

## LECTURE 5

### AMPS and GSM

## Characteristics of 1G Cellular Systems

3

- Use Cellular Concept to provide service to a geographic area (i.e. number of small adjacent cells to provide coverage)
  - Frequency Reuse
  - Handoff/Handover
- FDMA/FDD systems
  - Common Air Interface standards only
    - Analog Voice communications using FM
    - Digital Control channels for signaling
  - Adjustable Mobile Power levels
  - Macro Cells : 1-40 km radius
- Focus on AMPS system

## 1G Cellular Systems

2

- Goal: Provide basic voice service to mobile users over a large area
- 1 G Systems developed in late 70's/early 80's – deployed in 80's
  - Advanced Mobile Phone System (AMPS) - USA
  - Total Access Communications Systems (TACS) - UK
  - Nordic Mobile Telephone (NMT) System – Scandinavian PTTs
  - C450 - W. Germany
  - NTT System - Nippon Telephone & Telegraph (NTT) – Japan
- Incompatible systems using different frequencies!
  - Have similar characteristics though

## Characteristics of 1G Cellular Systems (continued)

4

- First generation systems targeted to few subscribers with car phones
  - Rapid growth in demand for cellular services
  - Availability of low cost, lightweight, portable handsets
  - → Growing demand for system capacity
- Capacity can be increased by smaller cells but:
  - More difficult to place base stations at locations for necessary radio coverage
- Increased signaling for handoffs, and more frequent handoffs
  - Base stations handle more access requests and registrations
  - Analog technology has limited options to combat interference effects from smaller cells
- Demand for 2G digital cellular
  - Also, incompatible first generation (analog) standards in Europe motivated new pan-European digital standard

# Summary of 1G systems

5

|   | Japan    | North America             | England                    | Scandinavia | Germany      |
|---|----------|---------------------------|----------------------------|-------------|--------------|
| System  | NTT      | AMPS                      | TACS                       | NMT         | C450         |
| Dwnlink Freq (MHz)                              | 870-885  | 869-894                   | 917-950                    | 463-467.5   | 461.3-465.74 |
| Uplink Freq (MHz)                               | 925-940  | 824-849                   | 872-905                    | 453-457.5   | 451.3-455.74 |
| Spacing between uplink and downlink bands (MHz) | 55       | 45                        | 45                         | 10          | 10           |
| Channel Spacing(kHz)                            | 25, 12,5 | 30                        | 25                         | 25          | 20           |
| Number of channels                              | 600      | 832<br>(control ch. 21×2) | 1320<br>(control ch. 21×2) | 180         | 222          |

# Summary of 1G Systems (continued)

6

*Audio signal modulated with FM; Control signal modulated with FSK*

|                                      | Japan  | North America                  | England                        | Scandinavia   | Germany                                       |
|--------------------------------------|--|--------------------------------|--------------------------------|---|---|
| System                               | NTT  | AMPS                           | TACS                           | NMT   | C450  |
| Coverage radius (km)                 | 5 -10  | 2-20                           | 2-20                           | 1.8-40  | 5-30  |
| Audio signal freq. deviation (kHz)   | ±5   | ±12                            | ±9.5                           | ±5  | ±4  |
| Control signal freq. deviation (kHz) | ±4.5   | ±8                             | ±6.4                           | ±3.5  | ±2.5  |
| Data Tx. Rate (kb/s)                 | 0.3  | 10                             | 8                              | 1.2   | 5.28  |
| Message Protection                   | Transmitted signal is checked when sent back to the transmitter by the receiver. | Principle of majority decision | Principle of majority decision | Receiving steps pre- determined according to the message content. | Message sent again when an error is detected. |

# AMPS

7

- Advanced Mobile Phone System is first generation wireless in US
  - Earlier systems used line of sight radio (e.g., AT&T's Improved Mobile Telephone Service in 1960s)
  - AT&T developed cellular concept in 1940s
  - 1971 proposed High Capacity Mobile Phone Service to FCC
  - 1979 FCC standardized it as AMPS in 800-900 MHz range
  - 1983 launched in Chicago
- Licenses for geographic service areas (similar to radio station model) – areas based on commercial trading zones
  - MSA: metro service area, RSA: rural service area

