Announcements

- Exam next class 9am-11:30am

- Check canvas about all scores and email TA if needed
1G
1st generation wireless network
• Basic voice service
• Analog-based protocols

2G
2nd generation wireless network
• Designed for voice
• Improved coverage and capacity
• First digital standards (GSM, CDMA)

3G
3rd generation wireless network
• Designed for voice with some data consideration (multimedia, text, internet)
• First mobile broadband

4G
4th generation wireless network
• Designed primarily for data
• IP-based protocols (LTE)
• True mobile broadband

5G?

The need for speed
in kilobits per second

2.4 kbps
64 kbps
2,000 kbps
100,000 kbps
Mobile Computing
Emergent Wireless Networks

- Wireless in self driving
- Wireless VR
- Google’s Loon
- Facebook’s Aquila
- Project Iris
- Farmbeats

Project Iris

Project Soli
Final Review
Final exam: last class
- Focus more on the material after mid-term
- 10-page cheat sheets

Questions?
Overview

- Physical layer
  - Signal propagation, modulation, multiplex, spread spectrum

- MAC layer
  - Medium access, reliability, efficiency

- Network layer
  - Internet, mesh, ad hoc, sensor, delay tolerant networks

- Transport layer
  - UDP, TCP
  - Wireless TCP
Overview (Cont.)

- Localization
  - GPS, WiFi, localization in multihop wireless networks
- Bluetooth, RFID, NFC
- Energy efficiency
- Cellular network
  - Cellular concepts, network provision, handoff, route a call
- Wireless network security and privacy
  - Network security, DoS, secure implants, finger print
Topics

- Physical layer
- MAC layer: 802.11 MAC
- Network layer
- Transport layer: TCP, wireless TCP
- Localization
- Bluetooth, RFID, NFC
- Energy efficiency
- Cellular network
- Wireless network security and privacy
Transport Layer
## Reliable Data Transfer Mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checksum</td>
<td>Detect bit errors</td>
</tr>
<tr>
<td>Timer</td>
<td>Detect packet loss at sender</td>
</tr>
<tr>
<td>Sequence number</td>
<td>Detect packet loss and duplicates at receiver</td>
</tr>
<tr>
<td>ACK</td>
<td>Inform sender that pkt has been received</td>
</tr>
<tr>
<td>NACK</td>
<td>Inform sender that pkt has not been received correctly</td>
</tr>
<tr>
<td>Window, pipelining</td>
<td>Increase throughput, and adapt to receiver buffer size and network congestion</td>
</tr>
</tbody>
</table>
TCP: Overview

- point-to-point:
  - one sender, one receiver

- reliable, in-order byte steam:
  - no "message boundaries"

- pipelined:
  - TCP congestion and flow control set window size

- send & receive buffers

full duplex data:
- bi-directional data flow in same connection
- MSS: maximum segment size

connection-oriented:
- handshaking (exchange of control msgs) init's sender, receiver state before data exchange

flow controlled:
- sender will not overwhelm receiver
TCP Flow Control

- receive side of TCP connection has a receive buffer:

- speed-matching service: matching the sending rate to the receiving app's drain rate

- Rcvr advertises spare room by including value of RcvWindow in segments

- Sender limits unACKed data to RcvWindow
  - guarantees receive buffer doesn't overflow

- app process may be slow at reading from buffer

flow control

- sender won't overflow receiver's buffer by transmitting too much, too fast
Principles of Congestion Control

Congestion:

- informally: “too many sources sending too much data too fast for *network* to handle”
- different from flow control
- manifestations:
  - lost packets (buffer overflow at routers)
  - long delay (queueing in router buffers)
- a top-10 problem!
Approaches towards congestion control

Two broad approaches towards congestion control:

End-end congestion control:
- no explicit feedback from network
- congestion inferred from end-system observed loss, delay
- approach taken by TCP

Network-assisted congestion control:
- routers provide feedback to end systems
  - single bit indicating congestion (SNA, DECbit, TCP/IP ECN, ATM)
  - explicit rate sender should send at (XCP)
TCP congestion control: additive increase, multiplicative decrease

- **Approach:** increase transmission rate (window size), probing for usable bandwidth, until loss occurs
  
  - *additive increase:* increase $\text{CongWin}$ by 1 MSS every RTT until loss detected
  
  - *multiplicative decrease:* cut $\text{CongWin}$ in half after loss

Saw tooth behavior: probing for bandwidth
TCP Congestion Control: details

- Sender limits transmission: 
  \[ \text{LastByteSent - LastByteAcked} \leq \text{CongWin} \]

- Roughly,
  
  \[ \text{rate} = \frac{\text{CongWin}}{\text{RTT}} \text{ Bytes/sec} \]

- Both CongWin and RTT are time-varying

How does sender perceive congestion?

- Loss event = timeout or 3 duplicate acks

TCP sender reduces rate (CongWin) after loss event

Three mechanisms:

- AIMD
- Slow start
- Conservative after timeout events
Summary: TCP Congestion Control

- When CongWin is below Threshold, sender is in slow-start phase, window grows exponentially.

- When CongWin is above Threshold, sender is in congestion-avoidance phase, window grows linearly.

- When a triple duplicate ACK occurs, Threshold set to CongWin/2 and CongWin set to Threshold.

