Global System for Mobile (GSM)

David Tipper
Associate Professor
Graduate Program of Telecommunications and Networking
University of Pittsburgh

Telcom 2700 Slides 8

Based largely on material from Jochen Schiller, Mobile Communications 2nd edition

Second Generation Cellular Systems

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

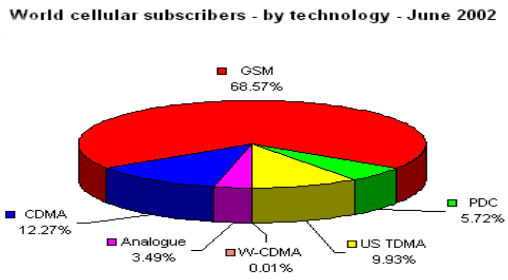
Global System for Mobile (GSM)

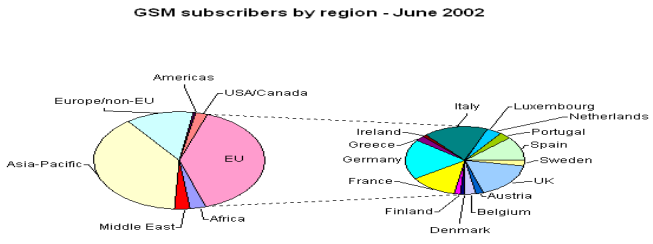
IS-95 (cellular CDMA)

GSM: History

- 1982 CEPT establishes Groupe Speciale Mobile
  - Motivation develop Pan-European mobile network
  - Support European roaming and interoperability in landline
  - Increase system capacity
  - Provide advanced features
  - Emphasis on **STANDARDIZATION,** supplier independence
  - Low cost infrastructure and terminals
- 1989 European Telecommunications Standardization Institute (ETSI) takes over standardization
  - changes name: *Global System for Mobile communication*
- 1990 First Official Commercial launch in Europe
- 1995 GSM Specifications ported to 1900 MHz band
- GSM is the most popular 2G technology

GSM Market





GSM Overview

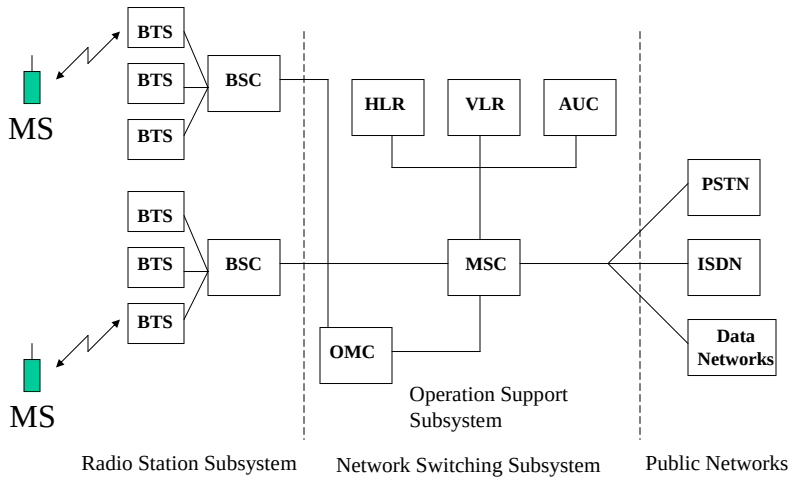
- FDD/ FDMA/TDMA – channel structure - 200 KHz channels – each carriers 8 voice channels
- Higher Quality than Analog Systems
  - Digital Voice 13.3Kbps
  - Slow frequency hopping, adaptive equalizer, error control coding, DTX
  - Low power handsets – support sleep mode
- Security with encryption
- Wide roaming capability
  - Subscriber Identity Modules (SIM cards)
- Digital data service
  - fax, circuit switched data
  - SMS short messaging service
- Additional features : call waiting, voice mail, group calling, caller id etc.

Architecture of the GSM system

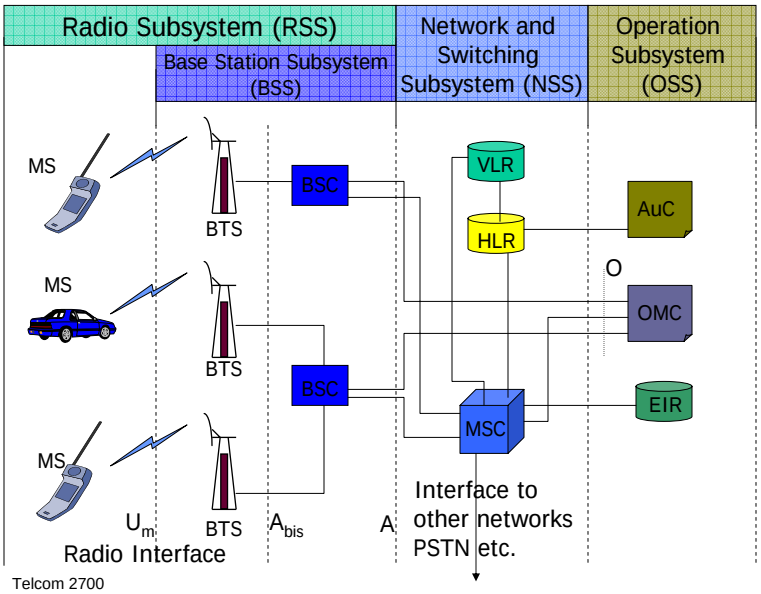
GSM is a PLMN (Public Land Mobile Network)

- Several providers can setup mobile networks following the GSM standard within each country
- Major components
  - MS (mobile station)
  - BTS (base transceiver station) or BS or cell site
  - BSC (base station controller)
  - MSC (mobile switching center)
  - LR (location registers): VLR, HLR
  - AUC(Authentication database), EIR (Equipment Identity Register)
- Subsystems
  - RSS (radio subsystem): covers all radio aspects
  - NSS (network and switching subsystem): call forwarding, handoff, switching, location tracking, etc.
  - OSS (operation support subsystem): management of the network
- **Standardized interfaces**
  - Allows provider to mix and match vendor equipment

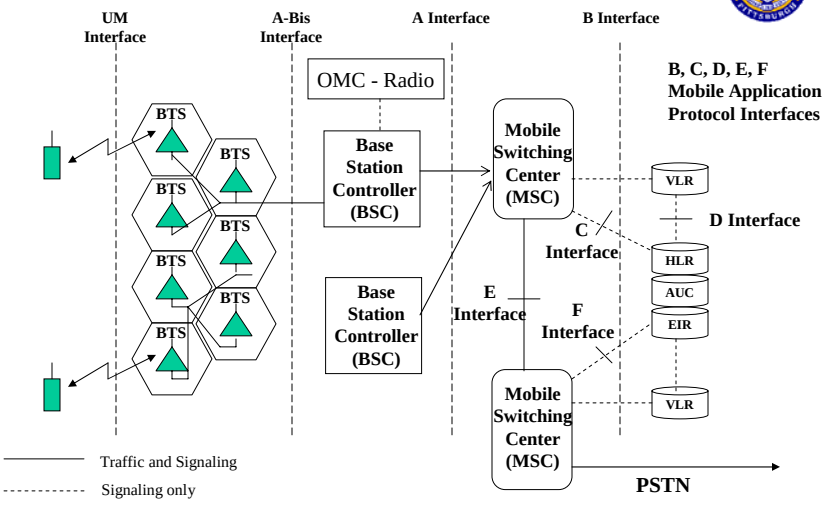
GSM System Architecture



Functional Architecture



GSM System Architecture



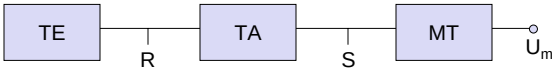
VLR = Visitor Location Register
HLR = Home Location Register
EIR = Equipment Identity Register
AUC = Authentication Center

BTS = Base Transceiver Station
ADC = Admission Data Center
OMC = Operation Maintenance Center

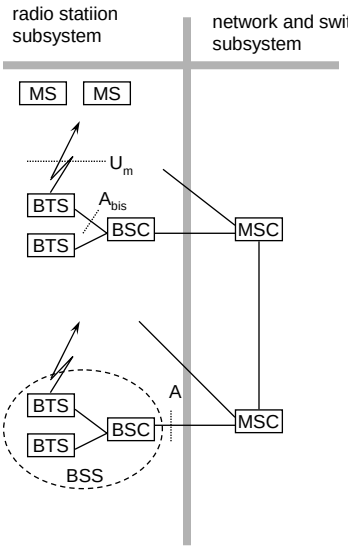
Mobile station

Terminal for the use of GSM services

- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - end-point of the radio interface (U_m)
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters (subscriber number, authentication key, PIN, etc.)