# MSAs and RSAs

8

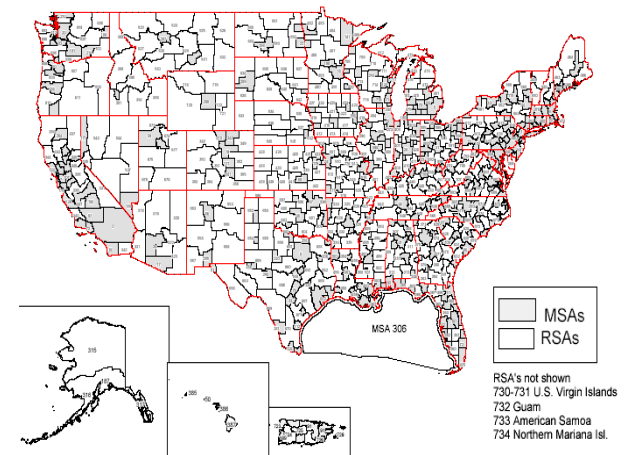
FCC allocated 2 licenses for each MSA,RSA

One license to local phone company: wireline common carrier (WCC)

Other license given out by lottery: radio common carrier (RCC)

Speculation and fraud in RCC lottery!

Metropolitan Statistical Areas and Rural Service Areas



## Frequency Allocation in AMPS

9

- Originally 40 MHz of spectrum separated into two bands of 20 MHz each (A and B band). Later expanded to 25 MHz each
  - A band lower spectrum went to RCC, B band to WCC
- FDD used with 45 MHz separation in uplink and downlink – prevents self interference.
- AMPS uses 30 kHz radio channels between mobile station and base stations (EIA/TIA-533 radio interface)
- Two service providers in area are each allocated 25 MHz => 12.5 MHz for each direction => 416 pairs of channels: split into 395 voice channels + 21 control channels for signaling
- Channels numbered consecutively 1-666, when expanded kept same numbering assuming 30 KHz channels even in places where no spectrum allowed
- $f(c)_{\text{uplink}} = 825,000 + 30 \times (c) \text{ KHz} \quad 1 \leq c \leq 799$
- $f(c)_{\text{uplink}} = 825,000 + 30 \times (c-1023) \text{ KHz} \quad 991 \leq c \leq 1023$
- $f(c)_{\text{downlink}} = f(c)_{\text{uplink}} + 45,000 \text{ KHz}$

## Initial AMPS System Operators

10

| Market No. | Area          | System Operator                    | No. of Cells | Switching Equipment |
|------------|---------------|------------------------------------|--------------|---------------------|
| 1          | New York      | W (B-Side) -Nynex Mobile (6/15/84) | 56           | AT&T                |
|            |               | NW-Metro One (A-Side) (4/5/86)     | 36           | Motorola            |
| 2          | LA            | W-PacTel Cellular (6/13/84)        | 81           | AT&T                |
|            |               | NW-LA Cellular (3/27/87)           | 38           | Ericsson            |
| 3          | Chicago       | W-Ameritech Mobile (10/13/83)      | 73           | AT&T                |
|            |               | NW-Cellular One (1/3/85)           | 31           | Ericsson            |
| 4          | Philadelphia  | W-Bell Atlantic Mobile (7/12/84)   | 38           | AT&T                |
|            |               | NW-Metrophone (2/12/86)            | 32           | Motorola            |
| 5          | Detroit       | W-Ameritech Mobile (9/21/84)       | 37           | AT&T                |
|            |               | NW-Cellular One (7/30/85)          | 31           | Ericsson            |
| 6          | Boston        | W-Nynex Mobile (1/1/85)            | 30           | AT&T                |
|            |               | NW-Cellular One (1/1/85)           | 10           | Motorola            |
| 7          | San Francisco | W-GTE Mobilnet (4/2/85)            | 28           | Motorola            |
|            |               | NW-Cellular One (9/26/86)          | 36           | Ericsson            |
| 8          | Washington    | W-Bell Atlantic Mobile (4/2/84)    | 46           | AT&T                |
|            |               | NW-Cellular One (12/16/83)         | 34           | Motorola            |
| 9          | Dallas        | W-SW Bell Mobile (7/31/84)         | 41           | AT&T                |
|            |               | NW-MetroCel (3/1/86)               | 28           | Motorola            |

