KUNGL TEKNISKA HÖGSKOLAN
Institutionen för mikroelektronik och informationsteknik

2G1330 Mobile and Wireless Network Architectures

GSM, GPRS, SMS, International Roaming, OAM

Lecture notes of G. Q. Maguire Jr.

For use in conjunction with *Wireless and Mobile Network Architectures*, by Yi-Bing Lin and Imrich Chlamtac, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Last modified: 2002.03.14:11:59

Lecture 3

- GSM (Chapters 9,10, and11), GPRS (Ch. 18), SMS (Ch. 12), International Roaming (Ch. 13), Operation/Administration/Maintainence (Ch. 14)

Global System for Mobile Communications(GSM)

- designed to be a digital (wide area) wireless network
- driven by european telecom manufacturers, operators, and standardization committees
- very widely used around the world

GSM Requirements

- Service portability
  - mobile should be able to be used in any of the participating countries with international roaming and standardized numbering & dialing (but possibly at different rates!)
  - usable for both wireline line services and for mobile service
  - usable when: walking, driving, boating, … (upto 250 km/h)
- Quality of service and Security
  - quality at least as good a previous analog systems
  - capable of offering encryption
- Good radio frequency utilization
  - high spectrum efficiency
  - co-existance with earlier systems in the same bands
- Modern network
  - following ITU recommendations - to allow efficient interoperation with ISDN networks
  - supporting voice and low rate data
  - standardized mobility and switching support
  - standardized interfaces between the subsystems - to allow a mix-and-match system
- System optimized to limit cost of mobiles (and to a lesser extent to limit the cost of the whole system)
  - GSM required higher complexity mobiles than earlier analog systems
  - subscriber cost less than or equal to existing analog systems

GSM Architecture

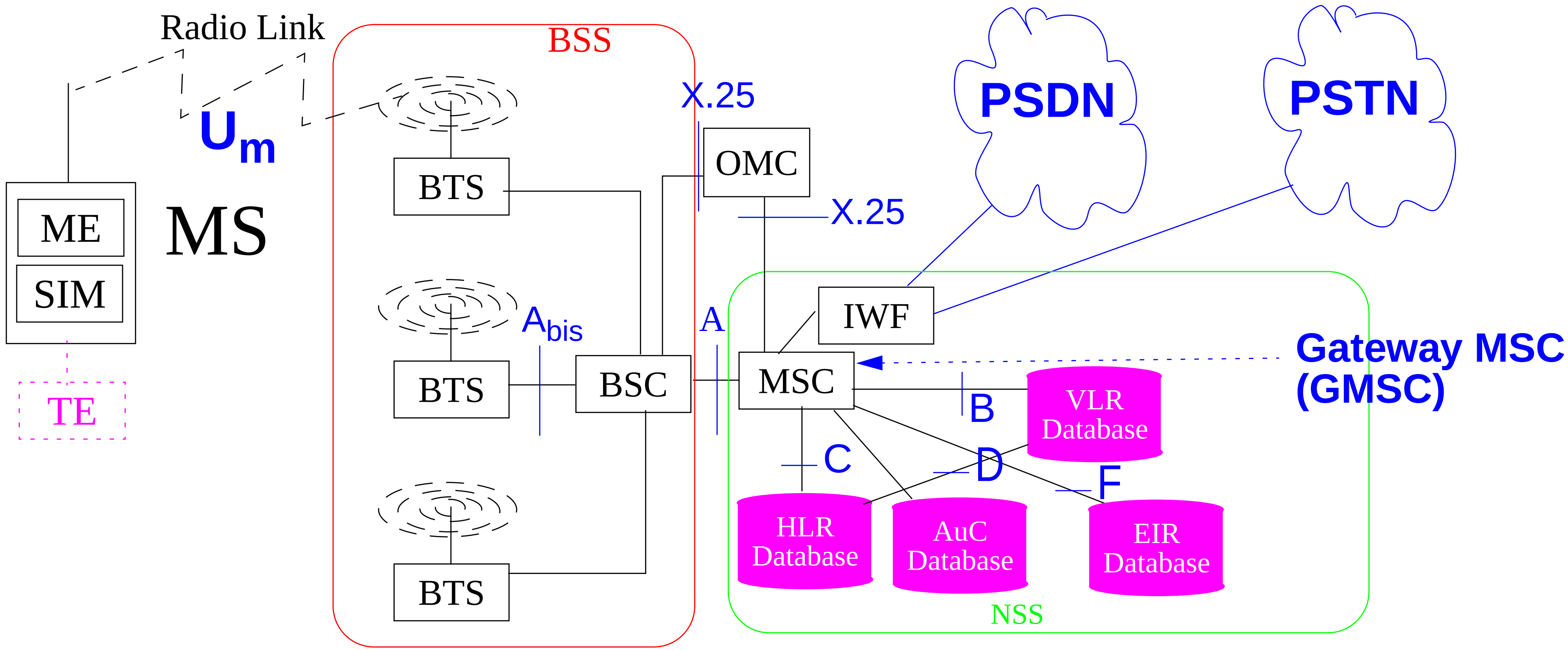


Figure 1: GSM Architecture

MS	Mobile Station
BSS	base station system
NSS	network and switching subsystem

Foundation

- Hybrid frequency-division/time-division multiple access
  - FDMA - division by frequency of the (maximum) 25 MHz allocated bandwidth into 124 carrier frequencies spaced 200 kHz apart.
    - One or more carrier frequencies assigned to each base station
  - Each carrier frequency divided in time, using TDMA
  - Fundamental unit of time in this TDMA scheme is a burst period approx. 0.577 ms long
  - Eight burst periods are grouped into a TDMA frame (approx. 4.615 ms) = basic unit for the definition of logical channels
  - A physical channel is one burst period per TDMA frame
  - Slow frequency at upto 217 times per second
    - hopping algorithm is broadcast on the broadcast control channel
    - helps alleviate multipath fading
    - co-channel interference is effectively randomized
    - Note: broadcast and common control channels are not subject to frequency hopping and are **always** transmitted on the same frequency
- Infrastructure based on Signalling System 7 (SS7)

GSM contributions

- Location-based mobility management
- Mobile assisted handover
- Temporary Mobile Subscriber ID (TMSI)

Distintive features of GSM

- Cooperative development by many actors from many countries
- preserved open interfaces between the subsystems (especially between infrastructure elements -- particularily between base stations and switches)
- specified a large number of interfaces!
- Phased release - since they could not make all the innovations in time for their targeted 1991 introduction
  - Phase 1 GSM spec. - 100 sections and 5,320 pages!
    - telephony - with some added features
    - emergency calls
    - data transmission at 2.4/4.8/9.6 kbit/s (transparent {the error correction done by a forward error correction (FEC) mechanism}/non-transparent {information is repeated when it has not been correctly received})
    - short message service (SMS)
  - Phase 2
    - non-voice services and enriched telephony

Mobile Station (MS)

- Subscriber Identity Module (SIM)
- Mobile Equipment (ME)
- Mobile Terminal (MT)

Subscriber Identity Module (SIM)

- small form factor - which can be removable and can be moved from one terminal to another
  - smart card (generally too large for handsets!)
  - plug-in SIM (the processor and contact from a smart card)
- **user** authenticated via a Personal Identity Number (PIN)
- if PIN entered incorrectly, N times, then phone is locked for all but emergency calls, until you enter a PIN unblocking key (PUK)
- contains subscriber information:
  - some which is fixed by operator (may include preferred network provider(s))
  - some which is changable by the user (list of short numbers, phone list, SMS messages, …)
- can be updated via:
  - keyboard
  - attached terminal equipment
  - over the air (OTA) via SMS message sent by operator/application/… built using SIM Toolkit
- often the SIM is owned by the operator
- profiles - operator/subscription info; SIMs are required to be able to hold at least two profiles
- contains International Mobile Subscriber Identity (IMSI)

Mobile Equipment (ME)

"the phone" itself - radio and radio interface, display, keyboard, etc.

performs: radio transmission and reception, authentication, handover, encoding and channel encoding.

note: ME with SIM can only make emergency (112) calls

Radios operate in one or more of the following bands:

- GSM900 since 900 MHz - the original frequency band
  - Uplink: 890..915 MHz (= mobile station to base station)
  - Downlink: 935..960 MHz (= base station to mobile station)
- GSM1800 (also known as DCS1800)
  - Uplink: 1710..1785 MHz
  - Downlink: 1805..1880 MHz
- GSM1900 (also known as PCS 900)
  - Uplink: 1850..1910 MHz
  - Downlink: 1930..1990 MHz

ME identified by International Mobile Equipment Identity (IMEI)

Power saving and interference reduction

- To reduce the MS's power consumption and minimize interference on the air interface, during pauses in speech the MS does not transmit - this is called: Discontinuous transmission (DTX)
  - "Comfort noise" is artificially generated by the MS
- Discontinuous reception (DRX) - mobile listens to the paging channel, but only needs to wake up for its sub-channel of the paging channel
- To minimize co-channel interference and to conserve power, both the mobiles and the base transceiver stations operate at the lowest power level that will maintain an acceptable signal quality
  - Power levels can be stepped up or down in steps of 2 dBm from the peak power for the class down to a minimum of 13 dBm (20 milliwatts for MS)
  - only one step at a time and each step takes 60ms
  - there are 16 power levels (i.e., 30 db of range)
  - terminal is typically only transmitting in one time slot (i.e., 1/8 of the time - so its radiated power is on average 8db lower than the set power level)
  - Both mobile station and BTS continually measure the signal strength or signal quality (based on the bit error ratio), and pass the information to the base station controller (which manages power levels).

