Ch. 6: Wireless and Mobile Networks

Background:
- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers!
- # wireless Internet-connected devices soon to exceed # 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

Chapter 6 outline

6.1 Introduction

Wireless
6.2 Wireless links, characteristics
  - CDMA
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)
6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
6.5 Principles: addressing and routing to mobile users
6.6 Mobile IP
6.7 Handling mobility in cellular networks
6.8 Mobility and higher-layer protocols
6.9 Summary
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**

Wireless, Mobile Networks 6-3
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

- **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>Data rate (Mbps)</th>
<th>Indoor 10-30m</th>
<th>Outdoor 50-200m</th>
<th>Mid-range outdoor 200m – 4 Km</th>
<th>Long-range outdoor 5Km – 20 Km</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11n</td>
<td>54</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11a,g</td>
<td>5-11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11b</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.15</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11a,g point-to-point</td>
<td>0.56</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4G: LTE WIMAX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3G: UMTS/WCDMA-HSPDA, CDMA2000-1xEVDO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5G: UMTS/WCDMA, CDMA2000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2G: IS-95, CDMA, GSM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11n point-to-point</td>
<td></td>
<td></td>
<td></td>
<td></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>no infrastructure</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></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

6.1 Introduction

Wireless
6.2 Wireless links, characteristics
  - CDMA
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)
6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
6.5 Principles: addressing and routing to mobile users
6.6 Mobile IP
6.7 Handling mobility in cellular networks
6.8 Mobility and higher-layer protocols
6.9 Summary

Wireless Link Characteristics (1)

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 at destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”
Wireless Link Characteristics (2)

- **SNR**: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a “good thing”)
- **SNR versus BER tradeoffs**
  - *given physical layer*: increase power -> increase SNR -> decrease BER
  - *given SNR*: choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

![SNR versus BER tradeoffs graph](image)

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
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) \times (chipping sequence)
- decoding: inner-product of encoded signal and chipping sequence
**Chapter 6 outline**

6.1 Introduction

**Wireless**

6.2 Wireless links, characteristics
   - CDMA

6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

6.4 Cellular Internet Access
   - architecture
   - standards (e.g., GSM)

**Mobility**

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

6.8 Mobility and higher-layer protocols

6.9 Summary
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 antennae
- 2.4-5 GHz range
- up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

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 [Chapter 8]
  - 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: $2^+$ 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

---

**Collision Avoidance: RTS-CTS exchange**

- RTS(A)
- RTS(B)
- RTS(A)
- RTS(A)
- RTS(A)
- RTS(A)
- CTS(A)
- CTS(A)
- DATA (A)
- ACK(A)
- ACK(A)

*avoid data frame collisions completely using small reservation packets!*

---

*Wireless, Mobile Networks 6-25*

*Wireless, Mobile Networks 6-26*
802.11 frame: addressing

<table>
<thead>
<tr>
<th>frame control</th>
<th>duration</th>
<th>address 1</th>
<th>address 2</th>
<th>address 3</th>
<th>seq control</th>
<th>address 4</th>
<th>payload</th>
<th>CRC</th>
</tr>
</thead>
</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

Wireless, Mobile Networks 6-27
**802.11 frame: more**

![Diagram of 802.11 frame structure]

- **frame duration of reserved transmission time (RTS/CTS)**
- **frame seq # (for RDT)**

<table>
<thead>
<tr>
<th>Protocol version</th>
<th>Type</th>
<th>Subtype</th>
<th>To AP</th>
<th>From AP</th>
<th>More frag</th>
<th>Retry</th>
<th>Power mgt</th>
<th>More data</th>
<th>WEP</th>
<th>Rsvd</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**frame type**
- (RTS, CTS, ACK, data)

---

**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

![Diagram of mobility within same subnet]

Wireless, Mobile Networks 6-29
802.11: advanced capabilities

Rate adaptation

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

![Graph showing BER vs SNR](image)

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

Power management

- node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame

- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame
802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps

Chapter 6 outline

6.1 Introduction
6.2 Wireless links, characteristics
  - CDMA
6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)
6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
6.5 Principles: addressing and routing to mobile users
6.6 Mobile IP
6.7 Handling mobility in cellular networks
6.8 Mobility and higher-layer protocols

6.9 Summary
Components of cellular network architecture

- MSC
  - connects cells to wired tel. net.
  - manages call setup (more later!)
  - handles mobility (more later!)

- 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

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

Wireless, Mobile Networks 6-35
2G (voice) network architecture

- Base station system (BSS)
- BTS
- BSC
- MSC
- Gateway MSC
- Public telephone network

Legend:
- Base transceiver station (BTS)
- Base station controller (BSC)
- Mobile Switching Center (MSC)
- Mobile subscribers

3G (voice+data) network architecture

- MSC
- Gateway MSC
- SGSN
- GGSN
- Public telephone network
- Public Internet

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

Legend:
- Serving GPRS Support Node (SGSN)
- Gateway GPRS Support Node (GGSN)
3G (voice+data) network architecture

Chapter 6 outline

6.1 Introduction

Wireless

6.2 Wireless links, characteristics
  - CDMA

6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

6.8 Mobility and higher-layer protocols

6.9 Summary
**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)

**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

Wireless, Mobile Networks 6-41

Wireless, Mobile Networks 6-42
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**

How do you contact a mobile friend?