## Mobility Management in AMPS

11

- Initially could not roam a whole lot
  - Restricted to limited geographical regions (MSA or RSA)
  - Legal hurdles, billing problems, proprietary systems in the backhaul
  - 1G standards are air interface standard only - basically didn't think it would be needed
    - Implementation of databases/signaling to handle mobility was not available/standardized
- Replaced by ad hoc measures
  - Manual clearing house approach
  - Follow-me roaming (GTE) – automated clearing house
    - User has to register when he goes to a new location

## Second Generation Cellular Systems

12

- Motivation for 2G Digital Cellular:
  - Increase System Capacity
  - Add additional services/features (SMS, caller ID, etc..)
  - Reduce Cost
  - Improve Security
  - Interoperability among components/systems (GSM only)
- 2G Systems
  - Pacific Digital Cellular ← orphan technology
  - North American TDMA (NA-TDMA) ← orphan technology
  - Global System for Mobile (GSM)
  - IS-95 (cellular CDMA)

# GSM: Global System of Mobile Communications

13

- A heterogeneous analog cellular implementation was observed in Europe in the 1980s
  - United Kingdom, Italy, Spain, Austria: TACS (900 MHz)
  - Scandinavia, Germany, The Netherlands, Spain: NMT (450 MHz, 900 MHz)
  - France: Radiocom
- 1987: 12 Member countries sign MOU for a common standard
- ETSI: European Telecommunications Standards Institute in 1989 took over the standardization of all cellular telephony in Europe
  - Strongly influenced by ISDN
  - Signaling System 7
    - Used for delivery of control messages/ establishment and tear down of calls.
    - Can support features like three way calling.

# GSM Objectives

14

- A broad offering of speech and data services
- Compatibility with wire-line networks
- Cross-border system access for all users
- Automatic roaming and handoff
- Efficient use of frequency spectrum
- Support for different types of mobile terminals (car, hand-held, portable)
- Digital transmission of signaling and user data
- Supplier independence
- Low infrastructure costs and terminal equipment costs

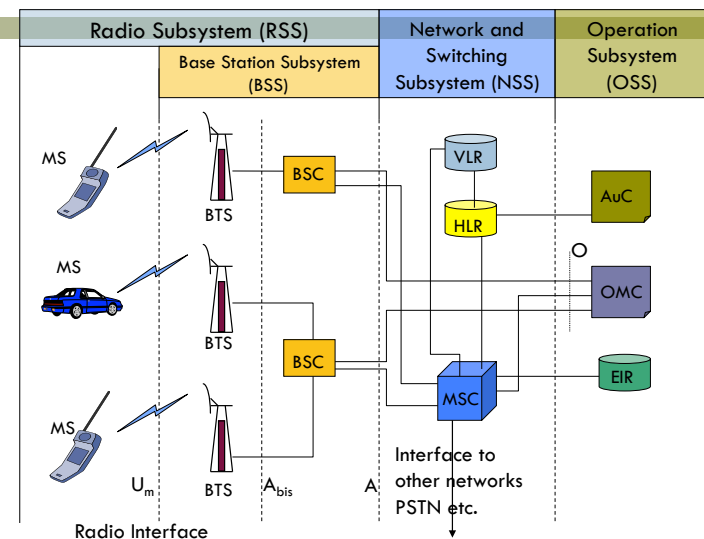
# GSM Details

15

- Based on TDMA/FDMA
- Each frequency carrier is 200 kHz wide and carries eight voice channels
- Example Spectrum in Europe
  - Uplink (Mobile to BS): 890-915 MHz
  - Downlink (BS to Mobile): 935-960 MHz
- Modulation Scheme: GMSK
- Optional Frequency Hopping

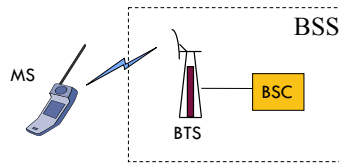
# Functional Architecture

16



## Radio Subsystem

17



- It is made of the Mobile Station (MS) and the Base Station Subsystem (BSS)
- It deals with the radio part of the GSM system

