Outline

- Last week:
  - WLAN/802.11
  - Architecture (Infrastructure / Ad Hoc)
  - Physical layer (OFDM, rate adaption)

- Today
  - Cellular networks
Overview of Wireless Networks

- **Wireless Personal Area Networks (WPANs)**
  - IEEE 802.15.1 (Bluetooth), IrDa, Zigbee, sensor networks, etc.

- **Wireless Local Area Networks (WLANs)**
  - IEEE 802.11, a, b, g, etc. (infrastructure and ad hoc)

- **Cellular Networks**
  - GSM, UMTS, EDGE, etc.
The Advent of Cellular Networks

- Prior to cellular, mobile radio telephone system was based on:
  - High power/transmitter/receivers
  - Could support about 25 channels
  - In a radius of 80 km

- To increase the network capacity
  - Multiple low-power transmitters (100W or less)
  - Small transmission radius → area split in cells
  - Each cell with its own frequencies
  - The same frequency can be reused at sufficient distance
The Hexagonal Pattern

- Used as an approximation for a cell
- Each cell features one base station with transmitter, receiver and control unit
- Equidistant access to neighboring cells
  - Center to center distance $d = \sqrt{3}R$
  - Center to corner radius $R$
Frequency re-use

- Adjacent cells are assigned different frequencies to avoid interference or crosstalk.
- Objective is to reuse frequency in nearby cells:
  - 10 to 50 frequencies assigned to each cell.
  - Transmission power controlled to limit power at that frequency escaping to adjacent cells.
  - The issue is to determine how many cells must intervene between two cells using the same frequency.
Minimum cell separation

- $N = \# \text{ of cells in a repetitious pattern, i.e. reuse factor}$
- $D = \text{minimum distance between centers of co-channels cells}$
Frequency reuse characterization

- Reuse factor $N$ follows the pattern
  - $I^2 + J^2 + I \times J, I, J = 0, 1, 2, 3, \ldots$
  - $I = 0, J = 2 \rightarrow N = 4$
  - $I = 1, J = 2 \rightarrow N = 7$

- Reuse ratio $q = D/R = \sqrt{3N}$ (proof in book Vijay Garg)

- Reducing $q \rightarrow$ reducing number of cells per cluster ($N$)
  - If total # of channels per cluster is constant, then channels per cell is increased $\rightarrow$ increasing system capacity
System capacity and interference

- $S =$ Total # of duplex channels available for use
- $K =$ total # of duplex channels per cell
- $S = k \times N$

- If a cluster is replicated $M$ times within a system, the total # of duplex channels $C$ can be used as a measure of capacity
  - $C = M \times k \times N = M \times S$

- Tradeoff:
  - If $N$ decreases $\rightarrow$ $k$ increases (since $S$ is a constant)
  - If $N$ decreases $\rightarrow$ $M$ increases (for a fixed geographical area)
  - $M$ increases $\rightarrow$ system capacity $C$ increases
  - Price: $D/R$ decreases $\rightarrow$ co-channel interference increases
Cell splitting

- Smaller cells have greater system capacity
  - Fine grain channel allocation
  - Better spacial reuse
- As traffic load grows, larger cells could split into smaller cells
- Requires careful power control and possibly more frequent handoffs for mobile stations
Cell Sectoring

- Cell divided into wedge shaped sectors
- 3-6 sectors per cell, each with own channel set
  - Subset of cell's channel per sector
  - Use of directional antennas
  - Decrease co-channel interference
Cellular Networks: Generations

- 1G: Once upon a time there was analog cellular communication
- 2G: early 80s, GSM, 9.6 kbit/s, 14.4 kbit/s with enhancements
  - Voice only
- 2.5G or GPRS: 140.8 kbit/s in theory, 56 kbit/s in practice
  - Connects GSM to IP network
- 2.75G or E-GPRS or EDGE (Enhanced Data Rates for GSM Evolution): 180 kbps effective
- 3G:
  - UMTS using WCDMA (Wideband CDMA) supports 14Mbps in theory. 384 kbps,
  - CDMA-2000: Leading 3G solution in Japan, United States, Canada
- 3.5G: UMTS is being upgraded to
  - HSPA (7.2 Mbit/s theory)
  - HSPA+ (up to 42 Mbit/s in theory)
- 4G: Long Term Evolution (LTE), 100 Mbit/s downlink
Multiple Access Methods vs Generations

- **FDMA**
  - AMPS, TACS, NMT

- **OFDMA**
  - HSOPA, Rev C, WIMAX

- **TDMA**
  - TDMA, PDC
  - GSM → GPRS/EDGE

- **CDMA**
  - CDMA → EVXDO
  - UMTS → HSDPA
  - TD-SCDMA

**Source:** nortel
GSM Architecture

Components:
- MS: Mobile Station
- BTS: Base Transceiver Station
- BSC: Base Station Controller
- MSC & GMSC: Switching Centers
- HLR, VLR: Databases storing user information