Consider friend frequently changing addresses, how do you find her?

- search all phone books?
- call her parents?
- expect her to let you know where he/she is?

I wonder where Alice moved to?
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

Wireless, Mobile Networks 6-45
**Mobility: registration**

**end result:**
- foreign agent knows about mobile
- home agent knows location of mobile

**Mobility via indirect routing**

**end result:**
- foreign agent intercepts packets, forwards to foreign agent
- foreign agent receives packets, forwards to mobile
- mobile replies directly to correspondent

Wireless, Mobile Networks 6-47
Indirect Routing: comments

- mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is \textit{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

Indirect routing: moving between networks

- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: \textit{ongoing connections can be maintained!}
Mobility via direct routing

1. Correspondent forwards to foreign agent
2. Foreign agent receives packets, forwards to mobile
3. Mobile replies directly to correspondent

- Overcome triangle routing problem
- Non-transparent to correspondent: Correspondent must get care-of-address from home agent
  - What if mobile changes visited network?
Accommodating mobility with direct routing

- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)

Chapter 6 outline

6.1 Introduction

Wireless
- 6.2 Wireless links, characteristics
  - CDMA
- 6.3 IEEE 802.11 wireless LANs (“Wi-Fi”)
- 6.4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 6.5 Principles: addressing and routing to mobile users
- 6.6 Mobile IP
- 6.7 Handling mobility in cellular networks
- 6.8 Mobility and higher-layer protocols

6.9 Summary
**Mobile IP**

- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

---

**Mobile IP: indirect routing**

- Permanent address: 128.119.40.186
- Care-of address: 79.129.13.2
- Packet sent by correspondent:
  - Dest: 79.129.13.2
  - Dest: 128.119.40.186
- Packet sent by home agent to foreign agent:
  - Dest: 128.119.40.186
  - A packet within a packet
- Foreign-agent-to-mobile packet:
  - Dest: 128.119.40.186
**Mobile IP: agent discovery**

- *agent advertisement*: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)

  - H,F bits: home and/or foreign agent
  - R bit: registration required

  ![Diagram of agent advertisement](image)

  - Type 9
  - Code 0
  - Checksum
  - Router address
  - H,F bits: home and/or foreign agent
  - R bit: registration required
  - Length
  - Sequence #
  - Registration lifetime
  - RBHFMGV
  - Reserved

  ![Diagram of registration example](image)

  - Foreign agent CDA: 79.129.13.2
  - HA: 128.119.40.7
  - MA: 128.119.40.186
  - Lifetime: 9999
  - Identification: 714
  - Encapsulation format
  - Registration req.
  - Registration reply
  - HA: 128.119.40.7
  - MA: 128.119.40.186
  - Lifetime: 4999
  - Identification: 714
  - Encapsulation format
  - Registration req.
  - Registration reply

  - Mobile agent MA: 128.119.40.186
  - CDA: 79.129.13.2
  - HA: 128.119.40.7
  - MA: 128.119.40.186
  - Lifetime: 9999
  - Identification: 714
  - Encapsulation format
  - Registration adv.
  - Registration req.
  - Registration reply

  - Visited network: 79.129.13/24
Components of cellular network architecture

recall:

Handling mobility in cellular networks

- **home network**: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - **home location register (HLR)**: database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- **visited network**: network in which mobile currently resides
  - **visitor location register (VLR)**: database with entry for each user currently in network
  - could be home network
**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.

**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.
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.

**GSM: handoff between MSCs**

- **Anchor MSC**: first MSC visited during call.
  - Call remains routed through anchor MSC.
- New MSCs add on to end of MSC chain as mobile moves to new MSC.
- Optional path minimization step to shorten multi-MSC chain.
### GSM: handoff between MSCs

- **anchor MSC**: first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end ofMSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

### Mobility: GSM versus Mobile IP

<table>
<thead>
<tr>
<th>GSM element</th>
<th>Comment on GSM element</th>
<th>Mobile IP element</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home system</strong></td>
<td>Network to which mobile user’s permanent phone number belongs</td>
<td><strong>Home network</strong></td>
</tr>
<tr>
<td>Gateway Mobile Switching Center, or “home MSC”. Home Location Register (HLR)</td>
<td>Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information</td>
<td><strong>Home agent</strong></td>
</tr>
<tr>
<td>Visited System</td>
<td>Network other than home system where mobile user is currently residing</td>
<td><strong>Visited network</strong></td>
</tr>
<tr>
<td>Visited Mobile services Switching Center. Visitor Location Record (VLR)</td>
<td>Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user</td>
<td><strong>Foreign agent</strong></td>
</tr>
<tr>
<td>Mobile Station Roaming Number (MSRN), or “roaming number”</td>
<td>Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.</td>
<td><strong>Care-of-address</strong></td>
</tr>
</tbody>
</table>

Wireless, Mobile Networks 6-65
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

Chapter 6 summary

**Wireless**
- wireless links:
  - capacity, distance
  - channel impairments
  - CDMA
- IEEE 802.11 ("Wi-Fi")
  - CSMA/CA reflects wireless channel characteristics
- cellular access
  - architecture
  - standards (e.g., GSM, 3G, 4G LTE)

**Mobility**
- principles: addressing, routing to mobile users
  - home, visited networks
  - direct, indirect routing
  - care-of-addresses
- case studies
  - mobile IP
  - mobility in GSM
- impact on higher-layer protocols