Radio Station Subsystem (RSS)



Components

- *MS* (Mobile Station)
- *BSS* (Base Station Subsystem): consisting of
  - *BTS* (Base Transceiver Station): antenna + digital radio equipment
  - *BSC* (Base Station Controller): controlling several transceivers, map radio channels (Um) onto terrestrial channels A

Interfaces

- U_m : radio interface
- A_{bis} : standardized, open interface with 16 kbit/s user channels
- *A*: standardized, open interface with 64 kbit/s user channels as in wired telephone network

Base Transceiver Station and Base Station Controller

Tasks of a RSS are distributed over BSC and BTS

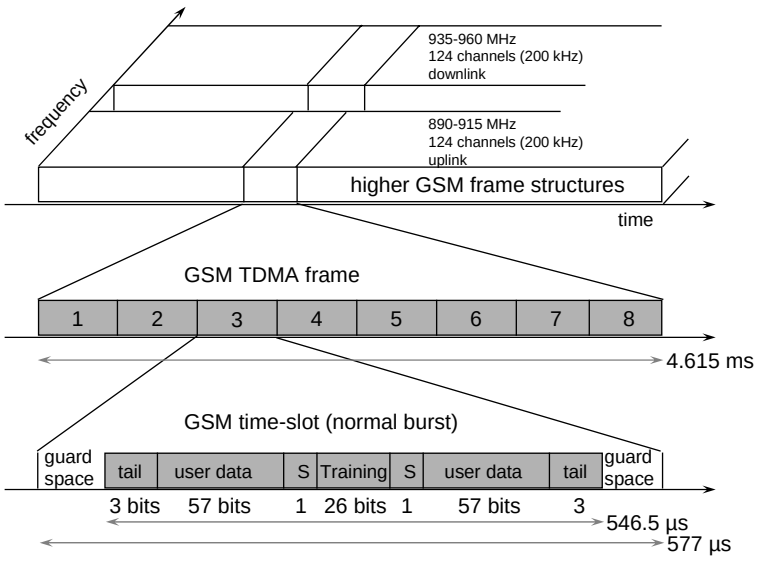
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial 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

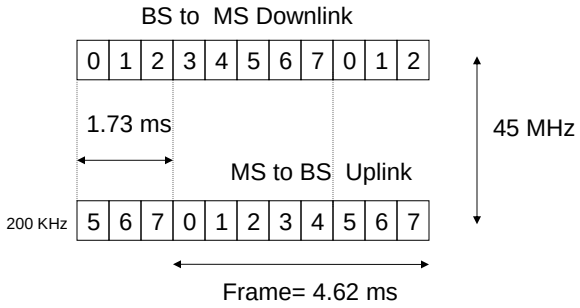
GSM Air Interface U_m

- Uses Physical **FDMA/TDMA/FDD** physical
  - In 900 MHz band: 890-915 MHz Uplink band, 935-960 MHz Downlink
  - Radio carrier is a 200kHz channel => 125 pairs of radio channels
    - Called Absolute Radio Frequency Channel Number (ARFCN)
    - ARFCN numbers given by f(n) = 890 +.2n MHz for Uplink band n = 0, …124
    - Corresponding downlink is f(n) + 45 MHz
    - Channels and ARFCN slightly different in other frequency bands
  - A TDMA frame is defined on the radio carrier (8 users per carrier)
    - Channel rate is 270.833 kbps
  - (RELPC) digital speech 13.3kbps
  - Two types of logical channels map onto physical channels
    - Control Channels (call setup, power adjustment, etc..)
    - Traffic Channels (voice or data) = 22.8kbps = 1 slot in a TDMA frame

GSM - TDMA/FDMA

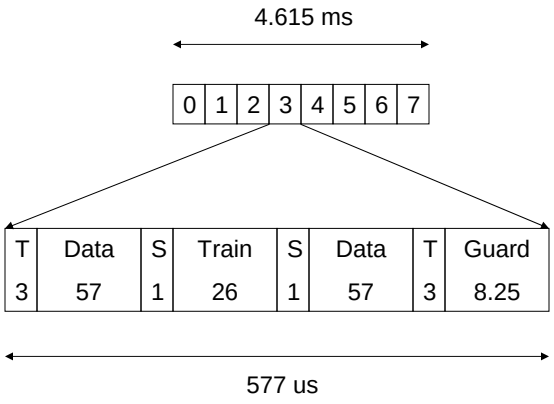


GSM: FDD Channels



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

GSM Normal Burst

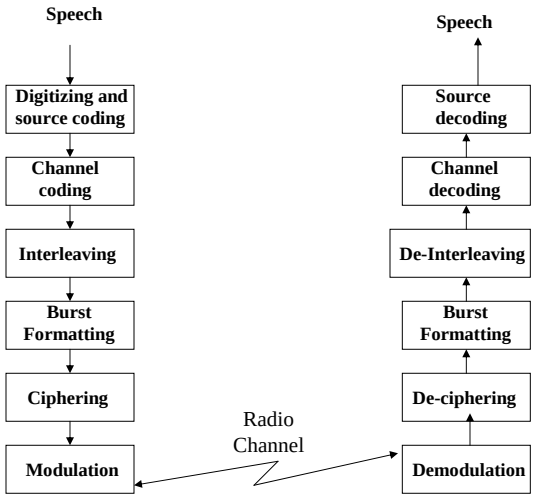


Training sequence is utilized for seting adaptive equalizer parameters

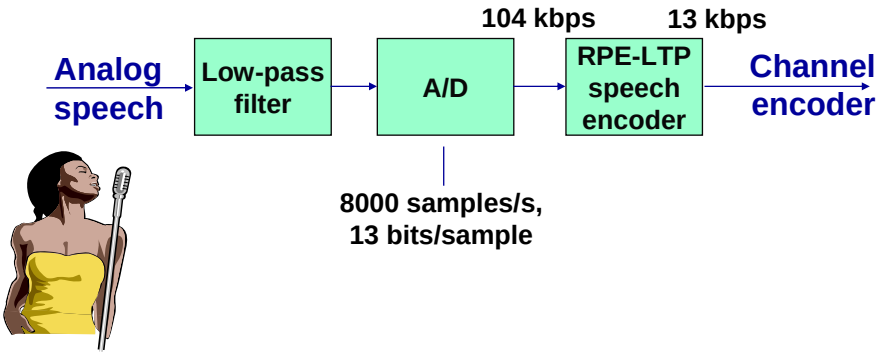
Guard Period = 30.5 microsecs
Needed to allow for clock misalignment and propagation time of mobiles as different distances from BTS

