Wireless Networking

CS 407
The Networking Stack

The Seven Layers of OSI

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

Transmit Data

Receive Data

Physical Link
What do they do?

Interact with apps
Rendering content
Group of flows
End-to-end
Addressing, routing
Channel contention
Signal to bits
What matters?

TCP/IP Stack

Interact with apps
Rendering content
Group of flows
End-to-end
Addressing, routing
Channel contention
Signal to bits
Examples

- Signal to bits
- Channel content
- Addressing, routing
- Group of flows
- End-to-end
- Interact with apps
- Rendering content
- TCP/IP Stack

Browser
HTTP
TCP, UDP
IP
802.11 (WiFi)
802.11 (WiFi)

Physical Link

The Seven Layers of OSI

User
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
TCP

- Transmission Control Protocol
- Connection-oriented
- Reliable
- Congestion Control
- Flow Control
- “End-to-end” semantics

- Source and Destination IP and port numbers
UDP

• User Datagram Protocol
• Connectionless
• Unreliable

• Source and Destination IP and port numbers
Wireless networking

- No wires!
- Shared media
- Interference and noise
- Bandwidth and range limits
- Variable performance
- Mobility
- Implications for higher network layers
Understand your assumptions

• Disconnected operations

• Delay tolerant

• Always on
Cellular vs WiFi

Cost: Expensive licensed spectrum
Range: 1 to 20 km
Tx power: 1-10 W
Protocols: Highly coordinated
Throughputs: ~ 10 Kbps – 2 Mbps

Cost: Cheap and unlicensed use
Range: ~100 m
Tx power: ~0.1 W
Protocols: Uncoordinated
Throughputs: ~ 1 Mbps – 100 Mbps
Cellular network planning

• Ideal - Hexagonal patterns

• In real life – Macro and Microcells
Impact of Wireless Environment on Networks

- The wireless spectrum
- Physical impairments
- Contention for the shared medium
- Effects of mobility
- Restrictions on terminal equipment
- Security
Wireless Spectrum (1)

- **Broadcast TV**
  - VHF: 54 to 88 MHz, 174 to 216 MHz
  - UHF: 470 to 806 MHz

- **FM Radio**
  - 88 to 108 MHz

- **Digital TV**
  - 54 to 88 MHz, 174 to 216 MHz, 470 to 806 MHz
Wireless Spectrum (2)

- **3G Broadband Wireless**
  - 746-794 MHz, 1.7-1.85 GHz, 2.5-2.7 GHz

- **Cellular Phone**
  - 800-900 MHz

- **Personal Communication Service (PCS)**
  - 1.85-1.99 GHz
Wireless Spectrum (3)

- **Wireless LAN (IEEE 802.11b/g)**
  - 2.4 GHz

- **Wireless LAN (IEEE 802.11a)**
  - 5 GHz

- **Bluetooth**
  - 2.45 GHz

- **Local Multipoint Distribution Services (LMDS)**
  - 27.5-31.3 GHz
Physical Impairments: Noise

• Unwanted signals added to the message signal
• May be due to signals generated by natural phenomena such as lightning or man-made sources, including transmitting and receiving equipment as well as spark plugs in passing cars, wiring in thermostats, etc.
• Sometimes modeled in the aggregate as a random signal in which power is distributed uniformly across all frequencies (white noise)
• Signal-to-noise ratio (SNR) often used as a metric in the assessment of channel quality
Physical Impairments: Interference

• Signals generated by communications devices operating at roughly the same frequencies may interfere with one another
  – Example: IEEE 802.11b and Bluetooth devices, microwave ovens, some cordless phones
  – CDMA systems (many of today’s mobile wireless systems) are typically interference-constrained

• Signal to interference and noise ratio (SINR) is another metric used in assessment of channel quality
Physical impairments: Fading (1)
Physical impairments: Fading (2)

• Strength of the signal decreases with distance between transmitter and receiver: path loss
  – Usually assumed inversely proportional to distance to the power of 2.5 to 5
• Slow fading (shadowing) is caused by large obstructions between transmitter and receiver
• Fast fading is caused by scatterers in the vicinity of the transmitter
**Diversity**

- A diversity scheme extracts information from multiple signals transmitted over different fading paths.
- Appropriate combining of these signals will reduce severity of fading and improve reliability of transmission.
- In space diversity, antennas are separated by at least half a wavelength:
  - Other forms of diversity also possible
  - Polarization, frequency, time diversity
Contention for the Medium