- When timeout occurs, Threshold set to CongWin/2 and CongWin is set to 1 MSS.
TCP in Wireless Networks

- **Transmission errors**
  - Random errors
  - Burst errors

- **Mobility**
  - Infrastructure wireless networks
  - Wireless ad hoc networks
Impacts of Random Errors

Random errors may cause fast retransmit
- Fast retransmit results in
  - retransmission of lost packet
  - reduction in congestion window
- Reducing congestion window in response to errors is unnecessary and reduces the throughput

Random errors may cause timeout
- Multiple packet losses in a window can result in timeout when using TCP-Reno (and to a lesser extent when using SACK)
Burst Errors May Cause Timeouts

- If wireless link remains unavailable for extended duration, a window worth of data may be lost
  - passing a truck
  - driving through the tunnel

- Timeout results in
  - Possibly long idle time
  - Slow start, which reduces congestion window to 1 MSS and reduces ssthresh to 1/2
  - Reduction in window and ssthresh in response to errors are unnecessary
Various Schemes

- Link-layer retransmissions
- Split connection approach
- TCP-Aware link layer
- TCP-Unaware approximation of TCP-aware link layer

- Inferring reasons for packet losses
  - Explicit notification
  - Receiver-based discrimination
  - Sender-based discrimination

Hide losses

Avoid congestion
Control under non-congestion losses
## Summary

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Idea</th>
<th>Who</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link layer</td>
<td>Link layer retx</td>
<td>Wireless end points</td>
<td>Hide wireless error</td>
</tr>
<tr>
<td>Split connection</td>
<td>Local retx + Independent optimization of wireless conn.</td>
<td>Base station</td>
<td>Hide wireless error</td>
</tr>
<tr>
<td>Snoop</td>
<td>Link layer retx + drop dup ACK at base station</td>
<td>Base station</td>
<td>Hide wireless error + avoid unnecessary cwnd reduction</td>
</tr>
<tr>
<td>Delayed dup ACK</td>
<td>Link layer retx + delay dup ACK at wireless host</td>
<td>Base station</td>
<td>Hide wireless error + avoid unnecessary cwnd reduction</td>
</tr>
</tbody>
</table>
## Summary (Cont.)

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Idea</th>
<th>Who</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELN</td>
<td>Tag dup ack with ELN if loss occurs at wireless link</td>
<td>Base station</td>
<td>Avoid unnecessary cwnd reduction</td>
</tr>
<tr>
<td>Receiver</td>
<td>When receiver believes that packet loss is due to errors, it sends a notification to the TCP sender</td>
<td>Receiver Sender</td>
<td>Avoid unnecessary cwnd reduction</td>
</tr>
<tr>
<td>Sender</td>
<td>When sender believes that packet loss is due to errors, it does not reduce cwnd.</td>
<td>Sender</td>
<td>Avoid unnecessary cwnd reduction</td>
</tr>
</tbody>
</table>
Techniques to Improve TCP Performance in Presence of Mobility
Classification

- Hide mobility from the TCP sender
- Make TCP adaptive to mobility
Using Fast Retransmits to Recover from Timeouts during Handoff

- During the long delay for a handoff to complete, a whole window worth of data may be lost
- After handoff is complete, acks are not received by the TCP sender
- Sender eventually times out and retransmits
- If handoff still not complete, another timeout will occur

- Performance penalty
  - Time wasted until timeout occurs
  - Window shrunk after timeout
Mitigation Using Fast Retransmit

- When MH is the TCP receiver: after handoff is complete, it sends 3 dupacks to the sender
  - this triggers fast retransmit at the sender
  - instead of dupacks, a special notification could also be sent

- When MH is the TCP sender: invoke fast retransmit after completion of handoff
M-TCP [Brown97]

- In the fast retransmit scheme [Caceres95]
  - Sender starts transmitting soon after handoff
  - But congestion window shrinks

- M-TCP attempts to avoid shrinkage in the congestion window
M-TCP Uses
TCP Persist Mode

- When a new ack is received with receiver’s advertised window = 0, the sender enters persist mode
- Sender does not send any data in persist mode
  - except when persist timer goes off
- When a positive window advertisement is received, sender exits persist mode
- On exiting persist mode, RTO and cwnd are same as before the persist mode
  - Reusing the old state is not always appropriate
TCP in Mobile Ad Hoc Networks
How to Improve Throughput

- Network feedback
- Inform TCP of route failure by explicit message
- Let TCP know when route is repaired
  - Probing
  - Explicit notification
- Reduces repeated TCP timeouts and backoff
Performance Improvement

Without network feedback

Ideal throughput
2 m/s speed

Actual throughput

With feedback
Signals for localization

- **Time**
  - GPS
  - Acoustic signal
  - Ultrasound

- **Signal strength**
  - RF signal: WiFi, bluetooth, sensor, UWB
  - Light
  - Magnetic field

- ...


Information used for Localization

- Time
- Signal strength (coarse or fine-grained)
- Phase difference
- Angle of arrival
- Mobility information
  - Accelerometer
  - Gyroscope
- Vision
GPS System: Overview

- In reality, receiver clock is not sync'd with satellites

Thus need one more satellite to have the right number of equations to estimate clock

\[
\begin{align*}
t^R_1 &= t^S + \frac{d_1}{c} + \delta_{\text{clock-drift}} \\
\|p - p_1\| &= c(t^R_1 - t^S - \delta_{\text{clock-drift}}) \\
&= c(t^R_1 - t^S) - c\delta_{\text{clock-drift}}
\end{align*}
\]

called pseudo range
GPS Messages

GPS SATELLITE SIGNALS

L1 CARRIER 1575.42 MHz
C/A CODE 1.023MHz
NAV/SYSTEM DATA 50 Hz
P-CODE 10.23 MHz
L2 CARRIER 1227.6 MHz

L1 SIGNAL

Mixer
Modulo 2 Sum

L2 SIGNAL
GPS: Summary

- GPS is among the simplest localization system in terms of topology

- Limitations of GPS
  - Hardware requirements vs. small devices
  - GPS jammed by adversaries
  - GPS spoofing
  - Obstructions to GPS satellites common
    - Each node needs LOS to 4 satellites
    - LOS hard to achieve in many environments, e.g., urban canyon, indoors, and underground
  - High energy consumption
Localization in Multihop Wireless Networks

