Wireless and Mobile Networks
Background:

- # wireless (mobile) phone subscribers now exceed # wired phone subscribers!
- # wireless Internet-connected devices soon to exceed # wireline Internet-connected devices
  - laptops, Internet-enabled phones promise anytime untethered Internet access
- two important (but different) challenges
  - **wireless**: communication over wireless link
  - **mobility**: handling the mobile user who changes point of attachment to network
Elements of a wireless network

**network infrastructure**

**wireless hosts**
- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility
Elements of a wireless network

- **network infrastructure**
  - typically connected to wired network
  - relay - responsible for sending packets between wired network and wireless host(s) in its “area”
    - e.g., cell towers, 802.11 access points
Elements of a wireless network

- **network infrastructure**

- **wireless link**
  - typically used to connect mobile(s) to base station
  - also used as backbone link
  - multiple access protocol coordinates link access
  - various data rates, transmission distance
Characteristics of selected wireless link standards

- **Indoor**: 10 – 30 m
- **Outdoor**: 50 – 200 m
- **Mid-range outdoor**: 200 m – 4 Km
- **Long-range outdoor**: 5 Km – 20 Km

Data rate (Mbps):
- **2G**: 54, 5-11, 1
- **3G**: 200, 384, .056
- **3G cellular enhanced**: .056

Standards:
- **IS-95, CDMA, GSM**
- **802.15**
- **802.11b**
- **802.11a,g**
- **UMTS/WCDMA-HSDPA, CDMA2000-1xEVDO**
- **802.16 (WiMAX)**
- **802.11n**
- **802.11a,g point-to-point**
Elements of a wireless network

- **infrastructure mode**
  - base station connects mobiles into wired network
  - handoff: mobile changes base station providing connection into wired network
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
## Wireless network taxonomy

<table>
<thead>
<tr>
<th>Infrastructure (e.g., APs)</th>
<th>Single hop</th>
<th>Multiple hops</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure</strong></td>
<td><strong>host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet</strong></td>
<td><strong>host may have to relay through several wireless nodes to connect to larger Internet: <em>mesh net</em></strong></td>
</tr>
<tr>
<td></td>
<td><strong>no base station, no connection to larger Internet (Bluetooth, ad hoc nets)</strong></td>
<td><strong>no base station, no connection to larger Internet. May have to relay some other nodes to reach a dest. MANET, VANET</strong></td>
</tr>
</tbody>
</table>
Wireless Link Characteristics (1)

Differences from wired link ....

- **decreased signal strength**: radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources**: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- **multipath propagation**: radio signal reflects off objects, ground, arriving at destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”
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
Signal propagation

- Propagation in free space always like light (straight line)
- Receiving power proportional to 1/d² in vacuum - much more in real environments (d = distance between sender and receiver)
- Receiving power additionally influenced by
  - fading (frequency dependent)
  - shadowing
  - reflection at large obstacles
  - refraction depending on the density of a medium
  - scattering at small obstacles
  - diffraction at edges
shadowing  reflection  refraction  scattering  diffraction
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 depending on the phases of the different parts
Effects of mobility

- Channel characteristics change over time and location
  - signal paths change
  - different delay variations of different signal parts
  - different phases of signal parts
    ➔ quick changes in the power received (*short term fading*)

- Additional changes in
  - distance to sender
  - obstacles further away
    ➔ slow changes in the average power received (*long term fading*)
Wireless Link Characteristics (2)

- **SNR**: signal-to-noise ratio
  - larger SNR - easier to extract signal from noise (a “good thing”)

- **SNR versus BER tradeoffs**
  - *given physical layer*: increase power -> increase SNR -> decrease BER
  - *given SNR*: choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)
Digital modulation

Modulation of digital signals known as Shift Keying

- **Amplitude Shift Keying (ASK)**
  - very simple
  - low bandwidth requirements
  - very susceptible to interference

- **Frequency Shift Keying (FSK)**
  - needs larger bandwidth

- **Phase Shift Keying (PSK)**
  - more complex
  - robust against interference
Advanced Frequency Shift Keying

- special pre-computation avoids sudden phase shifts → MSK (Minimum Shift Keying)
- bit separated into even and odd bits, the duration of each bit is doubled
- depending on the bit values (even, odd) the higher or lower frequency, original or inverted is chosen
- the frequency of one carrier is twice the frequency of the other \((f_2=2f_1)\)
- even higher bandwidth efficiency using a Gaussian low-pass filter → GMSK (Gaussian MSK), used in GSM
Example of MSK

