CS/ECE 438: Communication Networks
Fall 2019

6. Wireless & Mobile Networks
Chapter 6 : Wireless and Mobile Networks

Background:

• # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!

• # wireless Internet-connected devices equals # wireline Internet-connected devices
  • laptops, Internet-enabled phones promise anytime untethered Internet access

• two important (but different) challenges
  • wireless: communication over wireless link
  • mobility: handling the mobile user who changes point of attachment to network
Wireless Networks Increasingly Prevalent

Wireless Homes

Wireless Biomedical Implants

Wireless Wearables

Cellular Networks

Wireless Sensors

UAVs

Wireless Data Centers

Wireless VR

Wireless Vehicles
Increasing Demand for Wireless Connectivity
Increasing Demand for Wireless Connectivity

2020

- 4 BILLION Connected People
- $4 TRILLION Revenue Opportunity
- 25+ MILLION Apps
- 25+ BILLION Embedded and Intelligent Systems
- 50 TRILLION GBs of Data

Source: Mario Morales, IDC

THE INTERNET OF THINGS
An Explosion of connected possibility
Many Motivations for Wireless

• Unrestricted mobility / deployability
  • Unplugged from power outlet

• Significantly lower cost
  • No cable layout, service provision
  • Low maintenance

• Ease
  • Direct communication with minimum infrastructure
No Free Lunch

• Numerous challenges
  • Channel fluctuation
  • Lower bandwidth
  • Limited Battery power
  • Disconnection due to mobility
  • Security
  • ...
Can’t we use the rich “wireline” knowledge? 
In solving the wireless challenges
The Answer

Wireless channel: A dispersive medium
The PHY and MAC layer completely dissimilar

The whole game changes
Chapter 6: Outline

- Introduction
- Wireless Links
- Wireless MAC
- WiFi: 802.11 Wireless LANs
- Cellular Networks: 3G, LTE
- Mobility
Elements of a wireless network
Elements of a wireless network

- **wireless hosts**
  - laptop, smartphone
  - run applications
  - may be stationary (non-mobile) or mobile
    - wireless does *not* always mean mobility

- network infrastructure
Elements of a wireless network

- base station
  - typically connected to wired network
  - relay - responsible for sending packets between wired network and wireless host(s) in its “area”
    - e.g., cell towers, 802.11 access points
Elements of a wireless network

- **network infrastructure**
- **wireless link**
  - typically used to connect mobile(s) to base station
  - also used as backbone link
  - multiple access protocol coordinates link access
  - various data rates, transmission distance
Characteristics of selected wireless links

<table>
<thead>
<tr>
<th>Range</th>
<th>Data rate (Mbps)</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indoor 10-30m</td>
<td>1</td>
<td>802.15</td>
</tr>
<tr>
<td>Outdoor 50-200m</td>
<td>.384</td>
<td>2G: IS-95, CDMA, GSM</td>
</tr>
<tr>
<td>Mid-range outdoor 200m – 4 Km</td>
<td>.056</td>
<td>3G: UMTS/WCDMA-HSPDA, CDMA2000-1xEVDO</td>
</tr>
<tr>
<td>Long-range outdoor 5Km – 20 Km</td>
<td>.056</td>
<td>4G: LTWE WIMAX</td>
</tr>
<tr>
<td></td>
<td>1300</td>
<td>802.11 ac</td>
</tr>
<tr>
<td></td>
<td>450</td>
<td>802.11n</td>
</tr>
<tr>
<td></td>
<td>54</td>
<td>802.11a,g</td>
</tr>
<tr>
<td></td>
<td>5-11</td>
<td>802.11b</td>
</tr>
<tr>
<td></td>
<td></td>
<td>802.11a,g point-to-point</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.5G: UMTS/WCDMA, CDMA2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>802.11b</td>
</tr>
</tbody>
</table>
Elements of a wireless network

- **infrastructure mode**
  - base station connects mobiles into wired network
  - handoff: mobile changes base station providing connection into wired network
Elements of a wireless network

ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves
## Wireless network taxonomy

<table>
<thead>
<tr>
<th>infrastructure (e.g., APs)</th>
<th>single hop</th>
<th>multiple hops</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>infrastructure</strong></td>
<td>host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet</td>
<td>host may have to relay through several wireless nodes to connect to larger Internet: <em>mesh net</em></td>
</tr>
<tr>
<td><strong>no infrastructure</strong></td>
<td>no base station, no connection to larger Internet (Bluetooth, ad hoc nets)</td>
<td>no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET</td>
</tr>
</tbody>
</table>
Chapter 6: Outline

✓ Introduction

❑ Wireless Links

❑ Wireless MAC

❑ WiFi: 802.11 Wireless LANs

❑ Cellular Networks: 3G, LTE

❑ Mobility
Wireless Link Characteristics

*important* differences from wired link ....

