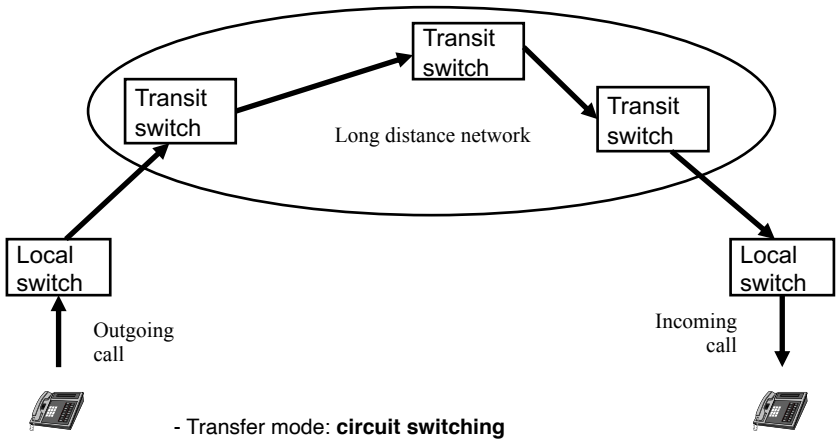
MOBILE COMPUTING

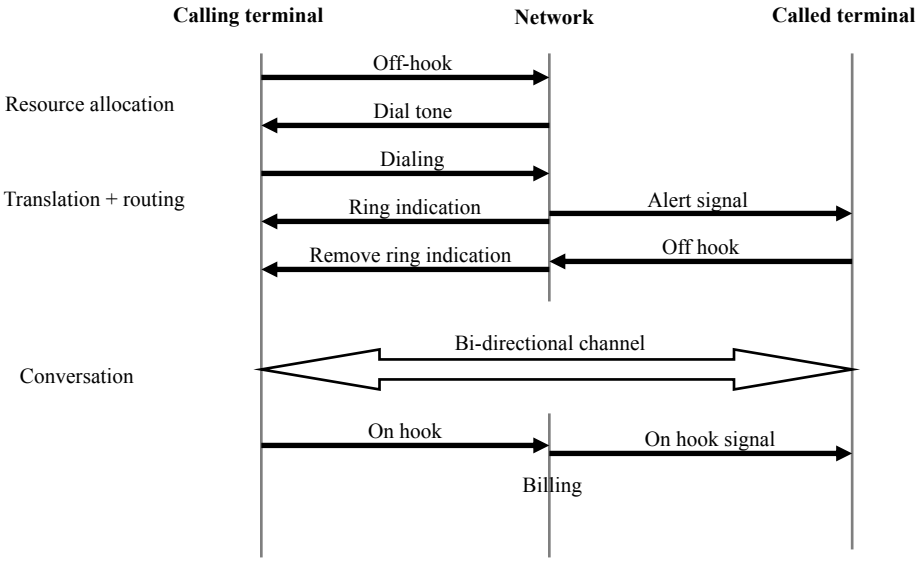
CSE 40814/60814
Spring 2021

Public Switched Telephone Network - PSTN



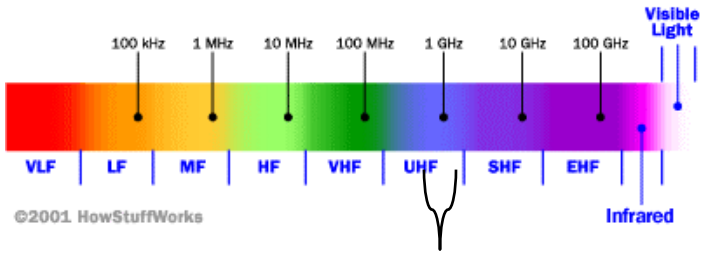
- Transfer mode: **circuit switching**
- All the network (except part of the access network) is digital
- Each voice channel is usually 64kb/s

Basic Call



Cellular Network Basics

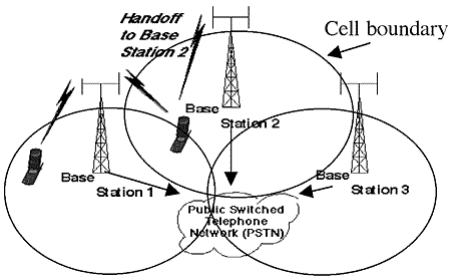
- Cellular network/telephony is a *radio*-based technology; radio waves are electromagnetic waves that *antennas* propagate
- Most signals are in the 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz frequency bands



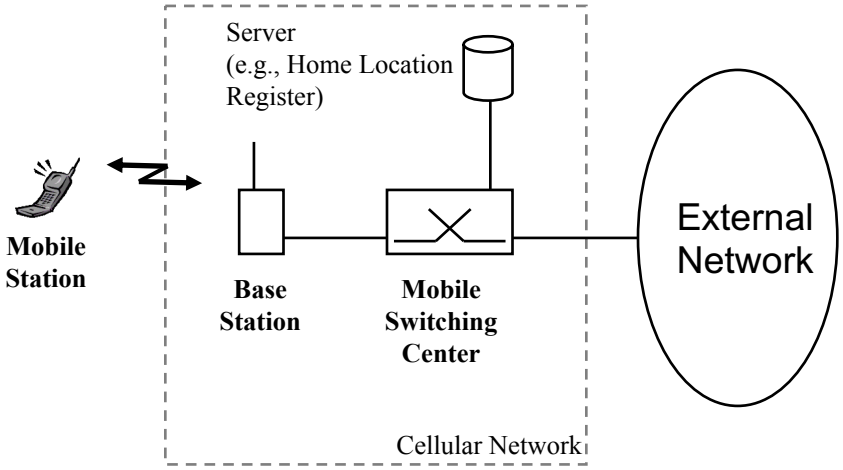
Cell phones operate in this frequency range (note the *logarithmic* scale)

Cellular Network

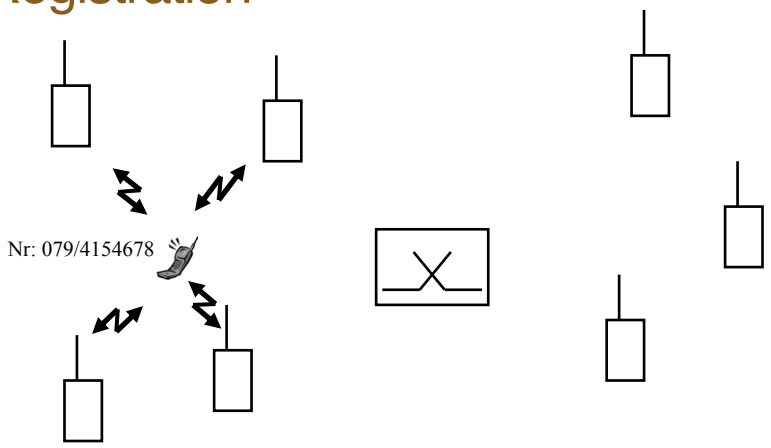
- **Base stations** transmit to and receive from mobile devices at the assigned spectrum
  - Multiple base stations use the same spectrum (**spectral reuse**)
- The service area of each base station is called a **cell**
- Each mobile terminal is typically served by the 'closest' base stations
  - **Handoff** when terminals move