- **data:**
  - even bits: 1 1 0 1 1 0 1
  - odd bits: 0 1 0 1 0 1

- **low frequency**
- **high frequency**

- **MSK signal**

- **bit values:**
  - even: 0 1 0 1
  - odd: 0 0 1 1

- **signal values:**
  - h n n h
  - - + +

- **Explanation:**
  - h: high frequency
  - n: low frequency
  - +: original signal
  - -: inverted signal
Advanced 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
  - symbol determines shift of sine wave
  - needs less bandwidth compared to BPSK
  - more complex

- **DQPSK - Differential QPSK (IS-136, PHS)**
  - Phase shift is not relative to a reference signal but to the phase of the previous two bits
Quadrature Amplitude Modulation

- **Quadrature Amplitude Modulation (QAM):** combines amplitude and phase modulation
  - it is possible to code one symbol using \( n \) bits
  - \( 2^n \) discrete levels, \( n=2 \) identical to QPSK
  - bit error rate increases with \( n \), but less errors compared to comparable PSK schemes

Example: 16-QAM (4 bits = 1 symbol)

- Symbols 0011 and 0001 have the same phase \( \phi \), but different amplitude \( a \).
- 0000 and 1000 have different phase, but same amplitude.
→ used in standard 9600 bit/s modems
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):

Hidden terminal problem
- B, A hear each other
- B, C hear each other
- A, C cannot hear each other
  means A, C unaware of their interference at B

Signal attenuation:
- B, A hear each other
- B, C hear each other
- A, C cannot hear each other
  interfering at B
MACA - collision avoidance

MACA (Multiple Access with Collision Avoidance) uses short signaling packets for collision avoidance
- RTS (request to send): a sender requests the right to send from a receiver with a short RTS packet before it sends a data packet
- CTS (clear to send): the receiver grants the right to send as soon as it is ready to receive

Signaling packets contain
- sender address
- receiver address
- packet size

Variants of this method can be found in IEEE802.11 as DFWMAC (Distributed Foundation Wireless MAC)
MACA examples

MACA avoids the problem of hidden terminals
- A and C want to send to
- A sends RTS first
- C waits after receiving CTS from B

MACA avoids the problem of exposed terminals
- B wants to send to A, C to another terminal
- now C does not have to wait for it cannot receive CTS from A
MACA variant: DFWMAC in IEEE802.11

sender

idle

packet ready to send; RTS

wait for the right to send

RxBusy

time-out; RTS

wait for ACK

ACK

time-out

NAK; RTS

CTS; data

receiver

idle

data; ACK

time-out

data; NAK

wait for data

ACK: positive acknowledgement

NAK: negative acknowledgement

RxBusy: receiver busy

RTS; CTS

RTS; RxBusy
Multiplexing

- Multiplexing in 4 dimensions
  - space \((s_i)\)
  - time \((t)\)
  - frequency \((f)\)
  - code \((c)\)

- Goal: multiple use of a shared medium

- Important: guard spaces needed!
**Frequency multiplex**

- Separation of the whole spectrum into smaller frequency bands
  A channel gets a certain band of the spectrum for the whole time

- Advantages:
  - no dynamic coordination necessary
  - works also for analog signals

- Disadvantages:
  - waste of bandwidth if the traffic is distributed unevenly
  - inflexible
  - guard spaces
Frequency multiplex
Time multiplex

- A channel gets the whole spectrum for a certain amount of time

- Advantages:
  - only one carrier in the medium at any time
  - throughput high even for many users

- Disadvantages:
  - precise synchronization necessary
Time multiplex
Time and frequency multiplex

- Combination of both methods
  - A channel gets a certain frequency band for a certain amount of time
  - Example: GSM

- Advantages:
  - better protection against tapping
  - protection against frequency selective interference
  - higher data rates compared to code multiplex
  - but, precise coordination required
Time and frequency multiplex
Code multiplex

- Each channel has a unique code
- All channels use the same spectrum at the same time

Advantages:
- bandwidth efficient
- no coordination and synchronization necessary
- good protection against interference and tapping