## MS Numbers

19

- International Mobile Subscriber Identity (IMSI)
  - Includes mobile country code, mobile network code and mobile subscriber identity (~15 digits)
- Temporary Mobile Subscriber Identity (TMSI)
  - Conceals the IMSI
- MS-ISDN Number (MSISDN)
  - ISDN like number used for calling (has a country code, national destination code, subscriber number)
- MS Roaming Number (MSRN)
  - Provides link to current location of the MS

## Mobile Station (MS)

18

- It has two parts
  - A part containing the hardware and software components related to the radio interface
  - A subscriber identity module (SIM)
    - A smart card like device that contains the identity of the subscriber
    - It can be used in portable devices (the user does not have to carry his MS)
    - PIN used to lock/unlock the MS
- Transmit power can be 0.8W to 20W
- Non-volatile memory contains authentication key, SIM type, subscriber number, a PIN, etc.
- Dynamically changeable data includes a list of BCCH's (later), the temporary number, ciphering key, list of blocked PLMNs etc.

## Base Station Subsystem (BSS)

20

- A BSS has two parts
  - It is controlled by a Base Station Controller (BSC)
  - It transmits using a Base Transceiver System (BTS)
- Interfaces to the MS via the  $U_m$  interface
- Contains parameters for the air interface such as GMSK modulation, status of carrier frequencies, the channel grid etc.
- Also contains parameters of the A-interface like PCM signals (64 kbps for a 4 kHz voice) carried over Frame Relay etc.

## Base Station Controller (BSC)

21

- Performs all functions necessary to maintain radio connections to an MS
- Manages several BTSs
- It multiplexes traffic onto radio channels
- Handles intra-BSS handoff
- Reserves radio channels and frequencies for calls
- Tasks also include paging and transmitting signaling data to the MSC

## BSC Vs BTS Functions

23

- Tasks of a RSS are distributed over BSC and BTS
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

| Functions                              | BTS | BSC |
|--|-----|-----|
| Management of radio channels           |     | X   |
| Frequency hopping (FH)                 | X   | X   |
| Management of logical channels         |     | X   |
| Mapping of logical onto radio channels |     | X   |
| Channel coding and decoding            | X   |     |
| Rate adaptation                        | X   | X   |
| Encryption and decryption              | X   | X   |
| Paging                                 | X   | X   |
| Uplink signal measurements             | X   |     |
| Traffic measurement                    |     | X   |
| Handover management                    |     | X   |

## Base Transceiver System (BTS)

22

- Includes all hardware
  - Transmitting and receiving facilities
  - Antennas
  - Speech coder and decoder
  - Rate adapter
- It can form a radio cell (100m – 35km)
- It can form a cell sector if directional antennas are employed
- Connects to the BSC via the A-bis interface

## The Network and Switching Subsystem (NSS)

24

- This is the “heart” of the GSM backbone
- Connections to the standard public network
- Performs handoffs
- Functions for worldwide localization of users
- Support for charging, accounting and roaming of users
- Consists of
  - MSC, HLR, VLR

## Mobile Services Switching Center (MSC)

25

- High performance digital ISDN switches
- Manages several BSCs
- A Gateway MSC (GMSC) connects different service providers and networks like the PSTN and ISDN
- SS-7 is used for signaling needed for connection set up, connection release, and handoff of connections
- Also handles call forwarding, multiparty calls, reverse charging, etc.

## Visitor Location Register

27

- It is associated with each MSC
- A dynamic database that stores all information about MSs that are in its location area associated with the MSC
- If a new MS comes into the LA, its information is copied from the HLR into the VLR

## Home Location Register (HLR)

26

- Equivalent of the generic “home database”
- Stores all user relevant information
  - ▣ Static information like MSISDN, authentication key, subscribed services etc.
  - ▣ Dynamic information like current location area (LA)
- For each user, there is exactly one HLR where the information is maintained
- Also supports charging and accounting