- **decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)

\[
P_{Rx} = \frac{G_{Tx} G_{Rx} \lambda^2}{(4\pi d)^2} P_{Tx}
\]

\[
Path Loss (dB) = 10 \log_{10} \frac{P_{Tx}}{P_{Rx}}
\]
Wireless Link Characteristics

important differences from wired link ....

- **decreased signal strength**: radio signal attenuates as it propagates through matter (path loss)

\[ h \propto \frac{\lambda}{d} e^{j2\pi d/\lambda} \]

\[ y(t) = h x(t) + n(t) \]

**Signal – to – Noise Ratio**:

\[ SNR = \frac{|h|^2 \times |x(t)|^2}{|n(t)|^2} = \frac{|h|^2 P_{Tx}}{N} \]
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  • High SNR – easier to extract signal from noise (a “good thing”)
    - Bits: 0 1 0 0
    - Signal: \[ \begin{array}{c}
    \text{Signal} \\
    \text{Noise} \\
    \text{Signal + noise}
    \end{array} \]
    - Low Bit Error Rate
  • Low SNR – hard to extract signal from noise (a “bad thing”)
    - Bits: 0 1 0 0
    - Signal: \[ \begin{array}{c}
    \text{Signal} \\
    \text{Noise} \\
    \text{Signal + noise}
    \end{array} \]
    - High Bit Error Rate

HIGH SNR ➔ Low Bit Error Rate
LOW SNR ➔ High Bit Error Rate
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  • High SNR ➔ Lower Bit Error ➔ Use higher order modulation i.e. pack more bits per symbol

BPSK: 1 bit per symbol

16 QAM: 4 bits per symbol

Bit Rate = Bandwidth × bits/symbol
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  • High SNR ➔ Lower Bit Error ➔ Use higher order modulation
    i.e. pack more bits per symbol

• Some types of modulations:
  • BPSK: Binary Phase Shift Keying
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  • High SNR ➔ Lower Bit Error ➔ Use higher order modulation i.e. pack more bits per symbol

• Some types of modulations:
  • BPSK: Binary Phase Shift Keying
  • QPSK: Phase Shift Keying
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  - High SNR ➔ Lower Bit Error ➔ Use higher order modulation i.e. pack more bits per symbol

• Some types of modulations:
  - BPSK: Binary Phase Shift Keying
  - QPSK: Quadrature Phase Shift Keying
  - QAM: Quadrature Amplitude Modulation
Wireless Link Characteristics

- **SNR**: signal-to-noise ratio
  - High SNR ➔ Lower Bit Error ➔ Use higher order modulation i.e. pack more bits per symbol

- Some types of modulations:
  - BPSK: Binary Phase Shift Keying
  - QPSK: Quadrature Phase Shift Keying
  - QAM: Quadrature Amplitude Modulation
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  • High SNR ➔ Lower Bit Error ➔ Use higher order modulation i.e. pack more bits per symbol

• Some types of modulations:
  • BPSK: Binary Phase Shift Keying
  • QPSK: Quadrature Phase Shift Keying
  • QAM: Quadrature Amplitude Modulation
  • FSK: Frequency Shift Keying
Wireless Link Characteristics

• SNR: signal-to-noise ratio
  • High SNR ➔ Lower Bit Error ➔ Use higher order modulation
    i.e. pack more bits per symbol

• Some types of modulations:
  • BPSK: Binary Phase Shift Keying
  • QPSK: Quadrature Phase Shift Keying
  • QAM: Quadrature Amplitude Modulation
  • FSK: Frequency Shift Keying
  • PAM: Pulse Amplitude Modulation
  • On-OFF Keying
Wireless Link Characteristics

• **SNR versus BER tradeoffs**
  
  - *given physical layer modulation:*
    
    Higher SNR $\rightarrow$ Low BER
  
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, coding) $\rightarrow$ rate adaptation

![Graph showing BER vs SNR for different modulation schemes](image-url)
Wireless Link Characteristics

• Given SNR, what is maximum rate that we can achieve?