Disadvantages:
- lower user data rates
- more complex signal regeneration

Implemented using spread spectrum technology
Code Multiplex

\[ k_1 \quad k_2 \quad k_3 \quad k_4 \quad k_5 \quad k_6 \]
Code Division Multiple Access (CDMA)

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- unique “code” assigned to each user; i.e., code set partitioning
- all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
- \textit{encoded signal} = (original data) X (chipping sequence)
- \textit{decoding}: inner-product of encoded signal and chipping sequence
- allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)}
Advantages:
- all terminals can use the same frequency, no planning needed
- huge code space (e.g. $2^{32}$) compared to frequency space
- interferences (e.g. white noise) is not coded
- forward error correction and encryption can be easily integrated

Disadvantages:
- Higher complexity of a receiver (receiver cannot just listen into the medium and start receiving if there is a signal)
- All signals should have the same strength at a receiver
- Good code for CDMA?
  - Should be **orthogonal** to other codes
  - Should have a good **autocorrelation**
Two vectors are called orthogonal if their inner product is 0.

1) Vectors $(2, 5, 0)$ and $(0, 0, 17)$ $\implies$ Orthogonal
   \[(2, 5, 0) \cdot (0, 0, 17) = 0 + 0 + 0 = 0\]

   Vectors $(3, -2, 4)$ and $(-2, 3, 3)$ $\implies$ Orthogonal
   \[(3, -2, 4) \cdot (-2, 3, 3) = -6 - 6 + 12 = 0\]

2) Vectors $(1, 2, 3)$ and $(4, 2, -6)$ $\implies$ Not orthogonal
   \[(1, 2, 3) \cdot (4, 2, -6) = 4 + 4 - 18 = -10 \neq 0\]

3) Vectors $(1, 2, 3)$ and $(4, 2, -3)$ $\implies$ Almost orthogonal
   \[(1, 2, 3) \cdot (4, 2, -3) = 4 + 4 - 9 = -1 \approx 0\]
CDMA Encode/Decode

**Sender**

Data bits:
- \( d_1 = -1 \)
- \( d_0 = 1 \)

Code:
- Slot 1: 1 1 1 1 -1 -1 -1
- Slot 0: 1 1 1 1 -1 -1 -1

**Receiver**

Received input:
- Slot 1: 1 1 1 1 -1 -1 -1
- Slot 0: 1 1 1 1 -1 -1 -1

Code:
- Slot 1: 1 1 1 1 -1 -1 -1
- Slot 0: 1 1 1 1 -1 -1 -1

Channel output

- \( Z_{i,m} = d_i \cdot c_m \)
- Slot 1 channel output: 1 1 1 1 -1 -1 -1
- Slot 0 channel output: 1 1 1 1 -1 -1 -1

**Equations**

- For sender:
  \( D_i = \sum_{m=1}^{M} Z_{i,m} \cdot c_m \)

- For receiver:
  \( d_1 = -1 \)
  \( d_0 = 1 \)
CDMA: two-sender interference

senders

data bits
- $d_0 = 1$
- $d_1 = -1$

code
- 1 1 1 1
- -1 -1 -1 -1

$Z_{i,m}^1 = d_i \cdot c_m^1$

channel, $Z_{i,m}^*$

$Z_{i,m}^2 = d_i \cdot c_m^2$

receiver 1

$M$

$\phi_i^1 = \sum_{m=1}^{M} Z_{i,m}^* \cdot c_m^1$

$\phi_i = 1$

slot 1 received input
- 2 2 2 2 2

slot 0 received input
- 2 2 2 2 2
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
- protection against narrow band interference
Spread spectrum technology

Side effects:
- coexistence of several signals without dynamic coordination
- tap-proof

Alternatives: Direct Sequence, Frequency Hopping
Effects of spreading and interference

i) Effects on the sender

ii) Effects on the user signal

iii) Narrowband interference on the receiver

iv) Broadband interference on the receiver

v) Interference on the user signal
Spreading and frequency selective fading

channel quality

1 2 3 4 5 6

frequency

narrow band signal

guard space

spread spectrum channels

channel quality

1

spread spectrum

frequency
DSSS (Direct Sequence Spread Spectrum)

XOR of the signal with pseudo-random number, chipping sequence
- many chips per bit (e.g., 128) result in higher bandwidth of the signal

Advantages
- reduces frequency selective fading
- in cellular networks
  - base stations can use the same frequency range
  - several base stations can detect and recover the signal
  - soft handover