**Given:**
Set of $n$ points
Positions of $k$ of them known
Distances between $m$ pairs of points

**Find:**
Positions of points which can be determined

Illustration:

Find locations to satisfy distance constraints
Typically under-constrained
- Modify the graph to avoid being under-constrained
  - Find most likely positions
  - Find all possible positions
RFID System

- Three components
  - RFID tag or transponder
    - Antenna, wireless transducer, encapsulating material
    - Passive tags: operating power induced by the magnetic field of RFID reader, which is feasible up to distances of 3 m, low price (a few US cents)
    - Active tags: on-chip battery powered, distances up to 100 m
  - RFID reader or transceiver
    - Antenna, transceiver, decoder
  - Data processing subsystem
RFID Overview

- **Data rate**
  - Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
  - 9.6 - 115 kbit/s

- **Transmission range**
  - Passive: up to 3 m
  - Active: up to 30-100 m
  - Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s

- **Frequency**
  - 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others

- **Security**
  - Application dependent, typ. no crypt. on RFID device

- **Cost**
  - Very cheap tags, down to < $1 (passive)

- **Availability**
  - Many products, many vendors

- **Connection set-up time**
  - Depends on product/medium access scheme (typ. 2 ms per device)

- **Quality of Service**
  - none

- **Manageability**
  - Very simple, same as serial interface

- **Special Advantages/Disadvantages**
  - Advantage: extremely low cost, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
  - Disadvantage: no QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/transmission of ID)
NFC

- Wireless Short Range Communication Technology
  - Based on RFID technology at 13,56 MHz
  - Operating distance typical up to 10 cm
  - Compatible with today’s field proven contactless RFID technology
  - Low bandwidth: data rate today up to 424 kilobits/s
NFC - Technical Basics (Cont.)

- It’s a contactless card and a contactless reader in one chip
- Applications aimed for are
  - Ticketing
  - Payment
  - Device Pairing

Short Range
13.56MHz
RF Link
NFC Security

- **Eavesdropping**
  - No protection
    - Use a Secure Channel

- **Data Modification**
  - No protection
    - Use Secure Channel

- **Man in the Middle Attack**
  - Protection

- **Replay attacks**
  - No protection
Classic Bluetooth

- Traditional Bluetooth is *connection oriented*. When a device is connected, a link is maintained, even if there is no data flowing.

- Sniff modes allow devices to sleep, reducing power consumption to give months of battery life.

- Peak transmit current is typically around 25mA.

- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for *coin cells* and energy harvesting applications.
## Bluetooth Low Energy

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>~ 150 meters open field</td>
</tr>
<tr>
<td>Output Power</td>
<td>~ 10 mW (10dBm)</td>
</tr>
<tr>
<td>Max Current</td>
<td>~ 15 mA</td>
</tr>
<tr>
<td>Latency</td>
<td>3 ms</td>
</tr>
<tr>
<td>Topology</td>
<td>Star</td>
</tr>
<tr>
<td>Connections</td>
<td>&gt; 2 billion</td>
</tr>
<tr>
<td>Modulation</td>
<td>GFSK @ 2.4 GHz</td>
</tr>
<tr>
<td>Robustness</td>
<td>Adaptive Frequency Hopping, 24 bit CRC</td>
</tr>
<tr>
<td>Security</td>
<td>128bit AES CCM</td>
</tr>
<tr>
<td>Sleep current</td>
<td>~ 1μA</td>
</tr>
<tr>
<td>Modes</td>
<td>Broadcast, Connection, Event Data Models, Reads, Writes</td>
</tr>
</tbody>
</table>
Physical Channels

- Two types of channels

3 Advertising Channels and 37 Data Channels

| Frequency | 2402 MHz | 2404 MHz | 2406 MHz | 2408 MHz | 2410 MHz | 2412 MHz | 2414 MHz | 2416 MHz | 2418 MHz | 2420 MHz | 2422 MHz | 2424 MHz | 2426 MHz | 2428 MHz | 2430 MHz | 2432 MHz | 2434 MHz | 2436 MHz | 2438 MHz | 2440 MHz | 2442 MHz | 2444 MHz | 2446 MHz | 2448 MHz | 2450 MHz | 2452 MHz | 2454 MHz | 2456 MHz | 2458 MHz | 2460 MHz | 2462 MHz | 2464 MHz | 2466 MHz | 2468 MHz | 2470 MHz | 2472 MHz | 2474 MHz | 2476 MHz | 2478 MHz | 2480 MHz |
|-----------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|---------|
Physical Channels

- Advertising channels avoid 802.11
Where does energy go?