Architecture of Cellular Networks

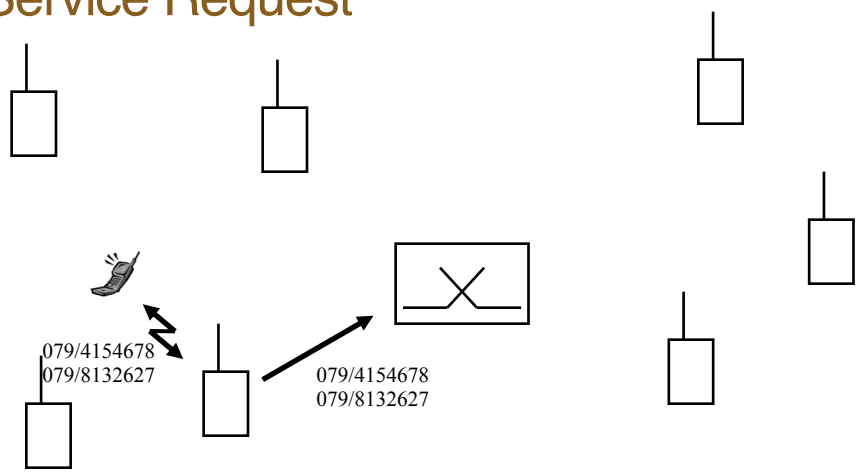


Registration

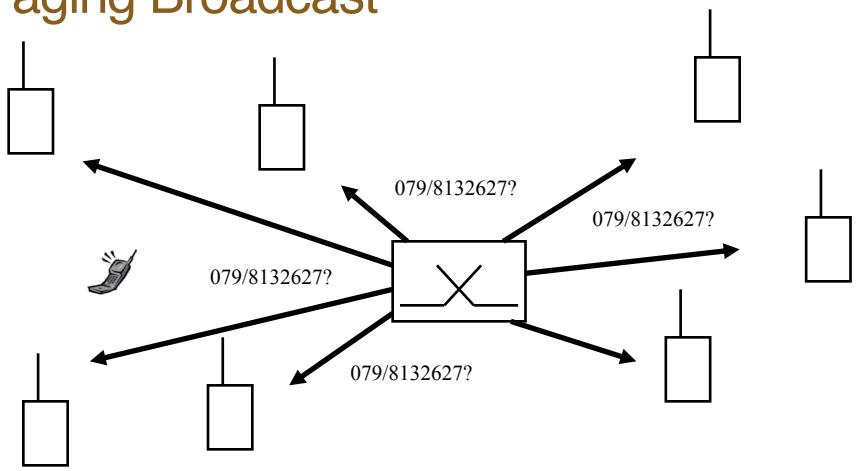


Tune on the strongest signal

Service Request

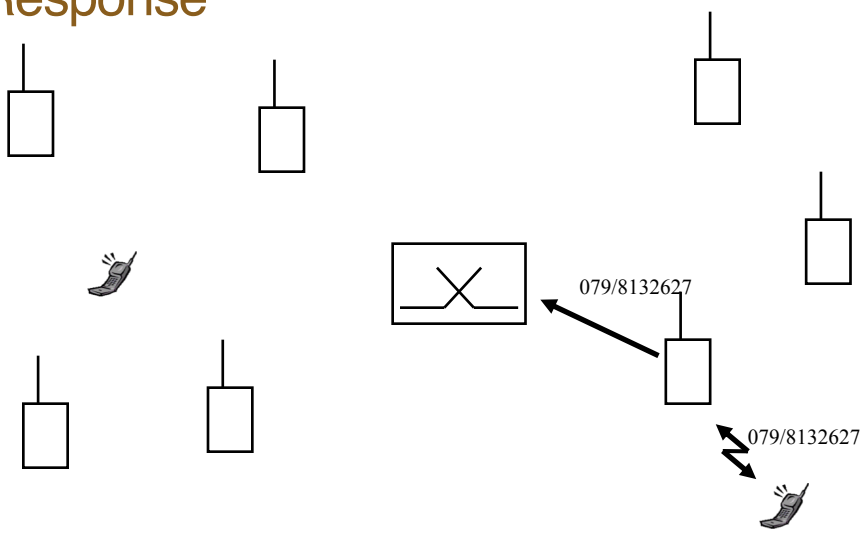


Paging Broadcast

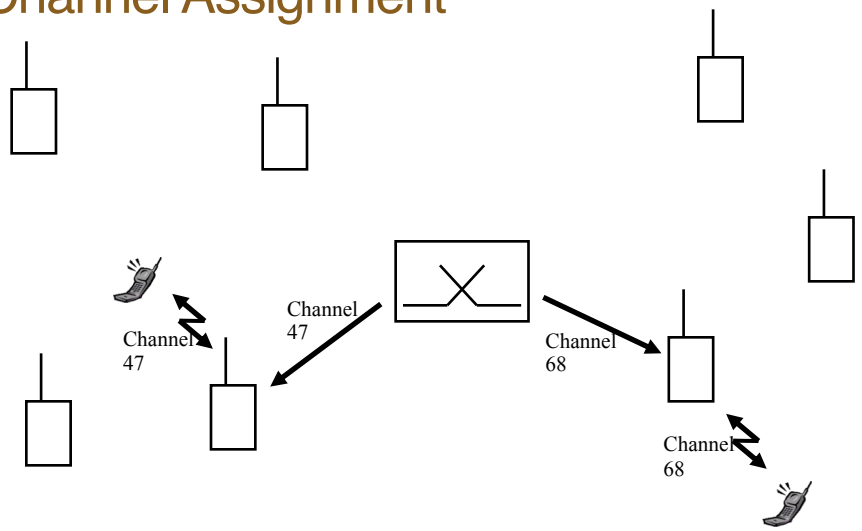


Note: paging makes sense only over a *small* area

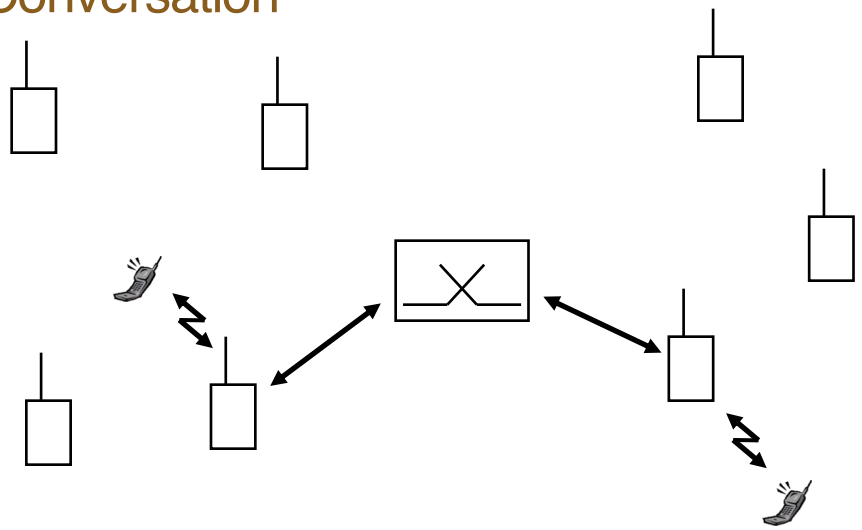
Response



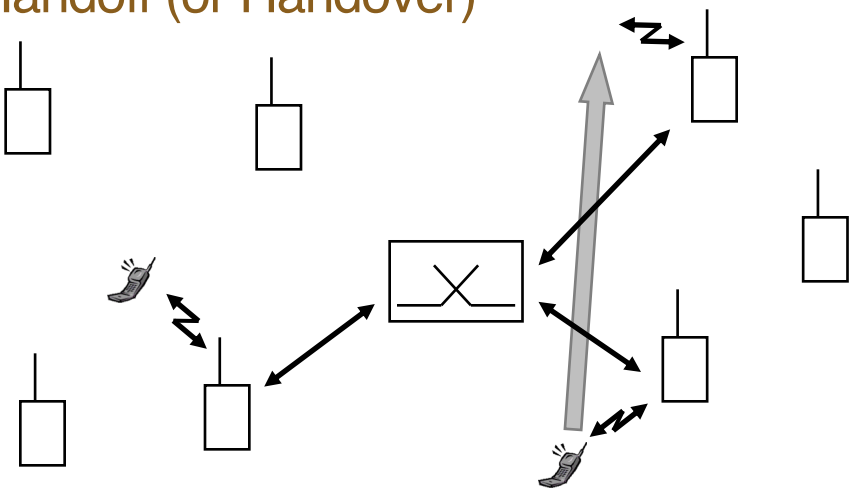
Channel Assignment



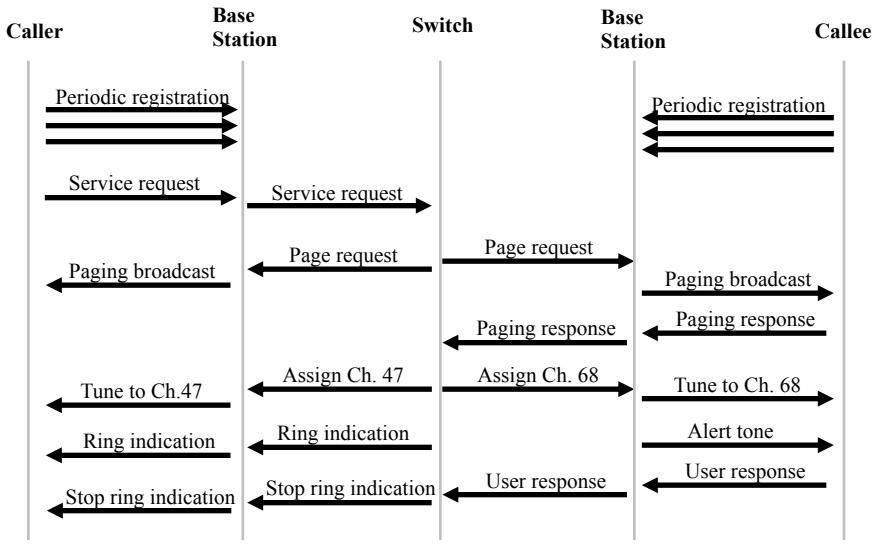
Conversation



Handoff (or Handover)



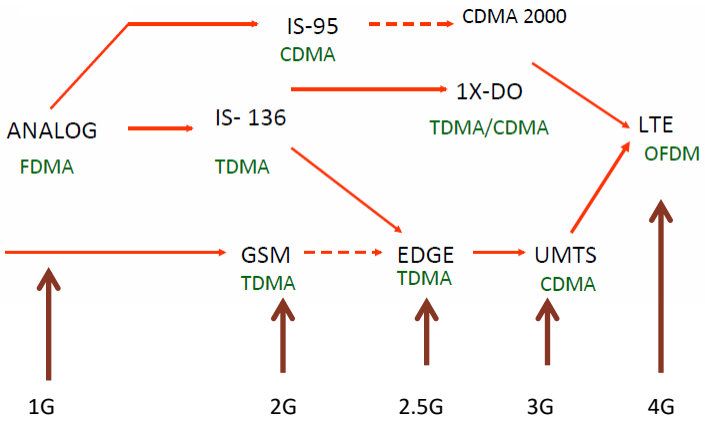
Message Sequence Chart



Cellular Network Generations

- It is useful to think of a cellular network in terms of ***generations***:
  - 0G: Briefcase-size mobile radio telephones
  - 1G: *Analog* cellular telephony
  - 2G: *Digital* cellular telephony