  • Shannon Capacity Theorem:

    \[ \text{Capacity} = \text{Bandwidth} \times \log_2(1 + \text{SNR}) \]
Wireless Link Characteristics

important differences from wired link ....

- **interference from other sources**: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well

![Diagram showing multiple wired links with no interference and multiple wireless links with interference](image-url)
Wireless Link Characteristics

*important differences from wired link ....

- *interference from other sources:* standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well

\[
\text{Signal} \ - \ \text{to} \ - \ \text{Interference & Noise Ratio:}
\]

\[
\text{SINR} = \frac{\text{Received Signal Power (PRx)}}{\text{Interference (I) + Noise (N)}}
\]

MAC Protocols necessary to avoid interference!
Wireless Link Characteristics

*important* differences from wired link ....

- **multipath propagation:** radio signal reflects off objects ground, arriving at destination at slightly different times

\[ y(t) = h_1 x(t - \tau_1) + h_2 x(t - \tau_2) + h_3 x(t - \tau_3) \]
important differences from wired link ....

- **multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times

\[ y(t) = \sum_{k} h_k x(t - \tau_k) = h(t) \ast x(t) \]
Wireless Link Characteristics

*important* differences from wired link ....

- **multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times

\[ y(t) = \sum_{k} h_{k} x(t - \tau_{k}) = h(t) * x(t) \]

First Path

Second Path

nth Path

Multi-tap Channel

Symbols arriving along late paths interfere with following symbols.

ISI: Inter-Symbol-Interference

Paths sum with different phases: Constructive/Destructive
Wireless Link Characteristics

**Frequency Selective Fading:**

*Example 2 paths with distance* $d_1 = 1m$, $d_2 = 1.06m$:

$$ h = h_1 + h_2 = \frac{\lambda}{d_1} \ e^{j2\pi d_1/\lambda} + \frac{\lambda}{d_2} \ e^{j2\pi d_2/\lambda} $$

@ $f_1 = 2.5GHz$ ($\lambda = 12 \ cm$):

$$ h = 0.12 \ e^{j\frac{2\pi}{3}} + 0.113 \ e^{j\frac{5\pi}{3}} \approx 0.006 $$

@ $f_2 = 5GHz$ ($\lambda = 6 \ cm$):

$$ h = 0.06 \ e^{j\frac{5\pi}{3}} + 0.05 \ e^{j\frac{5\pi}{3}} \approx 0.116 $$

17 $\times$ ➔ 24dB
**Wireless Link Characteristics**

*important* differences from wired link ....

- **multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times

\[
y(t) = \sum_{k} h_k x(t - \tau_k) = h(t) * x(t) \iff H(f)X(f)
\]

![Graph](Image)

Fading
Wireless Link Characteristics

*important* differences from wired link ....

- **multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times
  - Inter-Symbol-Interference
  - Frequency Selective Fading
Wireless Link Characteristics

important differences from wired link ....

- **multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times

- Solution:
  **OFDM: Orthogonal Frequency Division Multiplexing**

- Idea: transmit symbols in frequency not time.
Orthogonal Frequency Division Multiplexing
Channel Estimation and Correction

\[ h \propto \frac{\lambda}{d} e^{j2\pi d/\lambda} \]

\[ y(t) = h x(t) + n(t) \]

How to estimate and correct for channel?

Send Preamble Bits
Channel Estimation and Correction

\[ h \propto \frac{\lambda}{d} e^{j2\pi d/\lambda} \]

\[ y(t) = h \cdot x(t) + n(t) \]

Preamble Bits: Known bits

\[ x(0) = 1 \quad \Rightarrow \quad y(0) = h + n(0) \]
\[ x(1) = 1 \quad \Rightarrow \quad y(1) = h + n(1) \]
\[ x(2) = -1 \quad \Rightarrow \quad y(2) = -h + n(2) \]

Estimate channel: \( \hat{h} = \sum_k \frac{y(k)}{x(k)} \)

Correct channel: \( \tilde{x}(t) = \frac{y(t)}{\hat{h}} \)
Channel Estimation and Correction

\[ y(t) = h(t) \ast x(t) + n(t) \]

What about multi-tap channel?

