) announces broadcast packet
- Stations always awake to receive 'T' and 'D'
- Stations stay awake if they are listed as receiver in 'D' or 'T' packet
Cellular Networks
Overview of Wireless Networks

- **Wireless Personal Area Networks (WPANs)**
  - IEEE 802.15.1 (Bluetooth), IrDa, Zigbee, sensor networks, etc.

- **Wireless Local Area Networks (WLANs)**
  - IEEE 802.11, a, b, g, etc. (infrastructure and ad hoc)

- **Wireless Metro Area Networks (WMANs)**
  - IEEE 802.16 WiMAX

- **Wireless Wide Area Networks (WWANs)**
  - GSM, UMTS, EDGE, etc.
The Advent of Cellular Networks

Prior to cellular, mobile radio telephone system was based on:

- High power/transmitter/receivers
- Could support about 25 channels
- In a radius of 80 km

To increase the network capacity

- Multiple low-power transmitters (100W or less)
- Small transmission radius → area split in cells
- Each cell with its own frequencies
- The same frequency can be reused at sufficient distance
The Hexagonal Pattern

- Used as an approximation for a cell
- Each cell features on base station with transmitter, receiver and control unit
- Equidistant access to neighboring cells
  - Center to center distance $d = \sqrt{3}R$
  - Center to corner radius $R$
Frequency re-use

- Adjacent cells are assigned different frequencies to avoid interference or crosstalk
- Objective is to reuse frequency in nearby cells
  - 10 to 50 frequencies assigned to each cell
  - Transmission power controlled to limit power at that frequency escaping to adjacent cells
  - The issue is to determine how many cells must intervene between two cells using the same frequency.
N = # of cells in a repetitious pattern, i.e. *reuse factor*

D = minimum distance between centers of co-channels cells
Frequency reuse characterization

- Reuse factor $N$ follows the pattern
  - $I^2 + J^2 + I \times J, I, J = 0,1,2,3,\ldots$
  - $I = 0, J = 2 \rightarrow N = 4$
  - $I = 1, J = 2 \rightarrow N = 7$

- Reuse ratio $q = D / R = \sqrt{3N}$ (proof in book Vijay Garg)

- Reducing $q \rightarrow$ reducing number of cells per cluster ($N$)
  - If total # of channels per cluster is constant, then channels per cell is increased $\rightarrow$ increasing system capacity
System capacity and interference

- $S$ = Total # of duplex channels available for use
- $K$ = total # of duplex channels per cell
- $S = k\times N$

- If a cluster is replicated $M$ times within a system, the total # of duplex channels $C$ can be used as a measure of capacity
  - $C = MkN = MS$

- Tradeoff:
  - If $N$ decreases $\rightarrow$ $k$ increases (since $S$ is a constant)
  - If $N$ decreases $\rightarrow$ $M$ increases (for a fixed geographical area)
  - $M$ increases $\rightarrow$ system capacity $C$ increases
  - Price: $D/R$ decreases $\rightarrow$ co-channel interference increases
Cell splitting

- Smaller cells have greater system capacity
  - Fine grain channel allocation
  - Better spatial reuse
- As traffic load grows, larger cells could split into smaller cells
- Requires careful power control and possibly more frequent handoffs for mobile stations
Cell Sectoring

- Cell divided into wedge shaped sectors
- 3-6 sectors per cell, each with own channel set
  - Subset of cell's channel per sector
  - Use of directional antennas
  - Decrease co-channel interference
Power Control

Remember:

- Received signal at mobile needs to be sufficiently above background noise (SINR)
- Mobile transmission power minimized to avoid co-channel interference and save battery power
- With CDMA, need to equalize power from all mobiles at the base station
Power Control (2)

Two ways of power control

- **Open-Loop:**
  - No feedback from the BS,
  - BS transmits a pilot signal,
  - Transmitted power by MS inverse proportional to the pilot signal
  - Assumes forward and reverse link signal strength closely related

- **Closed-Loop:**
  - Signal strength from mobile to BS adjusted based on feedback from the BS
  - Signal strength from BS to mobile adjusted based on feedback from MS
  - Feedback: power level, SINR, error rate
Cellular Networks: Generations