Classmark

32 bit quantity indicating properties of a mobile station

- revision level
- RF power capability

Figure 2: Power classes

Class	GSM900	DCS1800	
1	20 W	1 W	vehicle mounted systems
2	8 W[a]	0.25 W	vehicle mounted systems
3	5 W		
4	2 W[b]		portable terminals
5	0.8 W		

a. 1W average if using a single time slot per frame

b. 250mW average if using a single time slot per frame

- (available) encryption procedures
- frequency capabilities (i.e., which bands)
- if the device is SMS capable

User ID ≠ Device ID

IMEI	International Mobile Equipment Identity	15 digits
IMSI	International Mobile Subscriber Identity	15 digits
TMSI	Temporary Mobile Subscriber Identity	32 **bits**

An important distinction in GSM is that due to the SIM card the user (or at least IMSI) can be identified separately from the device (MS).

TMSI is assigned by the VLR to a visiting subscriber

IMEI consists of:

- Type Approval Code (TAC)
- Final Assembly Code (FAC) to identify the final assembly plant
- Serial number - allocated to the manufacturers.

Mobile Terminal (MT)

Generally a PDA, PC, …

Interface can be serial (DTE-DCE) interface: serial cable, PCMCIA, IrDA; Bluetooth, …

AT commands:

AT Command	Description	AT Command	Description
+CNMI	New message inication to TE	+CMT	SMS Message Received
+CBM	New Cell-Broadcast Message (CBM)	+CNMA	New Message ACKnowledgement to ME/TE
+CMGC	Send Command	+CPMS	Preferred Message Storage
+CMGD	Delete Message	+CSCA	Service Center Address
+CMGL	List Message	+CSCB	Select Broadcast Message Type
+CMGR	Read Message	+CSDH	Show Text Mode Paramaters
+CMCS	Send Message	+CSMP	Set Text Mode Parameters
+CMGW	Write Message to Memory	+CRES	Restore Setting

Base Station System (BSS)

- one or more base transceiver station (BTS) and
- base station controller (BSC)

Base transceiver station (BTS)

Performs: channel coding/decoding and encryption/decryption

BTS includes: radio transmitters and receivers, antennas, the interface to the PCM facility, …

About 1/2 the processing is associated with transcoding speech channel to/from GSM coding

Base station controller (BSC)

BTSs are connected to a BSC which manages the radio resources

- call maintenance using the received signal strength sent by mobile stations normally every 480 ms
- initiate handovers to other cells,
- change BTS transmitter power, …

Task breakdown:

call activities	~20-25%
paging and SMS	~10-15%
mobility management	~20-25%
hardware checking/network triggered events	~15-20%

BSCs engineed for about 80% utilization, if overloaded, shed load by: (1) rejecting location updates, (2) rejecting MS originating calls, and (3) ignoring handoffs

Network and Switching Subsystem (NSS)

- MSCs
  - Gateway MSC (GMSC) has interconnections to other networks
- Databases
- Gateways

Databases

Home Location Register (HLR)	database for management of mobile subscribers, stores the international mobile subscriber identity(IMSI), mobile station ISDN number (MSISDN) and current visitor location register (VLR) address keeps track of the services associated with each MS an HLR may be used by multiple MSCs
Visitor Location Register (VLR)	caches some information from the HLR as necessary for call control and service provisioning for each mobile currently located in the geographical area controlled by this VLR connected to one MSC and is often integrated into the MSC
Authentication Center (AuC)	a protected database which has a copy of the secret key stored in each subscriber's SIM card this secret is used for authentication and encryption over the radio channel normally located close to HLR
Equipment Identity Register (EIR)	contains a list of all valid mobile station equipment within the network, where each mobile station is identified by its international mobile equipment identity (IMEI) - split into 3 databases: • White list: all known, good IMEIs • Black list: bad or stolen handsets • Grey list: handsets/IMEIs that are uncertain

Equipment Identity Register (EIR)

Optional in a GSM network, i.e., not required

EIR block (bars) calls from a MS, **not** from a subscriber.

Sometimes the AuC and EIR are combined.

Operation Sub-System (OSS)

- Operation and Maintenance Center
- Service management
  - subscription management for registering new subscriptions, modifying and removing subscriptions, as well as billing information
  - billing
  - fraud detection
  - …

Operation and Maintenance Center (OMC)

Manages the GSM functional blocks: MSC, BSC (and indirectly the BTSs)

Task: to maintain satisfactory operation of the GSM network

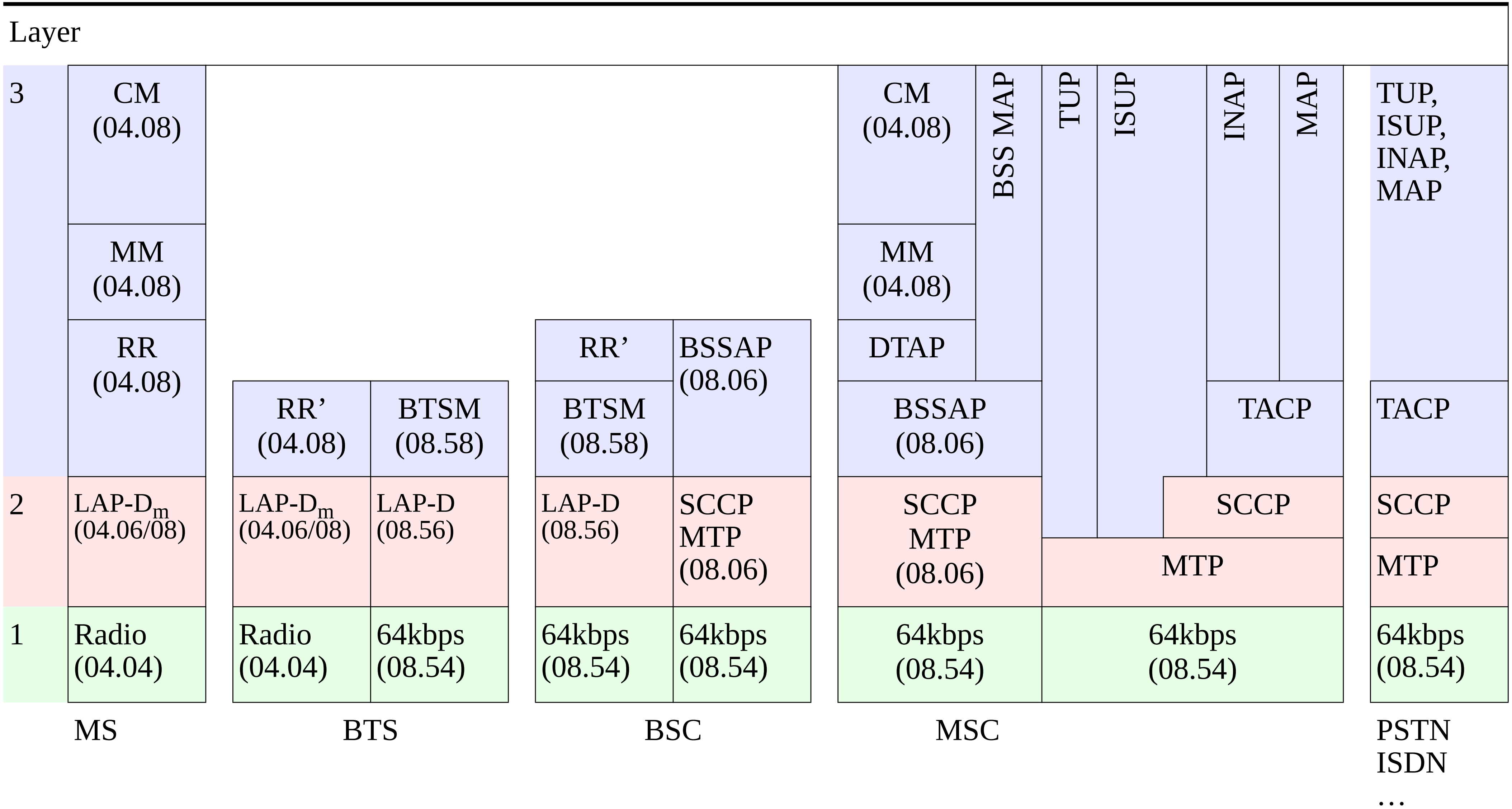
Based on observing system load, blocking rates, handovers,…

Activities:

- Network Management System (NMS)
  - modify network configuration
- equipment maintenance aiming at detecting,locating, and correcting faults

GSM Interfaces

Interface	Description
U_m	Radio link between MS and BTS
A_{bis}	between BTS and BSC, PCM 2 Mbit/s, G. 703
A	between BSC and MSC, PCM 2 Mbit/s, G. 703
B	between MSC and VLR (use MAP/TCAP protocols)
C	between MSC and HLR (MAP/TCAP)
D	between HLR and VLR (MAP/TCAP)
E	between two MSCs (MAP/TCAP + ISUP/TUP)
F	between MSC and EIR (MAP/TCAP)
G	between VLRs (MAP/TCAP)



Numbers in parentheses indicate the relevant ETSI-GSM recommendations.

