Wireless and 802.11 LANs

- wireless links:
  - shared, fading, interference, hidden terminal problem
- IEEE 802.11 ("wi-fi")
  - CSMA/CA reflects wireless channel characteristics
  - DIFS, SIFS, receiver ACK, RTS/CTS, NAV, ...

Mobility

- principles: addressing, routing to mobile users
  - home, visited networks
  - direct, indirect routing
  - care-of-addresses
- case studies
  - mobile IP

Readings: Textbook, Chapter 6, Sections 6.2-6.3, and Sections 6.5-6.6, 6.8
Chapter 6: 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
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

- **network infrastructure**

- **wireless hosts**
  - laptop, PDA, IP phone
  - run 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

**Network Infrastructure**
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 ad destination at slightly different times

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

- **802.11a,g**: 54 Mbps
- **802.11b**: 5-11 Mbps
- **802.15**: 1 Mbps
- **UMTS/WCDMA, CDMA2000**: 384 Kbps
- **IS-95 CDMA, GSM**: 56 Kbps

**Indoor**:
- 10 – 30m

**Outdoor**:
- 50 – 200m

**Mid range outdoor**:
- 200m – 4Km

**Long range outdoor**:
- 5Km – 20Km
Wireless Sensor Networking

Habitat/Environment Monitoring

Civil/ Military Applications

Home automation
Intelligent Transportation Systems (ITS)?
Intelligent Transportation Systems (ITS)

- ITS provides the transport safety and efficiency through sensing, computing and communications.
ITS (2/4)
ITS Services

Road Intersection Monitoring

Intersection Monitoring

Road Network Surveillance

Scan

Detect!

Road Sensing Data Delivery

Collision Detection Message
Collision Warning Message

Intelligent Travel Navigation

0.1T Elm St

30° Menu 2:09s

Main St Commerce St.
Road Networks?
**Code Division Multiple Access (CDMA)**

A set of Binary Chip Sequence Pairwise Orthogonal

\[-S \times T = (\sum_{i=1}^{m} S_i \times T_i)/m = 0\]

Examples:

- \(A = (-1 -1 -1 +1 +1 -1 +1 +1)\)
- \(B = (-1 -1 +1 -1 +1 +1 +1 -1)\)
- \(C = (-1 +1 -1 +1 +1 +1 -1 -1)\)
- \(D = (-1 +1 -1 -1 -1 +1 -1 -1)\)
Elements of a Wireless Network

- **network infrastructure**
  - 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
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 Infrastructure Mode

- 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
Ad Hoc Network Approach

• No access point (i.e., base station)
  - “peer-to-peer” mode
• wireless hosts communicate with each other
  - to get packet from wireless host A to B may need to route through wireless hosts X,Y,Z
• Applications:
  - “laptop” meeting in conference room, car
  - interconnection of “personal” devices
  - battlefield
• IETF MANET (Mobile Ad hoc Networks) working group
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 cannot hear each other
means A, C are unaware of their interference at B

Signal fading:
- B, A hear each other
- B, C hear each other
- A, C cannot hear each other
interfering at B
Hidden and Exposed Terminal Problems

- **Wireless networks:** hidden and exposed nodes
  - A->B and C->B: A can't hear C’s transmission
    - C hidden from A, can cause collision!
  - B->A and C->D: won’t interfere with each other, despite B can hear C’s transmission
    - C exposed to B, unnecessary backoff by B!
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);
    - often need to switch between transmitting vs. receiving mode
  - can’t sense all collisions in any case: hidden terminal, fading
  - goal: avoid collisions: CSMA/C(ollision)A(voidance)
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 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 timer
   timer counts down while channel idle
   transmit when timer expires
   if no ACK (e.g., due to collision or bit error),
   increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK
  return ACK after SIFS (ACK needed due
to hidden terminal problem)
Collision Avoidance Mechanisms

• Problem:
  - two nodes, hidden from each other, transmit complete frames to base station
  - wasted bandwidth for long duration!

• Solution:
  - small reservation packets
  - nodes track reservation interval with internal “network allocation vector” (NAV)
Avoiding Collisions (cont’d)

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 (large) data frame collisions using small reservation packets!
Collision Avoidance: Some Details

• Sender transmits RequestToSend (RTS) frame
• Receiver replies with ClearToSend (CTS) frame
• Neighbors...
  - see CTS: keep quiet
  - see RTS but not CTS: ok to transmit
• Receiver sends ACK when has frame
  - neighbors silent until see ACK
• Collisions
  - no collisions detection
  - known when don’t receive CTS
  - exponential backoff
Collision Avoidance: RTS-CTS Exchange

- sender transmits short RTS (request to send) packet: indicates duration of transmission
- receiver replies with short CTS (clear to send) packet
  - notifying (possibly hidden) nodes
- hidden nodes will not transmit for specified duration: NAV
Collision Avoidance: RTS-CTS Exchange

- RTS(A)
- RTS(B)
- reservation collision
- RTS(A)
- CTS(A)
- DATA (A)
- ACK(A)
- ACK(A)
- defer
# 802.11 Frame: Addressing