Disadvantages
- precise power control necessary

\[ \text{user data XOR chipping sequence} = \text{resulting signal} \]

\[ t_b: \text{bit period} \]
\[ t_c: \text{chip period} \]
DSSS (Direct Sequence 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

Disadvantages
- not as robust as DSSS
- simpler to detect
FHSS (Frequency Hopping Spread Spectrum)

- User data
  - Slow hopping (3 bits/hop)
  - Fast hopping (3 hops/bit)

$t_b$: bit period  
$t_d$: dwell time
FHSS (Frequency Hopping Spread Spectrum)
IEEE 802.11 Wireless LAN

- **802.11b**
  - 2.4 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code

- **802.11a**
  - 5 GHz range
  - up to 54 Mbps

- **802.11g**
  - 2.4 GHz range
  - up to 54 Mbps

- **802.11n**: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions
802.11 LAN architecture

- Wireless host communicates with base station
  - Base station = access point (AP)
- Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
  - Wireless hosts
  - Access point (AP): base station
  - Ad hoc mode: hosts only
IEEE standard 802.11
802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP’s name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically run DHCP to get IP address in AP’s subnet
802.11: passive/active scanning

**Passive Scanning:**
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: selected AP to H1

**Active Scanning:**
1. Probe Request frame broadcast from H1
2. Probes response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: selected AP to H1
IEEE 802.11: multiple access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don’t collide with ongoing transmission by other node
- 802.11: no collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can’t sense all collisions in any case: hidden terminal, fading
- goal: avoid collisions: CSMA/C(ollision)A(voidance)
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1. If sense channel idle for DIFS then
   transmit entire frame (no CD)
2. If sense channel busy then
   start random backoff time
   timer counts down while channel idle
   transmit when timer expires
   if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- If frame received OK
  return ACK after SIFS (ACK needed due to hidden terminal problem)
802.11 - competing stations - simple version

- **DIFS**: Distributed Inter-Frame Space
- **bo_e**: elapsed backoff time
- **bo_r**: residual backoff time
- **busy**: medium not idle (frame, ack etc.)
- **packet arrival at MAC**: "\[\]"
Avoiding collisions (more)

**idea:** allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Avoid data frame collisions completely using small reservation packets!
Collision Avoidance: RTS-CTS exchange
802.11 frame: addressing

- frame control
- duration
- address 1
- address 2
- address 3
- seq control
- address 4
- payload
- CRC

- frame seq #
  (for RDT)

- duration of reserved transmission time (RTS/CTS)

- frame type
  (RTS, CTS, ACK, data)

- Protocol version
- Type
- Subtype
- To DS
- From DS
- More frag
- Retry
- Power mgt
- More data
- WEP
- Rsvd
## MAC address format

<table>
<thead>
<tr>
<th>scenario</th>
<th>to DS</th>
<th>from DS</th>
<th>address 1</th>
<th>address 2</th>
<th>address 3</th>
<th>address 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>ad-hoc network</td>
<td>0</td>
<td>0</td>
<td>DA</td>
<td>SA</td>
<td>BSSID</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, from AP</td>
<td>0</td>
<td>1</td>
<td>DA</td>
<td>BSSID</td>
<td>SA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, to AP</td>
<td>1</td>
<td>0</td>
<td>BSSID</td>
<td>SA</td>
<td>DA</td>
<td>-</td>
</tr>
<tr>
<td>infrastructure network, within DS</td>
<td>1</td>
<td>1</td>
<td>RA</td>
<td>TA</td>
<td>DA</td>
<td>SA</td>
</tr>
</tbody>
</table>

**DS:** Distribution System  
**AP:** Access Point  
**DA:** Destination Address  
**SA:** Source Address  
**BSSID:** Basic Service Set Identifier  
**RA:** Receiver Address  
**TA:** Transmitter Address
802.11 frame: addressing

802.11 frame:
- AP MAC addr
- H1 MAC addr
- R1 MAC addr

802.3 frame:
- R1 MAC addr
- H1 MAC addr

dest. address
source address

address 1
address 2
address 3
802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which switch port can be used to reach H1
802.11: advanced capabilities

**Rate Adaptation**

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

1. SNR decreases, BER increase as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER
802.11: advanced capabilities

Power Management

- node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame

- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame
Power management

Idea: switch the transceiver off if not needed
States of a station: sleep and awake