GSM Layers

- Layer 1: Physical layer
  - physical transmission
  - channel quality measurements
  - GSM Rec. 04.04, PCM 30 or ISDN links are used (GSM Rec. 08.54 on A bis interface and 08.04 on A to F interfaces)
- Layer 2: Data link layer
  - Multiplexing of layer 2 connections on control/signaling channels
  - Error detection (based on HDLC)
  - Flow control
  - Transmission quality assurance
  - Routing
- Layer 3: Network layer
  - Connection management (air interface)
  - Management of location data
  - Subscriber identification
  - Management of added services (SMS, call forwarding, conference calls, etc.)

GSM Air interface

- Layer 1 (GSM Rec. 04.04): Um interface
- Layer 2 (GSM Rec. 04.05/06): LAP-D_m protocol (similar to ISDN LAP-D):
  - connectionless transfer of point-to-point and point-to-multipoint signaling channels
  - Setup and tear-down of layer 2 connections of point-to-point signaling channels
  - connection-oriented transfer with in order delivery, error detection and error correction
- Layer 3 (GSM Rec. 04.07/08) with sublayers for control signaling channel functions (BCH, CCCH and DCCH):
  - Radio resource management (RR): to establish and release stable connection between mobile stations (MS) and an MSC for the duration of a call and to maintain connection despite user movements - functions of MSC:
    - cell selection
    - handover
    - allocation and tear-down of point-to-point channels
    - monitoring and forwarding of radio connections
    - enabling encryption
    - change transmission mode
  - Mobility management (MM) handles the control functions required for mobility:
    - authentication
    - assignment of TMSI,

- management of subscriber location
- Connection management (CM) - set up, maintain and tear down calls connections:
  - Call control (CC): Manages call connections,
  - Supplementary service support (SS): Handles special services,
  - Short message service support (SMS): Transfers brief text messages

Neither the BTS nor the BSC interpret CM and MM messages, these messages are exchanged between the MSC or the MS using the direct transfer application part (DTAP) protocol on the A interface.

Radio Resource Management (RR) messages are mapped to or from the base station system application part (BSSAP) for exchange with the MSC:

- Transmission mode (change) management
- Cipher mode management
- Discontinuous transmission mode management
- Handover execution
- Call re-establishment
- RR-session release
- Load management
- SACCH procedures
  - radio transmission control (power&timing, downlink), (measurements, uplink)
  - -general information
- Frequency redefinition
- General information broadcasting (BCCH)

- cell selection information
- information for idle mode functions
- information needed for access
- cell identity

A_{bis} interface

Dividing line between the BSC function and the BTS

BSC and BTS can be connected using leased lines, radio links, metropolitan area networks (MANs), LANs {see UC Berkeley's ICEBERG}, …

Two channel types exist between the BSC and BTS:

- Traffic channels (TCH): configured in 8, 16 and 64 kbit/s formats - for transporting user data
- Signaling channels:configured in 16, 32, 56 and 64 kbit/s formats - for signaling purposes between the BTS and BSC

Each transceiver (transmitter + receiver) generally requires a signaling channel on the A_{bis} interface, data is sent as TRAU (Transcoder Rate Adapter Unit)[1] frames (for a 16 kbit/s traffic channel (TCH), 13.6 kbit/s are used for user data and 2.4 kbit/s for inband signaling, timing, and synchronization)

1. It is not defined where TRAU is placed, i.e., it could be part of BTS, BSC, or MSC.

A_{bis} protocols

- Layer 1 (GSM Rec. 08.54)
  - 2.048 Mbit/s (ITU-T: E1) or 1.544 Mbit/s (ANSI: T1) PCM facility
  - with 64/32/16 kbit/s signaling channels and 16 kbit/s traffic channels (4 per timeslot)
- Layer 2 (GSM Rec. 08.56)
  - LAP-D protocol used for data messaging between the BTS and BSC
  - SAPI refers to the link identifier transmitted in the LAPD protocol (inherited from ISDN)
- Layer 3 (GSM Rec. 08.58/04.08)
  - BTS management (BTSM) via three logical signaling connections identified by SAPI (Service Access Point Identifier):
    - SAPI 0 is used by all messages coming from or going to the radio interface
    - SAPI 62 provides O&M message transport between the BTS and BSC
    - SAPI 63 is used for dynamic management of TEIs as well as for layer 2 management functions.

A Interface

Defines interface between the BSC and MSC

TCHs are converted from 64 kbit/s to 16 kbit/s in the transcoder equipment, two cases based on where the transcoder equipment (TCE, i.e., TRAU) is located:

at BSC or BTS	traffic channel (TCH) occupies a complete 64 kbit/s timeslot in the 2 Mbit/s or 1.544 Mbit/s PCM link (layer 1, GSM Rec. 08.04)
at MSC	the TCHs are 16 kbit/s on the A interface

At least 2 time slots on the PCM link are needed for control and signaling purposes.

A interface protocols

Signaling protocol (layer 2+3) between BSC and MSC based on the SS7 standard and is transmitted along with the user data within the PCM facility. Normally timeslot 16 (TS16) of the 64 kbit/s frame is used.

The following protocols are employed:

- Layer 1 (GSM Rec. 08.04) either 2.048 Mbit/s (ITU-T: E1) or 1.544 Mbit/s (ANSI: T1) PCM link
- Layer 2 (GSM Rec. 08.06) SS7-based protocols
  - Message transfer part (MTP) protocol - transmission security between the BCS and MSC
  - Signaling connection control part (SCCP) protocol
  - SCCP connection can be initiated by a mobile station (MS) or an MSC
  - An SCCP connection can involve the following protocols:
  - From the MS:
    - MM: CM service request
    - RR: Paging response
    - MM: Location updating request
    - MM: CM re-establishment request
  - From the MSC:
    - Initiation of an “external handover” (BSSMAP: handover request).
  - MSC manages the SCCP connections

- Layer 3 (GSM Rec. 08.08)
  - Base station system application part (BSSAP) protocol
  - On MSC end:
    - Base station management application part (BSSMAP) protocol - counterpart to the RR protocol on the air interface
    - Direct transfer application part (DTAP) protocol transmits CC and MM messages transmitted transparently through the BTS and BSC

GSM Audio

- Speech coding - 20ms (i.e., 160) samples (8kHz @13 bits) are buffered then coded
- Error protection (codec specific)
- Error detection (CRC)
- Bad Frame Handling (substitution)
- Voice Activity Detection / Discontinuous Transmission (VAD/DTX)