T: tail bits, S:flag, Train: equalizer training sequence

GSM operation from speech Input to Output

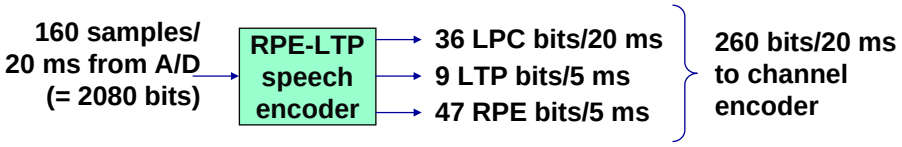


GSM Speech Coding



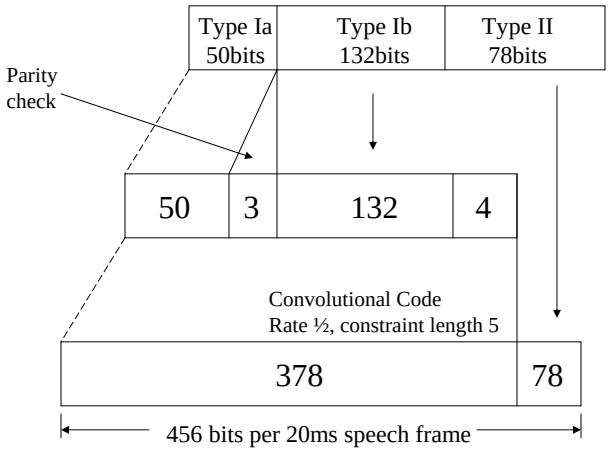
GSM Speech Coding (cont)

Regular pulse excited - long term prediction (RPE-LRP) speech encoder (RELP speech coder)

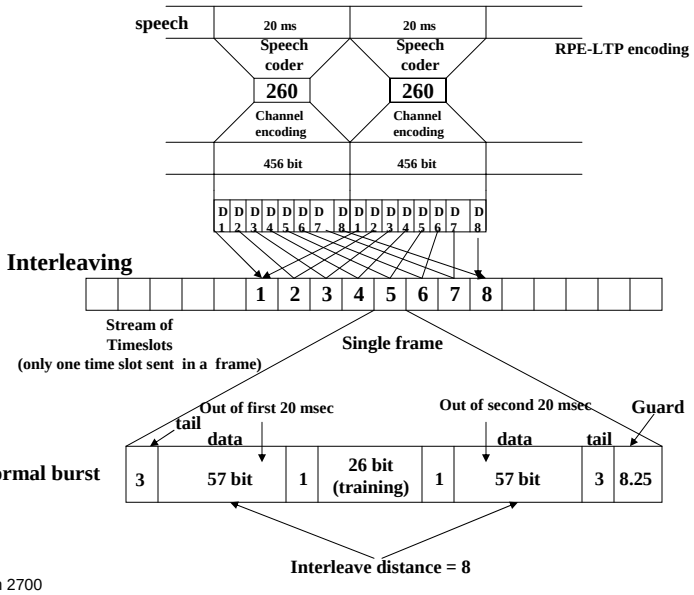


LPC: linear prediction coding filter
LTP: long term prediction – pitch + input
RPE: Residual Prediction Error:

Error protection for speech signals in GSM



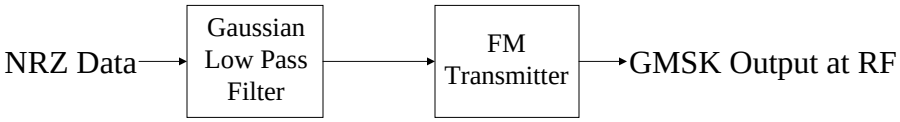
Interleaving Format



Modulation

- Variation on Frequency Shift Keying (FSK)
- Avoids sudden phase shifts ➔ MSK (Minimum Shift Keying)

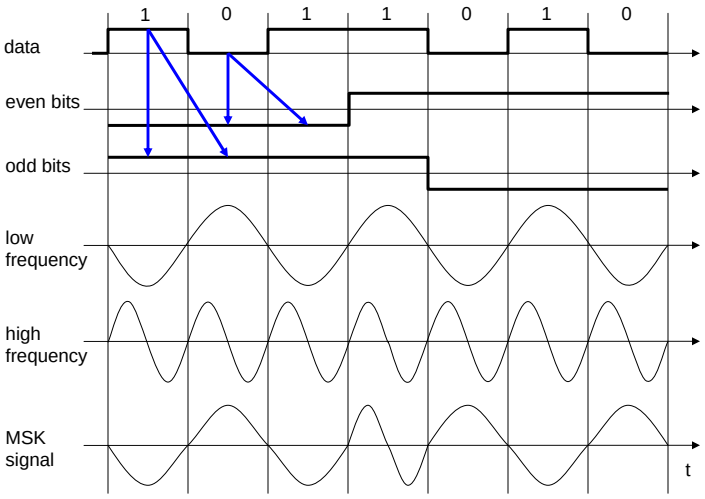
- Bit stream separated into even and odd bits, the duration of each bit is doubled



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

Example of MSK



bit	
even	0 1 0 1
odd	0 0 1 1
signal value	h n n h - - + +

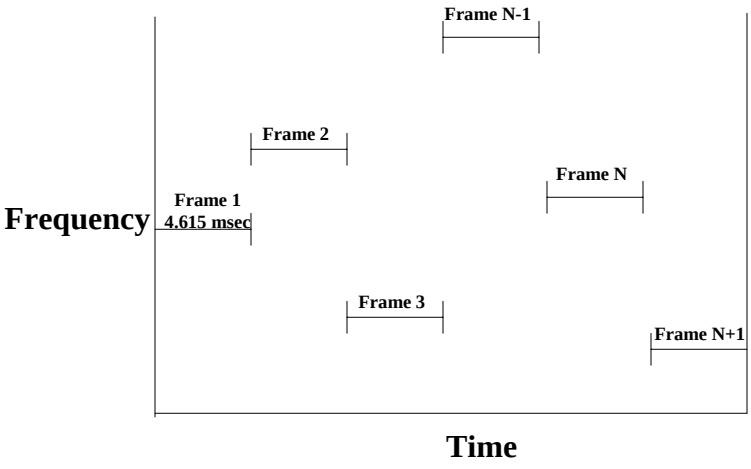
h: high frequency
n: low frequency
+: original signal
-: inverted signal

No phase shifts!

GSM Frequency Hopping

- Optionally, TDMA is combined with frequency hopping to address problem of channel fading
  - TDMA bursts are transmitted in a precalculated sequence of different frequencies (algorithm programmed in mobile station)
  - If a TDMA burst happens to be in a deep fade, then next burst most probably will not be
  - Helps to make transmission quality more uniform among all subscribers
  - Improves frequency resuse
  - Hops at the frame level – 217 hops/sec

Frequency-hopped signal in GSM



GSM Air Interface Specifications Summary

Parameter	Specifications
Reverse Channel Frequency	890 – 915 MHz
Forward Channel Frequency	935 – 960 MHz
ARFCN Number	0 to 124
Tx/Rx Frequency Spacing Tx/Rx Time Slot Spacing	45 MHz 3 Time slots
Modulation Data Rate	270.833333 kbps
Frame Period	4.615 ms
Users per Frame (Full Rate)	8
Time slot Period	576.9 μs
Bit Period	3.692 μs
Modulation	GMSK
ARFCN Channel Spacing	200 kHz
Interleaving (max. delay)	40 ms
Voice Coder Bit Rate	13.3 kbps

