CS386W: Wireless Networking

Lili Qiu
UT Austin

Fall 2019
Course Information

• Instructor: Lili Qiu, lili@cs.utexas.edu
• Office: GDC 6.806
• Lecture: M 1 - 4pm @ GDC 6.516
• Office hour: W 3-5pm or by appt.
• TA: Jian He, Fri. 2-4pm GDC 6.802FC
• Course homepage: http://www.cs.utexas.edu/~lili/classes/F19-CS386W
• http://piazza.com
Class Goals

• Learn wireless networking fundamentals
• Discuss challenges and opportunities in wireless networking research
• Obtain hands-on wireless research experience
Course Material

• Suggested references (2-hour library loan)
  - Mobile Communications by Jochen Schiller
  - 802.11 Wireless Networks: The Definitive Guide by Matthew S. Gast
  - Wireless Communications Principles and Practice by Ted Rappaport

• Selected conference and journal papers

• Other resources
  - MOBICOM, SIGCOMM, INFOCOM proceedings
Course Workload

• **Grading**
  - Classroom participation: 5%
  - Homework: 30%
  - Exam: 25%
  - Course project: 40%

• **Classroom participation**
  - Actively participate in class discussion
  - Make insightful comments and/or initiate interesting discussions

• **Homework**
  - Assignment
  - Paper review
    • Review form online
    • Starting next class, submit a review for one paper in each session of your choice at the beginning of each class (2 pages)
      • Your grade is determined by the highest 12 reviews
  - Project peer review
  - Next class 9/16: HW 1 + up to 2 paper reviews
How to read a paper?

• Three-pass approach
  
  – 1st pass
    • Read title, abstract, intro, conclusion, section title
    • Identify category, context, correctness, contributions
  
  – 2nd pass
    • Read the paper carefully but ignore proofs
    • Grasp the content of the paper
  
  – 3rd pass
    • Virtually re-implement the paper
    • Identify innovations, limitations, and future work

Paper Review Form

- Submit paper reviews in hardcopies at the beginning of every class

1. Summarize the paper in a few sentences.
2. What are the major strengths of the paper?
3. What are the major weaknesses of the paper?
4. What are the avenues for future work that you think are important? If you are asked to work on the problem studied in this paper, what will you do differently?
5. Detailed comments.
Course Workload (Cont.)

• In class exam: 12/2

• Course project
  - Goal: obtain hands-on experience in wireless networking research
  - Work by yourself or with another student
  - I’ll hand out a list of project topics next class
  - You may also choose your own topic approved by me
  - Project components
    • Initial report
    • Mid-point report
    • Final report (peer reviewed)
    • Presentation: 12/9
  - Vote for best project
UTCS Code of Conduct

• We will strictly enforce UTCS code of conduct
  - No sharing of course materials with current or future students
  - https://wikis.utexas.edu/display/coursematerials/Sample+Use+Statements+for+Syllabus
Course Overview

• **Part I: Introduction to wireless networks**
  - Physical layer
  - **MAC**
    • Introduction to MAC and IEEE 802.11
    • Rate adaptation
    • Packet recovery
  - **Routing**
    • Mobile IP
    • DSR, AODV, DSDV
  - **Transport protocols in wireless networks**
    • Problems with TCP over wireless
    • Other proposals
Course Overview (Cont.)

• Part II: Different types of wireless networks
  - Wireless LANs
  - Wireless mesh networks
  - Sensor networks
  - Vehicular networks
  - Cellular networks
  - Delay tolerant networks
  - Cognitive networks
  - Emergent networks
Course Overview (Cont.)