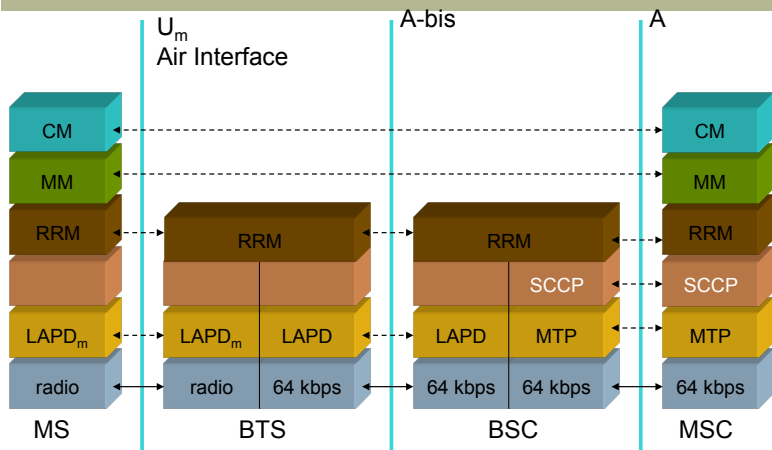
## The Operation Subsystem (OSS)

28

- Operation and Maintenance Center (OMC)
  - ▣ Monitors and controls all network entities using SS-7 and X.25
  - ▣ Traffic monitoring, status reports, accounting, billing etc.
- Authentication Center (AuC)
  - ▣ Algorithms for authentication and keys for encryption
  - ▣ Usually a special part of the HLR
- Equipment Identity Register (EIR)
  - ▣ Stores all device identifications
  - ▣ Contains blocked and stolen list and a list of valid and malfunctioning IMEI's

# GSM protocol architecture

29



CM: Connection Management; MM: Mobility Management; SCCP: Signal Connection Control Part  
RRM: Radio Resource Management; MTP: Message Transfer Part; LAPD: Link Access Protocol-D

# Layers

30

- Radio layer
  - FEC, Synchronization, channel quality estimation.
- LAPD
  - Variant of HDLC
  - Reliable link layer transfer
- Layer 3
  - Contains RRM which does channel setup, allocation, release etc.
- MM
  - Authentication, Location updating, Assigning a TMSI etc.
- CM
  - Call control – call establishment, release etc.
  - SMS – using control channels
  - Supplementary services – Caller ID, Call forwarding etc.

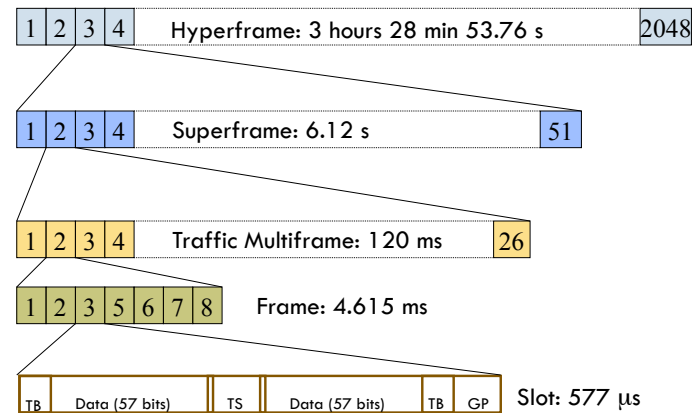
# Air Interface

31

- 25 MHz of bandwidth is divided into 124 frequency bands of 200 kHz each and two 100 kHz pieces on either side
- Carrier frequencies are given by:
  - $F_u(n) = 890.2 + 0.2(n-1)$  MHz  $n=1,2,3,\dots,124$
  - $F_d(n) = 935.2 + 0.2(n-1)$  MHz  $n=1,2,3,\dots,124$
- Example:
  - On the uplink, Channel 1 = 890.1-890.3 MHz
  - On the downlink, Channel 1 = 935.1-935.3 MHz
- Usually, Channels 1 and 124 will not be used if possible

