Chapter 6
Wireless and Mobile Networks

Chapter 6: Wireless and Mobile Networks

Background:
- # wireless (mobile) phone subscribers now exceed # wired phone subscribers!
- computer nets: laptops, palmops, PDAs, Internet-enabled phone 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

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, PDA, IP phone
  - run applications
  - may be stationary (non-mobile) or mobile
  - wireless does not always mean mobility

- network infrastructure
  - 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 Characteristics (1)**

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 strength**

- **Signal attenuation:**
  - B, A hear each other
  - B, C hear each other
  - A, C cannot hear each other

**Code Division Multiple Access (CDMA)**

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- 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
- encoded signal = (original data) X (chipping sequence)
- decoding: inner product of encoded signal and chipping sequence
- allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

**CDMA Encode/Decode**

- **Channel output Z<sub>m</sub>**
  - sender
  - channel output Z<sub>m</sub> = d<sub>i</sub>c<sub>m</sub>
  - i = 0, 1

**CDMA: two-sender interference**

- **channel output Z<sub>i</sub>**
- **channel output Z<sub>i'</sub>**

**Chapter 6 outline**

6.1 Introduction

- 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

6.2 Wireless links, characteristics

- 6.3 IEEE 802.11 wireless LANs ("wi-fi")
- 6.4 Cellular Internet access
  - architecture
  - standards (e.g., GSM)

6.3 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
  - 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
- wireless hosts
- access point (AP): base station
- ad hoc mode: hosts only

IEEE 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 AP
- scan channels, listening for beacon frames containing APs name (SSID) and MAC address
- select 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: H1 to selected AP

Active Scanning:
(1) Probe Request frame broadcast from H1
(2) Probes response frame sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent: H1 to selected AP

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

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

802.11 frame: addressing

802.11 frame: more

802.11: mobility within same subnet

802.11: advanced capabilities
802.11: advanced capabilities

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

802.16: WiMAX

- like 802.11 & cellular: base station model
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna
- unlike 802.11:
  - range ~ 6 miles ("city rather than coffee shop")
  - ~14 Mbps

802.16: WiMAX: downlink, uplink scheduling

- transmission frame
  - down-link subframe: base station to node
  - uplink subframe: node to base station

- WiMAX standard provide mechanism for scheduling, but not scheduling algorithm

Components of cellular network architecture

- MSC: connects cells to wide area net
- manages call setup (more later!)
- handles mobility (more later!)

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

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
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

Cellular standards: brief survey

2G systems: voice channels
- IS-136 TDMA: combined FDMA/TDMA (North America)
- GSM (global system for mobile communications): combined FDMA/TDMA
  - most widely deployed
- IS-95 CDMA: code division multiple access

3G systems: voice/data
- Universal Mobile Telecommunications Service (UMTS)
- CDMA-2000: CDMA in TDMA slots
  - data service: 1xEvolution Data Optimized (1xEVDO) up to 14 Mbps

Introduction to cellular networks, with a focus on 2G and 3G systems. The transition from 2G to 3G is highlighted, along with the evolution of mobile and data services.

Chapter 6 outline

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

What is mobility?

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

Cellular Internet

IEEE 802.11

voice and data channels

Handling mobility in time slots

combined FDMA/TDMA

CDMA-2000

TDMA/TDMA

Don’t drown in a bowl of alphabet soup: use this for reference only.

6: Wireless and Mobile Networks 6-37
6: Wireless and Mobile Networks 6-38
6: Wireless and Mobile Networks 6-39
6: Wireless and Mobile Networks 6-40
6: Wireless and Mobile Networks 6-41
6: Wireless and Mobile Networks 6-42
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
- **wide area network**
- **correspondent**

Mobility: more vocabulary

- **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

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

Mobility: registration

End result:
- Foreign agent knows about mobile
- Home agent knows location of mobile

6: Wireless and Mobile Networks 6-41
6: Wireless and Mobile Networks 6-44
6: Wireless and Mobile Networks 6-45
6: Wireless and Mobile Networks 6-46
6: Wireless and Mobile Networks 6-47


**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

**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: ongoing connections can be maintained!

**Mobility via Direct Routing: comments**
- 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
- 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

Packet sent by home agent to foreign agent: a packet within a packet

- Source address: 79.129.13.2
- Destination address: 128.119.40.186

Care-of address: 79.129.13.2

Permanent address: 128.119.40.186

Packet sent by correspondent

Mobile IP: agent discovery

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

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

- 0 or more care-of-addresses

Components of cellular network architecture

- Recall:
  - Wired public telephone network:
  - Different cellular networks, operated by different providers

- Components of cellular network architecture:
  - Correspondent
  - MGC
  - MSC
  - different cellular networks, operated by different providers
**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 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
  - IS-41 allows 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 of MSC chain as mobile moves to new MSC
  - IS-41 allows 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>Home system</td>
<td>Network to which mobile user's permanent phone number belongs</td>
<td>Home network</td>
</tr>
<tr>
<td>Gateway Mobile Switching Center, or &quot;home MSC&quot;, 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>Home agent</td>
</tr>
<tr>
<td>Visited System</td>
<td>Network other than home system where mobile user is currently residing</td>
<td>Visited network</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>Foreign agent</td>
</tr>
<tr>
<td>Mobile Station Roaming Number (MSRN), or &quot;roaming number&quot;</td>
<td>Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.</td>
<td>Care-of-address</td>
</tr>
</tbody>
</table>

---

### 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, CDMA-2000, UMTS)

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