• Part III: Wireless network management and security
  - Localization
  - Wireless network diagnosis
  - Wireless network security
History

• Tesla credited with first radio communication in 1893
• Wireless telegraph invented by Guglielmo Marconi in 1896
• First telegraphic signal traveled across the Atlantic ocean in 1901
• Used analog signals to transmit alphanumerical characters
Satellites

• Launched in 1960
• First satellites could carry 240 voice circuits
• In 1998 satellites carried:
  - 1/3 of all voice traffic
  - All television signals between countries!
• Modern satellites induce 250 ms propagation delay
• New ones in lower orbits can allow for data services such as Internet access
Mobile Phones

- 2-way 2-party communication using digital transmission technology
- In 2002 the number of mobile phones exceeded that of land lines
- More than 1 billion mobile phones!
- The only telecommunications solution in developing regions
- How did it all start?
Introduction to Wireless Networks
Mobile and Wireless Services – Always Best Connected

LAN, WLAN 600 Mbps

4G 10 Mbps
Bluetooth 500 kbit/s

4G/3G

0.5 – 10 Mbps

4G 10 Mbps

WLAN 600 Mbps

4G 10 Mbps

WLAN 600 Mbps

4G 10 Mbps
On the road
On the Road

UMTS, WLAN, DAB, GSM, WiMAX, LTE, cdma2000, TETRA, ...

GPS, 2G/3G/4G, WLAN, Bluetooth, Ad hoc networks, radios
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>China</td>
<td>3.9%</td>
<td>N/A</td>
<td>N/A</td>
<td>5.0%</td>
<td>N/A</td>
<td>93,500,000</td>
<td>Dec. H1, 2009</td>
</tr>
<tr>
<td>2</td>
<td>US</td>
<td>9.3%</td>
<td>11.5%</td>
<td>1.3%</td>
<td>22.1%</td>
<td>N/A</td>
<td>83,968,547</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>3</td>
<td>Japan</td>
<td>10.8%</td>
<td>2.9%</td>
<td>7.6%</td>
<td>21.3%</td>
<td>N/A</td>
<td>30,631,900</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>4</td>
<td>Germany</td>
<td>20.2%</td>
<td>1.0%</td>
<td>0.1%</td>
<td>29.4%</td>
<td>N/A</td>
<td>24,144,350</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>5</td>
<td>Mexico</td>
<td>13.7%</td>
<td>2.1%</td>
<td>0.0%</td>
<td>15.8%</td>
<td>N/A</td>
<td>17,267,285</td>
<td>Q4, 2009</td>
</tr>
<tr>
<td>6</td>
<td>France</td>
<td>21.4%</td>
<td>1.1%</td>
<td>0.0%</td>
<td>22.5%</td>
<td>N/A</td>
<td>18,009,500</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>7</td>
<td>UK</td>
<td>18.4%</td>
<td>5.3%</td>
<td>0.0%</td>
<td>23.7%</td>
<td>N/A</td>
<td>17,661,100</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>8</td>
<td>South Korea</td>
<td>10.1%</td>
<td>10.6%</td>
<td>9.2%</td>
<td>29.9%</td>
<td>N/A</td>
<td>15,709,771</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>9</td>
<td>Italy</td>
<td>15.4%</td>
<td>0.0%</td>
<td>0.4%</td>
<td>15.8%</td>
<td>N/A</td>
<td>12,447,533</td>
<td>Jun. Q1, 2009</td>
</tr>
<tr>
<td>10</td>
<td>India</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>1%</td>
<td>N/A</td>
<td>10,520,000</td>
<td>Oct. 2010</td>
</tr>
</tbody>
</table>
Last-Mile

- Many users still don’t have broadband
  - Reasons: out of service area; some consider expensive

Broadband speed is still limited
- DSL: 300Kbps – 6Mbps
- Cable modem: depends on your neighbors
- Insufficient for several applications (e.g., high-quality video streaming)
Disaster Recovery Network

• 9/11, Tsunami, Irene, Hurricane Katrina, China, South Asian, Haidi earthquakes …
  - Harvey: sensors, waze, drones, …
• 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, onboard 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

Ecosystems, Biocomplexity

Marine Microorganisms

Contaminant Transport

Seismic Structure Response
Wearable Technology
Internet of Things
Challenges in Wireless Networking Research
Challenge 1: Unreliable and Unpredictable Wireless Links

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

* Cerpa, Busek et. al

What Robert Poor (Ember) calls “The good, the bad and the ugly”
Challenge 2: Open Wireless Medium

