CS388: Wireless and Mobile Security
-- Introduction

Xiuzhen Cheng
cheng@gwu.edu

Mobile and Wireless Services - Always Best Connected

On the Road

Home Networking

Last-Mile

Disaster Recovery Network

- Many users still don't have broadband
  - End of 2002
  - Worldwide: 46 million broadband subscribers
  - US: 17% household have broadband
  - Reasons: out of service area, some consider expensive

Broadband speed is still limited
- DSL: 1.3 Mbps download, and 100-400Kbps upload
- Cable modem: depends on your neighbors
- Insufficient for several applications (e.g., high-quality video streaming)

- 9/11, Tsunami, Hurricane Katrina, South Asian earthquake ...
- Wireless communication capability can make a difference between life and death!
- How to enable efficient, flexible, and resilient communication?
  - Rapid deployment
  - Efficient resource and energy usage
  - Flexible: unicast, broadcast, multicast, anycast
  - Resilient: survive in unfavorable and untrusted environment
Environmental Monitoring

- Micro-sensors, on-board processing, wireless interfaces feasible at very small scale—can monitor phenomena “up close” enables spatially and temporally dense environmental monitoring

Embedded Networked Sensing will reveal previously unobservable phenomena

Challenges in Wireless Networking Research

Contaminant Transport

Seismic Structure Response

Ecosystems, Biocomplexity

Marine Microorganisms

Challenge 1: Unreliable and Unpredictable Wireless Links

- Wireless links are less reliable
- They may vary over time and space

*Corpa, Busek et. al

What Robert Poor (Ember) calls “The good, the bad and the ugly”

Challenge 2: Open Wireless Medium

- Wireless interference
- Hidden terminals
- Exposed terminal

Challenge 2: Open Wireless Medium

- Wireless interference
- Hidden terminals
- Exposed terminal
Challenge 2: Open Wireless Medium

- Wireless interference
  \[ S_1 \rightarrow R_1 \]
  \[ S_2 \rightarrow R_1 \]

- Hidden terminals
  \[ S_1 \rightarrow R_1 \rightarrow S_2 \]

- Exposed terminal
  \[ R_1 \rightarrow S_1 \rightarrow S_2 \rightarrow R_2 \]

- Wireless security
  - Eavesdropping, Denial of service, Jamming…

Challenge 3: Intermittent Connectivity

- Reasons for intermittent connectivity
  - Mobility
  - Environmental changes

- Existing networking protocols assume always-on networks

- Under intermittent connected networks
  - Routing, TCP, and applications all break

- Need a new paradigm to support communication under such environments

Challenge 4: Limited Resources

- Limited battery power
- Limited bandwidth
- Limited processing and storage power

Introduction to Wireless Networking

Internet Protocol Stack

- Application: supporting network applications
  - FTP, SMTP, HTTP
- Transport: data transfer between processes
  - TCP, UDP
- Network: routing of datagrams from source to destination
  - IP, routing protocols
- Link: data transfer between neighboring network elements
  - Ethernet, WiFi
- Physical: bits “on the wire”
  - Coaxial cable, optical fibers, radios

Physical Layer
Physical Layer Outline
• Signal
• Frequency allocation
• Signal propagation
• Multiplexing
• Modulation
• Spread Spectrum

Overview of Wireless Transmissions

Signals
• Physical representation of data
• Function of time and location
• Classification
  - continuous time/discrete time
  - continuous values/discrete values
  - analog signal = continuous time and continuous values
  - digital signal = discrete time and discrete values

Signals (Cont.)
• Signal parameters of periodic signals:
  - period $T$, frequency $f = 1/T$
  - amplitude $A$
  - phase shift $\phi$
  - sine wave as a special periodic signal for a carrier:

  $$s(t) = A \sin(2\pi ft + \phi t)$$

Fourier Transform: Every Signal Can be Decomposed as a Collection of Harmonics

$$g(t) = \frac{1}{T} + \sum_{n=1}^{\infty} \left[ a_n \cos(2\pi nt) + b_n \sin(2\pi nt) \right]$$

The more harmonics used, the smaller the approximation error.
Why Not Send Digital Signal in Wireless Communications?

- Digital signals need infinite frequencies for perfect transmissions.
- However, we have limited frequencies in wireless communications.

Frequencies for Communication

- VLF = Very Low Frequency
- LF = Low Frequency
- MF = Medium Frequency
- HF = High Frequency
- VHF = Very High Frequency
- UHF = Ultra High Frequency
- SHF = Super High Frequency
- EHF = Extra High Frequency
- UV = Ultraviolet Light

Frequency and wavelength: \( \lambda = \frac{c}{f} \), where \( c \approx 3 \times 10^8 \text{m/s} \), frequency \( f \).

Frequency vs. Bandwidth

- Frequency is a specific location on the electromagnetic spectrum.
- Bandwidth is the range between two frequencies.
  - Bandwidth is measured in Hertz.
  - A cellular operator may transmit signals between 824-849 MHz, for a total bandwidth of 25 MHz.