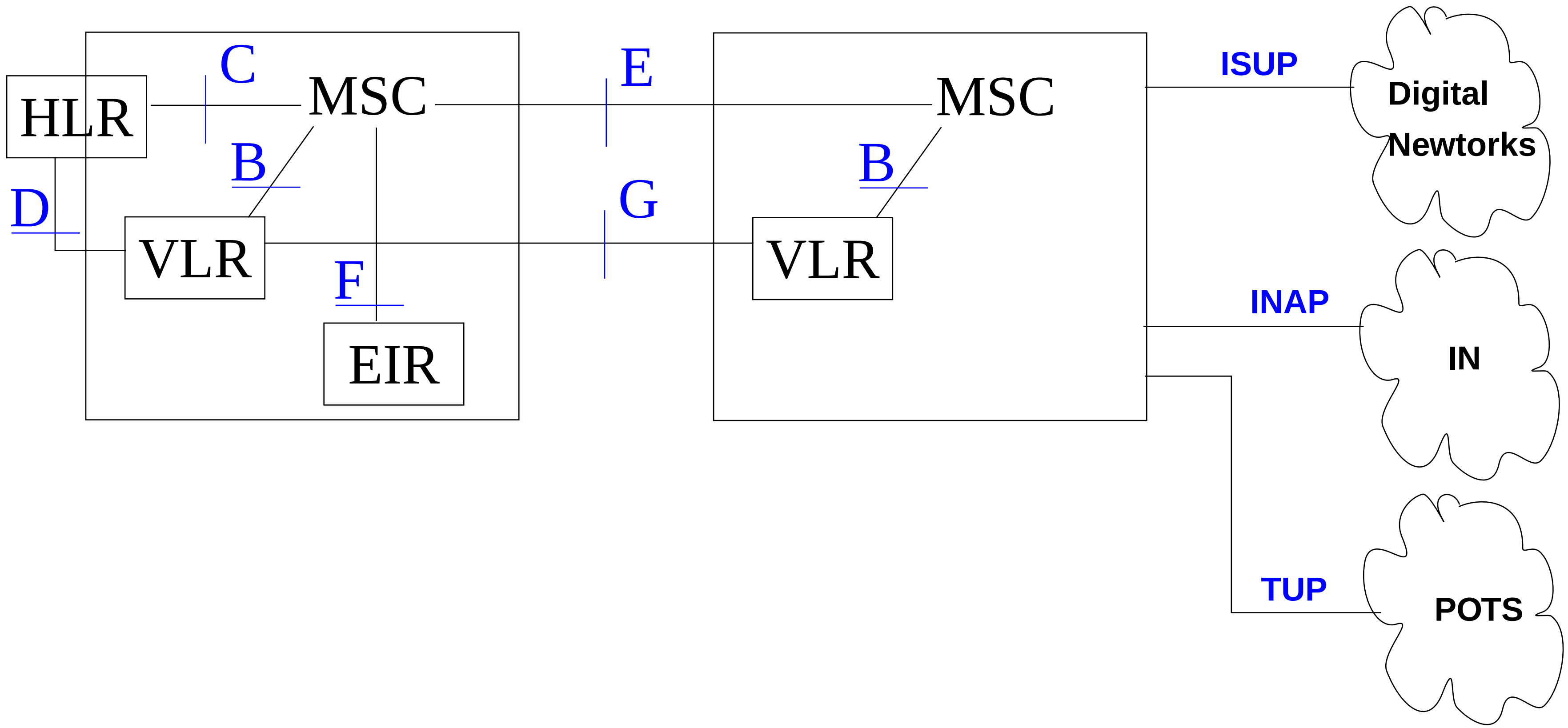
Manufacturer specific audio features:

- noise cancelling
- spectrum equalization
- echo cancellation

CODECs

Full rate (FR)	13 kbit/s , Regular pulse excitation - long term prediction (RPE-LTP)
Half rate (HR)	5.65 kbit/s VSELP
Enhanced full rate (EFR)	12.2 kbit/s ACELP
Adaptive Multi Rate (AMR)	ACELP, 12.2, 10.2, 7.95, 7.4, 6.7, 5.9, 5.15, 4.75 kbit/s
AMR wideband codec	(under standardization)

MSC interfaces



MSC protocols

- MAP (Mobile Application Part) (GSM Rec. 09.02)
  - controls queries to the different databases in the mobile radio network (HLR, VLR, and EIR)
  - responsibilities include access and location management, MSC-MSC handover, security functions, O&M, SMS, and supplementary services.
- TCAP (Transaction Capabilities Application Part)
  - provides universal calls and functions for handling requests to distributed application processes
- ISUP (ISDN User Part)
  - controls interworking (e.g. call setup/tear-down) between Public Land Mobile Networks (PLMNs) and other networks, and provides the same basic functionalities as TUP
- INAP (Intelligent Network Application Part)
  - implements intelligent supplementary services (e.g. free call, time-dependent routing functions in a central service center)
- TUP (Telephone User Part)
  - implements interworking between PLMNs and other networks
  - used to provide international connections and is being replaced by ISUP

GSM Logical Channels

Traffic channels		Full-rate (TCH/F) @ 22.8 kbit/s Half-rate (TCH/H) @ 11.4 kbit/s	Two way
Signaling channels	Broadcast channels	Frequency correction (FCCH)	base-to-mobile
		Synchronization (SCH)	
		Broadcast control (BCCH)	
	Common control channels	Paging (PCH)	
		Access Grant (AGCH)	
		Random access (RACH)	mobile-to-base
	Dedicated control channels	Stand-alone dedicated control channel (SDCCH)	two-way
		Slow associated control (SACCH)	
		Fast associated control (FACCH)	

Traffic channel (TCH)

Multiframe - group of 26 TDMA frames (120 ms long)

- 24 are used for traffic (voice or user data)
- 1 is used for the slow associated control channel (SACCH)
- 1 is currently unused

TCHs for the uplink and downlink are separated in time by 3 burst periods

- mobile station does not have to transmit and receive simultaneously
- simplifies the electronic circuitry; avoids antenna duplex filters
- reducing complexity helps to cut power consumption

Broadcast channels (BCH)

Carry only **downlink** information - mainly for synchronization and frequency correction.

However, it is the only channel capable of point-to-multipoint communications in which short messages are simultaneously transmitted to several mobiles.

- Broadcast control channel (BCCH)
  - General information, cell-specific; e.g. local area code (LAC), network operator, access parameters, list of neighboring cells, etc. A MS receives signals via the BCCH from many BTSs within the same network and/or different networks
  - tells MS what their initial power level should be
- Frequency correction channel (FCCH)
  - correction of MS frequencies
  - transmission of frequency standard to MS
  - also used for synchronization of an acquisition by providing the boundaries between timeslots and position of the first time slot of a TDMA frame
- Synchronization channel (SCH)
  - frame synchronization (TDMA frame number) and identification of base station
  - reception of one SCH burst provides a MS with all the information needed to synchronize with a given BTS

Common control channels (CCCH)

Uplink and downlink channels between the MS card and the BTS.

Convey information from the network to MSs and provide access to the network.

- Paging channel (PCH)
  - Downlink only
  - MS is informed (by the BTS) of incoming calls via the PCH.
- Access grant channel (AGCH)
  - Downlink only
  - BTS allocates a TCH or SDCCH to the MS, thus allowing the MS access to the network.
- Random access channel (RACH)
  - Uplink only
  - allows MS to request an SDCCH in response to a page or due to a call
  - MS chooses a random time to send on this channel (note: potential collisions with RACH transmissions from other MSs)

PCH and AGCH are transmitted in one channel called the paging and access grant channel (PAGCH) - they are separated in time.

Dedicated control channels (DCCH)

Responsible for roaming, handovers, encryption, etc.

- Stand-alone dedicated control channel (SDCCH)
  - communications channel between MS and the BTS
  - signaling during call setup -- before a traffic channel (TCH) is allocated
  - It takes ~480ms to transmit a message via SDDCH
- Slow associated control channel (SACCH)
  - always allocated to a TCH or SDCCH
  - used for “non-urgent” procedures: radio measurement data (e.g. field strengths) {information is used for handover decisions}, power control (downlink only), timing advance[1], …
  - 260bps channel - enough for reporting on the current cell and upto 6 neighbors about twice per second (if there is no other traffic for this channel)
  - note that the MS is told what frequencies to monitor (BTSs have a color code assigned to them so the that the MS can report on multiple BTSs which are using the same frequency)
- Fast associated control channel (FACCH)
  - similar to the SDCCH, but used in parallel to operation of the TCH
  - if the data rate of the FACCH is insufficient, “borrowing mode” is used (i.e., additional bandwidth borrowed from the TCH), this happens for messages associated with call establishment authentication of the subscriber, handover decisions, …

1. Transmission and reception of bursts at the base station must be synchronized, thus the MS must compensate for the propagation delays by advancing its transmission 0 .. 233 ms which is enough to handle cells of radius up to 35 km.

- It takes ~40ms to transmit a message via FACCH

GSM Timing

A **very elaborate** timing structure ranging from 1/4 of a bit (900ns) to an encryption hyperframe (3 hours 28 minutes and 53.76s)!