  - 3G: *High-speed* digital cellular telephony (including *video telephony*)
  - 4G: IP-based "anytime, anywhere" voice, data, and multimedia telephony at *faster* data rates than 3G (being deployed now)

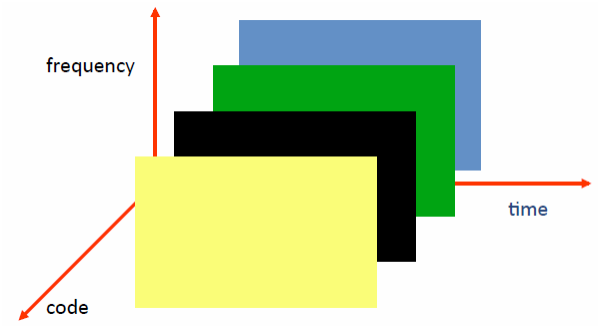
Evolution of Cellular Networks



The Multiple Access Problem

- The base stations need to serve many mobile terminals at the same time (both downlink and uplink)
- All mobiles in the cell need to transmit to the base station
- Interference among different senders and receivers
- So we need **multiple access scheme**

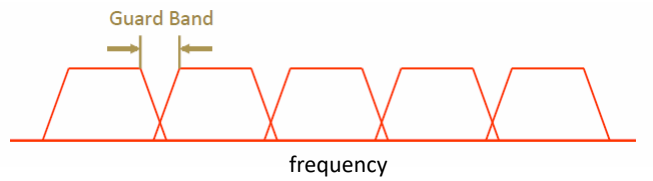
Multiple Access Schemes



3 orthogonal schemes:

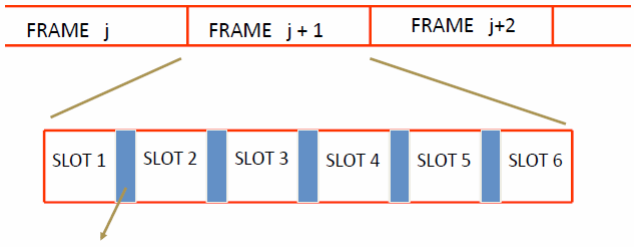
- Frequency Division Multiple Access (FDMA)
- Time Division Multiple Access (TDMA)
- Code Division Multiple Access (CDMA)