Bandwidth vs. Capacity

- Capacity is usually measured by Mega bits per second (Mbps).
- Bandwidth for a particular service is fixed, but the number of calls and the rate of data transmission is not (capacity).

An example: IEEE 802.11b (WiFi)

- Operating center frequency: 2.4 GHz.
  - There are 11 channels in 802.11b. Starting from 2.412 GHz to 2.462 GHz.
- Spectrum: 2.412 GHz ~ 2.462 GHz
- Bandwidth: 40 MHz.
- Capacity: 1, 2, 5.5, and 11 Mbps. Typical data rate is about 6.5 Mbps.

Why Need A Wide Spectrum: Shannon Channel Capacity

- The maximum number of bits that can be transmitted per second by a physical channel is:

\[
W \log_2 \left(1 + \frac{S}{N}\right)
\]

where \( W \) is the frequency range that the media allows to pass through, \( S/N \) is the signal noise ratio.
Signal, Noise, and Interference

- **Signal (S)**
- **Noise (N)**
  - Includes thermal noise and background radiation
  - Often modeled as additive white Gaussian noise
- **Interference (I)**
  - Signals from other transmitting sources
- SINR = S/(N+I) (sometimes also denoted as SNR)

Physical Layer Outline

- **Signal**
- **Frequency allocation**
- **Signal propagation**
- **Multiplexing**
- **Modulation**
- **Spread Spectrum**

Signal Propagation Ranges

- **Transmission range**
  - communication possible
  - low error rate
- **Detection range**
  - detection of the signal possible
  - no communication possible
- **Interference range**
  - signal may not be detected
  - signal adds to the background noise

Path Loss

- **Free space model**
  \[ P_r(d) = \frac{P G G_r \lambda^2}{(4\pi)^2 d^2 L} \]
- **Two-ray ground reflection model**
  \[ P_r(d) = \frac{P G G_r h^2 h_r^2}{d^2 L} \quad d_r = \frac{(4\pi h_r)}{\lambda} \]
- **Log-normal shadowing**
  \[ P(d)[dB] = \overline{P}(d)[dB] + X_n \]
- **Indoor model**
  \[ P_r(d)[dBm] = P_t(d)[dBm] - 10n \log(d) - \left\lfloor \begin{array}{ll} nW * \text{WAF} & nW < C \\ C * \text{WAF} & nW \geq C \end{array} \right\rfloor \]
  \[ P = 1 \text{ mW at } d=1 \text{m}, \text{what's } P_r \text{ at } d=2 \text{m}? \]

Signal Propagation

- Propagation in free space always like light (straight line)
- Receiving power proportional to 1/d²
  \( (d = \text{distance between sender and receiver}) \)
- Receiving power additionally influenced by
  - Shadow loss by obstructions
  - reflection at large obstacles
  - refraction depending on the density of a medium
  - scattering at small obstacles
  - diffraction at edges
  - fading (frequency dependent)

Multipath Propagation

- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction
- Time dispersion: signal is dispersed over time
  - interference with "neighbor" symbols, Inter Symbol Interference (ISI)
- The signal reaches a receiver directly and phase shifted
  - distorted signal based on the phases of different parts
Fading
- Channel characteristics change over time and location
  - e.g., movement of sender, receiver and/or scatters
  - Quick changes in the power received (short term/fast fading)
- Additional changes in
  - distance to sender
  - obstacles further away
- Slow changes in the average power received (long term/slow fading)

Physical Layer Outline
- Signal
- Frequency allocation
- Signal propagation
- Multiplexing
- Modulation
- Spread Spectrum

Multiplexing
- Goal: multiple use of a shared medium
- Multiplexing in 4 dimensions
  - space (s)
  - time (t)
  - frequency (f)
  - code (c)
- Important: guard spaces needed!

Space Multiplexing
- Assign each region a channel
- Pros
  - no dynamic coordination necessary
  - works also for analog signals
- Cons
  - Inefficient resource utilization

Frequency Multiplexing
- Separation of the whole spectrum into smaller frequency bands
- A channel gets a certain band of the spectrum for the whole time
- Pros:
  - no dynamic coordination necessary
  - works also for analog signals
- Cons:
  - waste of bandwidth if the traffic is distributed unevenly
  - Inflexible
  - guard spaces
Time Multiplex

- A channel gets the whole spectrum for a certain amount of time
  - Pros:
    - only one carrier in the medium at any time
    - throughput high even for many users
  - Cons:
    - precise synchronization necessary

Time and Frequency Multiplexing

- Combination of both methods
- A channel gets a certain frequency band for a certain amount of time (e.g., GSM)
  - Pros:
    - better protection against tapping
    - protection against frequency selective interference
    - higher data rates compared to code multiplex
  - Cons:
    - precise coordination required

Code Multiplexing

- Each channel has a unique code
- All channels use the same spectrum simultaneously
  - Pros:
    - bandwidth efficient
    - no coordination and synchronization necessary
    - good protection against interference and tapping
  - Cons:
    - lower user data rates
    - more complex signal regeneration
    - Implemented using spread spectrum technology