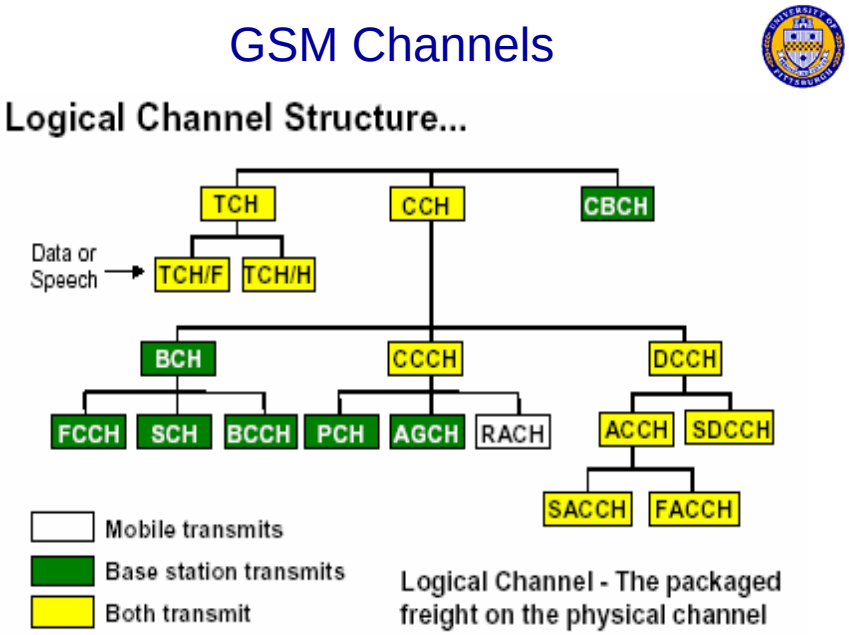
GSM System Identifiers

Notation	Name	Size (bits)	Description
IMSI	International mobile subscriber identity	15 digits (50 bits)	Directory number conforming to international convention – assigned by operating company to subscriber
TMSI	Temporary mobile subscriber identity	32 bits	Assigned by visitor location register to a subscriber
IMEI	International mobile equipment identifier	15 digits	Assigned by manufacturer to a mobile station
Ki	Authentication Key	128 bits	Secret key assigned by the operating company to a subscriber
Kc	Cipher Key	64 bits	Computed by network and mobile station
-	Mobile Station class mark	32 bits	Indicates properties of a mobile station
BSIC	Base Station identity code	6 bits	Assigned by operating company to each BTS
-	Training Sequence	26 bits	Assigned by operating company to each BTS
LAI	Location Area Identity	40 bits	Assigned by operating company to each BTS

GSM Channels

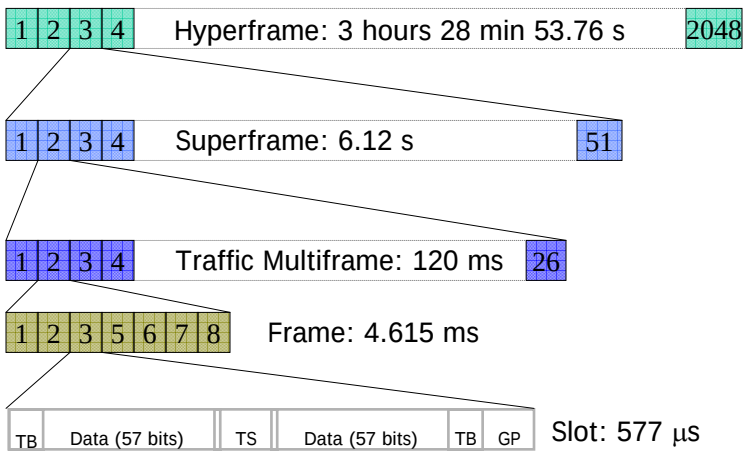
- Physical Channel – 1 time slot on a uplink/downlink radio carrier.
  - 125 radio carriers, 8 slots per carrier => 1000 physical channels
- Traffic Channels
  - Full rate (TCH/F) at 22.8 kb/s or half rate (TCH/H) at 11.4 kb/s
  - Physical channel = full rate traffic channel (1 timeslot) or 2 half rate traffic channels (1 timeslot in alternating frames)
  - Full rate channel may carry 13 kb/s speech or data at 12, 6, or 3.6 kb/s
  - Half rate channel may carry 6.5 kb/s speech or data at 6 or 3.6 kb/s
- Control Channels
  - Three groups of logical control channels
    1. BCH (broadcast channels): point-to-multipoint downlink only
    2. CCCH (common control channel): for paging and access
    3. DCCH (dedicated control channel): bi-directional point-to-point signaling

GSM Channels



Framing Scheme in GSM (Traffic Channels)

Framing scheme is implemented for encryption and identifying time slots



GSM Logical Channels (cont)

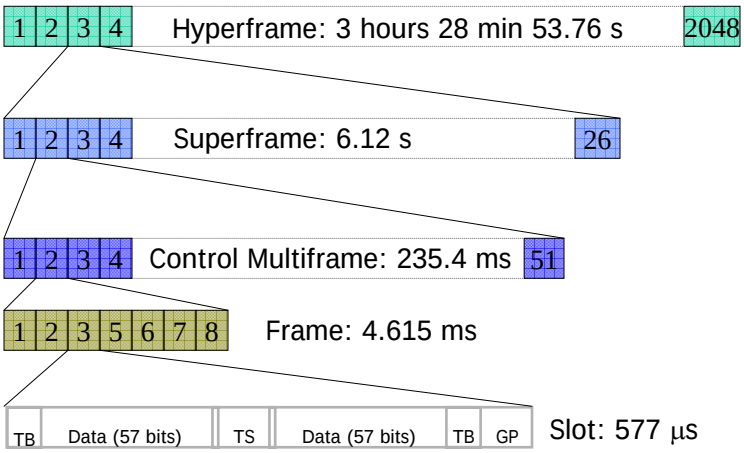
- **BCH (broadcast channels): point-to-multipoint downlink only**
  - BCCH (broadcast control channel): send cell identities, organization info about common control channels, cell service available, etc
  - FCCH (frequency correction channel): send a frequency correction data burst to effect a constant frequency shift of RF carrier
  - SCH (synchronization channel): send TDMA frame number and base station identity code to synchronize MSs
- **CCCH (common control channel): for paging and access**
  - PCH (paging channel): to page MSs
  - AGCH (access grant channel): to assign MSs to stand-alone dedicated control channels for initial assignment
  - RACH (random access channel): for MS to send requests for dedicated connections

GSM Logical Channels (cont)

- **DCCH (dedicated control channel): bidirectional point-to-point -- main signaling channels**
  - SDCCH (stand-alone dedicated control channel): for service request, subscriber authentication, equipment validation, assignment to a traffic channel
  - SACCH (slow associated control channel): for signaling associated with a traffic channel, eg, signal strength measurements
  - FACCH (fast associated control channel): for preemptive signaling on a traffic channel, eg, for handoff messages –sets S (stealing Flag in traffic slot)
- **Control channels are organized in a complex frame structure**
  - Certain ARFCNs are assigned as having a control channel – TS0 is used for control channel
  - One control channel per sector per cell.

Framing Scheme in GSM (Control Channels)

Framing scheme is implemented for encryption and identifying time slots



Control Channel Multiframe (Forward link TS0)

Control Multiframe = 51 TDMA Frames
235 ms

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	…	20	21	22	…	39	40	41	42	…	49	50
F	S	B	B	B	B	C	C	C	C	F	S	C	C	C		F	S	C		C	F	S	C		C	I

F: FCCH burst (BCH)
S: SCH burst (BCH)
B: BCCH burst (BCH)
C: PCH/AGCH burst (CCCH)
I: Idle

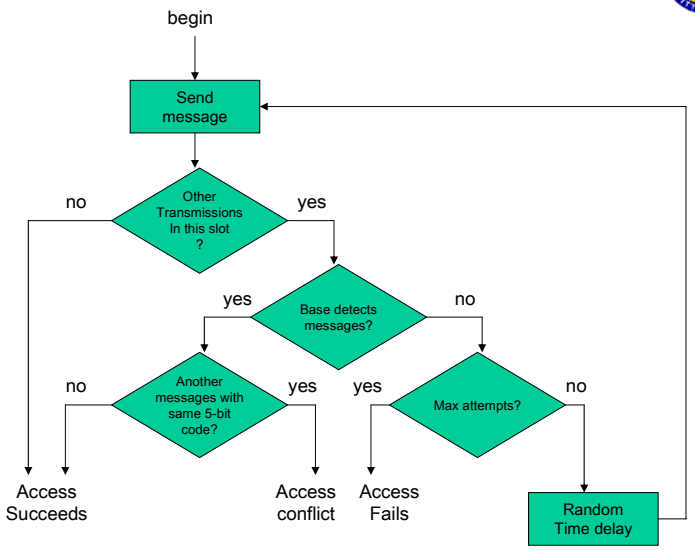
Control Channel Multiframe (Reverse link for TS0)

Control Multiframe = 51 TDMA Frames
235 ms

0	1	2	3	4	5	6	…….....	46	47	48	49	50
R	R	R	R	R	R	R		R	R	R	R	R

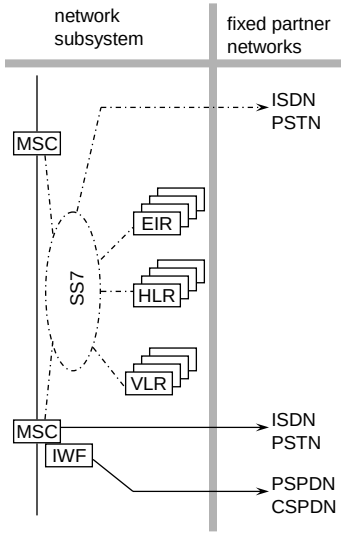
R: Reverse RACH burst (CH)

GSM Reverse Access Channel Protocol



GSM Access protocol for the random access channel RACCH.