Unit	Time		
bit	3.69us		
slot	156.25 bits (577 us)		
frame	8 slots (4.615 ms)		
traffic multiframe	26 frames (120 ms) or	control multiframe	51 frames (235.4 ms)
superframe	51 traffic multiframes or 26 control multiframes (6.12 s)		
hyperframe	2048 superframes (3 hours 28 minutes and 53.76s)		

Incoming Call

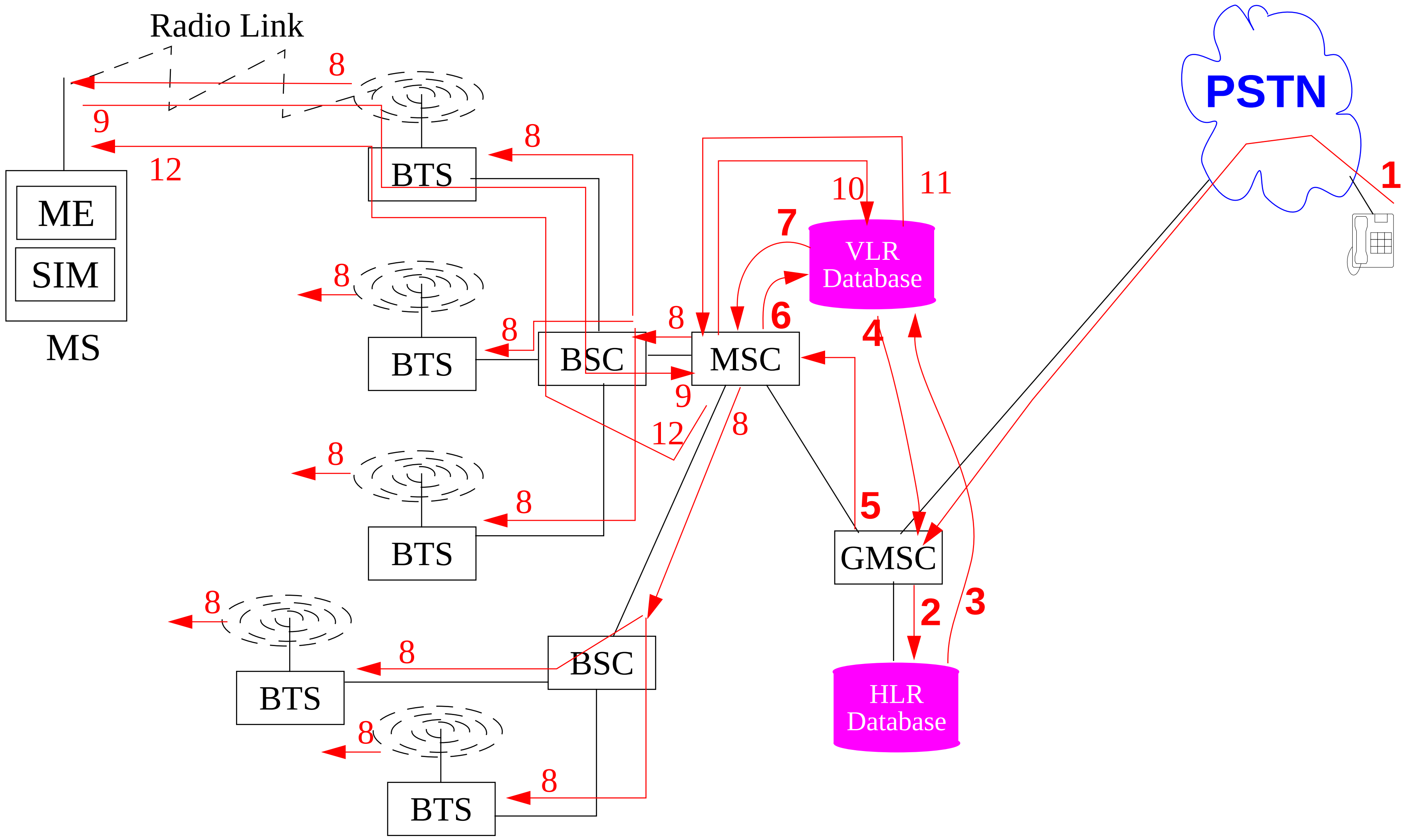


Figure 3: Call from fixed network to MS

Here we assume that we don’t know which cell the mobule is in only its rough location

1	incoming call is passed from the fixed network to the gateway MSC (GMSC)
2	based on the IMSI numbers of the called party, HLR is determined
3	HLR checks for the existence of the called number, then the relevant VLR is requested to provide a mobile station roaming number (MSRN)
4	reply transmitted back to the GMSC
5	connection is switched through to the responsible MSC
6	VLR is queried for the location range and reachability status of the mobile subscriber
7	if the MS is marked reachable, then a radio call is enabled
8	radio call is executed in all radio zones assigned to the VLR
9	reply from the MS in its current radio cell
10	when mobile subscriber telephone responds to the page, then complete all necessary secuity procedures
11	if this is successful, the VLR indicates to the MSC that call **can** be completed
12	call can be completed

Mobility Management (MM)

GSM network keeps track of which mobile telephones are powered on and active in the network.

The network keeps track of the last known location of the MS in the VLR and HLR.

Radio sites connected to the MSC are divided into “location areas” (LAs), thus when a call comes for an MS, the network looks for the MS in the last known location area.

Each BTS is assigned (by the operator) a 40 bit ID - called a location area identity (LAI), with three parts:

- mobile country code
- mobile network code
- location area code

Security

Use of TMSI rather than IMSI - reduces the need to send IMSI over the air (thus simply listening to the radio link it is harder to identify a given user).

Two major aspects of security: Authentication and Encryption

A3	Authentication algorithm
A5	Ciphering algorithm
A8	Ciphering key computation
K_i	secret encryption key - operator determines length , but it can be upto 128 bits
K_c	cypher key, computed based on K_i

Cipher mode management

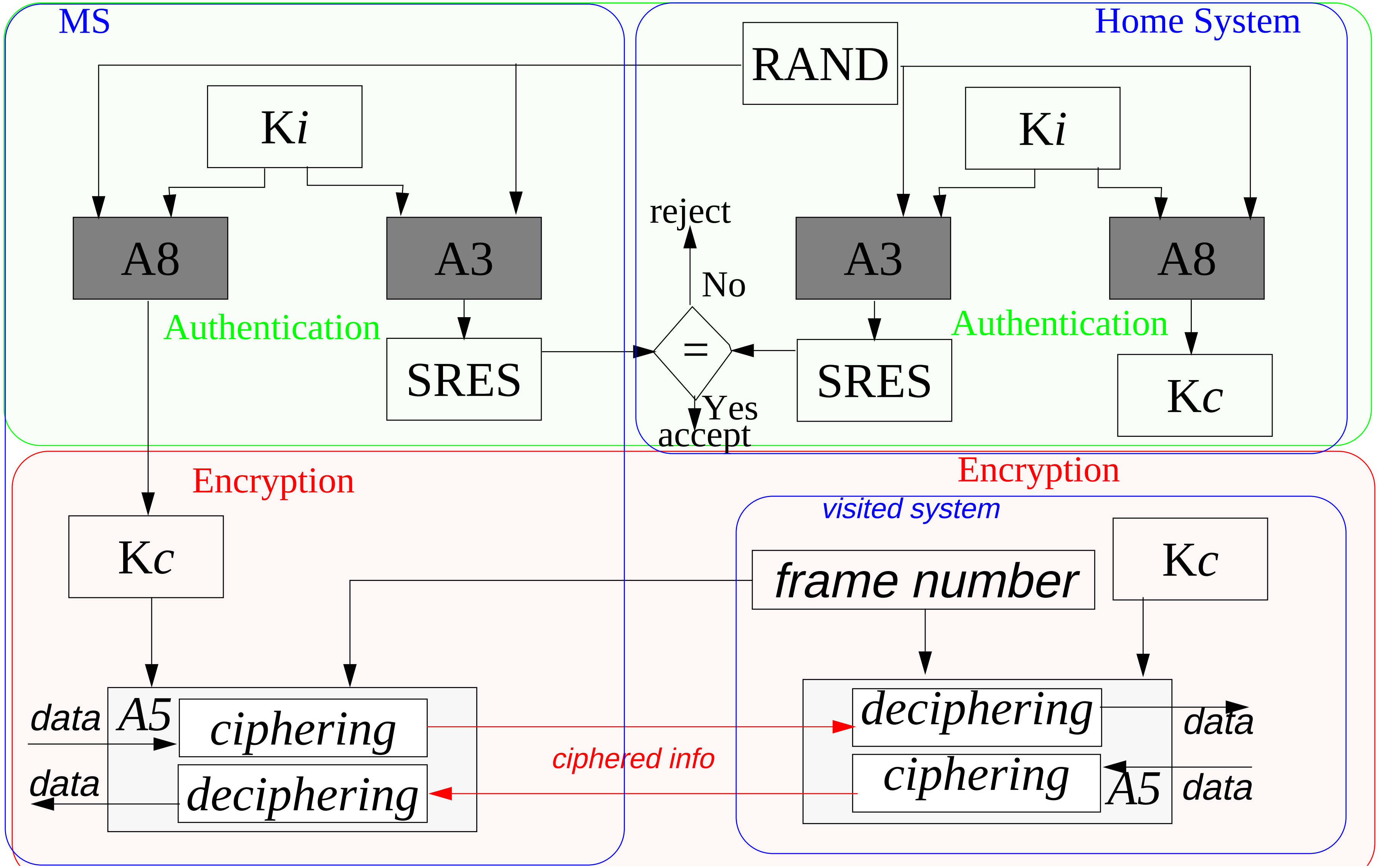
Connection always starts in non-ciphered mode, because ciphering requires a user specific key and the network has to know the identity of the subscriber before it can be used!