- If A and B simultaneously transmit to C over the same channel, C will not be able to correctly decode received information: a collision will occur.
- Need for medium access control mechanisms to establish what to do in this case (also, to maximize aggregate utilization of available capacity).
Effects of Mobility

- Destination address not equal to destination location
- Addressing and routing must be taken care of to enable mobility
- Can be done automatically through handoff or may require explicit registration by the mobile in the visited network
- Resource management and QoS are directly affected by route changes

Figure from Kurose & Ross
Form Factors

• Form factors (size, power dissipation, ergonomics, etc.) play an important part in mobility and nomadicity
  – Mobile computing: implies the possibility of seamless mobility
  – Nomadic computing: connections are torn down and re-established at new location

• Battery life imposes additional restrictions on the complexity of processing required of the mobiles units
Medium sharing approaches

• Time division multiple access (TDMA)

• Frequency division multiple access (FDMA)

• Code division multiple access (FDMA)
TDMA

- Examples
  - GSM
  - IS136
  - iDen
  - DECT
  - Satellite communications
TDMA

• Advantages
  • Active only during own time slot, can do anything else in other time slots
    • Measure the channel, search for other transmitters in different frequencies, etc.
    • Facilities inter-frequency handoffs efficiently (imagine a macrocell and a microcell operating in the same region with different frequencies)

• Disadvantages
  • Need guard slots to protect between two transmitters (to avoid very tight synchronization)
  • This wastes capacity of the channel
FDMA

- Frequency Division Multiple Access
  - Each user is given a separate “channel”
  - Channels are independent of each other

- Needs to implement guard band between channels
CDMA

- Use pseudorandom sequences that are orthogonal (cancel out)
CDMA example

- Assume dot product
- 4 orthogonal codes
  - $a \cdot b = 0$
CDMA example

• Consider a simpler model of 2 bit codes
  – Sender 0: (1, -1) and Sender 1: (1, 1)
  – Data: 1, 0, 1, 1 Data: 0, 0, 1, 1
    Encoded sender 0: (1, -1, -1, 1, 1, -1, 1, -1)
    Encoded sender 1: (-1, -1, -1, -1, 1, 1, 1, 1)
• Simultaneous transmit in medium:
  – (0, -2, -2, 0, 2, 0, 2, 0)
CDMA example

• Simultaneous transmit in medium:
  – (0, -2, -2, 0, 2, 0, 2, 0)
• Sender 0 code: (1, -1)
• Multiply received pattern with sender code
  – ((0, -2), (-2, 0), (2, 0), (2, 0)) . (1, -1)
  = (2, -2, 2, 2), i.e., 1, 0, 1, 1
CDMA example

• Sender 0 code = a, data = x
• Sender 1 code = b, data = y
• Sent a.x + b.y

• Decode a.(a.x + b.y) = (a.a) x + a.b.y = (a.a) x
CDMA

• Advantages
  – Avoids narrow-band interference
  – Does not require strong coordination across different transmitters
  – Uses much more bandwidth than minimum requirements
  – Can allow a single handset to simultaneously talk to two different base stations (use two codes) and achieves better handoffs

• Disadvantages
  – Need to balance transmit power of different transmitters
Asynchronous CDMA

• Synchronous CDMA assumes all users synchronized and use orthogonal codes

• In asynchronous, each user picks a pseudo-random code, and there is some unwanted interference from other sources
  – Equalizing received power from different sources is an important necessity
  – Adding more users, adds to the noise level and so gracefully degrades performance
Generations in Mobile Wireless Service

• First Generation (1G)
  – Mobile voice services

• Second Generation (2G)
  – Primarily voice, some low-speed data (circuit switched)

• Generation 2½ (2.5G)
  – Higher data rates than 2G
  – A bridge (for GSM) to 3G

• Third Generation (3G)
  – Seamless integration of voice and data
  – High data rates, full support for packet switched data
Evolution of Mobile Wireless (1)

Advance Mobile Phone Service (AMPS)
- FDMA
- 824-849 MHz (UL), 869-894 MHz (DL)
- U.S. (1983), So. America, Australia, China

European Total Access Communication System (E-TACS)
- FDMA
- 872-905 MHz (UL), 917-950 MHz (DL)
- Deployed throughout Europe
Cellular generations

- **1G – AMPS**
  - Advanced mobile phone systems
  - Used a FDMA style communication system
  - Separate channel for each user
  - Allowed for spatial frequency re-use

- Limitations:
  - Analog and hence susceptible to noise, eavesdropping
    - Can overhear ESN and replay
Cellular generations