- Display
- Hard disk
- Memory
- CPU
- Wireless communications
Radio Power Consumption

Incoming information → **Tx**: Sender → Channel → **Rx**: Receiver → Outgoing information

- $E_{\text{elec}}^{\text{Tx}}$: Transmit electronics
- $E_{\text{RF}}$: Power amplifier
- $E_{\text{elec}}^{\text{Rx}}$: Receive electronics

<table>
<thead>
<tr>
<th>Channel Type</th>
<th>$E_{\text{RF}}$</th>
<th>$E_{\text{elec}}^{\text{Tx}}$</th>
<th>$E_{\text{elec}}^{\text{Rx}}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>~ 1 km (GSM)</td>
<td>~ 8000 nJ/bit</td>
<td>~ 200 nJ/bit</td>
<td>~ 100 nJ/bit</td>
</tr>
<tr>
<td>~ 50 m (WLAN)</td>
<td>~ 300 nJ/bit</td>
<td>~ 200 nJ/bit</td>
<td>~ 400 nJ/bit</td>
</tr>
<tr>
<td>~ 10 m (Mote)</td>
<td>~ 600 nJ/bit</td>
<td>~ 200 nJ/bit</td>
<td>~ 400 nJ/bit</td>
</tr>
</tbody>
</table>

~ 1 km (GSM) ~ 50 m (WLAN) ~ 10 m (Mote)
Improve Energy Efficiency

- Sleep whenever possible
- **MAC**
  - Which node transmits
  - What packet
  - At what time
  - On what channel
  - With what RF power
  - What modulation and coding setting
- Reduce path loss via directional antennas and **MIMO**
- Exploit mobility for energy
- Harvest energy
Cellular Networks
Outline

- Introduction
- Frequency reuse
- Channel assignment strategies
- Techniques to increase capacity
- Handoff
- Cellular standards
Cellular Network Architecture

- Mobile Switching Center
- Public Telephone network and Internet
- Wired network
System Capacity

- Cluster repeated $M$ times in a system
- Total number of channels that can be used (capacity)
  - $C = MKN = MS$
M/M/c/c Queue

- Poisson arrival
- Exponential distributed service time
- c servers
- Buffer size: c
- Blocking probability = \( \frac{\alpha^c / c!}{\sum_{i=0}^{c} (\alpha^i / i!)} \)
  where \( \alpha \) is Offered load
Cell Size: Tradeoff

- Smaller cells $\Rightarrow$ higher $M$ $\Rightarrow$ higher $C$
  - Channel reuse $\Rightarrow$ higher capacity
  - Lower power requirements for mobiles

- Additional base stations required
- More frequent handoffs
- Greater chance of 'hot spots'
Effect of cluster size $N$

- channels unique in same cluster, repeated over clusters
- keep cell size same
  - large $N$: weaker interference, but lower capacity
  - small $N$: higher capacity, more interference need to maintain certain S/I level
- frequency reuse factor: $1/N$
  - each cell within a cluster assigned $1/N$ of the total available channels
Channel Assignment Strategies: Fixed Channel Assignments

- Each cell is allocated a predetermined set of voice channels.
- If all the channels in that cell are occupied, the call is blocked, and the subscriber does not receive service.
- Variation includes a borrowing strategy: a cell is allowed to borrow channels from a neighboring cell if all its own channels are occupied. This is supervised by the MSC.
Channel Assignment Strategies: Dynamic Channel Assignments

- Voice channels are not allocated to different cells permanently.
- Each time a call request is made, the serving base station requests a channel from the MSC.
- The switch then allocates a channel to the requested call based on a decision algorithm taking into account different factors: frequency re-use of candidate channel and cost factors.
- Dynamic channel assignment is more complex (real time), but reduces likelihood of blocking.
Interference and System Capacity

- major limiting factor in performance of cellular radio systems

- sources of interference:
  - other mobiles in same cell
  - a call in progress in a neighboring cell
  - other base stations operating in the same frequency band
  - Non-cellular system leaking energy into the cellular frequency band

- effect of interference:
  - voice channel: cross talk
  - control channel: missed or blocked calls

- two main types:
  - co-channel interference
  - adjacent channel interference
Two Major Sources of Interference

- **Best case co-channel interference**

  \[
  \frac{S}{I} = S/I\text{R} = \frac{S}{\sum_{i=1}^{i_0} I_i} = \frac{R^{-\alpha}}{D^{-\alpha}} \sum_{i=1}^{i_0} 1 = \left(\frac{R}{D}\right)^{-\alpha}/i_0
  \]

  - For a hexagonal geometry
    - \( \frac{D}{R} = \sqrt{3N} = Q \) - co-channel reuse ratio
    - \( \frac{S}{I} = \sqrt{3N} \) \( ]^{\alpha} / i_0 \)

- **Worst case co-channel interference**

  \[ \frac{S}{I} \sim R^{-4} / [2(D-R)^{-4} + 2(D+R)^{-4} + 2D^{-4}] \]
Increasing Capacity in Cellular Systems

- As demand for wireless services increases, the number of channels assigned to a cell is not enough to support the required number of users.
- Solution is to increase channels per unit coverage area.
Approaches to Increasing Capacity

- **Frequency borrowing**
  - Frequencies are taken from adjacent cells by congested cells

- **Cell splitting**
  - Cells in areas of high usage can be split into smaller cells

- **Cell sectoring**
  - Cells are divided into a number of wedge-shaped sectors, each with their own set of channels

- **Microcells**
  - Antennas move to buildings, hills, and lamp posts
Cell Splitting

- subdivide a congested cell into smaller cells
- each with its own base station, reduction in antenna and transmitter power
- more cells $\Rightarrow$ more clusters $\Rightarrow$ higher capacity
- achieves capacity improvement by essentially rescaling the system.
Cell Splitting from radius $R$ to $R/2$
Sectoring

- In basic form, antennas are omnidirectional.
- Replacing a single omni-directional antenna at base station with several directional antennas, each radiating within a specified sector.