Timing Synchronization Function (TSF)
- stations wake up at the same time

Infrastructure
- Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP

Ad-hoc
- Ad-hoc Traffic Indication Map (ATIM)
  - announcement of receivers by stations buffering frames
  - more complicated - no central AP
  - collision of ATIMs possible (scalability?)
Power saving with wake-up patterns (infrastructure)
Power saving with wake-up patterns (ad-hoc)
802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps
**802.16: WiMAX**

- **like 802.11 & cellular: base station model**
  - transmissions to/from base station by hosts with omnidirectional antenna
  - base station-to-base station backhaul with point-to-point antenna

- **unlike 802.11:**
  - range ~ 6 miles (“city rather than coffee shop”)
  - ~14 Mbps
802.16: WiMAX: downlink, uplink scheduling

- transmission frame
  - down-link subframe: base station to node
  - uplink subframe: node to base station

- WiMAX standard provide mechanism for scheduling, but not scheduling algorithm
Components of cellular network architecture

**MSC**
- connects cells to wide area net
- manages call setup (more later!)
- handles mobility (more later!)

**Cell**
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface*: physical and link layer protocol between mobile and BS
Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

- **combined FDMA/TDMA:** divide spectrum in frequency channels, divide each channel into time slots
- **CDMA:** code division multiple access
Cellular standards: brief survey

2G systems: voice channels

- **IS-136 TDMA**: combined FDMA/TDMA (North America)
- **GSM**: global system for mobile communications; combined FDMA/TDMA
  - most widely deployed
- **IS-95 CDMA**: code division multiple access

Don’t drown in a bowl of alphabet soup: use this for reference only
Cellular standards: brief survey

2.5 G systems: voice and data channels

- for those who can’t wait for 3G service: 2G extensions
- general packet radio service (GPRS)
  - evolved from GSM
  - data sent on multiple channels (if available)
- enhanced data rates for global evolution (EDGE)
  - also evolved from GSM, using enhanced modulation
  - data rates up to 384K
- CDMA-2000 (phase 1)
  - data rates up to 144K
  - evolved from IS-95
Cellular standards: brief survey

3G systems: voice/data

- Universal Mobile Telecommunications Service (UMTS)
  - data service: High Speed Uplink/Downlink packet Access (HSDPA/HSUPA)
- CDMA-2000: CDMA in TDMA slots
  - data service: 1xEvolution Data Optimized (1xEVDO) up to 14 Mbps
2G (voice) network architecture

Legend:
- Base transceiver station (BTS)
- Base station controller (BSC)
- Mobile Switching Center (MSC)
- Mobile subscribers
- Public telephone network

Base station system (BSS)

MSC

Gateway MSC
2.5G (voice+data) network architecture

Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

- voice network unchanged in core
- data network operates in parallel
Components of cellular network architecture

recall:

different cellular networks, operated by different providers
Handling mobility in cellular networks

- **home network**: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - **home location register (HLR)**: database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)

- **visited network**: network in which mobile currently resides
  - **visitor location register (VLR)**: database with entry for each user currently in network
  - could be home network
GSM: indirect routing to mobile

1. Call routed to home network
2. Home MSC consults HLR, gets roaming number of mobile in visited network
3. Home MSC sets up 2nd leg of call to MSC in visited network
4. MSC in visited network completes call through base station to mobile

Public switched telephone network

Mobile Switching Center

Home MSC consults HLR, gets roaming number of mobile in visited network

Home MSC sets up 2nd leg of call to MSC in visited network

MSC in visited network completes call through base station to mobile

Home Switching Center

Mobile

User
**GSM: handoff with common MSC**

- **Handoff goal:** route call via new base station (without interruption)

- **reasons for handoff:**
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - **GSM** doesn’t mandate why to perform handoff (policy), only how (mechanism)

- **handoff initiated by old BSS**
**GSM: handoff with common MSC**

1. old BSS informs MSC of impending handoff, provides list of 1+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call
8. MSC-old-BSS resources released
**GSM: handoff between MSCs**

- **anchor MSC**: first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain
**GSM: handoff between MSCs**

- **anchor MSC**: first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- IS-41 allows optional path minimization step to shorten multi-MSC chain

- **MSC**
  - Home MSC
  - anchor MSC
  - PSTN

(b) after handoff