System architecture: network and switching subsystem



Components

- *MSC* (Mobile Services Switching Center):
- *IWF* (Interworking Functions)

- *ISDN* (Integrated Services Digital Network)
- *PSTN* (Public Switched Telephone Network)
- *PSPDN* (Packet Switched Public Data Net.)
- *CSPDN* (Circuit Switched Public Data Net.)

Databases

- *HLR* (Home Location *R*egister)
- *VLR* (Visitor Location *R*egister)
- *EIR* (Equipment Identity Register)

Network and switching subsystem

NSS is the main component of the public mobile network GSM

- switching, mobility management, interconnection to other networks, system control

- Components
  - Mobile Services Switching Center (MSC)
    controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
- Databases (important: scalability, high capacity, low delay)
  - Home Location Register (HLR)
    central master database containing static user data, (mobile number, billing address, service subscribed, etc.) and dynamic data of all subscribers last VLR location
  - Visitor Location Register (VLR)
    local dynamic database for a subset of HLR data, including data about all user currently in the domain of the MSC attached to VLR

Mobile Services Switching Center

The MSC (mobile switching center) plays a central role in GSM

- switching functions
- additional functions for mobility support
- management of network resources
- interworking functions via Gateway MSC (GMSC)
- integration of several databases

- Functions of a MSC
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

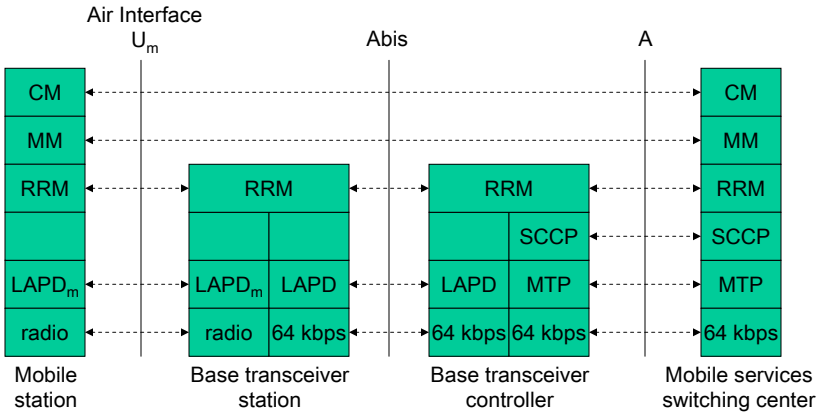
Operation subsystem

- OSS (Operation Subsystem) enables centralized operation, management, and maintenance
- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

GSM Protocol Stack

- Three Layers specified in the protocol
- Network layer has three sublayers
  1. Call Management
     - Establishment, maintenance, and termination of circuit-switched calls
  2. Mobility Management
     - Registration, authentication, and location tracking
  3. Radio Resource Management
     - Establishment, maintenance, and termination of radio channel connections
- Link Layer
  - Uses variation of ISDN LAPD protocol – termed $LAPD_m$
- Physical layer (already discussed)
  - Time slot on a 200 KHz carrier – absolute radio frequency channel number (ARFCN)

GSM Protocol Stack



CM: call management
MM: mobility management
RRM: radio resources management

SCCP: signal connection control part (SS7)
MTP: message transfer part (SS7)
LAPD: link access protocol-D channel (ISDN)

GSM Data Link $LAPD_m$ Messages

Table 7.2 Data Link Control Messages

Message Name	Function	Type	Purpose
SET ASYNCHRONOUS BALANCED MODE (SABM)	command	Unnumbered	initiate transfer of information messages
DISCONNECT	command	Unnumbered	terminate transfer of information messages
UNNUMBERED ACKNOWLEDGMENT (UA)	response	Unnumbered	confirm a command
RECEIVE READY	command or response	Supervisory	request transmission of information message
RECEIVE NOT READY	command or response	Supervisory	request retransmission of information message
REJECT	command or response	Supervisory	suspend transmission of information messages

GSM RRM Messages

Table 7.4 Radio Resources Management Messages

Message Name	Logical Channel	Transmitted by
SYNC CHANNEL INFORMATION	SCH	Base
SYSTEM INFORMATION (TYPE 1, 2, 3, 4, 5)	BCCH	Base
SYSTEM INFORMATION (TYPE 6)	SACCH	Base
CHANNEL REQUEST	RACH	Mobile
PAGING REQUEST (TYPE 1, 2, 3)	PCH	Base
IMMEDIATE ASSIGNMENT	AGCH	Base
IMMEDIATE ASSIGNMENT EXTENDED	AGCH	Base
IMMEDIATE ASSIGNMENT REJECT	AGCH	Base
ASSIGNMENT COMMAND*	FACCH	Base
ADDITIONAL ASSIGNMENT	FACCH	Base
PAGING RESPONSE	SDCCH	Mobile
MEASUREMENT REPORT	SACCH	Mobile
HANDOVER COMMAND*	FACCH	Base
HANDOVER ACCESS	TCH	Mobile
PHYSICAL INFORMATION	FACCH	Base
HANDOVER COMPLETE	FACCH	Mobile
CIPHERING MODE*	FACCH	Base
CHANNEL RELEASE	FACCH	Base
PARTIAL RELEASE*	FACCH	Base
FREQUENCY REDEFINITION	SACCH/ FACCH	Base
CLASSMARK CHANGE	SACCH/ FACCH	Mobile
CHANNEL MODE MODIFY*	FACCH	Base
RR STATUS	FACCH/ SACCH	Mobile/Base

GSM MM Messages

Table 7.5 Mobility Management Messages

Message Name	Transmitted by
AUTHENTICATION REQUEST	Base
AUTHENTICATION RESPONSE	Mobile
AUTHENTICATION REJECT	Base
IDENTITY REQUEST	Base
IDENTITY RESPONSE	Mobile
TMSI REALLOCATION COMMAND*	Base
LOCATION UPDATING REQUEST	Mobile
LOCATION UPDATING ACCEPT	Base
LOCATION UPDATING REJECT	Base
IMSI DETACH INDICATION	Mobile
CM SERVICE REQUEST*	Mobile
CM RE-ESTABLISHMENT REQUEST*	Mobile
MM-STATUS	Mobile/Base

GSM CM Messages

Table 7.6 Call Management Messages

Message Name	Transmitted by
Starting a Call	
SETUP	Mobile/Base
EMERGENCY SETUP	Mobile
CALL PROCEEDING	Base
PROGRESS‡	Base
CALL CONFIRMED	Mobile
ALERTING‡	Mobile/Base
CONNECT‡*	Mobile/Base
During a Call	
START DTMF*	Mobile
STOP DTMF*	Mobile
MODIFY*	Mobile/Base
USER INFORMATION‡	Mobile/Base
Ending a Call	
DISCONNECT‡	Mobile/Base
RELEASE‡	Mobile/Base
RELEASE COMPLETE‡	Mobile/Base
Abnormal Conditions	
STATUS	Mobile/Base
STATUS ENQUIRY	Mobile/Base
CONGESTION CONTROL	Mobile/Base

* There is also an acknowledgment message from the receiving network element corresponding to this message.

