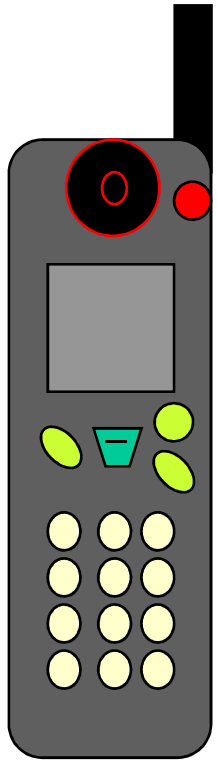
Global System for Mobile

Week 14

- GSM task and intention
- Services offered by GSM
- GSM architecture
- GSM Radio System
- Channels in GSM
- Example of GSM call
- Signal Processing in GSM



Note for
Wireless-Fall-2014 Class

These Slides are only for additional study.

This topic will not appear in Final Exam Paper

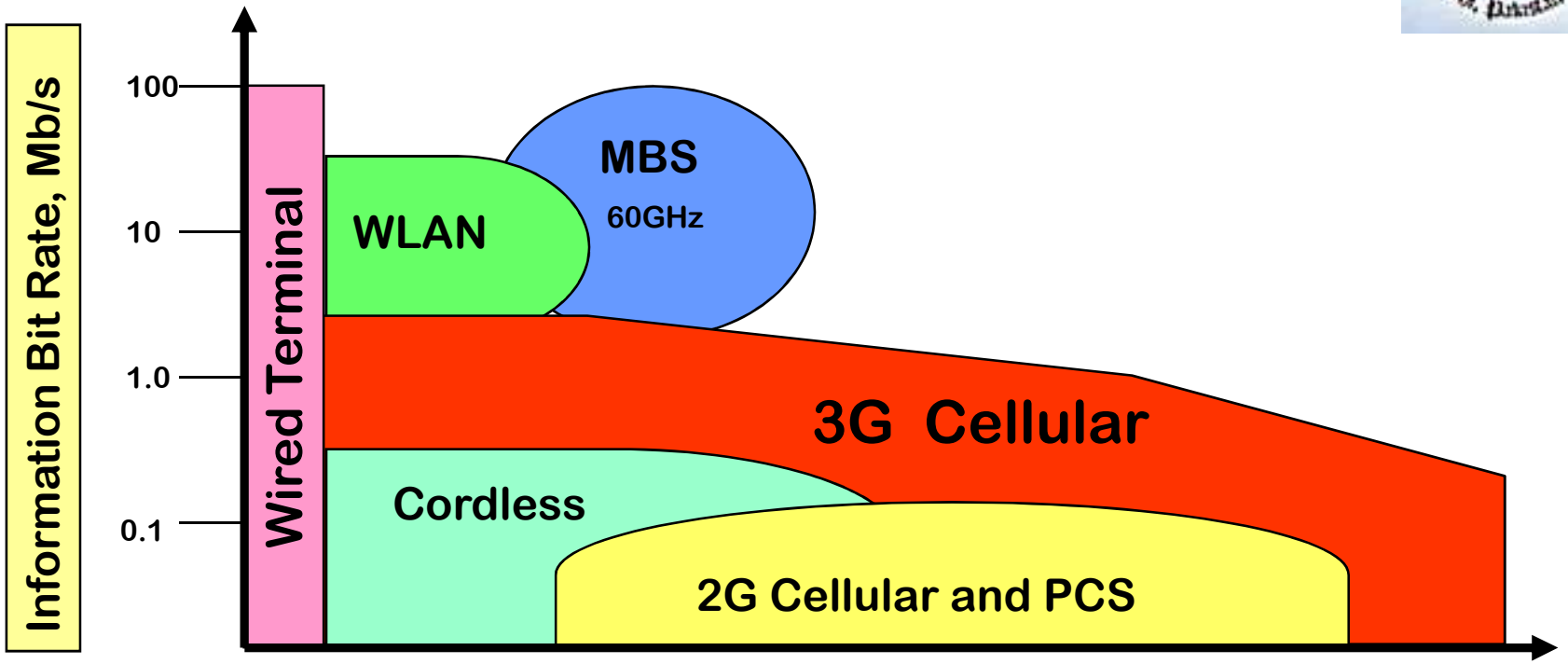
Global System for Mobile Communications (GSM)