<table>
<thead>
<tr>
<th>Field</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame control</td>
<td>2</td>
<td>Contains information about the frame, such as type and protocol used.</td>
</tr>
<tr>
<td>Duration</td>
<td>2</td>
<td>Represents the duration of the packet in microseconds.</td>
</tr>
<tr>
<td>Address 1</td>
<td>6</td>
<td>MAC address of wireless host or AP transmitting this frame.</td>
</tr>
<tr>
<td>Address 2</td>
<td>6</td>
<td>MAC address of wireless host or AP receiving this frame.</td>
</tr>
<tr>
<td>Address 3</td>
<td>6</td>
<td>MAC address of original (i.e., actual!) source or destination when frames are forwarded by AP.</td>
</tr>
<tr>
<td>Sequence control</td>
<td>2</td>
<td>Contains a sequence number for error correction and control purposes.</td>
</tr>
<tr>
<td>Address 4</td>
<td>6</td>
<td>MAC address used when frames are forwarded from one AP to another AP.</td>
</tr>
<tr>
<td>Payload</td>
<td>0 - 2312</td>
<td>Contains the actual data being transmitted.</td>
</tr>
<tr>
<td>CRC</td>
<td>4</td>
<td>Contains a cyclic redundancy check (CRC) for error detection.</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 original (i.e., actual!) source or destination when frames are forwarded by AP

**Address 4:** Used when frames are forwarded from one AP to another AP (MAC address of actual source)
802.11 Frame: Addressing

H1

AP

R1 router

Internet

802.11 Frame: Addressing

R1 MAC addr

AP MAC addr

dest. address

source address

802.3 frame

AP MAC addr
H1 MAC addr
R1 MAC addr

address 1
address 2
address 3

802.11 frame
802.11 Frame: More

- **frame control**
- **duration**
- **address 1**
- **address 2**
- **address 3**
- **seq control**
- **address 4**
- **payload**
- **CRC**

**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
Mobility with a Subnet (cont’d)

• **Scanning (selecting an AP)**
  - node sends `Probe` frame
  - all AP’s w/in reach reply with `ProbeResponse` frame
  - node selects one AP; sends it `AssociateRequest` frame
  - AP replies with `AssociationResponse` frame
  - new AP informs old AP via tethered network

• **When**
  - active: when join or move
  - passive: AP periodically sends `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
A Word about Bluetooth

- Low-power, small radius, wireless networking technology
  - 10-100 meters
- Omnidirectional
  - Not line-of-sight infrared
- Interconnects gadgets
- 2.4-2.5 GHz unlicensed radio band
- Up to 721 kbps

- Interference from wireless LANs, digital cordless phones, microwave ovens:
  - Frequency hopping helps
- MAC protocol supports:
  - Error correction
  - ARQ
- Each node has a 12-bit address
(Wide-Area) Mobility

• What is mobility?
• spectrum of mobility, from the network perspective:

- no mobility
- mobile wireless user, using same access point

- high mobility
- mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)
- mobile user, connecting/disconnecting from network using DHCP.
**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

**correspondent**

**wide area network**

---

CSci4211  802.11 Wireless and Mobile IP  41
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

Foreign 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 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: 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.

Not scalable to millions of mobiles.
Mobility: Registration

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

1. Foreign agent contacts home agent home: “this mobile is resident in my network”
2. Mobile contacts foreign agent on entering visited network
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.

Diagram:
- Home network
- Wide area network
- Visited network
- Home agent intercepts packets, forwards to foreign agent
- Foreign agent receives packets, forwards to mobile
- 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 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: **on going connections can be maintained!**
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.

Home network
Wide area network
Visited network
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 w/ 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

Permanent address: 128.119.40.186

Care-of address: 79.129.13.2

Packet sent by correspondent

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

Destination: 79.129.13.2

Destination: 128.119.40.186

Foreign-agent-to-mobile packet

Destination: 128.119.40.186
Mobile IP: Agent Discovery

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

![Diagram of Mobile IP: Agent Advertisement]

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type = 9</td>
<td>Code = 0</td>
</tr>
<tr>
<td>checksum</td>
<td>Router address</td>
</tr>
<tr>
<td>type = 16</td>
<td>length</td>
</tr>
<tr>
<td>sequence #</td>
<td>Registration lifetime</td>
</tr>
<tr>
<td>RBHFMGV bits</td>
<td>Reserved</td>
</tr>
</tbody>
</table>

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

0 or more care-of-addresses
Mobile IP: Registration Example

visited network: 79.129.13/24

home agent
HA: 128.119.40.7

foreign agent
COA: 79.129.13.2
ICMP agent adv.

registration req.
COA: 79.129.13.2
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 9999
identification: 714
encapsulation format
....

registration reply
HA: 128.119.40.7
MA: 128.119.40.186
Lifetime: 4999
Identification: 714
encapsulation format
....

Mobile agent
MA: 128.119.40.186
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
Wireless 802.11 and Mobility Summary

Wireless and 802.11 LANs
• wireless links:
  - shared, fading, interference, hidden terminal problem
• IEEE 802.11 (“wi-fi”)
  - CSMA/CA reflects wireless channel characteristics
  - DIFS, SIFS, receiver ACK, RTS/CTS, NAV, ...

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