# Framing Scheme in GSM (Traffic Channels)

32

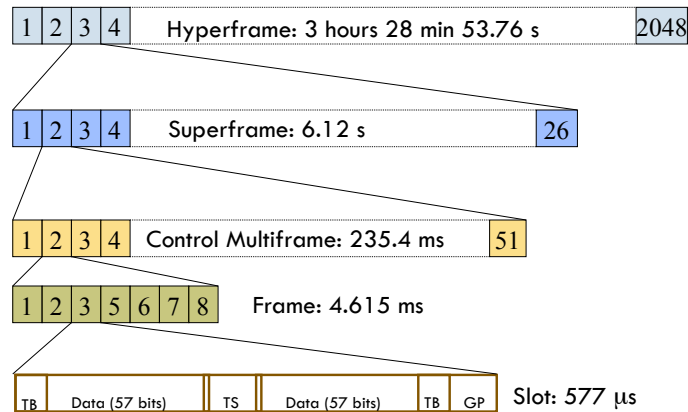


Framing scheme is implemented for encryption and identifying time slots



## Framing Scheme in GSM (Control Channels)

33



Framing scheme is implemented for encryption and identifying time slots

## One Time Slot (typical)

34



TB: Tail Bits (3 bits)

TS: Training Sequence (26 bits)

GP: Guard Period (8.25 bits)

- A time slot lasts 577 μs (546.5 μs of data and 30.5 μs of guard-time)
- Bits per slot =  $3 + 57 + 1 + 26 + 1 + 57 + 3 + 8.25 = 156.25$
- Bit rate =  $156.25 / 577 \mu s = 270.79 \text{ kbps}$

## Fields in a slot

35

- Tail bits – usually set to `0`; can be used to enhance receiver performance.
- Training – used to determine channel characteristics (multipath)
  - Choose the strongest signal if multiple signals are available due to multipath.
- Flags: Indicate whether burst contains user data or network control data.

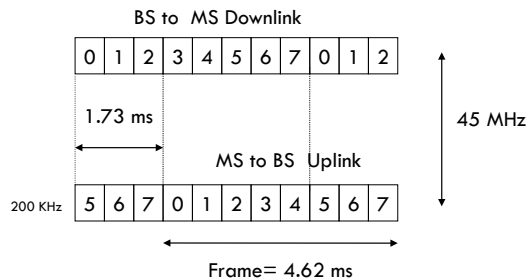
## Types of Time Slots

36

- Normal Burst
  - 57 data bits are encrypted voice or control traffic
- Synchronization Burst
  - Used for time synchronization of MS
- Frequency Correction Channel Burst
  - All bits are zero, sending an un-modulated carrier
  - Sync up correctly to the carrier frequency
- Access Burst
  - Random access and has larger guard period
  - Used for initial connection set up
- Dummy Burst
  - Sent by BTS sometimes when there is no data

## GSM: FDD Channels

37



Uplink and Downlink channels have a 3 slot offset – so that MS doesn't have to transmit and receive simultaneously  
MS can also take measurements during this offset time and delay between next frame

## Traffic Channel

39

- 20 ms of voice (260 bits @ 13kbps) is converted to 456 bits after CRC and convolutional encoding
- Effective data rate = 22.8 kbps
- 456 bits =  $8 \times 57$  bits
  - (Reminder: a time slot has two 57 bit units separated by a training sequence)
- Voice samples are interleaved and transmitted on the TCH
- Data and Control bits are also encoded to end up with 456 bits over 20 ms

## GSM Logical Channels

38

- No RF carrier or time slot is reserved for a particular task except the BCCH
  - Any time slot on any carrier can be used for almost any task
- Channels are of two types:
  - Traffic Channels (TCH)
    - Voice at 13 kbps (full rate) or 5.6 kbps (half rate)
  - Control Channels (CCH)
    - Broadcast, Common and Dedicated

## Broadcast Control Channels (Unidirectional)

40

- BCCH (Broadcast Control Channel)
  - Used to transmit cell identifier, available frequencies within and in neighbouring cells, options (like FH) etc.
  - Continuously active
  - Contains two sub-channels
    - FCCH (Frequency Correction Channel)
      - Uses a frequency correction burst
    - SCH (Synchronization Channel)
      - Time synchronization information