Physical Layer Outline

- Signal
- Frequency allocation
- Signal propagation
- Multiplexing
- Modulation
- Spread Spectrum

Modulation I

- Digital modulation
  - digital data is translated into an analog signal (baseband)
  - differences in spectral efficiency, power efficiency, robustness
- Analog modulation
  - shifts center frequency of baseband signal up to the radio carrier
  - Reasons
    - Antenna size is on the order of signal's wavelength
    - More bandwidth available at higher carrier frequency
    - Medium characteristics: path loss, shadowing, reflection, scattering, diffraction depend on the signal's wavelength

Modulation and Demodulation

- Radio transmitting and receiving signals
Modulation Schemes

- Amplitude Modulation (AM)
- Frequency Modulation (FM)
- Phase Modulation (PM)

Digital Modulation

- Modulation of digital signals known as Shift Keying
- Amplitude Shift Keying (ASK):
  - Pros: simple
  - Cons: susceptible to noise
  - Example: optical system, IFR

Digital Modulation II

- Frequency Shift Keying (FSK):
  - Pros: less susceptible to noise
  - Cons: requires larger bandwidth

Digital Modulation III

- Phase Shift Keying (PSK):
  - Pros:
    - Less susceptible to noise
    - Bandwidth efficient
  - Cons:
    - Require synchronization in frequency and phase → complicates receivers and transmitter

Phase Shift Keying

- BPSK (Binary Phase Shift Keying):
  - bit value 0: sine wave
  - bit value 1: inverted sine wave
  - very simple PSK
  - low spectral efficiency
  - robust, used in satellite systems
- QPSK (Quadrature Phase Shift Keying):
  - 2 bits coded as one symbol
  - needs less bandwidth compared to BPSK
  - symbol determines shift of sine wave
  - Often also transmission of relative, not absolute phase shift: DQPSK - Differential QPSK

Quadrature Amplitude Modulation

- Quadrature Amplitude Modulation (QAM):
  - combines amplitude and phase modulation
  - It is possible to code $n$ bits using one symbol
    - $2^n$ discrete levels
  - bit error rate increases with $n$

  - Example: 16-QAM (4 bits = 1 symbol)
  - Symbols 0011 and 0001 have the same phase $\phi$, but different amplitude $a$; 0000 and 1000 have same amplitude but different phase
  - Used in Modem
Physical Layer Outline
- Signal
- Frequency allocation
- Signal propagation
- Multiplexing
- Modulation
- Spread Spectrum

Spread spectrum technology
- Problem of radio transmission: frequency dependent fading can wipe out narrow band signals for duration of the interference
- Solution: spread the narrow band signal into a broad band signal using a special code
- Side effects:
  - coexistence of several signals without dynamic coordination
  - tap-proof
- Alternatives: Direct Sequence, Frequency Hopping

DSSS (Direct Sequence Spread Spectrum)
- XOR of the signal with pseudorandom number (chipping sequence)
  - generate a signal with a wider range of frequency: spread spectrum

FHSS (Frequency Hopping Spread Spectrum)
- Discrete changes of carrier frequency
  - sequence of frequency changes determined via pseudo random number sequence
- Two versions
  - Fast Hopping: several frequencies per user bit
  - Slow Hopping: several user bits per frequency
- Advantages
  - frequency selective fading and interference limited to short period
  - simple implementation
  - uses only small portion of spectrum at any time

FHSS: Example

Comparison between Slow Hopping and Fast Hopping
- Slow hopping
  - Pros: cheaper
  - Cons: less immune to narrowband interference
- Fast hopping
  - Pros: more immune to narrowband interference
  - Cons: tight synchronization \(\rightarrow\) increased complexity
Wireless Standards

IEEE 802.11a/b/g (Wi-Fi)

<table>
<thead>
<tr>
<th>802.11a</th>
<th>802.11b</th>
<th>802.11g</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 GHz</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>54 Mbps</td>
<td>11 Mbps</td>
<td>54 Mbps</td>
</tr>
</tbody>
</table>

Less interference, more bandwidth | Best over-all coverage range | Faster than 802.11b and better range than 802.11a
Not as widely implemented, shorter range | Not as fast as other technologies | Less range than 802.11b

IEEE 802.16 (WiMAX)

- 802.16d - A.K.A 802.16-2004
  - Intended for "last mile" connectivity at high data rates.
  - Point-to-multipoint only implementation
- 802.16e - Adds mobility
  - approved in December 2005.

IEEE 802.20 (MBWA)

- Mobile Broadband Wireless Access (MBWA) Working Group
  - 1 Mbps
  - Mobile speeds of 100mph
  - Could compete with 3G cellular
  - Licensed band use only

IEEE 802.11i (WPA2)

- Provide improvements to WiFi security
- Address security shortcomings in WEP
- Add user authentication
**Evolution Data Only (EvDO)**

- Available in Larger Metro Areas
  - Offered by Sprint, Verizon, Other
  - 700Mbps
- Supports Streaming Video

**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

**Why a wireless network is more subject to attacks?**