OFDM: Send bits in frequency domain

\[ h(t) \ast x(t) \iff H(f)X(f) \]

Channel estimation and correction can be done in frequency domain.

\[ \tilde{H}(f) = \frac{Y(f)}{X(f)} \]
Spread Spectrum

• Problem of radio transmission: frequency dependent fading can wipe out narrow band signals for duration of the interference

• Solution: spread the narrow band signal into a broad band signal using a special code
DSSS (Direct Sequence Spread Spectrum)

• XOR the signal with pseudonoise (PN) sequence (chipping sequence)

• Advantages
  • reduces frequency selective fading
  • Robust to interference
  • Multi-user

• Used in 3G & 802.11b
FHSS (Frequency Hopping Spread Spectrum)

- Discrete changes of carrier frequency
  - sequence of frequency changes determined via PN sequence

- Advantages
  - frequency selective fading and interference limited to short period
  - uses only small portion of spectrum at any time
  - Secure

- Used in bluetooth & military applications
Wireless Link Characteristics

*important* differences from wired link ....

- **decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources:** standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- **multipath propagation:** radio signal reflects off objects ground, arriving ad destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):

Hidden terminal problem

- B, A hear each other
- B, C hear each other
- A, C can not hear each other means A, C unaware of their interference at B

Signal attenuation:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B
Wireless network characteristics

Advantage of signal attenuation: Spatial Reuse

A’s signal strength

C’s signal strength

space
Wireless network characteristics

Problem: A wants to transmit a packet to C

Option 1: A increases its power such that its packet reaches C

Option 2: A sends that packet to B which intern send it to C
Problem: A wants to transmit a packet to C

Option 1: A increases its power such that its packet reaches C

Option 2: A sends that packet to B which intern send it to C

To double transmission range, we need: 4x more overall power!

To transmit over two hops, we need: 2x more overall power!
Wireless network characteristics

Multi-hop wireless networks:

- Increase TX power: increase transmission range by $N$ times, need $N^2 \times$ more power
- Multi-hop links: increase transmission range by $N$ times, need $N \times$ more power

Ad hoc multi-hop wireless networks!
Chapter 6: Outline

✓ Introduction

✓ Wireless Links

❑ Wireless MAC

❑ WiFi: 802.11 Wireless LANs

❑ Cellular Networks: 3G, LTE

❑ Mobility
The Channel Access Problem

- Multiple nodes share a channel
- Pairwise communication desired
  - Simultaneous communication not possible
- MAC Protocols
  - Suggests a scheme to schedule communication
    - Maximize number of communications
    - Ensure fairness among all transmitters
The Trivial Solution

- Transmit and pray
  - Plenty of collisions → poor throughput at high load
The Simple Fix

• Transmit and pray
  • Plenty of collisions $\rightarrow$ poor throughput at high load

• Listen before you talk
  • Carrier sense multiple access (CSMA)
  • Defer transmission when signal on channel

Can collisions still occur?
CSMA collisions

Collisions can still occur:
Propagation delay non-zero between transmitters

When collision:
Entire packet transmission time wasted

note:
Role of distance & propagation delay in determining collision probability
CSMA/CD (Collision Detection)

- Keep listening to channel
  - While transmitting

- If (Transmitted_Signal != Sensed_Signal)
  -> Sender knows it’s a Collision
  -> ABORT
2 Observations on CSMA/CD

• Transmitter can send/listen concurrently
  • If (Sensed - received = null)? Then success

• The signal is identical at Tx and Rx
  • Non-dispersive

The transmitter can DETECT if and when collision occurs
Unfortunately ...