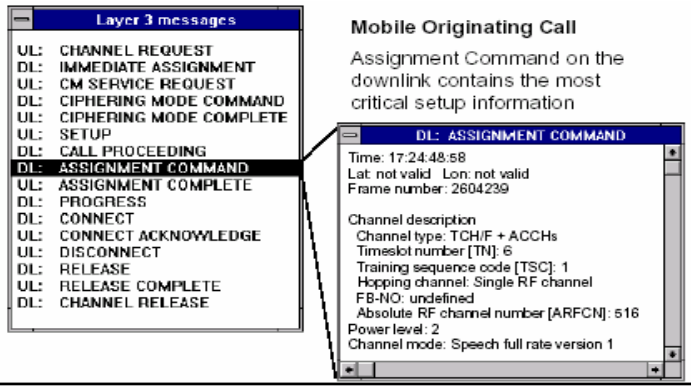
‡ This message contains an optional data field that carries user-to-user information as part of a GSM supplementary service.

Sample GSM Message

Assignment Command

message on FACCH used in handoff to inform of new channel info

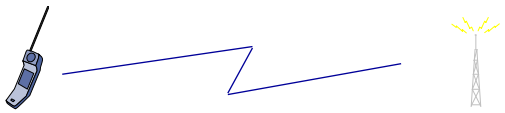
Bit Position	Information
1-4	Protocol Discriminator 0110 (RRM – message)
5-8	Transaction identifier
9-16	Message Type 00101110
17-40	Channel Description
41-48	Power Command
variable	Optional Data



GSM Call Management

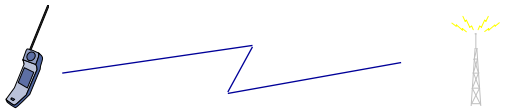
- Call Operation Types
  - Registration
    - Upon powering up, the MS scans common control channels and locks onto channel with strongest signal
    - Searches for FCCH on RF carrier, finds SCH to synch up
    - After synchronization the MS decodes BCCH – decides whether to update location register or not.
    - Once registered or locked on to BCCH
  - Mobile Originating (MO) Call
    - Mobile types in number presses Send
  - Mobile Terminating (MT) Call
    - Mobile registered and phone On – received incoming call

GSM Registration



Lock on strong freq. and find FCCH	**RF + FCCH** ←
Find SCH channel for sync. and training	**SCH sync + training** ←
Gets cell and system parameters	**BCCH system parameters** ←
Request stand alone dedicated channel	**RACH channel request** →
SDCCH established	**AGCH channel assignment** ←

GSM Registration (cont)



Make location update request	SDCCH location update →
Computes challenge response to verify identity	← SDCCH challenge
	SDCCH challenge response →
Initiate encryption of data for transmission	← SDCCH ciphered mode
	Ack ciphered mode →
Complete location update process	← Location update confirm
	Ack →

Location Registration

Register at power up/call placement/(power down)/ when detect a new location area id

Walkthrough Roaming case

1. Mobile-> MSC signals HLR update VLR pointer
2. Auc verifies user- may issue challenge/response
3. HLR – gives VLR mobile service profile
4. HLR – deregisters mobile from last VLR location

Target ITU-T bound on location registration ≤ 4sec

Location Update Types

- Intra – VLR (LAs attached to same VLR)
  - Only change LA id in VLR (local signaling)
  - Target ITU-T location update time ≤ 2 sec
- Inter –VLR (LAs attached to different VLR)
  - must signal HLR to update VLR pointer
  - Target ITU-T Location update time ≤ 4 sec

Location Update Call Flow

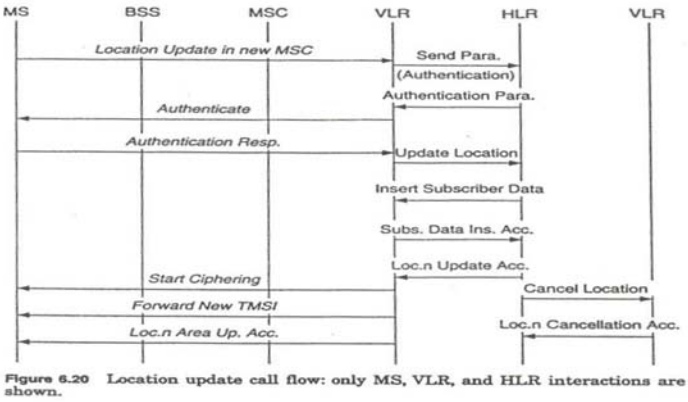
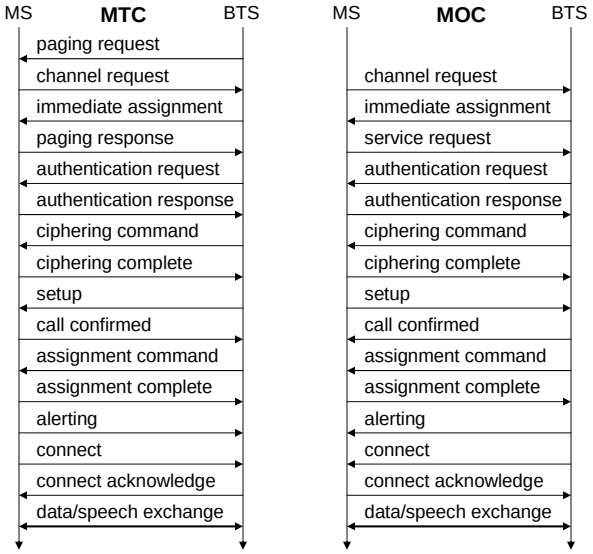
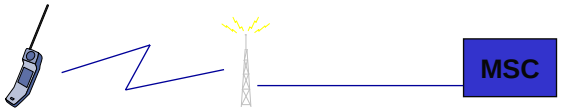


Figure 6.20 Location update call flow: only MS, VLR, and HLR interactions are shown.

MTC/MOC general behavior

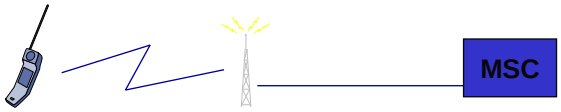


GSM MOC → Calling from MS



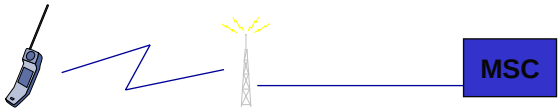
Dial called party	Setup Request →	
		Fetches subscriber info from VLR to process call, acks caller
	← Call Proceeding	
		Allocates trunk + radio channel
Tune to radio freq.	← Radio channel	
	Ack →	
	Complete →	Call connected through PSTN
	← Alerting	Alerts caller
	← Connect	Called party picks up
	Connect ack →	Call can proceed

GSM MTC → Calling to MS



		Incoming call from PSTN
Request dedicated control channel	← PCH page request	
	RACH channel request →	
	← AGCH assignment	Allocates control channel
Answer page	SDCCH paging response →	
	← SDCCH challenge	Request authentication
Computes response	SDCCH challenge response →	
	← SDCCH ciphering mode	Request ciphering on channel
Begin ciphering	Ciphering mode complete →	

GSM MTC → Calling to MS (cont)



	SDCCH setup ←	Notify call
Accept call	SDCCH setup ack →	
	SDCCH assignment ←	Assign traffic channel
Tune to freq.	Assignment complete →	
	FACCH alerting/connect ←	Alert called party
Start connection	FACCH connect ack →	