## Common Control Channels (Unidirectional)

41

- Used for all connection set up purposes
- The paging channel (PCH) is used for paging a mobile when it receives a call
- The random access channel (RACH) is used by the MS to set up a call
  - ▣ Slotted ALOHA on the RACH
- Access grant channel (AGCH) is used by the BTS to allocate a channel to the MS
  - ▣ This can be a TCH (start using voice)
  - ▣ Or a SDCCH (negotiate further for connection setup)

SDCCH: Stand alone dedicated CCH

## Pre-registration

43

- Upon powering up, the following events occur
  - ▣ MS scans common control channels and monitors the signal levels
  - ▣ It selects the channel with the largest signal strength
  - ▣ It will search for the FCCH on this RF carrier
    - If it is not available, it will try the next largest carrier
    - It will synchronize the RF carrier frequency
  - ▣ Repeats the same step for the SCH that occurs eight TDMA frames after the FCCH
  - ▣ After synchronization, the MS decodes the BCCH
  - ▣ BCCH contains information about the current cell, neighbouring cells, etc.
- If the location area has changed, the new location is updated by a registration procedure

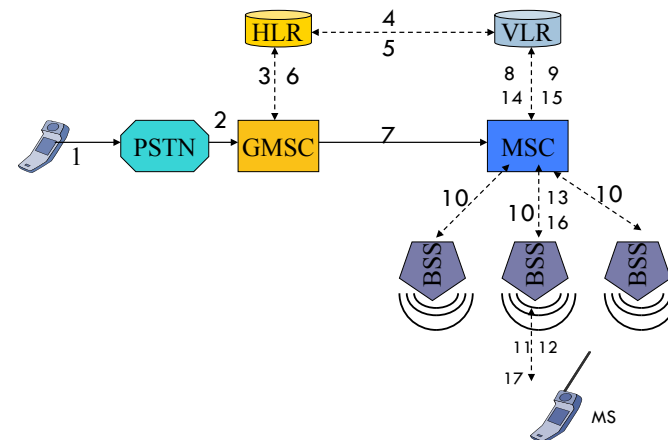
## Dedicated Control Channels (Bidirectional)

42

- As long as a MS has not established a TCH, it will use a stand-alone dedicated control channel (SDCCH) for signaling and call set up
  - ▣ Authentication
  - ▣ Registration, etc.
- Each TCH has a Slow Associated Control Channel (SACCH)
  - ▣ Exchange system information like channel quality, power levels, etc.
- A Fast Associated Control Channel (FACCH) is used to exchange similar information urgently ( during handoff for instance)

## Example: Mobile Terminated Call

44



## Mobile Terminated Call

45

- 1) User dials a phone number of a GSM subscriber
- 2) PSTN forwards the call set up to the GMSC
- 3) GMSC identifies the HLR and signals the call set up to it
- 4) HLR verifies number, does authentication etc. and requests the MSRN from the VLR
- 5) VLR sends the information to the HLR
- 6) HLR determines what MSC is involved and sends this information to the GMSC

## Mobile Terminated Call

47

- 13) BSS intimates the MSC
- 14) MSC requests authentication and security set up (encryption) from the VLR
- 15) VLR responds with the information
- 16) MSC sets up connection with the MS
- 17) Traffic channel is allocated

## Mobile Terminated Call

46

- 7) GMSC forwards the call set up to the MSC
- 8) MSC requests information about the MS from the VLR
- 9) VLR provides relevant information... is the mobile available, etc.
- 10) MSC initiates a paging of the mobile through all its BSSs
- 11) All of the BSSs transmit the page on their PCH
- 12) The MS answers one of the BSSs

## Handoff in GSM

48

- Reasons for Handoff
  - Signal quality handoff (user oriented)
  - Traffic Balancing Handoff (network oriented to ease traffic congestion by moving calls in a highly congested cell to a lightly loaded cell)
    - Needs significant overlap of adjacent cells
- Types of Handoff
  - Synchronous: Old and new cells are synchronized (100ms)
  - Asynchronous: MS must re-synchronize to new BTS after handoff (may take up to 200 ms)

## Mobile Assisted Handoff (MAHO)

49

- The BTS provides the MS a list of available channels in neighbouring cells via the BCCH
- MS monitors the RSS from the BCCH's of these neighbouring cells and reports these values to the MSC using the SACCH
- The BTS also monitors the RSS from the MS to make a HO decision
- Proprietary algorithms are used to decide when a handoff should be initiated