- **1G**
  - Had separate uplink and downlink frequencies
  - 824 to 849 MHz (uplink)
  - 869 to 894 MHz (downlink)
  - Each channel was 30 KHz wide
Evolution of Mobile Wireless (2)

Global System for Mobile communications (GSM)
- TDMA
- Different frequency bands for cellular and PCS
- Developed in 1990, expected >1B subscriber by end of 2003

IS-95
- CDMA
- 800/1900 MHz – Cellular/PCS
- U.S., Europe, Asia
General Packet Radio Services (GPRS)
• Introduces packet switched data services for GSM
• Transmission rate up to 170 kbps
• Some support for QoS

Enhanced Data rates for GSM Evolution (EDGE)
• Circuit-switched voice (at up to 43.5 kbps/slot)
• Packet-switched data (at up to 59.2 kbps/slot)
• Can achieve on the order of 475 kbps on the downlink, by combining multiple slots
Cellular generations

• 2G
  – GSM or Global System for Mobile Communications (voice)
  – 2.5G
    • Data extensions were called GPRS (Generalized Packet Radio Services)
    • Speeds further increased in EDGE (Enhanced Data rates for GSM Evolution)
  – Communication channels: 850/1900 MHz (Canada/US) or 900/1800 MHz
  – Uses TDMA communication
Cellular generations

• 2G
  – IS95
    • CDMA (Code Division Multiple Access)

  – CDMA allows parallel communication at the same time and frequency but using separate codes
Evolution of Mobile Wireless (4)

Universal Mobile Telecommunication Systems (UMTS)
- Wideband DS-CDMA
- Bandwidth-on-demand, up to 2 Mbps
- Supports handoff from GSM/GPRS

IS2000
- CDMA2000: Multicarrier DS-CDMA
- Bandwidth on demand (different flavors, up to a few Mbps)
- Supports handoff from/to IS-95
Fixed Wireless

• Microwave
  – Traditionally used in point-to-point communications
  – Initially, 1 GHz range, more recently in the 40 GHz region

• Local Multipoint Distribution Service (LMDS)
  – Operates around 30 GHz
  – Point-to-multipoint, with applications including Internet access and telephony
  – Virginia Tech owns spectrum in SW VA and surroundings

• Multichannel Multipoint Distribution Service (MMDS)
  – Operates around 2.5 GHz
  – Initially, for TV distribution
  – More recently, wireless residential Internet service
WLANs: IEEE 802.11 Family

• 802.11 working group
  – Specify an open-air interface between a wireless client and a base station or access point, as well as among wireless clients
• IEEE 802.11a
  – Up to 54 Mbps in the 5 GHz band
  – Uses orthogonal frequency division multiplexing (OFDM)
• IEEE 802.11b (Wi-Fi)
  – 11 Mbps (with fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band
  – Uses DSSS
• IEEE 802.11g
  – 20+ Mbps in the 2.4 GHz band
WLANs/WPANs: Bluetooth

• Cable replacement technology
• Short-range radio links
• Small, inexpensive radio chip to be plugged into computers, phones, palmtops, printers, etc.
• Bluetooth was invented in 1994
• Bluetooth Special Interest Group (SIG) founded in 1998 by Ericsson, IBM, Intel, Nokia and Toshiba to develop an open specification
  — Now joined by > 2500 companies
IEEE 802.11

- Characteristics
- Modes of operation
- Association, authentication and privacy
IEEE 802.11 Standard

• Final draft approved in 1997
• Operates in the 2.4 GHz industrial, scientific and medical (ISM) band
• Standard defines the physical (PHY) and medium access control (MAC) layers
  – Note that the 802.11 MAC layer also performs functions that we usually associated with higher layers (e.g., fragmentation, error recovery, mobility management)
• Initially defined for operation at 1 and 2 Mbps
  – DSSS, FHSS or infrared
  – Extensions (IEEE 802.11b, IEEE 802.11a, etc.) allow for operation at higher data rates and (in the case of 802.11a) different frequency bands
## Reference Model (1)

<table>
<thead>
<tr>
<th>Data Link Layer</th>
<th>Physical Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium Access Control (MAC) sublayer</td>
<td>MAC sublayer management</td>
</tr>
<tr>
<td>Physical Layer convergence procedure (PLCP) sublayer</td>
<td>PHY sublayer management</td>
</tr>
<tr>
<td>Physical medium Dependent (PMD) sublayer</td>
<td>station management</td>
</tr>
</tbody>
</table>
Reference Model (2)