Subsystems:
- RSS: Radio Subsystem
- NSS: Network and switching subsystem
- OSS: Operation subsystem
GSM: Radio Interface

- Frequency bands:
  - GSM 900: Uplink 880.0–915.0, Downlink 925.0–960.0
  - GSM 1800: 1710.0–1785.0, 1805.0–1880.0
  - Frequency division duplex (FDD) used to separate uplink and downlink

- Channels:
  - GSM 900: 124 channels, each 200kHz wide
  - GSM 1800: 374 channels, 200 kHz wide

- Each BTS manages, e.g., up to 10 channels for user data
  - Space Division Multiple Access (SDMA)

- Each channel is subdivided in continuous TDMA frames of duration 4.615 ms
  - Frame is subdivided into 8 time slots of 577 us
  - Each periodic (occurring every 4.615 ms) slots is called a physical channel
  - Time Division Multiple Access (TDMA)

- Physical channels are used to multiplex logical channels on top
  - Examples of logical channels: voice channel, data channel, control channel
Provider Spectrum Allocation

- **GSM 900**

- **GSM 1800**
NSS Databases

- **Home Location Register (HLR)**
  - Contains permanent and semi-dynamic data of all subscribers
    - Mobile subscriber ISDN number
    - International mobile subscriber identity (IMSI)
    - Current VLR and MSC
    - Mobile subscriber roaming number (MSRN)
  - This user-specific information exists once for each user in one HLR

- **Visitor Location Register (VLR)**
  - Local (dynamic) database for a subset of the user data
  - Includes data about all users currently in the domain of the VLR
  - When an MS enters into the area of the VLR, the VLR copies all relevant information from the HLR
    - Avoid frequent HLR updates and long-distance signaling with the HLR
  - VLR gets updated at MS startup and then periodically
    - If no update is received by VLR for some time it’s considered detached (e.g., roaming, new VLR takes over)
Call Setup (Mobile terminated call)

1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: request MSRN from VLR
6: forward responsible MSC to GMSC
7: forward call to current MSC
8, 9: get current status of MS
10, 11: paging of MS
12, 13: MS answers
14, 15: security checks
16, 17: set up connection
Call Setup (Mobile originated call)

1, 2: connection request
3, 4: security check
5-8: check resources (free circuit)
9-10: set up call
Handover

- Based on MS and BTS's periodic measurements of downlink and uplink quality
  - Measurements reports sent by the MS every 480 ms
- BSC collects all values from BTS and MS, calculates average and compares it with the HO_MARGIN (handover margin) threshold
  - Helps avoid the ping-pong effect
- Handover coordinated by either BSC or MSC depending on whether MS moves between two cells belonging to different MSCs or not
UMTS – Universal Mobile Telecommunications System

- 3G System
- Released ~2000
- Increased data rates
  - Up to 384 kbit/s (compared to 9.6 kbit/s or 14.4 kbit/s of GSM)
  - Up to 14.4 Mbit/s (in theory) with HSDPA (enhanced UMTS)

Main difference between UMTS and GSM
- GSM: FDMA and TDMA
- UMTS: Uses CDMA

Similarities between UMTS and GSM
- UMTS uses GSM infrastructure for user databases and call setup (VLR, HLR, MSC, GMSC)

UMTS Extensions: HSPA, HSPA+ (higher data rates)
CDMA in UMTS

- **Channelization**
  - Spread signal with orthogonal codes (channelization codes)
  - Does spread the signal into a wider band
  - Used to distinguish different physical channels of one transmitter
    - For downlink, channelization code is used to separate different physical channels of one cell
    - For uplink, channelization code is used to separate different physical channels of one MS

- **Scrambling**
  - XOR the signal with a orthogonal scrambling code
  - Signal stays within the band
  - Used to distinguish different transmitters
    - For downlink, scrambling code is used to separate different cells in one carrier
    - For uplink, scrambling code is used to separate different MS in one carrier
CDMA in UMTS: Downlink

- Spread signal of each channel with channelization code
  - Multiplex different channels

- Add the signals of different data channels

- Multiply with cell specific scrambling code
  - Protect different cells from each other
CDMA in UMTS: Uplink

- Each station spreads its different channels using orthogonal channelization codes...
  - Multiplex different channels
- ...and additionally multiplies the signal with its own spreading code
  - Protect different MS from each other
OVSF codes

- Can be used to generate a set of codes with varying size
- A valid set of codes has the following property:
  For any two codes, never one should be part of the other (orthogonal property)
- Example of a valid code set: (1,-1), (1,1,-1,-1),
  (1,1,1,1,1,1,1,1),(1,1,1,1,-1,-1,-1,-1,1,1,1,1,-1,-1,-1,-1),
  (1,1,1,1,-1,-1,-1,-1,-1,-1,1,1,1,1)

SF = Spreading Factor
Different code lengths allow for different data rates!

