SC250
Computer Networking I

Wireless Networks and Conclusion

Prof. Matthias Grossglauser

School of Computer and Communication Sciences
EPFL

http://lcawww.epfl.ch
Characteristics of Selected Wireless Standards

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

- **Indoor**: 10 – 30m
- **Outdoor**: 50 – 200m
- **Mid range outdoor**: 200m – 4Km
- **Long range outdoor**: 5Km – 20Km

- **2G**: IS-95 CDMA, GSM
- **3G**: UMTS/WCDMA, CDMA2000
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., cordless phone, microwave oven)
  - Multipath propagation: radio signal reflects off objects and ground, arriving at destination at slightly different times -> interference

- Communication across wireless link much more “difficult”
  - Bit errors and loss are unavoidable
  - Mobility makes things worse: fluctuations
IEEE 802.11 Wireless LAN

- **802.11b**
  - most common today
  - 2.4-5 GHz unlicensed radio spectrum
  - up to 11 Mbps
  - 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 two modes:
- base-station
- ad hoc
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

- BSSs combined to form distribution system (DS)
  - DS = “one wireless LAN”
802.11: Channels, Association

- **802.11b**: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - 3 independent channels (1,6,11)
  - 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
  - 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 possible!
  - 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**
  - If sense channel idle for DIFS then
    - transmit entire frame (no CD)
  - 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)

- Refinement:
  - 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 potential interferers
  - Sender transmits data frame
  - Other stations defer transmissions

Avoid data frame collisions completely using small reservation packets!
Collision Avoidance: RTS-CTS Exchange

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

Reservation collision

Time line with RTS(A) and RTS(B) overlapping, indicating a collision. AP defers to avoid collision.
Another Problem: Exposed Terminal

- C wants to send to D
  - ok, B's signal to weak at D to interfere
  - but C does not send because of carrier sensing

Solution:
- RTS/CTS again
- C had heard RTS(B) before, but not CTS(B) sent by A
- This means: A cannot hear C, therefore C can send without interfering with B->A
Conclusion

- **TCP/IP architecture:**
  - Concept of layers:
    - each protocol belongs to one layer *only*
    - each layer can only rely on services of layer below
  - Such an architecture doesn't just happen - its benefits have to be formulated, players (equipment and software vendors, developers, etc.) have to commit
  - TCP/IP has no certification authority for compliance
  - The architecture can evolve or fall apart if it does not satisfy needs

- **Case study: layer violation in NATs**
  - NAT: “hides” several IP addresses behind a single IP address
  - Breaks the TCP/IP layers
  - Why? Mainly shortage of IP addresses
NAT: Network Address Translation

All datagrams leaving local network have same single source NAT IP address: 138.76.29.7, different source port numbers

Datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)
NAT: Network Address Translation

- **Motivation:** local network uses just one IP address as far as outside world is concerned:
  - no need to be allocated range of addresses from ISP:
    - just one IP address is used for all devices
  - can change addresses of devices in local network without notifying outside world
  - can change ISP without changing addresses of devices in local network
  - devices inside local net not explicitly addressable, visible by outside world (a security plus).
NAT: Network Address Translation

Implementation: NAT router must:

- outgoing datagrams: replace (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  ... remote clients/servers will respond using (NAT IP address, new port #) as destination addr.

- remember (in NAT translation table) every (source IP address, port #) to (NAT IP address, new port #) translation pair

- incoming datagrams: replace (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table
NAT: Network Address Translation

1: Host 10.0.0.1 sends datagram to 128.119.40, 80

S: 10.0.0.1, 3345
D: 128.119.40.186, 80

2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

S: 138.76.29.7, 5001
D: 128.119.40.186, 80

3: Reply arrives dest. address: 138.76.29.7, 5001

S: 128.119.40.186, 80
D: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

S: 128.119.40.186, 80
D: 10.0.0.1, 3345

NAT translation table

<table>
<thead>
<tr>
<th>WAN side addr</th>
<th>LAN side addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>138.76.29.7, 5001</td>
<td>10.0.0.1, 3345</td>
</tr>
<tr>
<td>……</td>
<td>……</td>
</tr>
</tbody>
</table>

138.76.29.7

10.0.0.4
NAT: Network Address Translation

- **16-bit port-number field:**
  - >60,000 simultaneous connections with a single LAN-side address!

- **NAT is controversial:**
  - Routers should only process up to layer 3
  - Violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - Address shortage should instead be solved by IPv6

- **Other examples of layer violations:**
  - Firewalls
  - Application-layer switches
  - Transparent proxies
  - ...
SC250: Summary and Outlook

- Topics covered:
  - Principles underlying computer networks
  - Architecture of TCP/IP and the Internet: end-to-end principle, layers, protocols
  - Touched on many topics, not always with sufficient level of detail (but there are more classes coming...)
  - You now understand the Internet, its underlying principles, and you are able to design & implement Internet applications

- The IP hourglass... will it withstand the test of time?
Anything left to learn? Don't worry… :-)

- Network design: as a networking engineer, how do you design a network, given some specifications?
  - User population, cost, robustness and security requirements, manageability/operations support…
- Error control and correction: coding, information theory
- Physical layer: digital communications, information theory
- Security: cryptography, systems aspects
- More sophisticated service models for multimedia
- Wireless and mobile networking: mobile IP, ad hoc (infrastructure-less networks),…