- GSM is a second generation mobile cellular system developed to solve incompatibility of a large number cellular standards throughout Europe
- However, GSM achieved worldwide success. Recent statistics show that there are 600 million worldwide subscribers of GSM
- Group Speciale Mobile (GSM) & Digital Cellular System 1800 (DCS-1800)
  - Adopted in June 1987

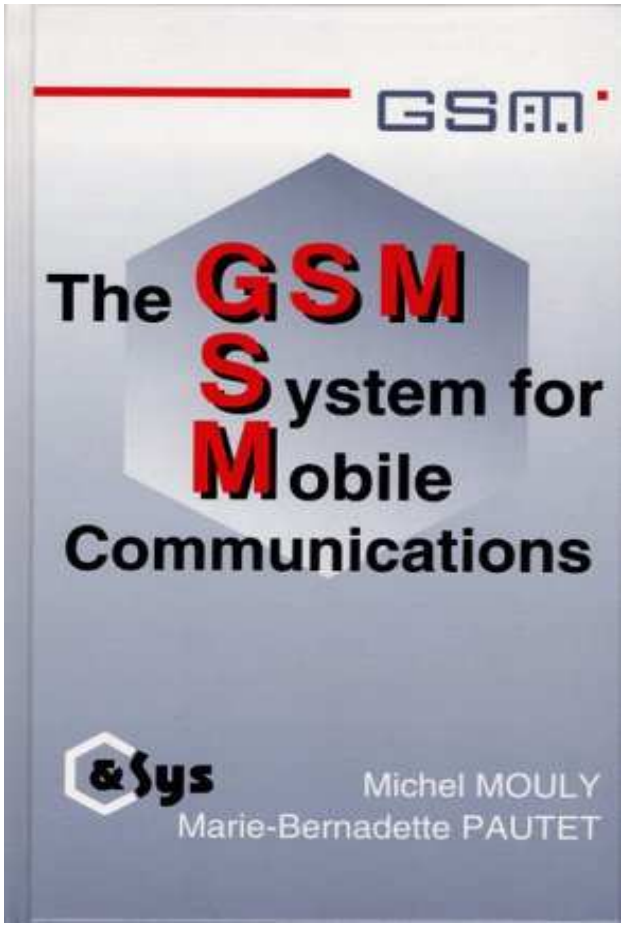
Migration Path to 3G Mobile Comm. Systems

- First Major Migration Path
  - I Gen, 80's, ETACS (C-450,NMT-450..), (FDMA), Analog
  - II Gen, 90's, **GSM**, GPRS, EDGE, (TDMA) Digital
  - III Gen, 00's, W-CDMA , (CDMA), All Digital
- Second Major Migration Path
  - I Gen, 80's, AMPS, (FDMA), Analog
  - II Gen, 90's, IS-54 (TDMA), IS-95 (CDMA), Digital
  - III Gen, 00's, Cdma2000 (CDMA), All Digital

Third Generation Wireless



GSM Book



The Gsm System for Mobile Communications

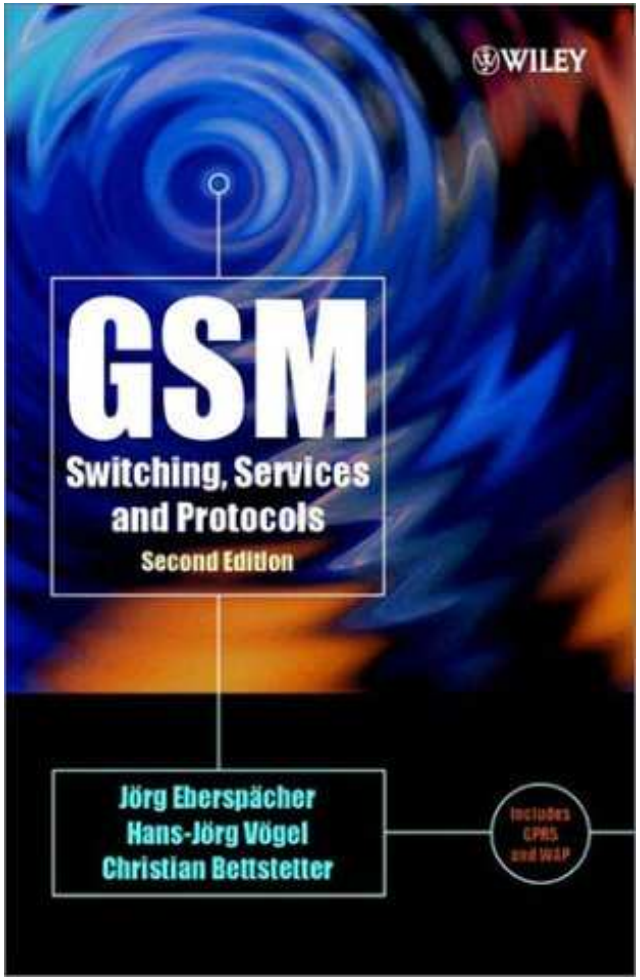
by: Michel Mouly,
Marie-Bernadette Pautet