3 sectors

6 sectors
Sectoring

- achieves capacity improvement by essentially rescaling the system.
- less co-channel interference, number of cells in a cluster can be reduced
- Larger frequency reuse factor, larger capacity
Micro Cell Zone Concept

- Large control base station is replaced by several lower powered transmitters on the edge of the cell.
- The mobile retains the same channel and the base station simply switches the channel to a different zone site and the mobile moves from zone to zone.
- Since a given channel is active only in a particular zone in which mobile is traveling, base station radiation is localized and interference is reduced.
Handoffs

Level at A

Handoff threshold
Minimum acceptable signal to maintain the call

Δ

Level at B

A

B
Choice of Margin

- ∆ too small:
  - Insufficient time to complete handoff before call is lost
  - More call losses

- ∆ too large:
  - Too many handoffs
  - Burden for MSC
Styles of Handoff

- **Network Controlled Handoff (NCHO)**
  - in first generation cellular system, each base station constantly monitors signal strength from mobiles in its cell
  - based on the measures, MSC decides if handoff necessary
  - mobile plays passive role in process
  - burden on MSC
Styles of Handoff

- **Mobile Assisted Handoff (MAHO)**
  - present in second generation systems
  - mobile measures received power from surrounding base stations and report to serving base station
  - handoff initiated when power received from a neighboring cell exceeds current value by a certain level or for a certain period of time
  - faster since measurements made by mobiles, MSC don’t need monitor signal strength
Types of Handoff

- **Hard handoff** - (break before make)
  - FDMA, TDMA
  - mobile has radio link with only one BS at anytime
  - old BS connection is terminated before new BS connection is made.
Types of Handoff

- **Soft handoff (make before break)**
  - CDMA systems
  - Mobile has simultaneous radio link with more than one BS at any time
  - New BS connection is made before old BS connection is broken
  - Mobile unit remains in this state until one base station clearly predominates
Brief Outline of Cellular Process

- Telephone call placed to mobile user
- Telephone call made by mobile user
Telephone call to mobile user

- Step 1 - The incoming telephone call to Mobile X is received at the MSC.
- Step 2 - The MSC dispatches the request to all base stations in the cellular system.
- Step 3 - The base stations broadcast the Mobile Identification Number (MIN), telephone number of Mobile X, as a paging message over the FCC throughout the cellular system.
Telephone call to mobile user

- **Step 4** - The mobile receives the paging message sent by the base station it monitors and responds by identifying itself over the reverse control channel.

- **Step 5** - The base station relays the acknowledgement sent by the mobile and informs the MSC of the handshake.

- **Step 6** - The MSC instructs the base station to move the call to an issued voice channel within the cell.
Telephone call to mobile user

- Step 7 - The base station signals the mobile to change frequencies to an unused forward and reverse voice channel pair.

- At the same time, another data message (alert) is transmitted over the forward voice channel to instruct the mobile to ring.
Telephone Call Placed by Mobile

- Step 1 - When a mobile originates a call, it sends the base station its telephone number (MIN), electronic serial number (ESN), and telephone number of called party. It also transmits a station class mark (SCM) which indicates what the maximum power level is for the particular user.

- Step 2 - The cell base station receives the data and sends it to the MSC.
Telephone Call Placed by Mobile

- Step 3 - The MSC validates the request, makes connection to the called party through the PSTN and validates the base station and mobile user to move to an unused forward and reverse channel pair to allow the conversation to begin.
Example 6

What is the number of users in a cell when each system has 63 voice channels, reuse factor of 7, blocking probability of 1%, and average user load of 0.03 [Erlang].
Solution 6

- Each cell has $\frac{63}{7} = 9$ channels
- 9 channels @ block rate = 1% $\rightarrow$ 3.783 [Erlang]
- $3.783 / 0.03 = 126$ users
Example 6 (Cont.)

What is the total number of users in the entire network when the network has 5 clusters?
Example 6 (Cont.)

126 * 7 * 5 = 4410 users for the network
Question 1

- How are voice calls routed in the cellular network?
Solution 1
Solution 1 (Cont.)

Home Network
- MSC

Visited network
- MSC
- Mobile

src

Home Network
- MSC

Visited network
- MSC
- Mobile

src
Question 2

- Practice lookup table:
Question 3

- A cellular provider bought 4 MHz spectrum. Each call occupies 100 kHz. Each user uses his/her phone 10%. The target blocking rate is within 3%. How many users can it serve if it has one cell tower.

- How many users can it serve if it has 40 cells with a cluster size of 10 under the same target blocking rate?
Solution 3

- 4 MHz/ 100 kHz = 40 channels
  40 channels @ 3% blocking $\Rightarrow$ 32.4 Erlangs
  32.4 Erlangs/(0.1 Erlang/users) $\Rightarrow$ 324 users

- 40 channels/10 cells = 4 channels/cell
  4 channels/cell @ 3% blocking $\Rightarrow$ 1.26 Erlangs
  1.26 Erlangs/(0.1 Erlang/users) = 12.6 users
  12.6* 40 = 504 users
Wireless network security
What is network security?

Confidentiality: only sender, intended receiver should “understand” message contents
  - sender encrypts message
  - receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and availability: services must be accessible and available to users
There are bad guys (and girls) out there!