- **Wireless interference**

  ![Diagram]

  S1  →  R1
  S2  →  R2
Challenge 2: Open Wireless Medium

- **Wireless interference**
  - S1 → R1
  - S2 → R2

- **Hidden terminals**
  - S1 → R1 R2 → S2
Challenge 2: Open Wireless Medium

- **Wireless interference**
  
  S1 → R1
  
  S2 → R1

- **Hidden terminals**
  
  S1 → R1 ← R2

- **Exposed terminal**
  
  R1 ← S1 ← S2 → R2
Challenge 2: Open Wireless Medium

- **Wireless interference**
  
  ![Diagram of wireless interference]

- **Hidden terminals**
  
  ![Diagram of hidden terminals]

- **Exposed terminals**
  
  ![Diagram of exposed terminals]

- **Wireless security**
  - Eavesdropping, Denial of service, ...
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

Sensors, embedded controllers

Mobile phones
- voice, data
- simple graphical displays
- GSM

PDA
- data
- simpler graphical displays
- 802.11

Laptop
- fully functional
- standard applications
- battery; 802.11

Sims, embedded controllers
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
Outline

• Signal
• Frequency allocation
• Signal propagation
• Multiplexing
• Modulation
• Spread Spectrum
Overview of Wireless Transmissions

sender

bit stream

source coding

channel coding

modulation

analog signal

receiver

bit stream

source decoding

channel decoding

demodulation
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
- Signal parameters of periodic signals:
  - period $T$, frequency $f=1/T$
  - amplitude $A$
  - phase shift $\varphi$
  - sine wave as special periodic signal for a carrier:

$$s(t) = A_t \sin(2\pi f_t t + \varphi_t)$$
Fourier Transform: Every Signal Can be Decomposed as a Collection of Harmonics

\[ g(t) = \frac{1}{2} c + \sum_{n=1}^{\infty} a_n \sin(2\pi n ft) + \sum_{n=1}^{\infty} b_n \cos(2\pi n ft) \]

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

- **Digital signals need**
  - infinite frequencies for perfect transmission
  - however, we have limited frequencies in wireless communications
VLF = Very Low Frequency
LF = Low Frequency, submarine
MF = Medium Frequency, radio
HF = High Frequency, radio
VHF = Very High Frequency, TV
UHF = Ultra High Freq. phone
SHF = Super High Freq. WiFi
EHF = Extra High Frequency
UV = Ultraviolet Light

Frequency and wave length: $\lambda = c/f$, wave length $\lambda$, speed of light $c \approx 3 \times 10^8 \text{m/s}$, frequency $f$
## Frequencies and Regulations

- **ITU-R** holds auctions for new frequencies, manages frequency bands worldwide (WRC, World Radio Conferences)

<table>
<thead>
<tr>
<th>Europe</th>
<th>USA</th>
<th>Japan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cellular Phones</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMTS (FDD) 1920-1980, 2110-2190</td>
<td><strong>TDMA, CDMA, GSM 1850-1910, 1930-1990</strong></td>
<td></td>
</tr>
<tr>
<td>UMTS (TDD) 1900-1920, 2020-2025</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cordless Phones</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CT1+</strong> 885-887, 930-932</td>
<td><strong>PACS 1850-1910, 1930-1990</strong></td>
<td><strong>PHS 1895-1918</strong></td>
</tr>
<tr>
<td><strong>CT2</strong> 864-868</td>
<td><strong>PACS-UB 1910-1930</strong></td>
<td><strong>JCT 254-380</strong></td>
</tr>
<tr>
<td><strong>DECT</strong> 1880-1900</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Wireless LANs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IEEE 802.11</strong> 2400-2483</td>
<td><strong>902-928</strong></td>
<td><strong>IEEE 802.11 2471-2497</strong></td>
</tr>
<tr>
<td><strong>HIPERLAN 2</strong> 5150-5350, 5470-5725</td>
<td><strong>IEEE 802.11 2400-2483 5150-5350, 5725-5825</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Others</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RF-Control</strong> 27, 128, 418, 433, 868</td>
<td><strong>RF-Control 315, 915</strong></td>
<td><strong>RF-Control 426, 868</strong></td>
</tr>
</tbody>
</table>
Why Need A Wide Spectrum
Why Need A Wide Spectrum: Shannon Channel Capacity