OVSF codes

- Can be used to generate a set of codes with varying size
- A valid set of codes has the following property:
  For any two codes, never one should be part of the other (orthogonal property)
- Example of a valid code set: \((1,-1), (1,1,-1,-1), (1,1,1,1,1,1,1,1,1), (1,1,1,1,-1,-1,-1,-1,-1,1,1,1,1,-1,-1,-1,-1)

SF = Spreading Factor
Power Control

- Remember:
  - With CDMA, need to equalize power from all mobiles at the base station
  - Mobile transmission power minimized to avoid co-channel interference and save battery power

Two ways of power control in UMTS:

- Open-Loop:
  - No feedback from the BS,
  - BS transmits a pilot signal,
  - Transmitted power by MS inverse proportional to the pilot signal
  - Assumes forward and reverse link signal strength closely related

- Closed-Loop:
  - Signal strength from mobile to BS adjusted based on feedback from the BS
  - Signal strength from BS to mobile adjusted based on feedback from MS
  - Feedback: power level, SINR, error rate
LTE/4G

- Long Term Evolution
- Successor of UMTS
- New radio interface (not like HSDPA which was extending UMTS)
  - MIMO based
- Fully packet switched (in contrast to GSM and UMTS which are circuit switched)
- Uses OFDMA on downlink and SC-FDMA on uplink
- Goal: 300 Mbit/s for Download und 75 Mbit/s for Upload
- Launched by Swisscom 2012
Stations get one or more resource blocks assigned for one or more time slots.

Scheduling decision possible every 1 ms.

Stations listen on control channel to learn schedule.
PAPR Problem of OFDMA

- OFDMA can have a high peak to average power ratio (PAPR)
  - Right side of figure: subcarriers reach their minimum amplitude at the same time
- PAPR requires sophisticated amplifier and uses more power
  - No big problem for base stations
  - Problem for mobile phones
SC-FDMA on LTE uplink

- Instead of sending one symbol per subcarrier, SC-FDMA sends a mix of all symbols on all subcarriers during on slot
  - Example: send $x_1 + x_2$ on one subcarrier, and $x_1 - x_2$ on another subcarrier
- Reduces PAPR
Architecture vs Generations: GSM

Radio Access Network
- UE
- BTS
- BSC
- GERAN

FDMA/TDMA

Core Network
- Circuit Switched Domain
- GMSC
- VLR/HRL
- MSC
- PSTN

voice
Architecture vs Generations: UMTS

Radio Access Network

- **UE**
- **NodeB**
- **RNC**
- **UTRAN**
- CDMA

Core Network

- **Circuit Switched Domain**
- **Packet Switched Domain**

- **PSTN**
- **Servers, PDNs**

*data gateway infrastructure from GPRS*
Architecture vs Generations: LTE

Radio Access Network

- UE
- OFDMA
- eNB

Evolved UTRAN (E-UTRAN)

- evolved node B

Core Network

- Evolved Packet Core (ECP)
- Packet Switched Domain
  - MME
  - HSS
  - S-GW
  - P-GW

Servers, PDNs
Voice and Text Messages over LTE

Two ways of power control

- Third Party Voice over IP
  - Example: Skype or other similar applications
  - VoIP provider can send LTE signaling messages to reserve a dedicated channel
  - Little investment needed by LTE network operator (at best a partnership with the VoIP provider)

- The IP Multimedia Subsystem (IMS)
  - Separate network to control multimedia services such as VoIP
  - Uses Session Initiation Protocol (SIP) for signaling
SIP Basics

- End users (e.g., phone) identified through
  - SIP URI ('SIP:alice@sipcall.ch'), or through
  - Phone numbers

- SIP works with ENUM which provides a mapping a service for phone numbers to URIs

- SIP methods (or messages)
  - INVITE: Invites a user to join a call
  - ACK: Confirms that a client has received a final response to an INVITE
  - BYE: Terminates a call
  - REGISTER: Let's the system know about the current location of a user
SIP Architecture

- Main components: SIP proxies and location server
- Each end host has its own outbound proxy (provider specific)
  - Gateway for all SIP messages originating from a user
SIP Registration

- Happens periodically (when phone starts or moves)
- SIP user tells SIP server its current location
SIP call setup (SIP INVITE)

- SIP INVITE message has two main tasks
  - Locate the destination device
  - Exchange session parameters (TCP/IP endpoints, protocols, etc.)
SIP INVITE message

- SIP is text based
- Example of an INVITE message (basic part):

```text
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com:5060;branch=z9hG4bK776asdhds
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>; tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

- Optional part can hold information about the data protocol to be used (e.g., protocol type, code type, etc..)
References