**Q:** What can a “bad guy” do?

**A:** A lot!

- **eavesdrop:** intercept messages
- actively **insert** messages into connection
- **impersonation:** can fake (spoof) source address in packet (or any field in packet)
- **hijacking:** “take over” ongoing connection by removing sender or receiver, inserting himself in place
- **denial of service:** prevent service from being used by others (e.g., by overloading resources)
Types of Cryptography

- Crypto often uses keys:
  - Algorithm is known to everyone
  - Only “keys” are secret

- Public key cryptography
  - Involves the use of two keys

- Symmetric key cryptography
  - Involves the use of one key

- Hash functions
  - Involves the use of no keys
  - Nothing secret: How can this be useful?
**Symmetric key cryptography**

Symmetric key crypto: Bob and Alice share same (symmetric) key: $K_s$

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

**Q:** how do Bob and Alice agree on key value?
Public key cryptography

Bob's public key

Bob's private key

plaintext message, m

encryption algorithm

K_B^+(m)
ciphertext

decryption algorithm

m = K_B^-(K_B^+(m))

plaintext message
RSA: Creating public/private key pair

1. Choose two large prime numbers $p$, $q$. (e.g., 1024 bits each)

2. Compute $n = pq$, $z = (p-1)(q-1)$

3. Choose $e$ (with $e < n$) that has no common factors with $z$. ($e$, $z$ are “relatively prime”).

4. Choose $d$ such that $ed - 1$ is exactly divisible by $z$. (in other words: $ed \mod z = 1$).

5. Public key is $(n, e)$. Private key is $(n, d)$.
RSA: Encryption, decryption

0. Given \((n,e)\) and \((n,d)\) as computed above

1. To encrypt message \(m\) (<\(n\)), compute
   \[c = m^e \mod n\]

2. To decrypt received bit pattern, \(c\), compute
   \[m = c^d \mod n\]

Magic happens!

\[m = (m^e \mod n)^d \mod n\]
**RSA example:**


- $e=5$ (so $e$, $z$ relatively prime).
- $d=29$ (so $ed-1$ exactly divisible by $z$).

Encrypting 8-bit messages.

<table>
<thead>
<tr>
<th>bit pattern</th>
<th>$m$</th>
<th>$m^e$</th>
<th>$c = m^e \mod n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00001100</td>
<td>12</td>
<td>24832</td>
<td>17</td>
</tr>
</tbody>
</table>

```
c = m^e \mod n
```

```
c = c^d \mod n
```

```
m = c^d \mod n
```

Encrypt: $c = m^e \mod n$

Decrypt: $m = c^d \mod n$
Why does RSA work?

- Must show that $c^d \mod n = m$
  where $c = m^e \mod n$

- Fact: for any $x$ and $y$: $x^y \mod n = x^{(y \mod z)} \mod n$
  where $n = pq$ and $z = (p-1)(q-1)$

- Thus,
  $c^d \mod n = (m^e \mod n)^d \mod n$
  $= m^{ed} \mod n$
  $= m^{(ed \mod z)} \mod n$
  $= m^1 \mod n$
  $= m$
RSA: another important property

The following property will be very useful later:

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

use public key first, followed by private key
use private key first, followed by public key

Result is the same!
Why \( K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m)) \) ?

Follows directly from modular arithmetic:

\[
(m^e \mod n)^d \mod n = m^{ed} \mod n = m^{de} \mod n = (m^d \mod n)^e \mod n
\]
Why is RSA Secure?

- Suppose you know Bob’s public key (n,e). How hard is it to determine d?
- Essentially need to find factors of n without knowing the two factors p and q.
- Fact: factoring a big number is hard.

Generating RSA keys

- Have to find big primes p and q
- Approach: make good guess then apply testing rules (see Kaufman)
Session keys

- Exponentiation is computationally intensive
- DES is at least 100 times faster than RSA

Session key, $K_S$

- Bob and Alice use RSA to exchange a symmetric key $K_S$
- Once both have $K_S$, they use symmetric key cryptography
Message Integrity

- Allows communicating parties to verify that received messages are authentic.
  - Content of message has not been altered
  - Source of message is who/what you think it is
  - Message has not been replayed
  - Sequence of messages is maintained
- Let's first talk about message digests
Message Digests

- Function $H(\cdot)$ that takes as input an arbitrary length message and outputs a fixed-length string: "message signature"
- Note that $H(\cdot)$ is a many-to-1 function
- $H(\cdot)$ is often called a "hash function"

Desirable properties:
- Easy to calculate
- Irreversibility: Can't determine $m$ from $H(m)$
- Collision resistance: Computationally difficult to produce $m$ and $m'$ such that $H(m) = H(m')$
- Seemingly random output
Internet checksum: poor message digest

Internet checksum has some properties of hash function:

- produces fixed length digest (16-bit sum) of input
- is many-to-one

- But given message with given hash value, it is easy to find another message with same hash value.
- Example: Simplified checksum: add 4-byte chunks at a time:

<table>
<thead>
<tr>
<th>message</th>
<th>ASCII format</th>
<th>message</th>
<th>ASCII format</th>
</tr>
</thead>
<tbody>
<tr>
<td>I O U 1</td>
<td>49 4F 55 31</td>
<td>I O U 9</td>
<td>49 4F 55 39</td>
</tr>
<tr>
<td>0 0 . 9</td>
<td>30 30 2E 39</td>
<td>0 0 . 1</td>
<td>30 30 2E 31</td>
</tr>
<tr>
<td>9 B O B</td>
<td>39 42 D2 42</td>
<td>9 B O B</td>
<td>39 42 D2 42</td>
</tr>
<tr>
<td></td>
<td>B2 C1 D2 AC</td>
<td></td>
<td>B2 C1 D2 AC</td>
</tr>
</tbody>
</table>

different messages but identical checksums!
Hash Function Algorithms

- **MD5 hash function** widely used (RFC 1321)
  - computes 128-bit message digest in 4-step process.
- **SHA-1** is also used.
  - US standard [NIST, FIPS PUB 180-1]
  - 160-bit message digest
Message Authentication Code (MAC)

$s = \text{shared secret}$

- Authenticates sender
- Verifies message integrity
- No encryption!
- Also called “keyed hash”
- Notation: $MD_m = H(s || m); \text{send } m || MD_m$
Playback attack

\[ MAC = f(\text{msg}, s) \]

Transfer $1M from Bill to Trudy

Transfer $1M from Bill to Trudy
Defending against playback attack: nonce

MAC = \( f(\text{msg}, s, R) \)
Digital Signatures

Cryptographic technique analogous to handwritten signatures.