GSM Features

- Discontinuous Transmission (DTX)
  - Handset/BSC contain voice activity detectors (much of a conversation is silence!)
  - If no speech detected NO information is transmitted – TDMA slot left empty
  - Saves battery power in mobile
  - Reduces co-channel and adjacent channel interference
  - *Comfort Noise* is periodically played back if long silence period
- Power control
  - Both mobile and BTS regulate power (increase and decrease)
  - Mobile power adjusted in 2 dB levels, BTS power adjusted in 4 dB levels
  - Conserves battery power in mobile
  - Reduces interference
- Mobile Assisted Handoff (MAHO)
  - Mobile takes measurements of signals strength of radio channels in adjacent cells - reports to BSC and MSC to pick cell for handoff
- Sleep Mode
  - Handset once registered with network will be assigned a sleep mode level
  - Checks paging channel for page/SMS periodically depending on level

GSM Mobility Management

- Mobility Types
  - Track location of users for incoming calls/SMS
    - Location registration/authentication/paging
    - Divide coverage area into non-overlapping groups of cells – assign each a unique id
    - Location Area ID periodically broadcast by each cell
      - As a mobile moves/turns phone on – it listens to location area id – if different from last one registered in – performs a location update/authentication procedure with VLR and possibly HLR
  - Call in progress mobility
    - Handoff call from one BTS to another BTS
    - MAHO by mobile reporting measurements of signal strength

Location Management

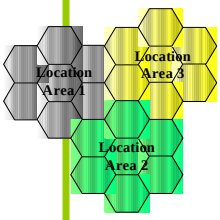
Location Area (LA)

- Divide coverage into non-overlapping groups of cells
- Assign each LA a unique id
- Location Area ID is periodically broadcast by each cell

Two level database hierarchy HLR/VLR

- HLR points to VLR where mobile located
- VLR entry points to LA where mobile last located

In large networks may have HLR split among regions with aggregate info cross region



Location Area and Cell Identification Parameters

MCC – Mobile Country Code
Uniquely identify the country of the GSM subscriber

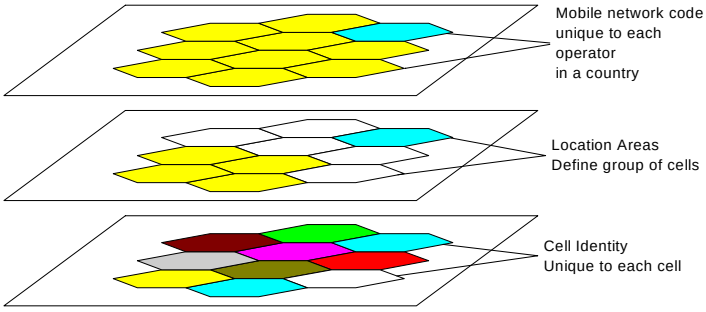
MNC – Mobile Network Code
Identifies the GSM operator within the country. Each country can have several GSM operators each having a unique MNC.

LAC – Location Area Code
Defines a location area, which consists of a group of cells. Each MNC can have several LACs.

CI – Cell Identity
Uniquely identifies a cell in a location area.

LAI – Location Area Identity
Uniquely identifies a location area in the network
Made up of MCC + MNC + LAC

CGI – Cell Global Identifier
Uniquely identifies the cell within the network
Made up of LAI + CI



GSM Handoffs

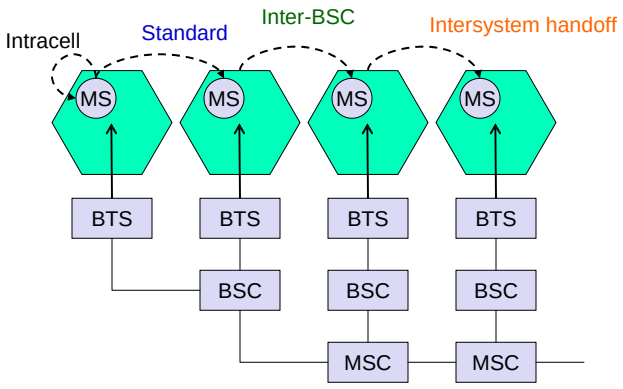
Handoff major decision-making stages

- Identify the need
- Identify the candidate
- Evaluate the candidates
- Select a target cell

Types of handoffs

- Intra-Cell : Handoff between sectors of same cell
- Intra-BSS: if old and new BTSs are attached to same base station
  - MSC is not involved
- Intra-MSC: if old and new BTSs are attached to different base stations but within same MSC
- Inter-MSC: if MSCs are changed
  - Handoff Forward, Handoff Back, Handoff to a Third

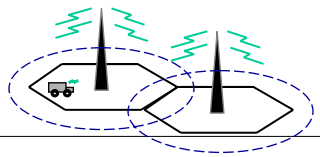
Types of Handoff



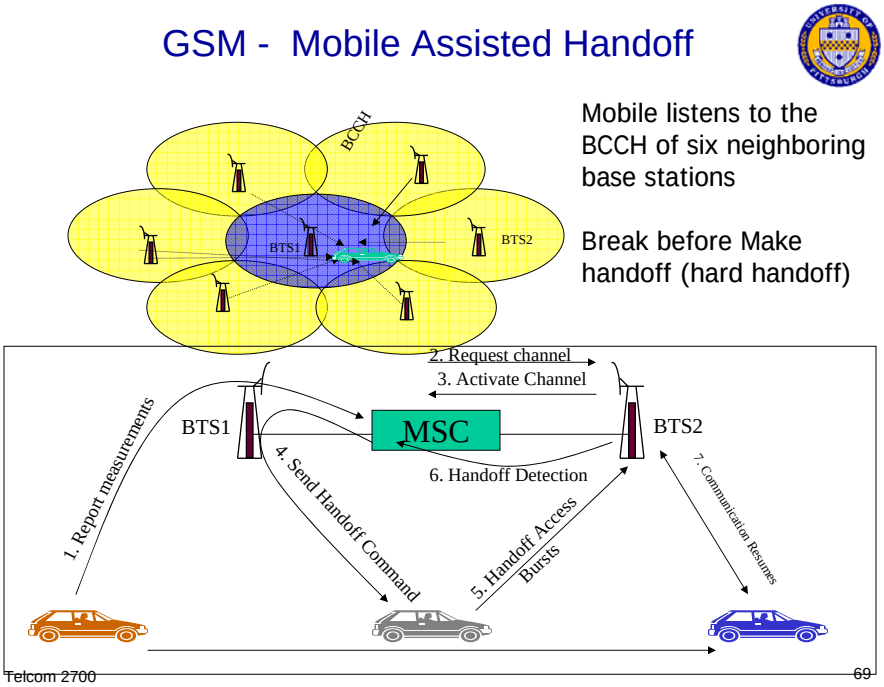
GSM - Handoff

Handoff initiation:

- Base station or MS notices signal is weakening (when the received signal strength goes below a certain threshold value)
- Base station or MS sends a handoff measurement request message to its BSC/MSC
- BSC/MSC requests
  - neighbor base stations to report their reception of mobile's signal strength
  - MS to measure strength of neighbor base stations on downlink
  - (called Mobile Assisted Handoff)
- BSC/MSC picks neighbor base station with highest received signal strength combination in up and downlink to handoff too



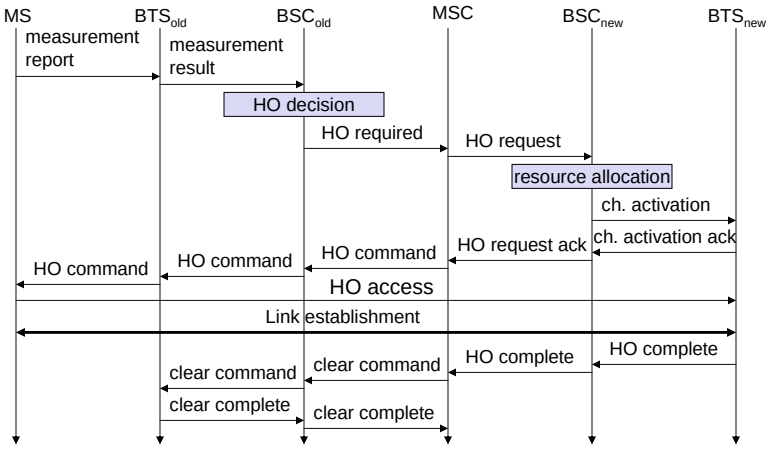
GSM - Mobile Assisted Handoff



Mobile listens to the BCCH of six neighboring base stations

Break before Make handoff (hard handoff)