Hardcover – 701 pages

June 1992,
Telecom Publishing

ISBN: 0945592159

GSM Recent Book



GSM Switching, Services and Protocols, 2nd Edition

by Joerg Eberspaecher, Hans-Joerg Voegel, Christian Bettstetter

Hardcover – 346 pages 2 edition (April 16, 2001)

John Wiley & Sons;
ISBN: 047149903X

GSM Services

- GSM/DCS is targeted to include a variety of services
- These can be divided into
  - telephony (also referred to as **teleservices**)
    - speech between portable units
    - fax transmission
  - data (also referred to as **bearer services**)
    - Data (from 300 to 9.6 kbs)
  - **supplementary ISDN services**
    - call forwarding, barring of outgoing/incoming calls, call hold/waiting etc.
    - Short message services (SMS)

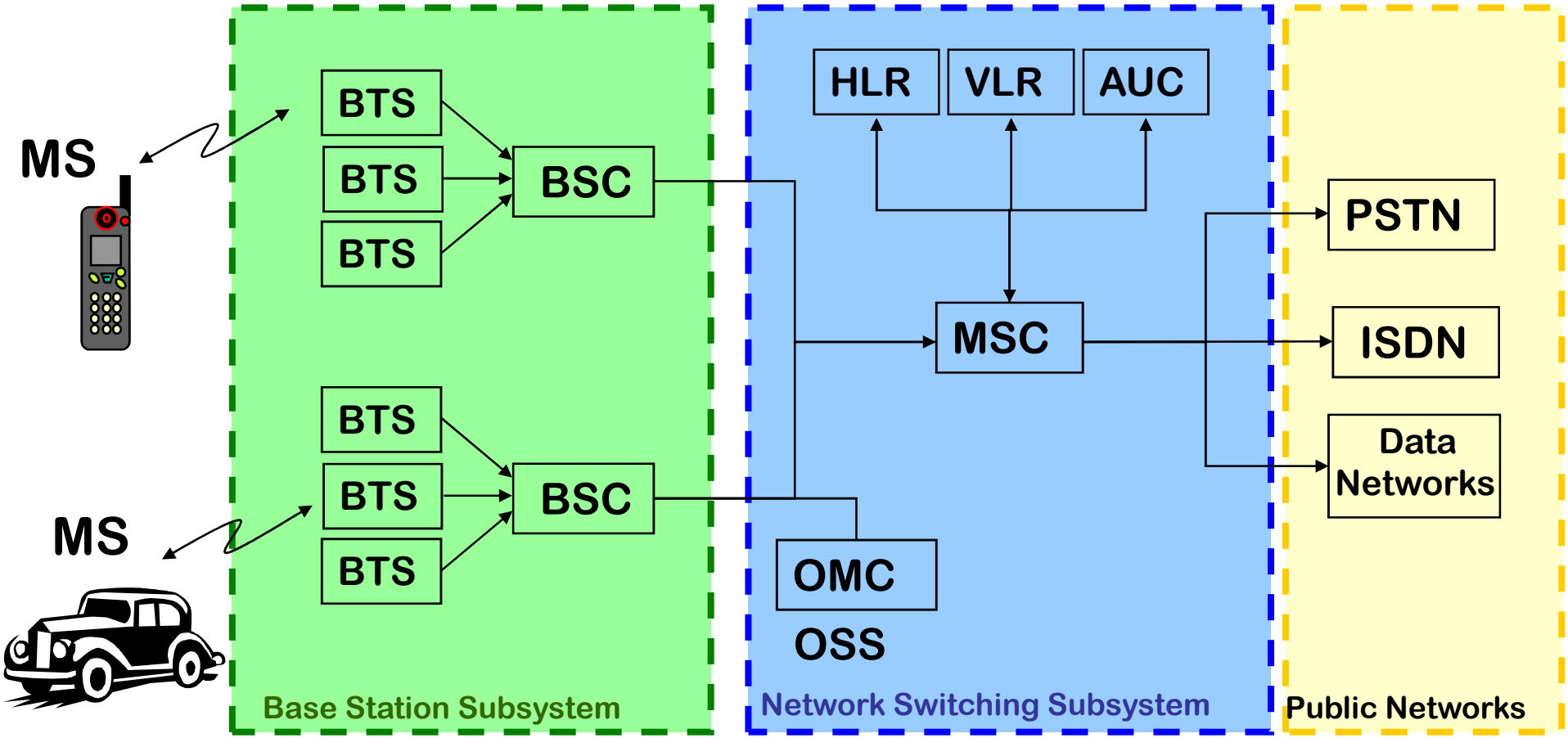
Subscriber Identity Module

- Subscriber Identity Module is a small memory device (a little database) that stores:
  - Subscriber identification number
  - The networks and countries where subscriber is entitled to service, privacy keys e.t.c (user/customer profile)
- SIM is inserted in a mobile phone and it is the SIM that gives mobile phone identity
- SIM could be inserted into any GSM compliant terminal such as hotel phone, public phone e.t.c.
- All made calls will be billed to the owner of SIM card and all incoming calls will be directed to the terminal with the SIM card