Frequency Division Multiple Access



- **Each mobile is assigned a separate frequency channel for the duration of the call**
- Sufficient **guard band** is required to prevent adjacent channel interference
- Usually, mobile terminals will have **one downlink frequency band and one uplink frequency band**
- Different cellular network protocols use different frequencies
- Frequency is a precious and scarce resource
  - Cognitive radio research

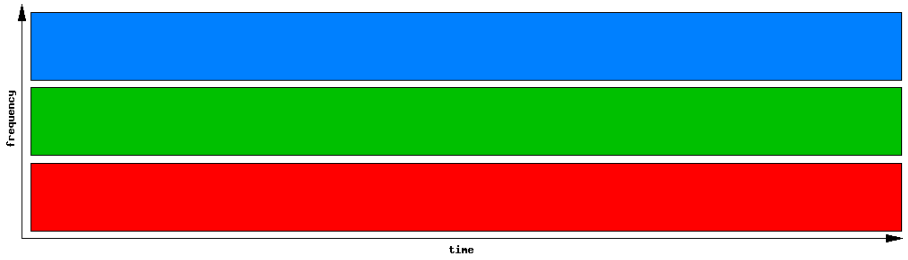
Time Division Multiple Access



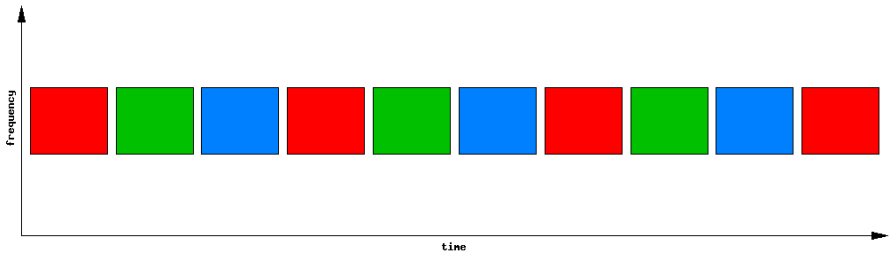
Guard time – signals transmitted by mobile terminals at different locations do not arrive at the base station at the same time

- Time is divided into **slots** and only one mobile terminal transmits during each slot
- Each user is given a specific slot. No competition in cellular network
  - Unlike Carrier Sensing Multiple Access (CSMA) in Wi-Fi

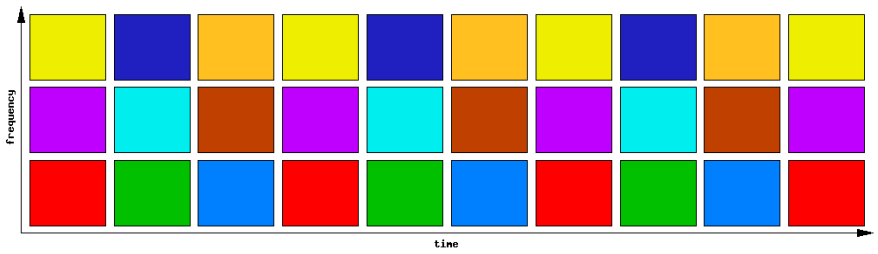
FDMA (1G)



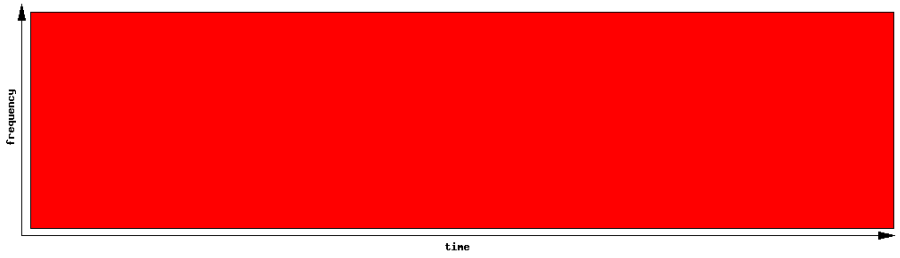
TDMA



F/TDMA (2G)

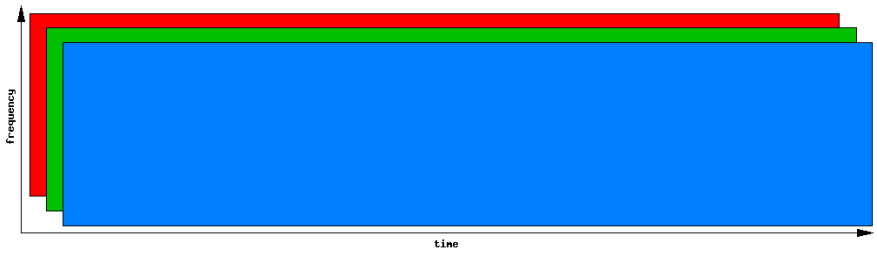


CDMA

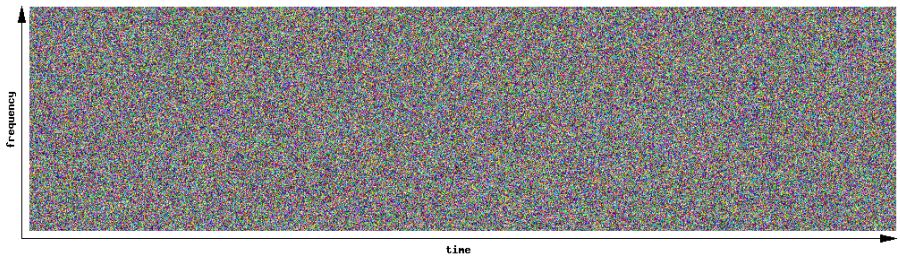


Uses the whole band!