• Physical Medium Dependent (PMD) sublayer
  – Defines a method for transmitting and receiving data through the medium, including modulation and coding
  – Dependent on whether DSSS, FHSS or IR is used

• Physical Layer Convergence Procedure (PLCP) sublayer
  – Maps MAC layer PDUs into a packet suitable for transmission by the PMD sublayer
  – Performs carrier sensing

• MAC sublayer
  – Defines access mechanism, based on CSMA
  – Performs fragmentation and encryption of data packets
IEEE 802.11b

- Standard released in 1999
- 2.4 – 2.483 GHz band
- Uses DSSS
- Data rates of up to 11 Mbps
  - Data rates are automatically adjusted for noisy conditions, so can operate at 1, 2, 5.5 or 11 Mbps
- Modes of operation
  - Infrastructure-based
  - Ad-hoc
- Most widely implemented to date
Infrastructure Mode (1)

- Basic Service Set (BSS)
- Access point serves as a local bridge
- Stations communicate through the access point, which relays frames to/from mobile stations
Infrastructure Mode (2)

- Extended Service Set (ESS)
- A set of infrastructure BSSs
- Access points communicate among themselves to forward frames between BSSs and to facilitate movement of stations between BSSs
Ad Hoc Mode

- Independent Basic Service Set (IBSS) or Peer to Peer
- Stations communicate directly with each other
- When no direct link is feasible between two stations, a third station may act as a relay (multi-hop communications)
Distribution Systems

• The architectural component used to interconnect BSSs is the distribution system (DS)

• DS enable mobile device support
  – Address-to-destination mapping
  – Seamless integration of several BSSs

• In practice, an access point implements DS services
Integration with Wired LANs

Wireless Environment and Wireless LANs

STA 1

STA 2

AP

IEEE 802.x LAN

Portal

STA 3

STA 4

BSS 1

BSS 2

DS
Association

• To deliver a message within the DS, must know which AP to access for a given mobile station
• Before a station is allowed to send a message through an AP, it must associate itself with that AP
  – At any given time, a station must be associated with no more than one AP
  – An AP may be associated with multiple stations
• As it moves between BSSs, a mobile station may reassociate itself with a different AP
Authentication

• 802.11 provides link-level authentication between stations

• 802.11 also supports shared key authentication
  – Requires that wired equivalent privacy (WEP) be enabled
  – Identity is demonstrated by knowledge of a shared, secret, WEP encryption key

• Typically, authentication is performed at association with an AP
Privacy

• Default state is “in the clear” – messages are not encrypted

• Optional privacy mechanism, WEP, is provided
  – Goal is to achieve a level of security at least as good as in a wired LAN

• Note that encryption provided by WEP is relatively easy to break
Bluetooth

- Characteristics
- Comparison with IEEE 802.11
Introduction

• Motivation: cable replacement in peripherals and embedded devices

• Named after Harald Blaatand “Bluetooth” II, king of Denmark 940-981 A.D.

• Estimated > 670 M Bluetooth-enabled devices by 2005
Requirements

- Universal framework to integrate a diverse set of devices in a seamless, user-friendly, efficient manner
- Devices must be able to establish ad hoc connections
- Support for data and voice
- Similar security as cables
- Simple, small, power-efficient implementation
- Inexpensive!

Wireless Environment and Wireless LANs
63
Characteristics

• Operates in the ISM band (like 802.11b)
• Frequency hopping spread spectrum
• Up to 720 kbps data transfer with a range of 10 m
  – Transmission rate decreases if interference from other devices is present
• Master/slave architecture
  – A collection of master + slaves is called a piconet
  – Up to 7 slave devices may communicate with a master
  – Piconets can be linked together to form a scatternet
### Comparison with 802.11

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Bluetooth</th>
<th>IEEE 802.11b</th>
<th>IEEE 802.11a</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spectrum</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
</tr>
<tr>
<td>Max Data Rate</td>
<td>725 kbps</td>
<td>11 Mbps</td>
<td>54 Mbps</td>
</tr>
<tr>
<td>Connections</td>
<td>Point-to-Multipoint</td>
<td>Point-to-Point</td>
<td>Point-to-Point</td>
</tr>
<tr>
<td>Frequency Selection</td>
<td>FHSS</td>
<td>DSSS</td>
<td>OFDM</td>
</tr>
<tr>
<td>Circuit cost (est. 2001)</td>
<td>$ 11.00</td>
<td>$ 46.00</td>
<td>N/A</td>
</tr>
</tbody>
</table>