- **1G**: Once upon a time there was analog cellular communication
- **2G**: early 80s, GSM, 9.6 kbit/s, 14.4 kbit/s with enhancements
- **2.5G or GPRS**: 140.8 kbit/s in theory, 56 kbit/s in practice
- **2.75G or E-GPRS or EDGE (Enhanced Data Rates for GSM Evolution)**: 180 kbps effective
- **3G**:
  - UMTS using WCDMA (Wideband CDMA) supports 14Mbps in theory. 384 kbps,
  - CDMA-2000: Leading 3G solution in Japan, United States, Canada
- **3.5G**: UMTS is being upgraded to
  - HSPA (7.2 Mbit/s theory)
  - HSPA+ (up to 42 Mbit/s in theory)
- **4G**: Long Term Evolution (LTE), 100 Mbit/s downlink
Cellular Networks: Generations (2)

- **2G Digital**
  - N-CDMA (IS-95, N.A., Korea, Hong Kong, Japan)
  - TDMA (IS-54/136, N.A., GSM, Europe, PDC, Japan)

- **W-CDMA Technology**
  - Wideband CDMA
  - cdma2000
  - TD-CDMA

- **3G Multimedia**
  - HSPA
  - Up to 10 Mbps

- **3G+ Interactivity**
  - Up to 100 Mbps
  - TDD-LTE, FDD-LTE
  - WiMAX, HSPA+

- **4G**
  - IMT-2000
    - Up to 2 Mbps Data Rate
    - Global Roaming
    - High-Quality Multimedia
      - Internet Access
      - Video Conference

Timeline:
- Mid-90s
- 2000
- 2005
- 2010
GSM Architecture

Components:
- MS: Mobile Station
- BTS: Base Transceiver Station
- BSC: Base Station Controller
- MSC & GMSC: Switching Centers
- HLR, VLR: Databases storing user information

Subsystems:
- RSS: Radio Subsystem
- NSS: Network and switching subsystem
- OSS: Operation subsystem
GSM: Radio Interface

- Frequency bands:
  - GSM 900: Uplink 880.0–915.0, Downlink 925,0–960,0
  - GSM 1800: 1710.0–1785.0, 1805.0–1880.0
  - Frequency divisionduplex (FDD) used to separate uplink and downlink

- Channels:
  - GSM 900: 124 channels, each 200kHz wide
  - GSM 1800: 374 channels, 200 kHz wide

- Each BTS manages, e.g., up to 10 channels for user data
  - Space Division Multiple Access (SDMA)

- Each channel is subdivided in continuous TDMA frames of duration 4.615 ms
  - Frame is subdivided into 8 time slots of 577 us
  - Each periodic (occurring every 4.615 ms) slots is called a **physical channel**
  - Time Division Multiple Access (TDMA)
GSM TDMA frame and slots

- Data transmitted in small portions called bursts
  - Interleaved with control information
GSM: Logical Channels

- Physical channels are used to multiplex logical channels on top
  - Logical channel uses every $n^{th}$ physical slot
  - Examples of logical channels
    - Traffic channels (voice, data)
    - Control channels (call setup, synchronization, authentication, etc)
Provider Spectrum Allocation

- GSM 900

- GSM 1800
NSS Databases

- **Home Location Register (HLR)**
  - Contains permanent and semi-dynamic data of all subscribers
    - Mobile subscriber ISDN number
    - International mobile subscriber identity (IMSI)
    - Current VLR and MSC
    - Mobile subscriber roaming number (MSRN)
  - This user-specific information exists once for each user in one HLR

- **Visitor Location Register (VLR)**
  - Local (dynamic) database for a subset of the user data
  - Includes data about all users currently in the domain of the VLR
  - When an MS enters into the area of the VLR, the VLR copies all relevant information from the HLR
    - Avoid frequent HLR updates and long-distance signaling with the HLR
  - VLR gets updated at MS startup and then periodically
    - If no update is received by VLR for some time it's considered detached (e.g., roaming, new VLR takes over)
References

- Robust Rate Adaptation for 802.11 Wireless Networks, Starsky Wong, Hao Yang, Songwu Lu, Vaduvur Bharghavan, Mobicom'06