Both observations do not hold for wireless

Leading to ...
Wireless Medium Access Control

Signal power

SINR threshold

Distance
Wireless Media Disperse Energy

A cannot send and listen in parallel

Signal not same at different locations
Collision Detection Difficult

- Signal reception based on SINR
  - Transmitter can only hear itself
  - Cannot determine signal quality at receiver
Red signal >> Blue signal

Red < Blue = collision

X
A
B
C
D

Signal power

SINR threshold

Distance
Important: C has not heard A, but can interfere at receiver B

C is the hidden terminal to A
Important: X has heard A, but should not defer transmission to Y

X is the exposed terminal to A

X

Signal power

SINR threshold

Distance

Y

C

D
Hidden and Exposed Terminal Problems

Critical to wireless networks even today
IEEE 802.11

RTS = Request To Send

CTS = Clear To Send
IEEE 802.11

Data

ACK

silenced

silenced

silenced

silenced

silenced
But is that enough?
RTS/CTS

• Does it solve hidden terminals?
  • Assuming carrier sensing zone = communication zone

E does not receive CTS successfully → Can later initiate transmission to D. Hidden terminal problem remains.
Hidden Terminal Problem

• How about increasing carrier sense range ??
  • E will defer on sensing carrier → no collision !!!
Hidden Terminal Problem

• But what if barriers/obstructions ??
  • E doesn’t hear C → Carrier sensing does not help
Exposed Terminal

• B should be able to transmit to A
  • RTS prevents this
Exposed Terminal

• B should be able to transmit to A
  • Carrier sensing makes the situation worse
Multiplexing

- Multiplexing in 4 dimensions
  - space ($s_i$)
  - time ($t$)
  - frequency ($f$)
  - code ($c$)
Frequency multiplex

• Separation of spectrum into smaller frequency bands
• Channel gets band of the spectrum for the whole time
• Advantages:
  • no dynamic coordination needed
  • works also for analog signals
• Disadvantages:
  • waste of bandwidth if traffic distributed unevenly
  • inflexible
  • guard spaces
Time multiplex

- Channel gets the whole spectrum for a certain amount of time
  - Advantages:
    - only one carrier in the medium at any time
    - throughput high even for many users
  - Disadvantages:
    - precise synchronization necessary
Time and frequency multiplex

• A channel gets a certain frequency band for a certain amount of time (e.g. GSM)

• Advantages:
  • better protection against tapping
  • protection against frequency selective interference
  • higher data rates compared to code multiplex

• Precise coordination required
Code multiplex

- Each channel has unique code
- All channels use same spectrum at same time
- Advantages:
  - bandwidth efficient
  - no coordination and synchronization
  - good protection against interference
- Disadvantages:
  - lower user data rates
  - more complex signal regeneration
- Implemented using spread spectrum technology
Code Division Multiple Access (CDMA)

• unique “code” assigned to each user; i.e., code set partitioning
  • all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
  • allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)

• encoded signal = (original data) X (chipping sequence)
• decoding: inner-product of encoded signal and chipping sequence
• Example codes: Gold Codes, Walsh Codes
CDMA encode/decode

sender

data bits
\[ d_1 = -1 \]
\[ d_0 = 1 \]

channel output \( Z_{i,m} = d_i \cdot c_m \)

code
\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
\end{array}
\]

slot 1

receiver

received input

code
\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
\end{array}
\]

slot 1

channel output

channel output

\[ D_i = \sum_{m=1}^{M} Z_{i,m} \cdot c_m \]

\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
\end{array}
\]

slot 1

channel output

channel output

\[
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
\end{array}
\]

slot 0

channel output

channel output

\[ d_1 = -1 \]
\[ d_0 = 1 \]
CDMA: two-sender interference

**Senders**

**Sender 1**
- Data bits: \(d_1 = -1\)
- Code: \([-1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1]\)

**Sender 2**
- Data bits: \(d_2^1 = 1, d_2^2 = -1\)
- Code: \([-1, 1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1]\)

**Channel**
- Channel sum: \(Z_{i,m}^1 = d_i^1 c_m^1\)
- Channel sum: \(Z_{i,m}^2 = d_i^2 c_m^2\)

**Receiver 1**
- Using same code as sender 1, receiver recovers sender 1’s original data from summed channel data!

Channel sums together transmissions by sender 1 and 2.
Code Division Multiple Access (CDMA)

• Ideally, need codes to have good:
  Auto-correlation properties: $c_i(t) \cdot c_i(t) = 1$
  Cross-correlation properties: $c_i(t) \cdot c_j(t) = 0$ for $j \neq i$

\[
\left( \sum_i h_i d_i(t) c_i(t) \right) \cdot c_i(t) = h_i d_i(t)
\]