CDMA (sometimes shown like this:)

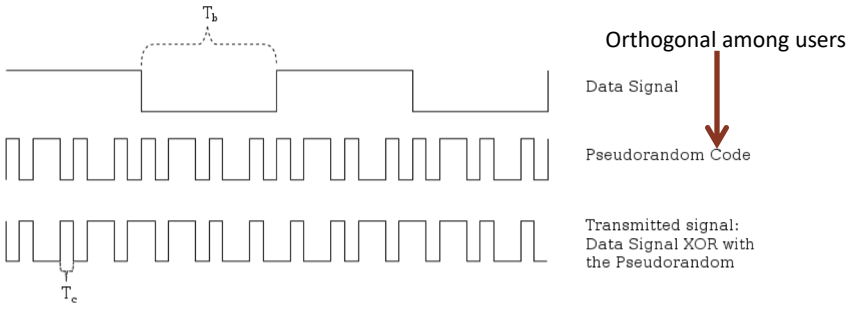


CDMA (3G) (or this:)



Code Division Multiple Access

- Use of **orthogonal codes** to separate different transmissions
- Each symbol of bit is transmitted as a larger number of bits using a user-specific code – **spreading**
  - Bandwidth occupied by the signal is much larger than the information transmission rate
  - But all users use the same frequency band together



Basics: Some Math

1	1	-1	-1
x	x	x	x
1	-1	1	-1
=	=	=	=
1	-1	-1	1

CDMA Example

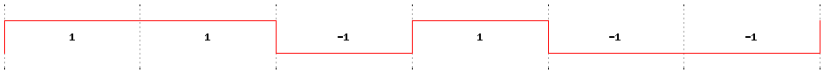
Low-Bandwidth Signal:

High-Bandwidth Spreading Code:

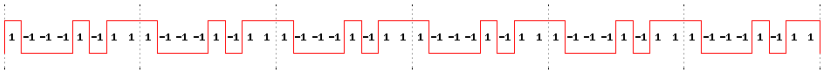
...repeated...

CDMA Example

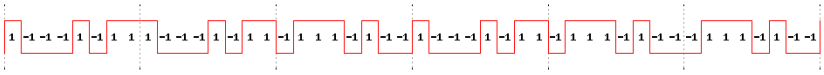
Low-Bandwidth Signal:



High-Bandwidth Spreading Code:



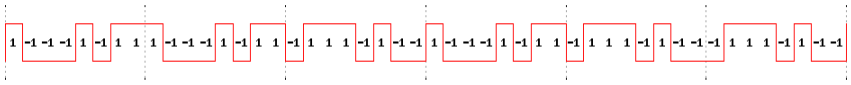
Mix is a simple multiplication



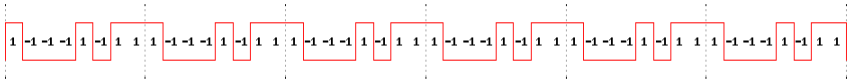
… and then transmit.

CDMA Example

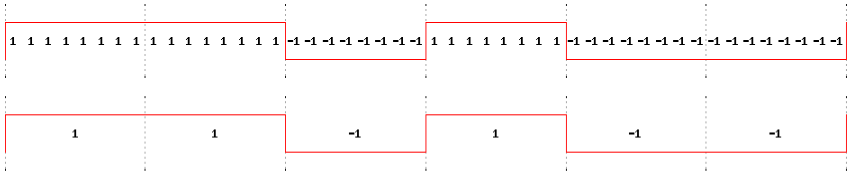
To Decode / Receive, take the signal:



Multiply by the **same** Spreading Code:

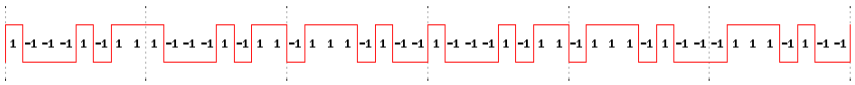


… to get ...

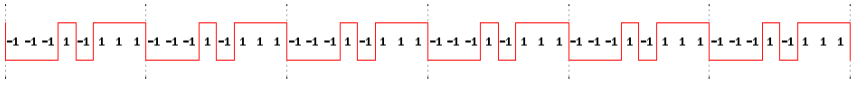


What If We Use Wrong Code?

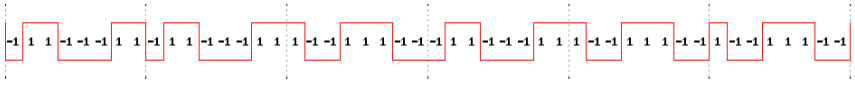
Take the same signal:



Multiply by the **wrong** Spreading Code:



… you get ...



… which clearly hasn't recovered the original signal.
Using wrong code is like being off-frequency.

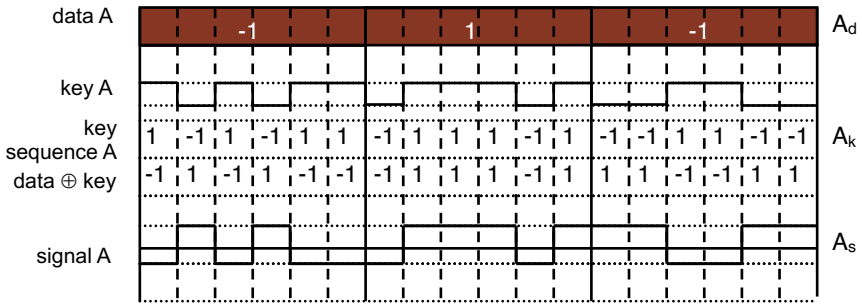
CDMA

- Requires right code AND accurate timing!

CDMA in theory

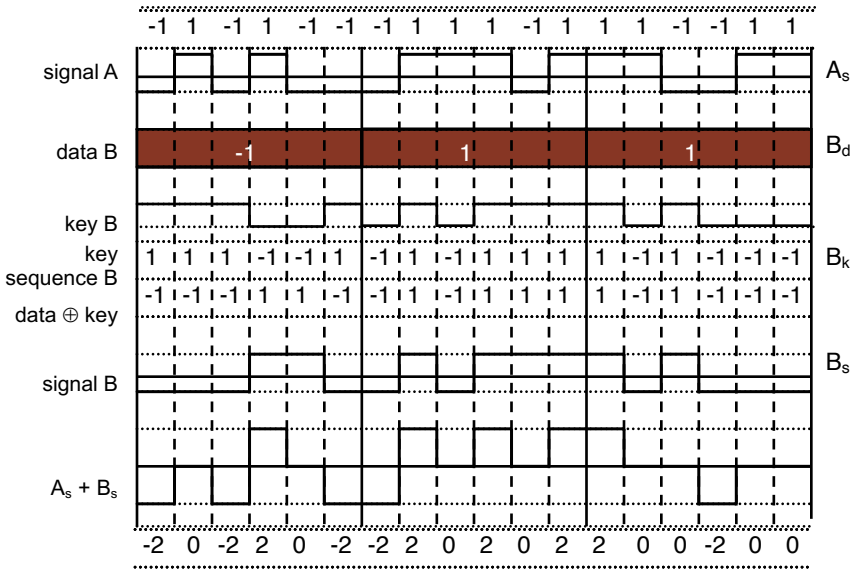
- Sender A
  - sends A_d = 1, key A_k = 010011 (assign: “0”= -1, “1”= +1)
  - sending signal $A_s = A_d * A_k$ = (-1, +1, -1, -1, +1, +1)
- Sender B
  - sends B_d = 0, key B_k = 110101 (assign: “0”= -1, “1”= +1)
  - sending signal $B_s = B_d * B_k$ = (-1, -1, +1, -1, +1, -1)
- Both signals superimpose in space
  - interference neglected (noise etc.)
  - $A_s + B_s$ = (-2, 0, 0, -2, +2, 0)
- Receiver wants to receive signal from sender A
  - apply key A_k bitwise (inner product)
    - A_e = (-2, 0, 0, -2, +2, 0) • A_k = 2 + 0 + 0 + 2 + 2 + 0 = 6
    - result greater than 0, therefore, original bit was “1”
  - receiving B
    - B_e = (-2, 0, 0, -2, +2, 0) • B_k = -2 + 0 + 0 - 2 - 2 + 0 = -6, i.e. “0”