Authentication

User authentication normally takes place when the MS is turned on (user must key in a PIN code on the handset in order to activate the hardware before this automatic procedure can start).

Authentication occurs with each incoming call and outgoing call. This is based on checking that “Ki” (secret encryption key) stored in the AuC matches the “Ki” stored in SIM card of the MS.

Authentication and Encryption



GSM data rates

The following table of data rates is from page 39 of [5]

Connection Type[a]	Two-way delay
TCH/F9.6 T	330 ms
TCH/F9.6 NT	> 330 ms
TCH/F4.8 T	330 ms
TCH/F2.4 T	200 ms
TCH/H4.8 T	600 ms
TCH/H4.8 NT	> 600 ms
TCH/H2.4 T	600 ms

a. T = Transparent, NT = Non-transparent

System engineering

The operator must choose how many of each element (MSC, BSC, BTS, …) to order, what capacity each must have, where to install them, …

Since traffic does not remain constant

- simply installing a large enough capacity for long term traffic is not cost effective
- Therefore, system engineering is an on-going activity

Note: goal of cellular planning is to choose the cell sites and cell parameters (frequency allocation, capacity, power, etc.) to provide economically continuous coverage and support the required traffic density (not an easy task)

Table of parameters, from page 101 of [5]

Area	Parameters
Cell planning	frequencies
	beacon frequencies
	hopping sequences
	power control parameters
	handover parameters
	cell selection parameters
	BSIC
Dimensioning	# of common channels
	# of traffic channels
	location areas
	periodic location updating
Load control	overload control parameters

GSM Network Optimization

Based on network performance & utilization, subscriber behavior, and (QoS)

Test methods:

- Traffic analysis:the signaling channels in the PCM frame are monitored and analyzed on the A bis and A interfaces
- Bit error ratio test (BERT): bit error measurement at the PCM level and the GSM-specific level (TRAU frame)
  - PCM bit error ratio (BER) is used to verify the quality of lines leased from fixed network operators
  - By evaluating the control bits in the TRAU, a bit error probability can be determined (uplink) during actual communications (in-service) {No easy measurement of the downlink BER}
  - More accurate radio link BER measurement (out-of-service) measurement in which the 260 data bits in the TRAU frame are checked using a pseudo-random bit sequence (PRBS)
- Alarm monitoring - checking PCM links for layer 1 alarms
- Network quality test: lots of measurements - including:
  - island problems, detection of coverage holes, interference, network load regarding signaling and traffic,handover failures, Receive level (RXLEV) surveillance, bit error ratio of a BTS (RXQUAL), multipath interference and propagation delays, frequency interference (due to nearby frequency reuse), call completion/disconnect rate, indications of system overload.

Features

Call Waiting (CW)	{network-based feature} users with a call in progress receive an audible beep to alert them that there is an incoming call for their MS The incoming call can be: • accepted {the original call is put on hold}, • sent to voice mail, or • rejected {in this case the caller will receive a busy signal}
Call Hold (CH)	allows the MS to “park” an “in progress call”, to make additional calls or to receive incoming calls
Call Forwarding (CF)	{network-based feature} allows calls to be sent to other numbers under conditions defined by the user Conditions can be either unconditional or dependent on certain criteria (no answer, busy, not reachable)
Calling Line ID	caller’s network to delivers the calling line ID (telephone no.) to the GSM network; GSM telephone displays the originating telephone number
…	

GSM Phase 2+

- High Speed Circuit Switched Data (HSCSD)
- General Packet Radio Service (GPRS)

High Speed Circuit Switched Data (HSCSD)

Idea is simple	use several time slots out of each TDMA frame for one data connection
Reality	this is taxing for the RF power systems

In the basic GSM model TX/RX activities, the terminal can be implemented using one frequency synthesizer (even though it takes some time for the synthesizer to change from one frequency to another) - because of the offset of 3 slots between transmit and receiver.

If you only use 2 slot, you just need a synthesizer that changes faster, but at 3 slots you potentially need to transmit and receive at the same time.

At eight time slots (i.e., continuous transmission):

- monitoring neighboring base stations would require an independent receiver
- the terminal will be more expensive than one slot terminals
- power consumption will be **much** higher

Multi-slot systems have required changes in: ciphering, frequency hopping, and generally radio resource management functions.

HSCSD depends on:

- Terminal Adapation Function (TAF)
- Interworking Functions (IWF)
- enhanced RLP to handle multilink (aka multiple time slot) operation

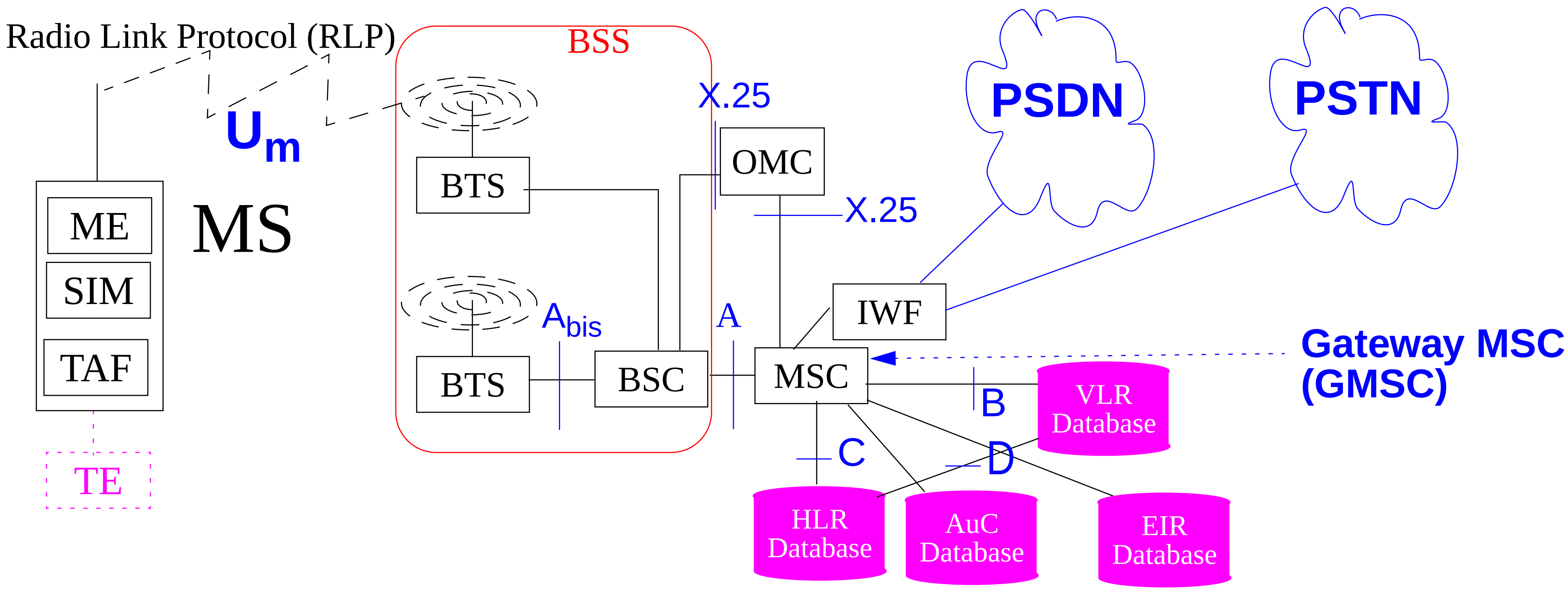


Figure 4: GSM/HSCSD Architecture

Nokia's Card Phone 2.0: HSCSD at upto 43.2 kbps (without data compression)

General Packet Radio Service (GPRS)

GPRS features:

- True packet radio system - sharing network and air interface resources
- Volume based charging
- TCP/IP (Internet & Intranet) interworking, SMS over GPRS, (and X.25 interworking)
- Peak data rate from 9.05 kbps .. 171.2 kbps
- Protocols designed for evolution of radio
  - EDGE - new GSM modulation
  - Migration into 3rd Generation

GPRS nodes

GPRS introduces new network elements

- Serving GPRS Support Node (SGSN)
  - authentication & authorization, GTP tunneling to GGSN, ciphering & compression, mobility management, session management, interaction with HLR,MSC/VLR, charging & statistics, as well as NMS interfaces.
- Gateway GPRS Support Node (GGSN)
- interfacing to external data networks (basically it is a network router) encapsulating data packets in GTP and forwarding them to right SGSN, routing mobile originated packets to right destination, filtering end user traffic, as well as collecting charging and statistical information of data network usage

GPRS is the result of committees trying to “adapt” Mobile IP to GSM systems.