- sender (Bob) digitally signs document, establishing he is document owner/creator.
- Goal is similar to that of a MAC, except now use public-key cryptography
- verifiable, nonforgeable: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document
Digital Signatures

Simple digital signature for message $m$:

- Bob signs $m$ by encrypting with his private key $K_B^-$, creating “signed” message, $K_B^-(m)$

Bob’s message, $m$

Dear Alice
Oh, how I have missed you. I think of you all the time! …(blah blah blah)
Bob

Bob’s private key

Public key encryption algorithm

Bob’s message, $m$, signed (encrypted) with his private key

$K_B^-(m)$
Digital signature = signed message digest

Bob sends digitally signed message:

large message \( m \) → \( H: \text{Hash function} \) → \( H(m) \) → digital signature (encrypt) → \( K_B^-(H(m)) \) → encrypted msg digest

Alice verifies signature and integrity of digitally signed message:

large message \( m \) → \( H: \text{Hash function} \) → \( H(m) \) → \( K_B^-(H(m)) \) → encrypted msg digest

Bob's private key \( K_B^- \)

Bob's public key \( K_B^+ \)

Digital signature = signed message digest
Digital Signatures (more)

- Suppose Alice receives msg m, digital signature $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob’s public key $K_B^+$ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- If $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob’s private key.

Alice thus verifies that:
- Bob signed m.
- No one else signed m.
- Bob signed m and not m’.

Non-repudiation:
- Alice can take m, and signature $K_B^-(m)$ to court and prove that Bob signed m.
Does digital signature guarantee authenticity?
Certification Authorities

- Certification authority (CA): binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides “proof of identity” to CA.
  - CA creates certificate binding E to its public key.
  - Certificate containing E’s public key digitally signed by CA
    - CA says “this is E’s public key”
Certification Authorities

- When Alice wants Bob’s public key:
  - gets Bob’s certificate (Bob or elsewhere).
  - apply CA’s public key to Bob’s certificate, get Bob’s public key
Certificates: summary

- Primary standard X.509 (RFC 2459)
- Certificate contains:
  - Issuer name
  - Entity name, address, domain name, etc.
  - Entity’s public key
  - Digital signature (signed with issuer’s private key)
- Public-Key Infrastructure (PKI)
  - Certificates and certification authorities
  - Often considered “heavy”
Insecurity of 802.11
WEP Algorithm Encryption

RC4: Rivest Cipher 4
Most widely used software stream cipher (used in SSL and WEP)
Designed by Ron Rivest of RSA Security in 1987
WEP Algorithm Decryption

IV ⊕ Cipher ⊕ RC4(k,IV) = Message CRC(M)
Stream cipher properties

- Given two ciphers $C_1, C_2$ using the same $RC4(v,k)$, $C_1 \oplus C_2 = P_1 \oplus P_2$

- Two conditions required for this class of attacks to succeed:
  - Availability of ciphertexts where keystream is used more than once.
  - Partial knowledge of some of the plain texts.
Finding instances of keystream reuse

- Shared key $k$ changes rarely.
- Reuse of IV causes reuse of keystream.
- IV are public.
IV Usage

- **IV size is only 24 bits** ➔ inherent limit
  - Busy access point of 5Mbps will exhaust available space in 11 hours.

- **Common practices make IV reuse more often**
  - Random IV selection
    - Birthday paradox: on random IV selection 5000 packets are needed to find a collision
  - Common PCMCIA cards set IV to zero and increment it by 1 for each packet ➔ keystreams corresponding to low-valued IVs are reused many times
  - Standard only recommends but not requires change of IV on every packet
Exploiting keystream reuse

- Trial and errors
  - Many fields of IP traffic are predictable.
  - For example: login sequences.
- Send known text and sniff the encrypted text
- AP broadcast both encrypted and unencrypted form when subnet has both WEP and non-WEP clients
- As the number of reused keystream increases breaking them becomes easier.
Consequences of the Attack

- Compromise confidentiality of messages
- Compromise access control
- Compromise data integrity
Message Modification

- Checksum used is CRC-32 which is a linear function of the message:
- In other words, checksum distributes over the XOR operation. \( C(x \oplus y) = C(x) \oplus C(y) \)
- RC4 stream cipher also linear.
The attack

Given $C$ we would like to create $C'$ s.t. $C'$ decrypts to $M'$ instead of $M$. 