• Need orthogonal codes:
  For $N$ users, length of code is exponential in $N \rightarrow 2^{N-1}$

• Near Far Effect Problem $\rightarrow$ need power management
Chapter 6: Outline

✓ Introduction

✓ Wireless Links

✓ Wireless MAC

❑ WiFi: 802.11 Wireless LANs

❑ Cellular Networks: 3G, LTE

❑ Mobility
IEEE 802.11 Wireless LAN

802.11b
• 2.4-5 GHz unlicensed spectrum
• up to 11 Mbps
• direct sequence spread spectrum (DSSS) in physical layer
  • all hosts use same chipping code

802.11a
• 5-6 GHz range
• up to 54 Mbps

802.11g
• 2.4-5 GHz range
• up to 54 Mbps

802.11n: multiple antenna
• 2.4-5 GHz range
• up to 200 Mbps

802.11ad/ay: Millimeter wave
• 2.4, 5, 60 GHz range
• Up to 7 Gbps

802.11ac: multiple antenna
• 2.4-5 GHz range
• Up to 1.69 Gbps
802.11 LAN architecture

- Wireless host communicates with base station
  - Base station = access point (AP)

- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - Wireless hosts
  - Access point (AP): base station
  - Ad hoc mode: hosts only
802.11: Channels, association

• 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  • AP admin chooses frequency for AP
  • interference possible: channel can be same as that chosen by neighboring AP!

• host: must *associate* with an AP
  • scans channels, listening for *beacon frames* containing AP’s name (SSID) and MAC address
  • selects AP to associate with
  • may perform authentication
  • will typically run DHCP to get IP address in AP’s subnet
**802.11: passive/active scanning**

**passive scanning:**
1. beacon frames sent from APs
2. association Request frame sent: H1 to selected AP
3. association Response frame sent from selected AP to H1

**active scanning:**
1. Probe Request frame broadcast from H1
2. Probe Response frames sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent from selected AP to H1
IEEE 802.11: multiple access

- avoid collisions: $2^+ \text{ nodes transmitting at same time}$
- 802.11: CSMA - sense before transmitting
  - don’t collide with ongoing transmission by other node
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can’t sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions*: CSMA/C(ollision)A(voidance)
IEEE 802.11 MAC Protocol: CSMA/CA

**802.11 sender**

1. if sense channel idle for **DIFS** then  
   transmit entire frame (no CD)

2. if sense channel busy then  
   start random backoff time  
   timer counts down while channel idle  
   transmit when timer expires  
   if no ACK, increase random backoff interval,  
   repeat 2

**802.11 receiver**

- if frame received OK  
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)
Avoiding collisions (more)

**idea:** allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

*avoid data frame collisions completely using small reservation packets!*
Collision Avoidance: RTS-CTS exchange

- RTS(A) reservation collision
- RTS(B) defer
- CTS(A) defer
- DATA (A) defer
- ACK(A) defer
# 802.11 frame: addressing

<table>
<thead>
<tr>
<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</td>
<td>address 1</td>
<td>address 2</td>
<td>address 3</td>
<td>seq control</td>
<td>address 4</td>
<td>payload</td>
<td>CRC</td>
</tr>
</tbody>
</table>

- **Address 1**: MAC address of wireless host or AP to receive this frame
- **Address 2**: MAC address of wireless host or AP transmitting this frame
- **Address 3**: MAC address of router interface to which AP is attached
- **Address 4**: used only in ad hoc mode
### 802.11 Frame: More

**Diagram: 802.11 Frame Structure**

- **Frame Control**: 2 bytes, contains frame type, subtypes, and more fields.
- **Duration**: 2 bytes, indicates the duration of reserved transmission time (RTS/CTS).
- **Address**: 6 bytes, for source and destination addresses.
- **Sequence Control**: 2 bytes, includes seq control and address 4.
- **Payload**: Variable length, contains data payload.
- **CRC**: 4 bytes, cyclic redundancy check.