The figure is over simplified - since the GGSN could also interwork to PSDNs.

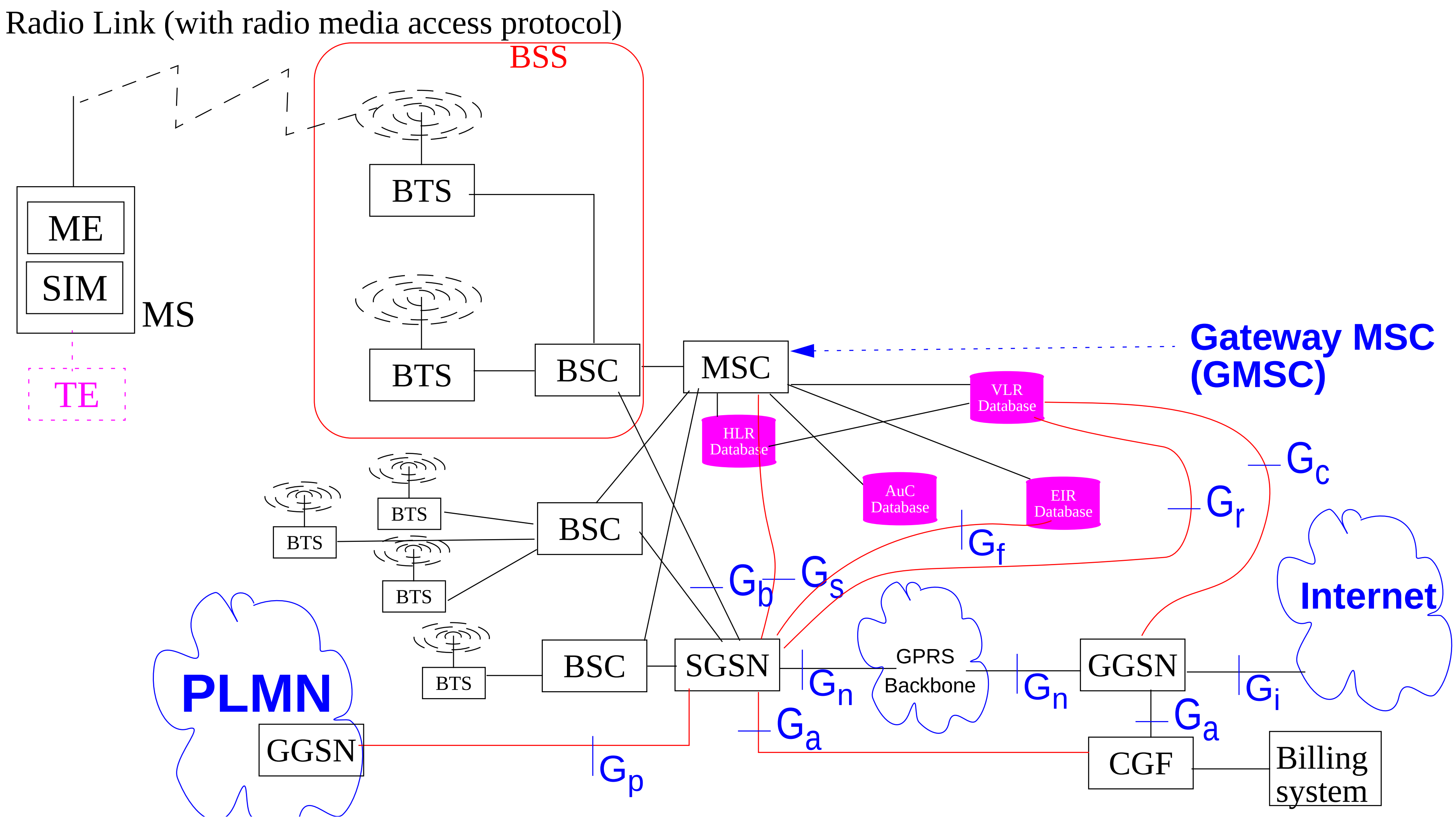


Figure 5: GSM/GPRS Architecture

GPRS Interfaces

G_a	Charging data collection interface between a CDR transmitting unit (e.g. a SGSN or a GGSN)
G_b	between a SGSN and a BSS
G_c	between a GGSN and a HLR
G_d	between a SMS-GMSC and a SGSN, and between a SMS-IWMSC and a SGSN
G_f	between an SGSN and a EIR
G_i	reference point between GPRS and an external packet data network
G_n	between two GSNs within the same PLMN
G_p	between two GSNs in different PLMNs (G_p interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs.)
G_r	between an SGSN and a HLR
G_s	between a SGSN and a MSC/VLR

GPRS Coding Schemes

Four schemes (but only CS1 and CS2 are in early systems)

Coding Scheme	CS1	CS2	CS3	CS4
User Data Rate	9.05 kbps	13.4 kbps	15.6 kbps	21.4 kbps
Correction Capability	Highest			None
Worst-link Buget	135 dB	133dB	131 dB	128.5 dB
Maximum Cell Range	450 m	390 m	350 m	290 m
40 bytes (320 bits) of payload see [9], pg. 33	1956 bits	1132 bits	1018 bits	625 bits
1500 bytes (12000 bits)	55787 bits	32490 bits	27218 bits	19345 bits

For comparison for GSM the worst-case link budget is 142.5 dB and the maximum cell range is 730 m.

But the real problem is that GPRS uses *interleaving* to spread the effect of burst errors - but this means that the delay is always high!

Unstructured Supplementary Service Data (USSD)

When MS can not recognize text - it simply passes it to the network as USSD.

USSD supports all digits, asterisk (*), and punt (#) keys.

A USSD server is connected to the HLR via MAP and to servers (which actually provide a specific service) via TCP/IP.

USSD is thought to be ~7x faster than SMS for two-way transactions.

Short Message Service (SMS)

Short Message Service (SMS) offers connectionless (message) delivery (similar to “two-way-paging”)

If the GSM telephone is not turned on, the message is held for later delivery. To Ensure that each time a message is delivered to an MS, the network expects to receive an acknowledgement from the MS that the message was correctly received.

SMS supports messages up to 140 octets (160 characters of GSM default Alphabet - see GSM 03.38) in length.

SMS concatination - combines several messages

SMS compression - defined standard for compression of content

With internation roaming these messages can be delivered by any GSM network around the world to where ever the MS currently is.

Two types of messages: **cell broadcast** and **point-to-point service**

Short Message Service Architecture

SM-SC	Short Message Service Centre
SMS GMSC	SMS Gateway MSC
IWMSC	Interworking MSC