CDMA on signal level I

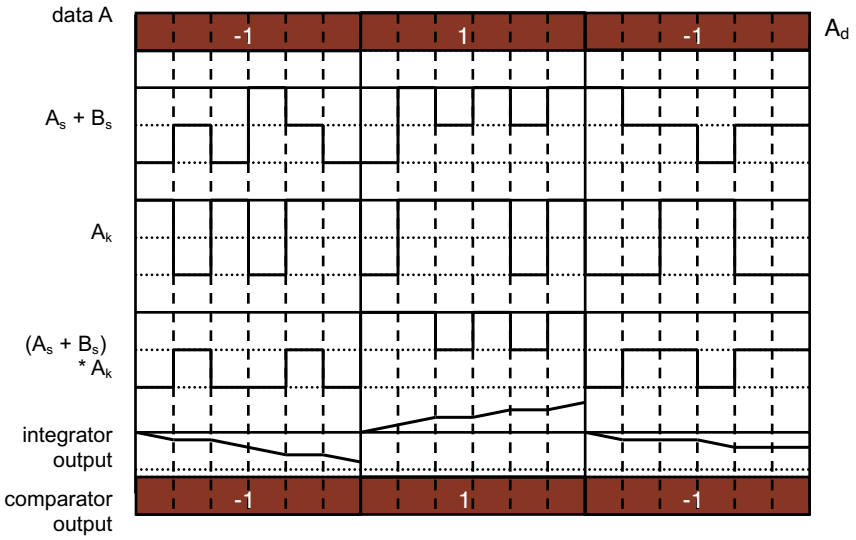


Real systems use much longer keys resulting in a larger distance between single code words in code space.

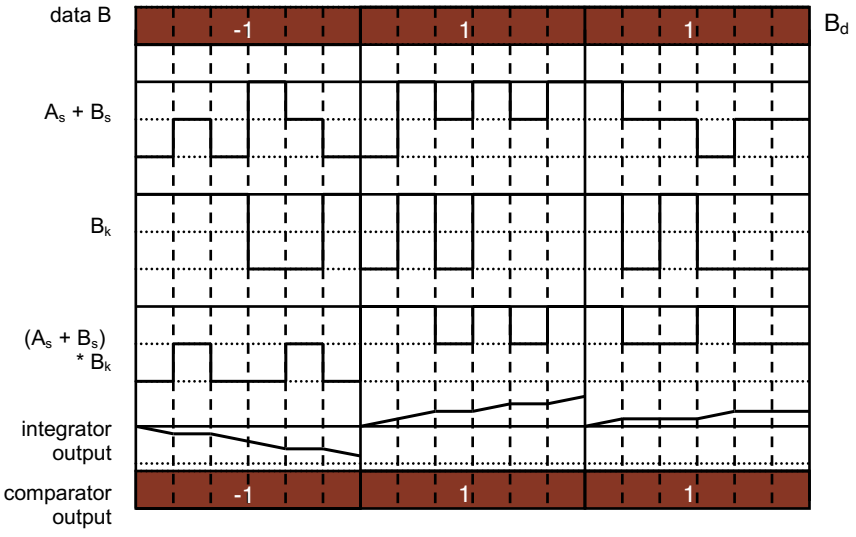
CDMA on signal level II



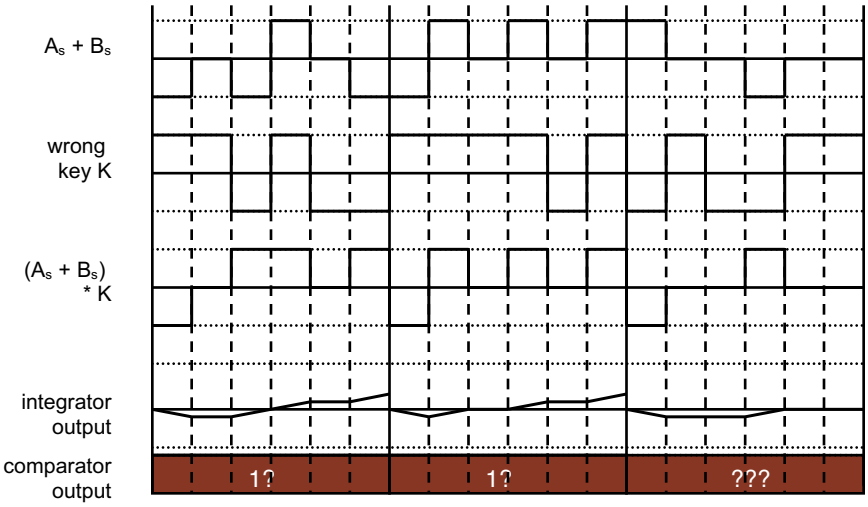
CDMA on signal level III



CDMA on signal level IV



CDMA on signal level V



Access method CDMA

- CDMA (Code Division Multiple Access)
  - all terminals send on the same frequency probably at the same time and can use the whole bandwidth of the transmission channel
  - each sender has a unique random number, the sender XORs the signal with this random number
  - the receiver can “tune” into this signal if it knows the pseudo random number, tuning is done via a correlation function
- 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
- 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

GSM (2G)

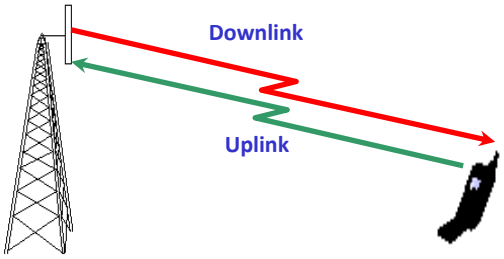
- Abbreviation for Global System for Mobile Communications
- Concurrent development in USA and Europe in the 1980s
- The European system was called GSM and deployed in the early 1990s

GSM Services

- Voice, 3.1 kHz
- **Short Message Service (SMS)**
  - 1985 GSM standard that allows messages of at most 160 chars. (incl. spaces) to be sent between handsets and other stations
  - Multi-billion $ industry
- General Packet Radio Service (GPRS)
  - GSM upgrade that provides IP-based packet data transmission up to 114 kbps
  - Users can “simultaneously” make calls and send data
  - GPRS provides “always on” Internet access and the Multimedia Messaging Service (MMS) whereby users can send rich text, audio, video messages to each other
  - Performance degrades as number of users increase
  - GPRS is an example of **2.5G telephony – 2G service similar to 3G**