**Frame Type**
- **RTS, CTS, ACK, Data**

<table>
<thead>
<tr>
<th>Field</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol version</td>
<td>2</td>
</tr>
<tr>
<td>Type</td>
<td>2</td>
</tr>
<tr>
<td>Subtype</td>
<td>4</td>
</tr>
<tr>
<td>To AP</td>
<td>1</td>
</tr>
<tr>
<td>From AP</td>
<td>1</td>
</tr>
<tr>
<td>More frag</td>
<td>1</td>
</tr>
<tr>
<td>Retry</td>
<td>1</td>
</tr>
<tr>
<td>Power mgt</td>
<td>1</td>
</tr>
<tr>
<td>More data</td>
<td>1</td>
</tr>
<tr>
<td>WEP</td>
<td>1</td>
</tr>
<tr>
<td>Rsvd</td>
<td>1</td>
</tr>
</tbody>
</table>
802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1
Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER
Chapter 6: Outline

✓ Introduction
✓ Wireless Links
✓ Wireless MAC
✓ WiFi: 802.11 Wireless LANs
❑ Cellular Networks: 3G, LTE
❑ Mobility
Components of cellular network architecture

**Cell**
- Covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface*: physical and link layer protocol between mobile and BS

**MSC**
- Connects cells to wired tel. net.
- Manages call setup (more later!)
- Handles mobility (more later!)

Diagram:
- Mobile Switching Center (MSC)
- Public telephone network
- Wired network
- Hexagonal cells with mobile users and base stations

Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

- **combined FDMA/TDMA**: divide spectrum in frequency channels, divide each channel into time slots
- **CDMA**: code division multiple access
2G (voice) network architecture

Base station system (BSS)

BTS

BSC

MSC

Gateway

Public telephone network

Legend

Base transceiver station (BTS)

Base station controller (BSC)

Mobile Switching Center (MSC)

Mobile subscribers
Key insight: new cellular data network operates in parallel (except at edge) with existing cellular voice network

- voice network unchanged in core
- data network operates in parallel
3G (voice+data) network architecture

radio network controller

radio interface
(WCDMA, HSPA)

radio access network
Universal Terrestrial Radio Access Network (UTRAN)

core network
General Packet Radio Service (GPRS) Core Network

public Internet

Public telephone network

MSC

Gateway MSC

SGSN

GGSN

Public Internet
3G versus 4G LTE network architecture

3G

- Universal Terrestrial Radio Access Network (UTRAN)
- Radio network controller
- MSC
- SGSN
- GGSN
- Gateway MSC

4G-LTE

- Evolved Packet Core (EPC)
- HSS
- MME
- G
- S-GW
- P-GW

Public telephone network

Public Internet
4G: differences from 3G

- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- no separation between voice and data – all traffic carried over IP core to gateway
Mobile Technologies from 1G – 5G

- **1G**
  - Year: Early 1980s
  - Standards: AMPS, TACS
  - Technology: Analog
  - Bandwidth: Narrow Band
  - Data rates: < 80–100 Kbps

- **2G**
  - Year: 1991
  - Standards: GSM, GPRS, EDGE
  - Technology: Digital
  - Bandwidth: Narrow Band
  - Data rates: < 80–100 Kbps

- **3G**
  - Year: 2001
  - Standards: UMTS / HSPA
  - Technology: Digital
  - Bandwidth: Broad Band
  - Data rates: up to 2 Mbps

- **4G**
  - Year: 2010
  - Standards: LTE, LTE Advanced
  - Technology: Digital
  - Bandwidth: Mobile Broad Band
  - Data rates: 4G-like experience
  - 1 hr HD movie in 6 minutes

- **5G**
  - Year: 2020-2030
  - Technology: Digital
  - Bandwidth: Ubiquitous connectivity
  - Data rates: Fiber-like experience
  - 1 hr HD movie in 6 seconds

5G is about Communication, Storage, Processing...
5G: Unified Air Interface

- **Enhanced Mobile Broadband (eMBB)**
  - 100+ Mbps avg. throughput
  - 10+ Gbps peak throughput

- **Massive Machine Type Communications (mMTC)**
  - $10^6$/km$^2$ connection density
  - Low cost/energy connectivity

- **Ultra-Reliable, Low-Latency Communications (uMTC)**
  - 99.999% service availability
  - 1 – 10 ms latency

- **Applications**
  - Mobile video and gaming
  - Cloud computing and storage
  - High speed connectivity
  - Billions of connected devices
  - Sensor networks
  - IoT / M2M / D2D
  - Tactile Internet
  - Natural disaster relief
  - E-Medicine and Health care
Chapter 6: Outline

✓ Introduction
✓ Wireless Links
✓ Wireless MAC
✓ WiFi: 802.11 Wireless LANs
✓ Cellular Networks: 3G, LTE
❑ Mobility
What is mobility?