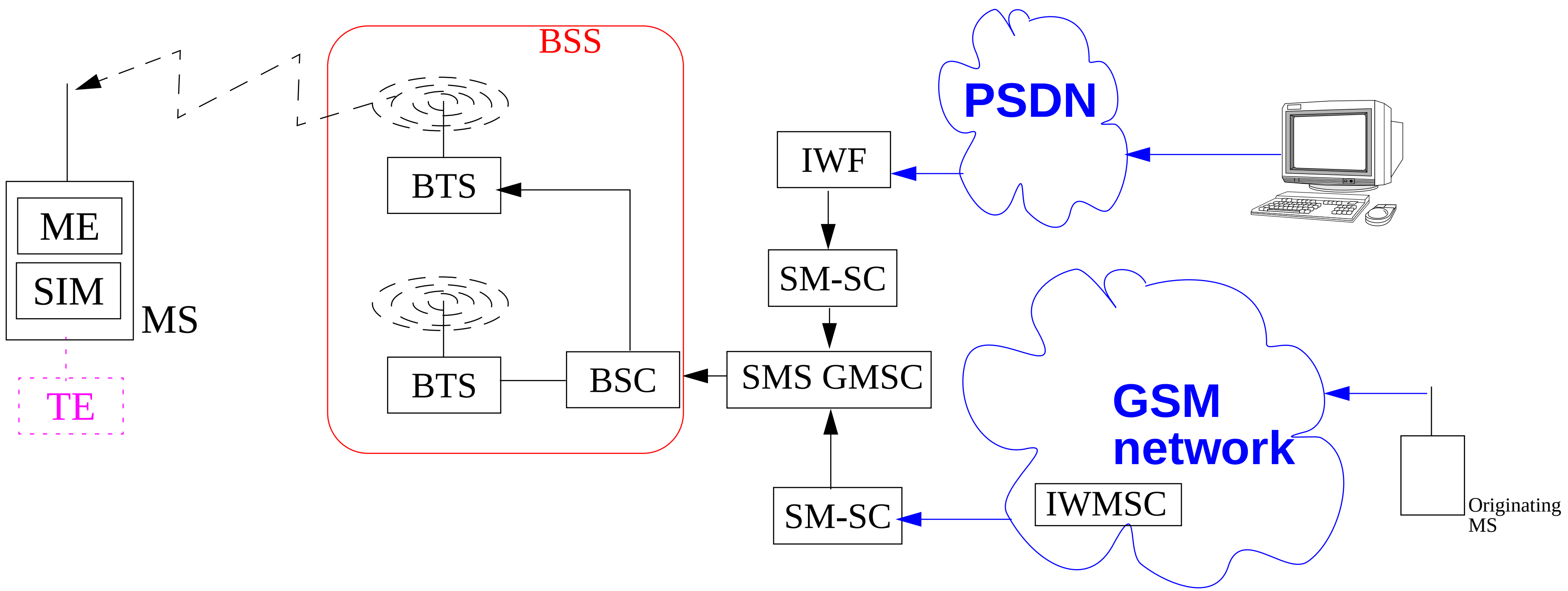


Figure 6: SMS Architecture

SM-SCs

- High reliability
- High availability
- High performance
- existing SM-SCs talk TCP/IP as well as other protocols

There exist SMS brokers from whom you can buy SMS capacity in bulk, they receive your messages and then transfer them to operators that they have agreements with.

Three kinds of SMSs

User-specific	display to a user
ME-specific	ME processes the message when it is received
	Nokia has special function to play ring tone, display a business card, modify the default icon, …
SIM-specific	SIM processes the message when it is received
	(for use via SIM toolkit applications)

Entering Short Messages

To improve the speed of entering SMSs (and other text)

- Full keyboards (such as Ericsson's Chat Board)
- Onscreen keyboard (such as Plam's on-screen keyboard)
- Fitaly keyboard - arranges letters based on their frequency and probability transitions in English (see page 43 of [11])
- Predictive text input algorithms
  - Tegic T9 - utilizes numeric keypad and probability to work out probably string (see page 45 of [11])
  - e-acute's Octave keyboard (see pages 46-47 of [36])
- Handwriting recogntion
  - Word recognition, such as Psion's CalliGrapher (see pages 47-48 of [36])
  - Character recognition, such as Palm's Graffiti (see pages 48-49 of [36]) and
  - CJKOS - an OS extension for Palm for Chinese, Japanese, and Korean (see page 49 of [36])
- Speech recognition

Voice Messaging System (VMS)

A value-added service which redirects incoming calls (i.e., forwards them) to a voice mailbox when MS is turned off, low on battery, left unattended (after ringing for xx seconds) or temporarily out of coverage.

A Voice Message Alert (VMA) can be send (via SMS) to the MS to let the user know there is a waiting voice message.

Note that you can use SMS’s “replace message” facility - to over-write last VMA - thus there will only be one message with the latest status voice messages (for example saying: “You have N voice messages waiting”).

Voice Profile for Internet Mail (VPIM)

Voice Profile for Internet Mail (VPIM) Version 2 is currently a Proposed Standard (RFC 2421) Applicability Statement, it is an application of Internet Mail originally intended for sending voice messages between voice messaging systems

http://www.ema.org/vpim

http://www.ietf.org/html.charters/vpim-charter.html

VPIM v3 Specification add extensions: IMAP voice extensions, voice directory profiles, content negotiation details for voice and partial non-delivery notifications.

International Roaming

GSM's roaming feature allows a user to make and receive calls in **any** GSM network and to use the same user-specific services worldwide.

Requires a roaming agreement between the individual operators.

Good news	With worldwide roaming the MS is accessible via the same phone number everywhere!
Bad news	It could be very expensive - much more expensive than you think!

The basic problem is that when you roam to another network (for example, in another country) - your Mobile Station ISDN number (MSISDN) *still looks like it is in your home network*. {This is one of the more stupid aspects of GSM.}

Worst is if you are in the same (non-home) network as the person you are calling, as this results in two international calls! This is due to tromboning. For four solutions see section 13.2 of [12], pages 242-249.

Operation/Administration/Maintainence

Operation/Administration/Maintainence (OA&M) follows ITU-T;s Telecommuncations Management Network (TMN) model, which has several components:

Operations system (OS)	OS uses Operating System Function (OSF) to provide overall management, billing, account, management of mobile equipment, HLR measurement, …
Network Element Functions (NEFs)	provides monitoring and control of Network Elements (NEs): HLR, VLR, AuC, EIR, MSC, BSC, and BTS
Data Communication Network	OS, NEs, and other TMN elements via Data Communication Function (DCF)
Mediation device (MD)	adapts the OS to a specfic NE
Q-Adapter (QA)	uses Q-adapter function to adapte non-TMN equipment
Workstation (WS)	OA&M personnel interact with OS via Workstation functions (WSFs)

I personally find this ITU-T speak! But you have to talk the talk to walk the walk!

Enhanced Data Rates for GSM Evolution (EDGE)

- enhanced modulation technique designed to increase network capacity and data rates in GSM networks
- provide data rates up to 384 Kbps.
- EDGE lets operators without a 3G license compete with 3G networks (since the data rates are comparable in the wide area)

GSM/EDGE Radio Access network (GERAN)

the radio interface used in Enhanced Data Rates for GSM Evolution (EDGE)

Maximum data rate: 384 kbps

EGRPS

EGPRS = EDGEan extension/enhancement of GPRS including 4 new Data Packet Traffic Channels using 8-PSK modulation and a incremental redundancy mechanism extended to the GMSK based data packet traffic channels.

- Support for simultaneous, multiple radio access bearers with different QoS profiles.
- New bearer classes:
  - Conversational Class - Voice & video conferencing where small delay is required
  - Streaming Class - Capable of processing as transfer is taking place, needs somewhat constant delay and throughput
  - Interactive Class - on-line applications
  - Background Class - Delay insensitive but requires few errors (may require multiple re-transmissions to hide errors)

Further reading

GSM

[1] M. Mouly and MB Paulet, *The GSM System for Mobile Communications*, Mouly and Paulet, 1992

[2] M. Mouly and MB Paulet, Current evolution of the GSM systems, IEEE Personal Communications, vol. 2, no. 5, pp. 9-19, 1995.

[3] David J. Goodman, *Wireless Personal Communications Systems*, Chapter 7, GSM: Pan-European Digital Cellular System, Addison-Wesley, 1997, ISBN 0-201-63470-8

[4] Marc Kahabka, GSM Pocket Guide revised version Vol. 2, Acterna Eningen GmbH, 72795 Eningen u. A., Germany *http://www.acterna.com/downloads/application_notes/gsm_SW-EN-PG02-1100-AE.pdf*-

[5] Petri Jarske, The GSM System, Principles of Digital Mobile Communication Systems, 2001 edition, Technical University Tampere, Finland

http://www.cs.tut.fi/kurssit/83150/DigiCom2001.PDF

[6] Sudeep Kumar Palat, “Replication of User Mobility Profiles for Location Management in Mobile Networks”, Dr. Ing. dissertation, Norwegian University of Science and Technology, Dept. of Telematics, 12 Jan. 1998.

[7] GSM security
http://www.isaac.cs.berkeley.edu/isaac/gsm.html

GPRS

[8] Jari Hämäläinen, “Design of GSM High Speed Data Services”, Dr. Tech. dissertation ,Tampere University of Technology, Department of Information Technology, 4 October 1996.

[9] Jouni Mikkonen, “Quality of Services in Radio Access Networks”, Dr. Tech. dissertation,Tampere University of Technology, Department of Information Technology, 19 May 1999.

[10] Don Zelmer, “GPRS, EDGE, & GERAN: Improving the performance of GSM & TDMA Wireless by Packet Capabilities”, Cingular Wireless LLC,

SUPERCOMM 2001, Atlanta, Georgia, Wednesday, June 6, 2001
http://www.atis.org/atis/Pictures/Supercomm01/Presentationfolder/T1P1zelmer3Gtemplate2.PDF

SMS

[11] Jochen Burkhardt, Dr. Horst Henn, Stefan Hepper, Klaus Rintdoff, and Thomas Schäck, *Pervasive Computing: Technology and Architecture of Mobile Internet Applications*, Addison-Wesley, 2002, ISBN 0-201-72215-1

International Roaming

[12] Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, , Chapter 13, John Wiley & Sons, 2001, ISBN 0-471-39492-0

Operation/Administration/Maintainence

[13] Yi-Bing Lin and Imrich Chlamtac, *Wireless and Mobile Network Architectures*, Chapter 14, John Wiley & Sons, 2001, ISBN 0-471-39492-0