$\text{Message} \oplus \text{CRC}(M) = \text{RC4}(k, IV) \oplus \Delta \oplus \text{CRC}(\Delta) = \text{RC4}(k, IV) \oplus \text{Message} \oplus \text{CRC}(M) = \text{RC4}(k, IV) \oplus M' \oplus \text{CRC}(M')$
Summary of Weakness

- **RC4 is efficient but not secure**
  - $C_1 \otimes C_2 = P_1 \otimes P_2 \Rightarrow$ Accurately inferring $P_1$ and $P_2$ allows you to get keystream

- **CRC is not secure**

- **Frequent reuse of IV**
  - Inherent limit of 24-bit
  - Practical use: make reuse even more frequent

- **Poor key management**
  - Key is shared among many entities and rarely changes

- **All three security goals are violated**
  - Confidentiality
  - Access control
  - Data integrity
Countermeasure

- Improve key management
  - Everyone has its own key
  - Prevent key reuse
- Use more secure cryptographic algorithms
- Use end-to-end security (e.g., VPN)
Wireless Security

- DoS attacks and defenses
  - Physical layer: jamming
  - MAC layer: greedy MAC
  - Network layer: routing attacks
  - Transport layer: cross layer attacks

- Cellular network security

- WiFi Fingerprint
Jamming attack models

- **Constant jammer**
  - Always emit random bits of radio signal

- **Deceptive jammer**
  - Always emit preamble bits

- **Random jammer**
  - Alternate between sleeping and jamming states
    -> Conserve Energy

- **Reactive jammer**
  - Transmit signal when jammer senses channel activity
    -> Harder to detect
Summary

- Present four different jammer attack models
- Develop detection schemes
  - SS, carrier sensing time, and PDR alone is not enough
  - PDR + signal strength
    - Reactive consistency check
    - Due to node mobility, PDR window length and SS granularity should be selected carefully.
  - PDR + location information
    - Proactive consistency check
    - Given location information a priori, only need normal PDR.
      - Density of network matters
      - May not work well under obstacles
      - Cannot determine jam for isolated nodes.
      - Freq. of location advertisement matters
Questions

- What are limitations in the detection schemes?
Misbehavior Techniques

- **MAC greedy misbehavior on data path**
  - Scramble CTS frames
    - Action: Cheater hears RTS frame destined to another node, intentionally causes collision of CTS
    - Effect?
  - Scramble DATA/ACK frame
    - Effect?
  - Transmit RTS or DATA after SIFS as opposed to DIFS
  - Increasing NAV to prevent other nodes within range from transmitting
  - Reduce the backoff time
  - A cheater can combine several of the above techniques or dynamically change its misbehavior
Components of Domino
Ariadne

- Three conditions of secure routing
  - Target Authentication
    - To authenticate destination of route request
  - Data authentication
    - To authenticate nodes in route request and route reply
    - TESLA
      - Shared symmetric key
        - Route reply packet has MAC list of all nodes in route
    - Digital signature
      - Route reply packet has signature list instead
  - Per-hop hashing
    - To verify that no hop is omitted
Stealthy DoS schemes

- Can attackers launch DoS by manipulating a small amount of traffic?
  - Harder to detect

- Jellyfish
  - Cross-layer attack
  - Exploit the feedback-based protocol (TCP)
  - Types of attacks
    - JF reorder attack
    - JF periodic dropping attack
    - JF delay variance attack
How to identify a node?
Implicit Identifier Summary

- Network destinations
- SSIDs in probes
- Broadcast pkt sizes
- MAC protocol fields

• More implicit identifiers exist

→ Results we present establish a lower bound
Summary

Implicit identifiers can accurately identify users

- Individual implicit identifiers give evidence of identity
- We can identify many users in all environments
- Some users much more distinguishable than others

Understanding implicit identifiers is important

- Pseudonyms are not enough
- We establish a lower bound on their accuracy

Eliminating them poses research challenges
Results: Multiple Feature Accuracy

Some users much more distinguishable than others

Public networks:
~20% users identified
>90% of the time

<table>
<thead>
<tr>
<th>Feature</th>
<th>Public</th>
<th>Home</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>netdests</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ssids</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>bcast</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>fields</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
Other Types of Fingerprints

- Device and software fingerprints
- RF environment fingerprints
- Traffic fingerprints
- User fingerprints
Fundamental Problem

Many exposed bits are (or can be used as) identifiers that are linked over time.

<table>
<thead>
<tr>
<th>Discover</th>
<th>802.11 probe</th>
<th>Is Bob’s Network here?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>802.11 beacon</td>
<td>Bob’s Network is here</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentica...</th>
<th>802.11 auth</th>
<th>Proof that I’m Alice</th>
</tr>
</thead>
<tbody>
<tr>
<td>and Bind</td>
<td>802.11 auth</td>
<td>Proof that I’m Bob</td>
</tr>
<tr>
<td></td>
<td>MAC addr, seqno, ...</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Send Data</th>
<th>MAC addr, seqno, ...</th>
<th></th>
</tr>
</thead>
</table>
Problem: Long-Term Linking

802.11 beacon  Alice’s iPod is here
MAC: 12:34:56:78:90:ab

802.11 beacon  Alice’s iPod is here
MAC: 12:34:56:78:90:ab

Is Alice’s iPod here?

Alice’s friend?

Easy to identify and relate devices over time
Problem: Short-Term Linking

3-9 data streams overlap each 100 ms, on average

Easy to isolate distinct packet streams
Problem: Short-Term Linking

Isolated data streams are more susceptible to side-channel analysis on packet sizes and timing

- Exposes keystrokes, VoIP calls, webpages, movies, ...

[Liberatore, CCS ‘06; Pang, MobiCom ’07; Saponas, Usenix Security ’07; Song, Usenix Security ‘01; Wright, IEEE S&P ‘08; Wright, Usenix Security ‘07]
Goal: This Protocol

Bootstrap

SSID: Bob’s Network
Key: 0x2384949...

Username: Alice
Key: 0x348190...

Discover

Authenticating and Bind

Send Data
Discussion

- How to save your smartphone energy?
- How to keep smartphone secure?
- Name one benefit of cellular network over WiFi network and one benefit of WiFi over cellular network. Can we achieve the best of both?
- Why is each network designed in that way? Room for improvement?