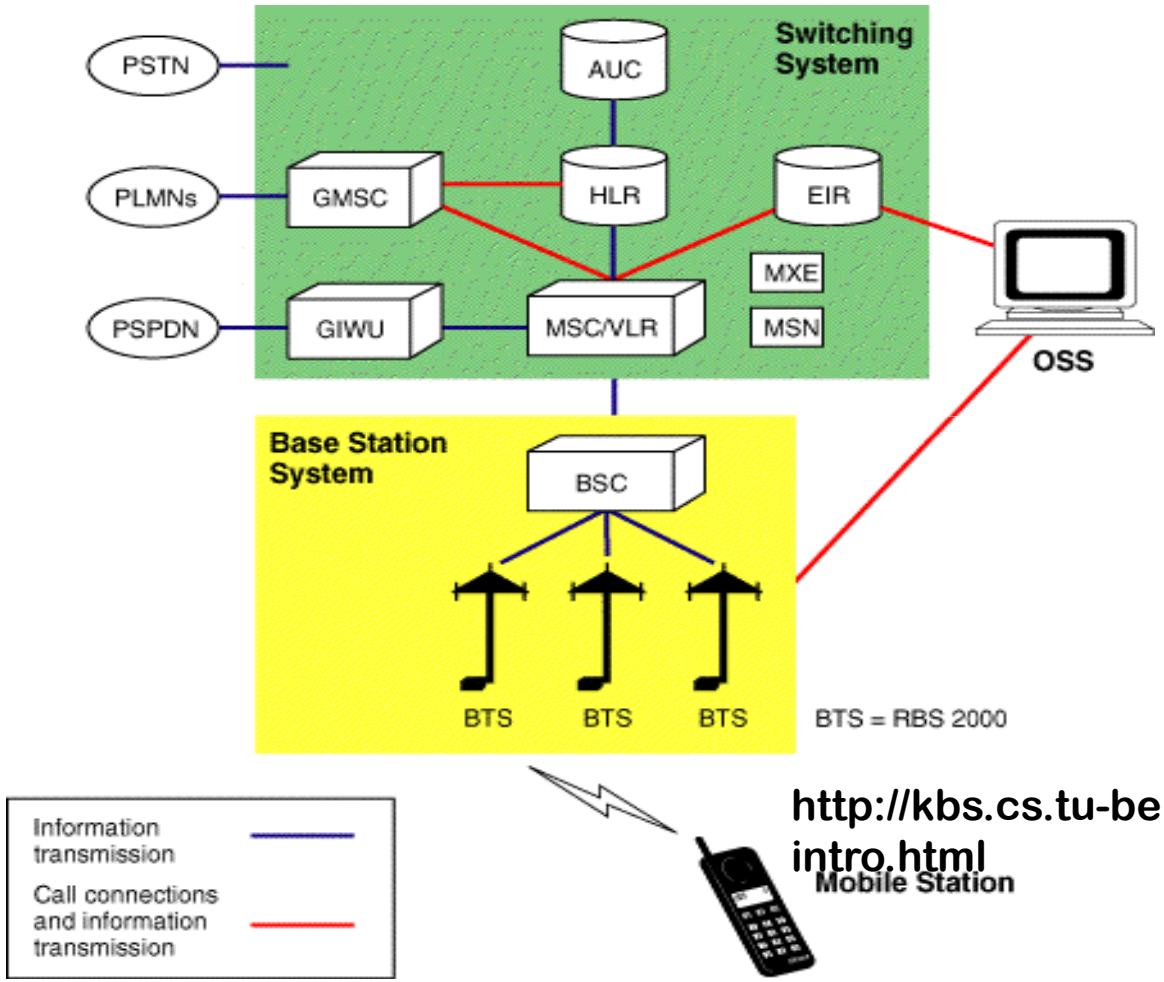
GSM System

- GSM consists of three major components
  - Base Station Systems (BSS)
  - Switching Systems (SS)
  - Operation and Support Systems (OSS)