GSM Channels

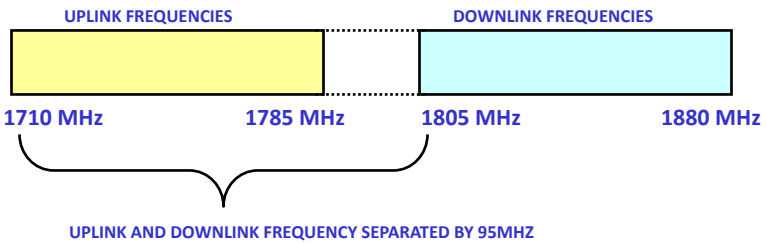
Channels



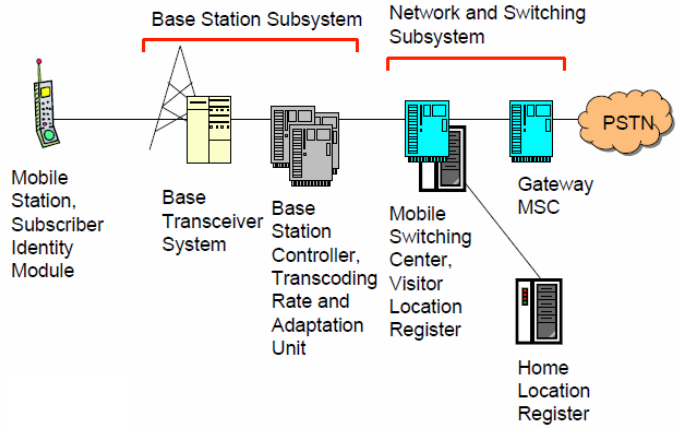
- Physical Channel: Each timeslot on a carrier is referred to as a physical channel
- Logical Channel: Variety of information is transmitted between the MS and BTS. Different types of logical channels:
  - Traffic channel
  - Control Channel

GSM Frequencies

- Originally designed on 900MHz range, now also available on 800MHz, 1800MHz and 1900 MHz ranges.
- **Separate uplink and downlink frequencies**
  - One example channel on the 1800 MHz frequency band, where RF carriers are spaced every 200 kHz



GSM Architecture

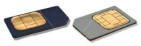


Mobile Station (MS)

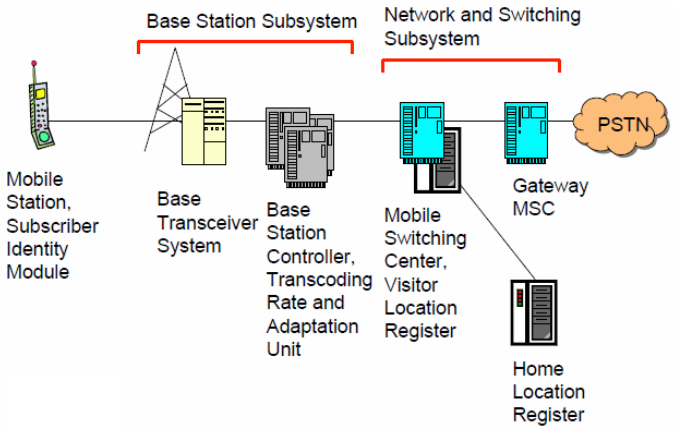
- MS is the user's handset and has two parts
- Mobile Equipment
  - Radio equipment
  - User interface
  - Processing capability and memory required for various tasks
    - Call signalling
    - Encryption
    - SMS
  - Equipment **IMEI** (Intl. Mobile Equipment Identity) number (like serial number)
- Subscriber Identity Module (SIM)

Subscriber Identity Module

- A small smart card
- Subscriber **IMSI** (Intl. Mobile Subscriber Identity) number
  - 64 bit number; includes:
  - MCC (Mobile Country Code): 3 decimal places, intl. standardized
  - MNC (Mobile Network Code): 2 decimal places, network within country
  - MSIN (Mobile Subscriber Identification Number): max. 10 decimal places
- Subscriber's own information (telephone directory)
- Can also be used in other systems besides GSM, e.g., some WLAN access points accept SIM based user authentication



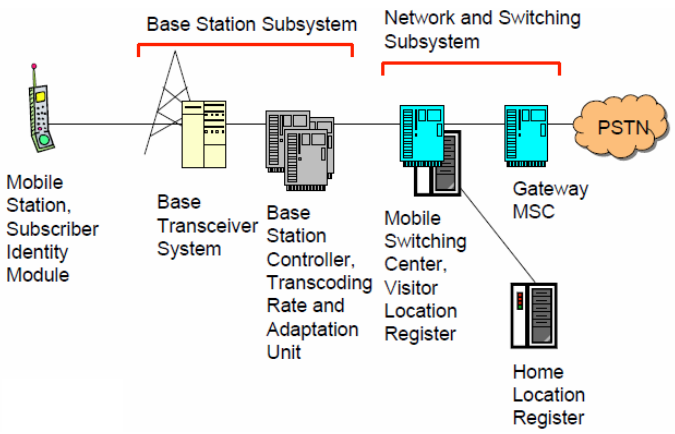
GSM Architecture



Base Station Subsystem

- Transcoding Rate and Adaptation Unit (TRAU)
  - Performs coding between the 64kbps PCM coding used in the backbone network and the 13kbps coding used for the Mobile Station (MS)
- Base Station Controller (BSC)
  - Controls the channel (time slot) allocation implemented by the BTSes
  - Manages the handovers within BSS area
  - Knows which mobile stations are within the cell and informs the MSC/VLR about this
- Base Transceiver System (BTS)
  - Controls several transmitters
  - Each transmitter has 8 time slots (some used for signaling) on a specific frequency

GSM Architecture



Network and Switching Subsystem

- The backbone of a GSM network is a telephone network with additional cellular network capabilities
- **Mobile Switching Center (MSC)**
  - A typical telephony exchange (ISDN exchange) which supports mobile communications
  - **Visitor Location Register (VLR)**
    - A database, part of the MSC
    - Contains the location of the active Mobile Stations
- **Gateway Mobile Switching Center (GMSC)**
  - Links the system to PSTN and other operators
- **Home Location Register (HLR)**
  - Contain subscriber information, including authentication information in Authentication Center (AuC)
- Equipment Identity Register (EIR)
  - International Mobile Station Equipment Identity (IMEI) codes, e.g., for blacklisting stolen phones

Home Location Register

- One database per operator
- Contains all the permanent subscriber information
  - MSISDN (Mobile Subscriber ISDN number) is the telephone number of the subscriber
  - International Mobile Subscriber Identity (IMSI) is a 15 digit code used to identify the subscriber
  - IMSI code is used to link the MSISDN number to the subscriber's SIM (Subscriber Identity Module)
  - Charging information
  - Services available to the customer
- Also the subscriber's present Location Area Code, which refers to the MSC, which can connect to the MS

Other Systems

- Operations Support System
  - The management network for the whole GSM network
  - Usually vendor dependent
  - Very loosely specified in the GSM standards
- Value added services
  - Voice mail
  - Call forwarding
  - Group calls
- Short Message Service Center
  - Stores and forwards the SMS messages
  - Like an E-mail server
  - Required to operate the SMS services