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

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

where \( W \) is the frequency range that the media allows to pass through, S/NR 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
- $\text{SINR} = S/(N+I)$ (sometimes also denoted as SNR)
dB and Power conversion

• dB
  - Denote the difference between two power levels
  - \((P_2/P_1)[\text{dB}] = 10 \times \log_{10} (P_2/P_1)\)
  - \(P_2/P_1 = 10^{(A/10)}\)
  - Example: \(P_2 = 100\ P_1\), \(P_2/P_1=10\ \text{dB}\)

• dBm and dBW
  - Denote the power level relative to 1 mW or 1 W
  - \(P[\text{dBm}] = 10 \times \log_{10}(P/1\text{mW})\)
  - \(P[\text{dBW}] = 10 \times \log_{10}(P/1\text{W})\)
  - Example: \(P = 0.001\ \text{mW}, P = 100\ \text{W}\)
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
Outline

• Signal
• Frequency allocation
• Signal propagation
• Multiplexing
• Modulation
• Spread Spectrum
Signal Propagation

- Does signal propagation via a straight line?
Signal Propagation

- Propagation in free space always like light (straight line)
- Receiving power proportional to $1/d^2$
  ($d = \text{distance between sender and receiver}$)
- Receiving power additionally influenced by
  - shadowing
  - reflection at large obstacles
  - refraction depending on the density of a medium
  - scattering at small obstacles
  - diffraction at edges
  - fading (frequency dependent)
Path Loss

- **Free space model**
  \[ P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \]

- **Two-ray ground reflection model**
  \[ P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \]
  \[ d_c = \frac{(4\pi h_t h_r)}{\lambda} \]

- **Log-normal shadowing**
  \[ P(d)[dB] = \bar{P}(d)[dB] + X_\sigma \]

- **Indoor model**
  \[ P_r(d)[dBm] = P_t(d)[dBm] - 10n \log\left(\frac{d}{d_0}\right) - \begin{cases} nW \ast WAF & nW < C \\ C \ast WAF & nW \geq C \end{cases} \]

- **P = 1 mW at d0=1m, what’s Pr at d=2m?**
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)
Real world example
Outline

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

• Goal: multiple use of a shared medium

• Multiplexing in different dimensions
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:**
- more complex signal regeneration
- need precise power control

**Implemented using spread spectrum technology**
Outline

• Signal
• Frequency allocation
• Signal propagation
• Multiplexing
• Modulation
• Spread Spectrum
Modulation I

- **Digital modulation**
  - Digital data is translated into an analog signal (baseband)
  - Difference in spectral efficiency, power efficiency, robustness

- **Analog modulation**
  - Shifts center frequency of baseband signal up to the radio carrier
  - Reasons?
Modulation I

• Digital modulation
  - Digital data is translated into an analog signal (baseband)
  - Difference 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

101101001

radio transmitter

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

![Graph of FSK waveform](image-url)
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
How to send more bits?
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; 0000 and 1000 have same amplitude but different phase
  - Used in Modem
More QAMs

64QAM Constellation

512-QAM Constellation

1024-QAM Constellation

128 points in one quadrant

256 Points in one Quadrant (1 point represent 10 binary bits)
Why not always use the highest QAM?
How do we decide which modulation to use?
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 pseudo-random 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

user data

slow hopping (3 bits/hop)

fast hopping (3 hops/bit)

t_b: bit period
t_d: dwell time
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 → increased complexity
Recap

• Name 5 layers in the Internet protocol stack.
• Pros and cons of layering.
• What is a signal?
• Difference between analog vs. digital signal?
• How do we represent different signals?
• Does a signal always follow a straight line?
• Path loss models
Recap (Cont.)

• Why do we need a wide bandwidth?
• What is multipath propagation?
• Types of multiplexing?
• Types of modulation?
• What is spread spectrum?