## Measurement Reporting

51

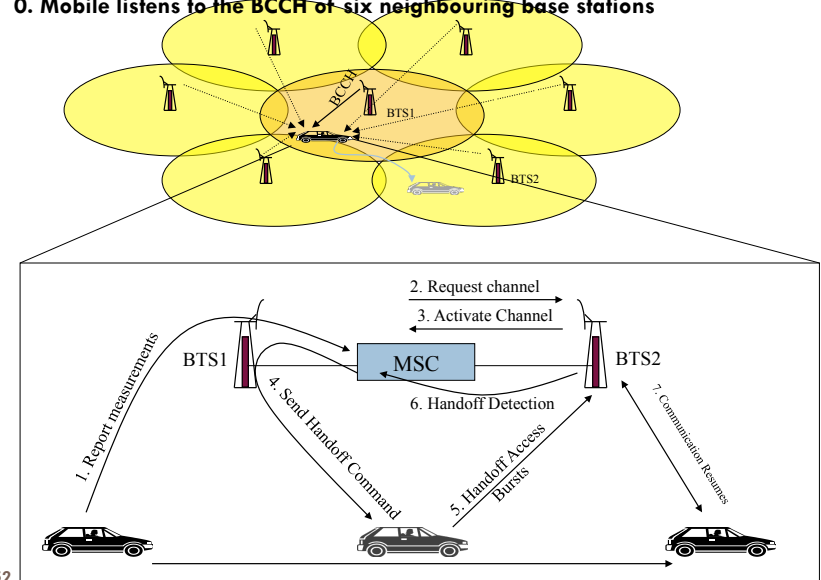
- Mean value of 100 measurements of 24 TCH bursts are sent
- Neighbouring cell RSS is measured based on the continuously keyed BCCH of the neighbouring cells
- The MS sends the following data
  - ▣ RSS of the traffic channel
  - ▣ BER of the traffic channel
  - ▣ RSS of the BCCH of up to six neighbouring cells and the corresponding BSIC (Base station identity code)
    - BSIC distinguishes between co-channel cells
  - ▣ Frequency of these BCCH's

## Handoff Criteria

50

- Roundtrip time can be measured and corrected by the BTS for all MSs
  - ▣ This is used in handoff when a MS moves beyond a certain distance from the BTS
- Mobile measurements are sent to the MSC once or twice a second (480 to 960 ms via the SACCH)
- Gross bit error rate
- Cell capacity, number of free channels, number of new connections waiting etc.

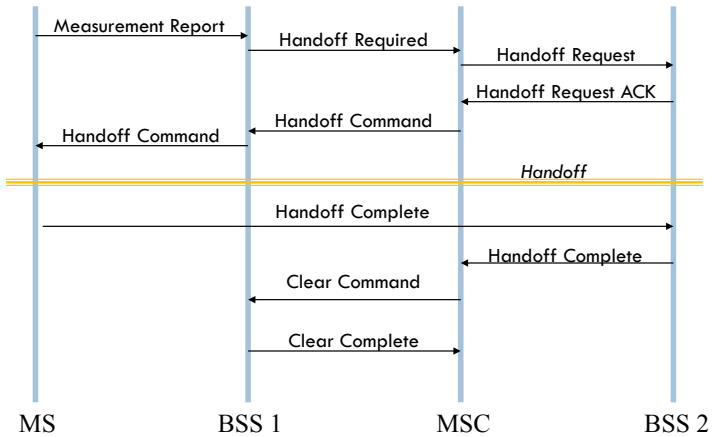
### 0. Mobile listens to the BCCH of six neighbouring base stations



52

## Handoff Executed with an MSC

53



## Data Services in GSM

54

- Circuit switched data at a maximum data rate of 9.6 kbps
- Short messaging service (SMS)
  - ▣ Short alphanumeric messages can be exchanged by the MS and the GSM system
  - ▣ Point-to-point and broadcast services are available
  - ▣ An SMSMC (SMS Message Center) is responsible for store-and-forward service