(Wireless) Internet Routing

Review of Wireless Networking
(with Routing in Mind)
Review of Wireless Networking

- Architecture of wireless networks
- Wireless PHY
- Wireless MAC
  - 802.11

PHY: physical layer / MAC: medium access control (layer)
Architecture of Wireless Networks

- **Keywords:**
  - Single-hop vs. multi-hop
  - Infrastructure based vs. point to point or ad-hoc/mesh

- *Most wireless networks today have a single wireless hop*
Single-Hop Wireless Networks

- Cellular networks: GSM, 3G, 4G (IP based)
- Wireless LAN
- PAN/BAN (Bluetooth)

Generally infrastructure based (access point or base station), not much (wireless) routing necessary

PAN: personal area network / BAN: body area network
Cellular Networks

Typical Base Station (BS): connects mobiles into wired network

Public telephone network, and Internet

Wireless
Wi-Fi (802.11) Networks

Typical Access Point (AP)

Internet

hub, switch or router

Wireless
Single-Hop Networks with No Infrastructure

- Bluetooth “piconet”, master/slave structure
- Simple peer to peer connections
Multi-Hop Wireless Networks

- Wireless infrastructure
  - Mesh networks
- Client mobility, not infrastructure
- Wireless routing becomes necessary
Mesh Networks with Internet Access

- **Wireless infrastructure** (backbone)
  - Static backbone
- **Gateways to the Internet**
  - Eg: Freifunk, Seattle Wireless
- **Clients connects to AP**
  - Transparent wireless network
  - Mobility, roaming
Multi-Hop Wireless Networks

- **No infrastructure:** ad-hoc network
  - MANET: Mobile Ad Hoc Networks
  - Sensor networks
  - VANET

- **Origins:** packet radio networks
  (1978, “Advances in packet radio technology”)

- **Nodes:** transmit, receive, forward
- **Nodes can be mobile**
- **Wireless routing becomes necessary**
Master/Slave Multi-Hop Wireless Network

- Bluetooth ("Scatternet")
  - Master is a slave
- No infrastructure
Why Multi-Hops Wireless Networks?

- Ease of deployment
- Speed of deployment
- Decreased dependence on infrastructure
Because There are Many Applications

- Personal area networking
  - Cell phone, laptop, ear phone, wrist watch

- Military environments
  - Soldiers, tanks, planes

- Civilian environments
  - Mesh networks
  - Taxi cab network
  - Meeting rooms
  - Sports stadiums
  - Boats, small aircraft
  - Environmental monitoring

- Emergency operations
  - Search-and-rescue
  - Policing and fire fighting
There are Many Variations

- Fully Symmetric Environment
  - All nodes have identical capabilities and responsibilities

- Asymmetric Capabilities
  - Transmission ranges and radios may differ
  - Battery life at different nodes may differ
  - Processing capacity may be different at different nodes
  - Speed of movement

- Asymmetric Responsibilities
  - Only some nodes may route packets
  - Some nodes may act as leaders of nearby nodes (e.g., cluster head)
There Really are Many Variations

- Traffic characteristics may differ in different ad hoc networks
  - Bit rate
  - Timeliness constraints
  - Reliability requirements
  - Unicast / multicast / geocast
  - Host-based addressing / content-based addressing / capability-based addressing

- May co-exist (and co-operate) with an infrastructure-based network
Many, Many, Many Variations...

- Mobility patterns may be different
  - People sitting at an airport lounge
  - New York taxi cabs
  - Kids playing
  - Military movements
  - Personal area network

- Mobility characteristics
  - Speed
  - Predictability
    - Direction of movement
    - Pattern of movement
  - Uniformity (or lack thereof) of mobility characteristics among different nodes
Standardisation Effort: MANET@IETF

- MANET IETF working group (http://www.ietf.org/html.charters/manet-charter.html)
  - “standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion or other factors”
  - Work on unicast routing protocol, multicast forwarding and neighbor discovery
  - More later...
- RFCs: 2501, 3561, 3626, 3684, 4728, 5449
**Wireless Networks Architecture: Summary**

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

This course?: routing in multi-hop wireless networks, cellular network access and backhaul, mobility
**Wireless Network Specifics and Challenges**

- **Dynamic topology:** client and/or node mobility, node failures, time-varying links
  - Mobility: route loss, packet loss, network partition
  - Mesh network: dynamic backbone, clients roaming

- **Wireless PHY and link**
  - Time-varying
  - Low reliability (packet loss)
  - Limited bandwidth
  - Limited transmission range
  - Shared and broadcast medium (security)
  - Bidirectional and unidirectional links, asymmetric links

- **Energy-constrained operation**
  - Especially for ad hoc networks
Wireless Physical Layer

Unlike a wired connection!

- **Characteristics**
  - Time-varying channel: propagation, connectivity and available capacity
  - Shared medium: interference, collisions

- **Consequences for the upper layers: links exhibit**
  - Time-varying behavior: connectivity, rate
  - Low reliability: packets are lost (typical $10^{-2}$ PER)
  - Smaller bandwidth than wired counterpart (10 to 100 Mbit/s)
  - Asymmetric / bidirectional and unidirectional links
PHY or PHY? Radio Waves vs Bits

- Depends whom you talk to!

