Wireless and Mobile Networks

- Background:
  - # wireless (mobile) phone subscribers now exceeds # wired phone subscribers!
  - computer nets: laptops, palmtops, PDAs, Internet-enabled phone promise anytime untethered Internet access
- two important (but different) challenges
  - communication over wireless link
  - handling mobile user who changes point of attachment to network

Outline

1 Introduction

Wireless
- 2 Wireless links, characteristics
  - CDMA
- 3 IEEE 802.11 wireless LANs ("wi-fi")
- 4 Cellular Internet Access
  - architecture
  - standards (e.g., GSM)

Mobility
- 5 Principles: addressing and routing to mobile users
- 6 Mobile IP
- 7 Handling mobility in cellular networks
- 8 Mobility and higher-layer protocols
9 Summary

Elements of a wireless network

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

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

- 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

Elements of a wireless network

- network infrastructure
- elements of a wireless network
Characteristics of selected wireless link standards

- 9.6 Kbps
- 14 Kbps
- 28.8 Kbps
- 56 Kbps
- 54 Mbps
- 5-11 Mbps
- 1 Mbps
- IS-95 CDMA, GSM
- UMTS/WCDMA, CDMA2000

Elements of a wireless network

- Infrastructure mode: base station connects mobiles into wired network
- Standoff: mobile changes base station providing connection into wired network
- Indoor: 10 – 30m
- Outdoor: 50 – 200m
- Mid range outdoor: 200m – 4Km
- Long range outdoor: 5Km – 20Km

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 Link Characteristics

- 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

multiple wireless links 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:
  - A, C can not hear each other
  - Means A, C unaware of their interference at B
- Signal fading:
  - A, C can not 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)
IEEE 802.11 Wireless LAN

- **802.11b**
  - 2.4-5 GHz unlicensed radio spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
    - widely deployed, using base stations

- **802.11a**
  - 5.6 GHz range
  - up to 54 Mbps

- **802.11g**
  - 2.4-5 GHz range
  - up to 54 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

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/CollisionAvoidance

CDMA Encode/Decode

sender

channel output $Z_n(t)$

data bits

code

$Z_1$ and $Z_0$

slot 1

slot 0

received input

code

$D_n = \sum_{m=1}^{M} Z_{i,m} \cdot c_m$

$D_1$

$D_0$

$M$

slot 1

slot 0

channel output

receiver

CDMA: two-sender interference

senders

channel output $Z_n(t)$

data bits

code

$Z_1$ and $Z_0$

slot 1

slot 0

receiver

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
- RTS 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

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 3: used only in ad hoc mode

802.11 frame: more

Duration of reserved transmission time (RTS/CTS)
Frame seq # (for reliable ARQ)
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

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

Components of cellular network architecture

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

2.5 G systems: voice and data channels
- for those who can’t wait for 3G service: 2G extensions
- general packet radio service (GPRS)
  - evolved from GSM
  - data sent on multiple channels (if available)
- enhanced data rates for global evolution (EDGE)
  - also evolved from GSM, using enhanced modulation
  - Date rates up to 384K
- CDMA-2000 (phase 1)
  - data rates up to 144K
  - evolved from IS-95
Cellular standards: brief survey

3G systems: voice/data
- Universal Mobile Telecommunications Service (UMTS)
- GSM next step, but using CDMA
- CDMA-2000

... more (and more interesting) cellular topics due to mobility (stay tuned for details)

What is mobility?

- spectrum of mobility, from the network perspective:

  - no mobility
  - mobile user, using same access point
  - 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 cellphone)

Mobility: Vocabulary

- home network: permanent "home" of mobile (e.g., 128.119.40/24)
- permanent address: address in home network, can always be used to reach mobile (e.g., 128.119.40.186)
- home agent: entity that will perform mobility functions on behalf of mobile, when mobile is remote

Mobility: more vocabulary

- permanent address: remains constant (e.g., 128.119.40.186)
- care-of-address: address in visited network (e.g., 79.129.13.2)
- visited network: network in which mobile currently resides (e.g., 79.129.13/24)
- correspondent: wants to communicate with mobile
- home agent: entity in visited network that performs mobility functions on behalf of 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 she is?

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: permanent address of mobile nodes in residence via usual routing table exchange. 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.

## Mobility via Indirect Routing

1. Correspondent addresses packets using home address of mobile.
2. Home agent intercepts packets, forwards to foreign agent.
3. Foreign agent receives packets, forwards to mobile.
4. Mobile replies directly to 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 the same network.

## Mobility via Direct Routing

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

### 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 updates 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)

Mobile IP

- RFC 3220
- 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

- mobile agent: MA
  - visited network: 79.129.13/24
  - home agent: HA
  - foreign agent
  - care-of-address: COA

Mobile IP: registration example

- mobile agent
  - HA: 128.119.40.7
  - COA: 79.129.13.2
  - registration request
  - registration reply

Mobile IP: agent discovery

- agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)
Components of cellular network architecture

- 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

Handling mobility in cellular networks

GSM: indirect routing to mobile

1. old BSS informs MSC of impending handoff, provides list of 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

GSM: handoff with common MSC

1. old BSS informs MSC of impending handoff, provides list of 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

GSM: handoff between MSCs

- anchor MSC: first MSC visited during call
- 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 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>Mobile IP element</th>
<th>GERAN (GSM)</th>
<th>GERAN (GSM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>mobile MSC</td>
<td>visited MSC</td>
<td>home system</td>
<td>visited system</td>
</tr>
<tr>
<td>anchor MSC</td>
<td>home system</td>
<td>home agent</td>
<td>home network</td>
</tr>
<tr>
<td>VLR</td>
<td>VLR</td>
<td>visited MSC</td>
<td>foreign agent</td>
</tr>
<tr>
<td>MSRN</td>
<td>MSRN</td>
<td>visited system</td>
<td>care-of-address</td>
</tr>
<tr>
<td>HLR</td>
<td>HLR</td>
<td>home network</td>
<td>routable 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 retransmissions), and handoff
  - TCP interprets loss as congestion, will decrease congestion window unnecessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links