- spectrum of mobility, from the *network* perspective:
  
  - no mobility
  - mobile wireless user, using same access point
  - mobile user, connecting/disconnecting from network using DHCP.
  - mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)
  - high mobility
**Mobility: vocabulary**

**home network**: permanent “home” of mobile (e.g., 128.119.40/24)

**home agent**: entity that will perform mobility functions on behalf of mobile, when mobile is remote

**permanent address**: address in home network, *can always* be used to reach mobile (e.g., 128.119.40.186)
Mobility: more vocabulary

- **permanent address**: remains constant (e.g., 128.119.40.186)
- **visited network**: network in which mobile currently resides (e.g., 79.129.13/24)
- **care-of-address**: address in visited network. (e.g., 79,129.13.2)
- **foreign agent**: entity in visited network that performs mobility functions on behalf of mobile.
- **correspondent**: wants to communicate with mobile

Wide area network
Mobility: approaches

- **let routing handle it:** routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end-systems
- **let end-systems handle it:**
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile
Mobility: approaches

- *let routing handle it*: routers advertise permanent address of mobiles in their residence via usual routing table exchange.
  - routing tables indicate where each mobile located
  - no changes to end systems
- *let end-systems handle it*:
  - *indirect routing*: communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing*: correspondent gets foreign address of mobile, sends directly to mobile

*not scalable to millions of mobiles*
Mobility: registration

end result:

• foreign agent knows about mobile
• home agent knows location of mobile
Mobility via indirect routing

1. Correspondent addresses packets using the home address of the mobile.
2. Home agent intercepts the packets and forwards them to the foreign agent.
3. Foreign agent receives the packets, forwards them to the mobile.
4. Mobile replies directly to the correspondent.
Indirect Routing: comments

- mobile uses two addresses:
  - **permanent address**: used by correspondent (hence mobile location is *transparent* to correspondent)
  - **care-of-address**: used by home agent to forward datagrams to mobile

- foreign agent functions may be done by mobile itself

- **triangle routing**: correspondent-home-network-mobile
  - inefficient when correspondent, mobile are in same network
Mobility via direct routing

1. Correspondent requests, receives foreign address of mobile.
2. Correspondent forwards to foreign agent.
3. Foreign agent receives packets, forwards to mobile.
4. Mobile replies directly to correspondent.
Components of cellular network architecture

recall:

wired public telephone network

different cellular networks, operated by different providers
GSM: indirect routing to mobile

1. Call routed to home network
2. Home MSC consults HLR, gets roaming number of mobile in visited network
3. Home MSC sets up 2nd leg of call to MSC in visited network
4. MSC in visited network completes call through base station to mobile

- HLR (Home Location Register)
- VLR (Visitor Location Register)
- Mobile Switching Center (MSC)
- Home network
- Visited network
- Correspondent
- Public switched telephone network
GSM: handoff with common MSC

- **handoff goal**: route call via new base station (without interruption)

- reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesn't mandate why to perform handoff (policy), only how (mechanism)

- handoff initiated by old BSS
GSM: handoff with common MSC

1. old BSS informs MSC of impending handoff, provides list of 1+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call
8. MSC-old-BSS resources released
Chapter 6: Outline

✓ Introduction
✓ Wireless Links
✓ Wireless MAC
✓ WiFi: 802.11 Wireless LANs
✓ Cellular Networks: 3G, LTE
✓ Mobility
Wireless, mobility: impact on higher layer protocols

• logically, impact *should* be minimal ...
  • best effort service model remains unchanged
  • TCP and UDP can (and do) run over wireless, mobile

• ... but performance-wise:
  • packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  • TCP interprets loss as congestion, will decrease congestion window un-necessarily
  • delay impairments for real-time traffic
  • limited bandwidth of wireless links