Bits (digital PHY) → Coding Modulation → Waveforms (analog PHY) → Amp → BPF → LNA → Demodulation Decoding → Bits (digital PHY)

From MAC

Waveforms (analog PHY) → To MAC
Propagation is Time-Varying

Because of mobility or mobile environment

- **Path loss:**
  - Free space: Friis,
  - Real life: logarithmic, $1/r^a$

- **Shadowing**
  - Obstacles: buildings, trees

- **Fading**
  - Multipath

---

Pictures: Ganesan CS691aa 07, Reddy 07
Received Power is not Uniform

- Reasons
  - Propagation
  - Antenna gain
  - Hardware issues
Non-Uniform Packet Reception Probability

- Contour prob. of packet reception around a single node
- Setup: around 160 nodes in a grid with 60 cm spacing
- Heavy-tail behavior
Received Power is not Uniform

- Connectivity is not a unit-disc

![RSSI: low power](image1)

![RSSI: high power](image2)

Pictures: Ganesan CS601aa 07
Received Power is Time-Varying
Rate of a Link Depends on the Received Power

\[ R = f(SNR) \quad SNR = \frac{P_r}{I+N} \]

- Link rate is time-varying
Detour: Interference

Where does I come from?

Remember! We have a shared medium: “INTERFERENCE”

- In-system interference
  - APs in the same building

- External interference
  - Bluetooth on 802.11
  - Microwave oven on DECT phone

And N?

- Thermal noise in the hardware
Typical Network Behavior: Variable Packet Loss

Packet loss variability as function of the distance
Typical Network Behavior: Reception Rate Changes Over Time
Links are Asymmetric

Node A can transmit to node B but node B cannot transmit to node A

- Achtung! Signal propagation (path loss, shadowing, fading) is not asymmetric!

- But hardware is not perfect
  - Frequency mismatch
  - Variation of transmission power
  - AGC changing the thresholds
  - Different noise levels and noise floors

- And links are time-varying
- And shared

AGC: automatic gain control
Wireless Physical Layer Summary

From a routing point of view

- Links are asymmetric
- Links are not reliable
  - Fading, interference
- Links are time-varying
  - Connectivity (neighbors or reachable nodes)
  - Rate
    - Delivery probability or packet error rate (PER)
- Broadcast by default: overhearing
Wireless Medium Access Control (MAC)

Remember! We have a shared medium

- MAC: arbitrate (point to point) transmissions between nodes

- Compared to classic Ethernet
  - Collision detection is very hard
  - No full duplex (requires extra transceivers)
  - Not a single rate guaranteed
Typical Issues a MAC Must Solve

- Competing nodes
- Hidden terminal
- Exposed node
Hidden terminal problem
- B, A hear each other
- B, C hear each other
- A, C cannot hear each other

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

A's signal strength

C's signal strength

space
Exposed Terminal
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

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

Reservation collision and defer
802.11: advanced capabilities

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.

![Graph showing BER vs SNR for different modulation techniques, QAM256 (8 Mbps), QAM16 (4 Mbps), BPSK (1 Mbps), with an operating point indicated.]
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
# 802.11 Transmission Channels

- **802.11** = 802.11b, 802.11g, 802.11a, 802.11n
- **802.11b/g**: ISM band at 2.5 GHz
  - 2.400–2.500 GHz
- **802.11a**: 5 GHz U-NII band
  - From 5.15 to 5.825 GHz

![Diagram of 802.11 channels](wikipedia)
Wireless MAC Summary

From a routing point of view

- Links are not reliable
  - Collisions
- Links are time-varying
  - Delay
Wireless Internet Routing

- This course: routing in MANET/ad hoc networks and mesh networks
  - Internet? = Gateway(s) wireless/wired

- Challenges of routing in wireless networks
  - High time variability
  - Dynamic topology
  - Links: unreliable, asymmetric, time-varying
Backup Slides

- More on 802.11
Backup Slides

- More on 802.11
- GSM network architecture
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: 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
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 4**: used only in ad hoc mode

<table>
<thead>
<tr>
<th>Field</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame control</td>
<td>2</td>
<td>2 bytes of frame-specific control information.</td>
</tr>
<tr>
<td>Duration</td>
<td>2</td>
<td>2 bytes indicating the transmission duration.</td>
</tr>
<tr>
<td>Address 1</td>
<td>6</td>
<td>6 bytes identifying the recipient MAC address.</td>
</tr>
<tr>
<td>Address 2</td>
<td>6</td>
<td>6 bytes identifying the sender MAC address.</td>
</tr>
<tr>
<td>Address 3</td>
<td>6</td>
<td>6 bytes identifying the AP interface MAC address.</td>
</tr>
<tr>
<td>Address 4</td>
<td>6</td>
<td>6 bytes used only in ad hoc mode.</td>
</tr>
<tr>
<td>Sequence Control</td>
<td>2</td>
<td>2 bytes indicating the sequence number.</td>
</tr>
<tr>
<td>Payload</td>
<td>0 - 2312</td>
<td>The data payload of the frame.</td>
</tr>
<tr>
<td>CRC</td>
<td>4</td>
<td>4 bytes of cyclic redundancy check (CRC)</td>
</tr>
</tbody>
</table>
802.11 frame: addressing

802.11 frame:
- AP MAC addr
- H1 MAC addr
- R1 MAC addr

802.3 frame:
- R1 MAC addr
- H1 MAC addr

address 1
address 2
address 3

Internet

router

H1

AP
# 802.11 frame: more

<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)
- **Duration of reserved transmission time (RTS/CTS)**
- **Frame seq # (for RDT)**

![Diagram of 802.11 frame structure](attachment:image.png)
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
GSM Network Architecture

Structure of a GSM network (from Wikipedia)