Handoff Procedure



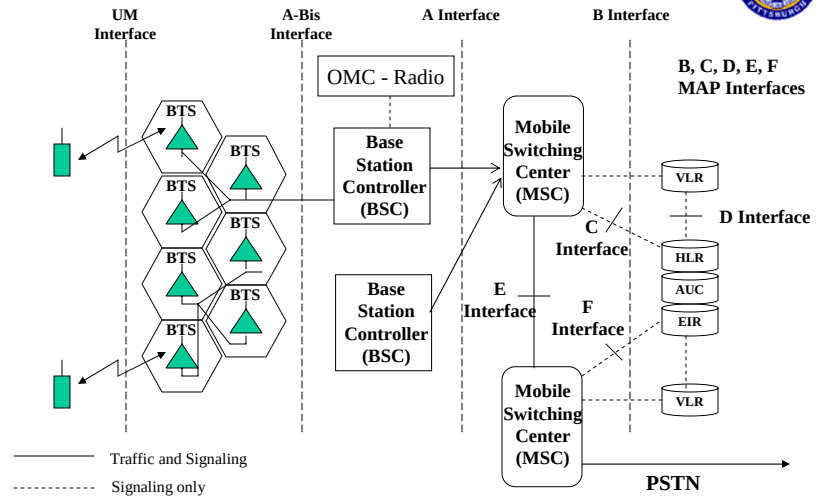
Security in GSM

Security services
- access control/authentication
  - user ⌫ SIM (Subscriber Identity Module): secret PIN (personal identification number)
  - SIM ⌫ network: challenge response method
- confidentiality
  - voice and signaling encrypted on the wireless link (after successful authentication)
- anonymity
  - temporary identity TMSI (Temporary Mobile Subscriber Identity)
  - newly assigned at each new location update (LUP)
  - encrypted transmission

3 algorithms specified in GSM
- A3 for authentication ("secret", open interface)
- A5 for encryption (standardized)
- A8 for key generation ("secret", open interface)

"secret":
• A3 and A8 available via the Internet
• network providers can use stronger mechanisms

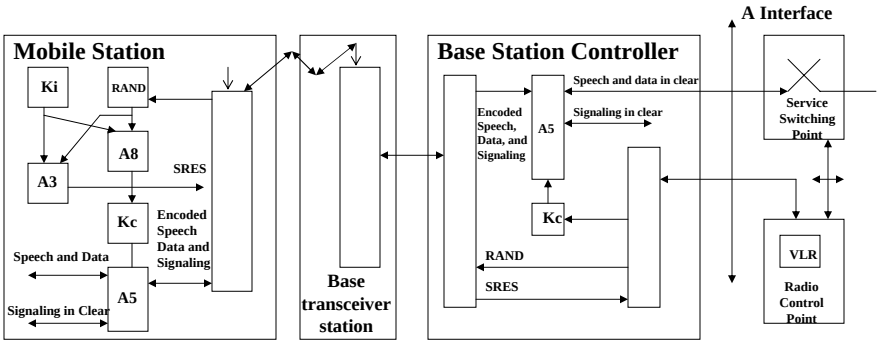
GSM System Architecture



VLR = Visitor Location Register
HLR = Home Location Register
EIR = Equipment Identity Register
AUC = Authentication Center

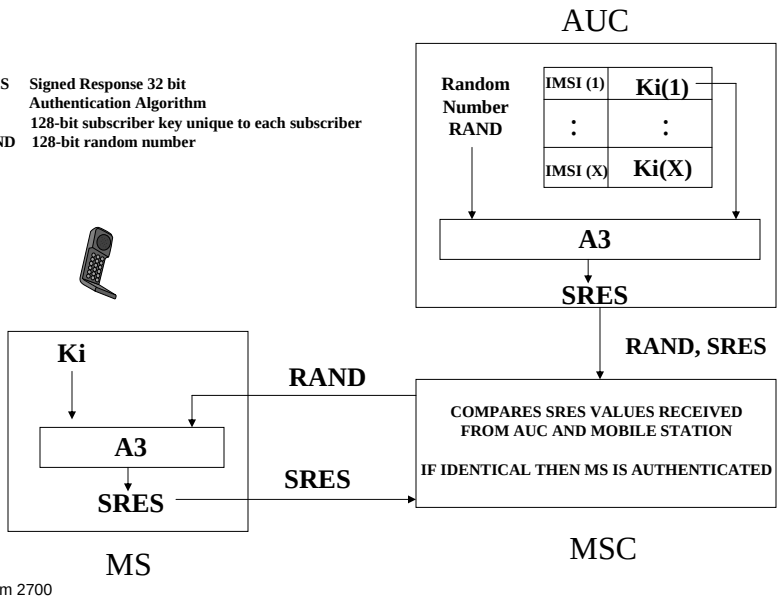
BTS = Base Transceiver Station
ADC = Admission Data Center
OMC = Operation Maintenance Center

Authentication and Encoding

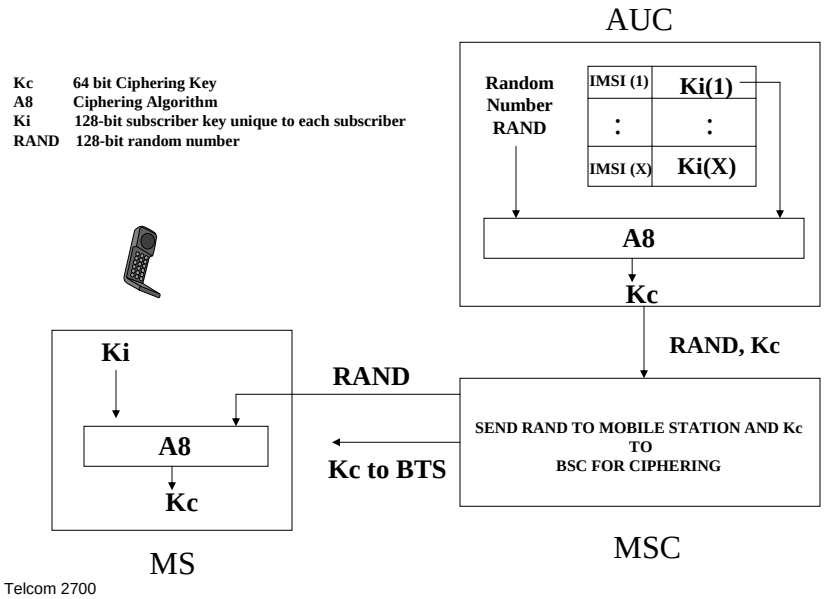


Authentication Procedure in GSM

SRES Signed Response 32 bit
A3 Authentication Algorithm
Ki 128-bit subscriber key unique to each subscriber
RAND 128-bit random number



Ciphering Procedure in GSM



Data services in GSM

Circuit Switched Data transmission standardized at 9.6 kbit/s

- advanced coding allows 14.4 kbit/s in a standard TDMA slot
- Widely deployed and used by WAP GSM phones
- not enough bandwidth for multimedia applications

HSCSD (High-Speed Circuit Switched Data)

- already standardized
- bundling of several time-slots on a radio carrier to get higher data rate : called AIUR (Air Interface User Rate)
  maximum rate 57.6 kbit/s using 4 slots, 14.4 kbps each
  (4 slot limit to allow MS to transmit then listen to downlink channel)
- Advantages: ready to use, constant quality, simple no additional equipment needed in network just software upgrades
- Disadvantage: channels blocked for voice transmission, expensive, not supported by all service providers

Most operators now have 2.5G solutions like GRPS or EDGE in place – 3G slowly being rolled out