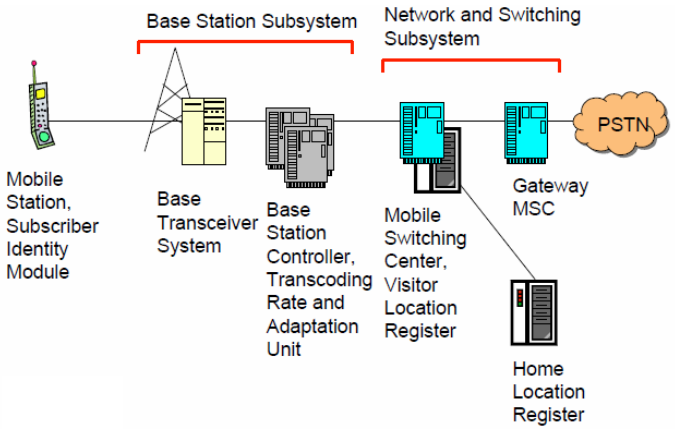
Location Updates

- The cells overlap and usually a mobile station can ‘see’ several transceivers (BTSes)
- The MS monitors the identifier for the BSC controlling the cells
- When the mobile station reaches a new BSC’s area, it requests a location update
- The update is forwarded to the MSC, entered into the VLR, the old BSC is notified and an acknowledgement is passed back

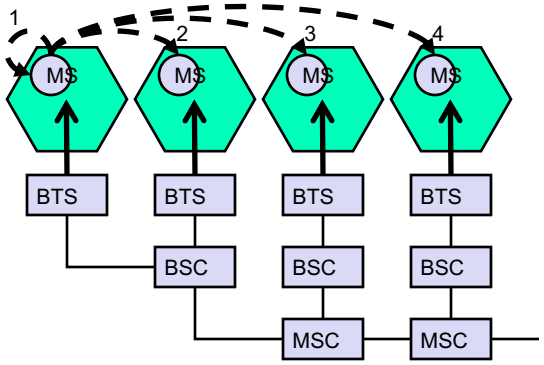
Handoff (Handover)

- When a call is in process, the changes in location need special processing
- Within a BSS, the BSC, which knows the current radio link configuration (including feedbacks from the MS), prepares an available channel in the new BTS
- The MS is told to switch over to the new BTS
- This is called a **hard handoff**
  - In a **soft handoff**, the MS is connected to two BTSes simultaneously

GSM Architecture

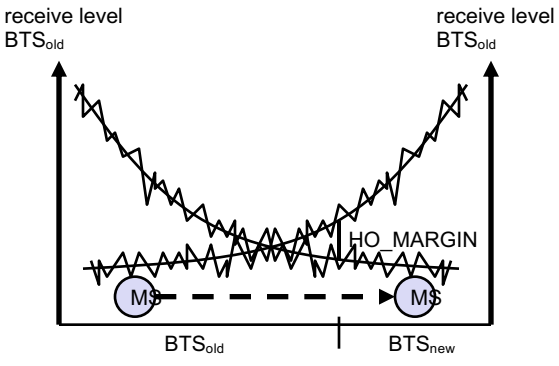


4 Types of Handover

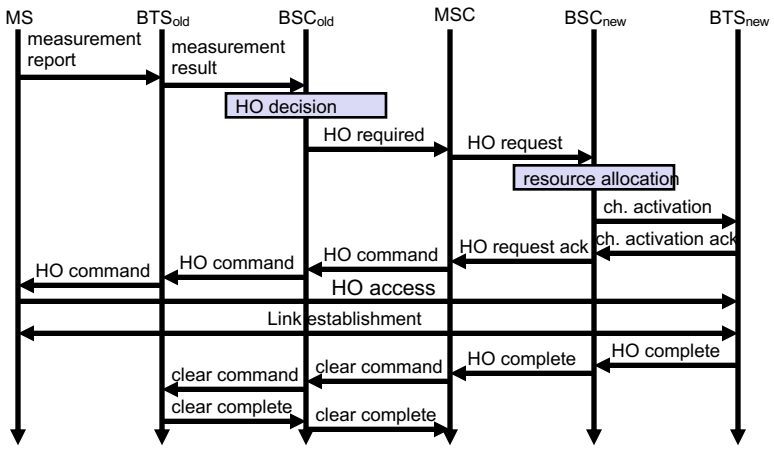


Primary reasons for handover: MS moves out of range & cell traffic too high (load balancing)

Handover Decision



Example of Handover Procedure



Roaming

- When a MS enters another operators network, it can be allowed to use the services of this operator
  - Operator to operator agreements and contracts
  - Higher billing
- The MS is identified by the information in the SIM card and the identification request is forwarded to the home operator
  - The home HLR is updated to reflect the MS's current location

4G (LTE)

- LTE stands for Long Term Evolution
- Data transfer rates of 100 Mbps downlink and 50 Mbps uplink
- Based on UMTS 3G technology
- Optimized for all-IP traffic
- Simplified upgrade path from 3G networks

Major LTE Radio Technogies

- Uses Orthogonal Frequency Division Multiplexing (OFDM) for downlink
- Uses Single Carrier Frequency Division Multiple Access (SC-FDMA) for uplink
- Uses Multi-input Multi-output (MIMO) for enhanced throughput
- Reduced power consumption
- Higher RF power amplifier efficiency (less battery power used by handsets)

5G Challenges & Scenarios*

Avalanche of
Traffic Volume

Further expansion of mobile broadband

Additional traffic due to communicating machines

"1000x in ten years"

Massive growth in
Connected Devices
"Communicating machines"

"50 billion devices in 2020"

Large diversity of
Use cases & Requirements

Device-to-Device Communications

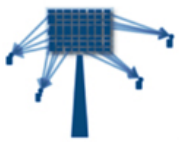
Car-to-Car Comm.

New requirements and characteristics due to communicating machines

5G Technologies

Massive MIMO

Dramatically increase number of antenna elements on base station

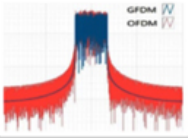


Ultra-Dense Networks

Substantially reduce cell sizes to handle more users

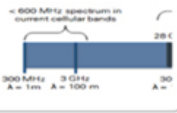
5G Waveforms

Improve bandwidth utilization through signal structure improvements such as NOMA, GFDM, FBMC, and UFMC



mmWave

Utilize potential of extremely wide bandwidths at frequency ranges once thought impractical for commercial wireless



Summary

1G	2G	3G	4G	5G
1981	1992	2001	2010	2020(?)
2 Kbps	64 Kbps	2 Mbps	100 Mbps	10 Gbps
Basic voice service using analog protocols	Designed primarily for voice using the digital standards (GSM/CDMA)	First mobile broadband utilizing IP protocols (WCDMA / CDMA2000)	True mobile broadband on a unified standard (LTE)	'Tactile Internet' with service-aware devices and fiber-like speeds
				?