GSM System Architecture



GSM900/DCS1800

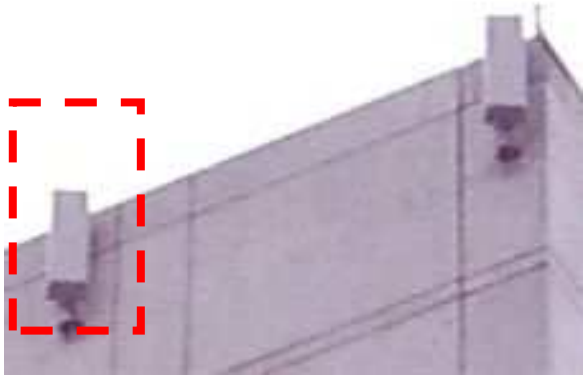


http://kbs.cs.tu-berlin.de/~jutta/gsm/js-intro.html

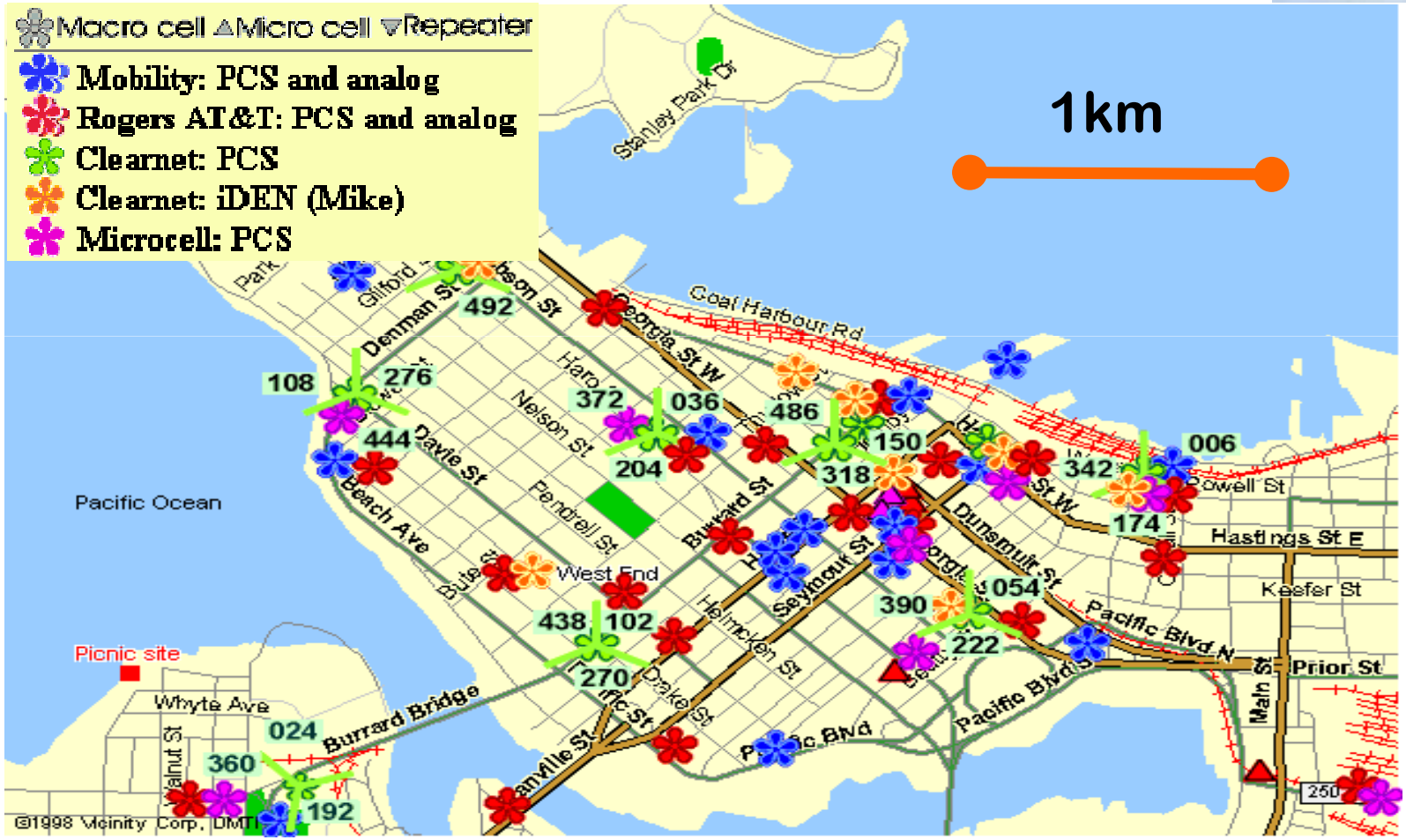
Components - MSs and BTSs

- Interface with the ***mobile stations*** (MS) is provided through ***base transceiver stations*** (BTS)
- These two components work with a range of radio channels across an air interface
- The BTS acts as the interface of the MS to the GSM network
- BTS are controlled by ***base station controllers*** (BSC)

Base Station Towers and Equipment



BTS Positions



Components - BSCs

- BSCs are responsible for:
  - handover operations of the calls
  - controlling the MS power
  - frequency administration between the BTSs and MSs.
- BSCs are quite complex and do much of the 'house keeping' activities between the BTSs and MSs
- BSC may be co-located with either a BTS or a MSC

Components - MSCs

- MSC is the heart of the GSM network and is responsible for setting up, managing and clearing calls as well as routing the calls to the proper cells.
- It also provide the interface to the public switched telephony network - Gateway MSC
- Complete telephone exchange

Components - HLR and VLR

- GSM uses two databases one for permanent information storage - home location register (HLR) and the other for temporary information storage - visitor location register (VLR)
- HLR correlates a subscriber to its area
  - Identifying information about the user (IMSI)
  - Home subscription base
  - Supplementary services

Components - HLR and VLR

- HLR also keeps information on the location of its 'home' subscribers - in which VLR a subscriber is registered
  - VLR stores information about subscribers in its particular area, MS are switched on or off
- Supplementary services activated or deactivated
- Used extensively during call setup and authentication

Components - AC

- The authentication center (AC or AUC) is used to protect each subscriber from unauthorized access or from use of a subscription by unauthorized persons.
- Also used for authentication operations when a subscriber registers with the network

Components - EIR

- Equipment identity register (EIR) is used for the registration of the type of equipment that exists at the mobile station.
- It can also be used to provide security features
  - Blocking calls that have been determined to come from stolen mobile stations
  - Preventing certain stations from using the network that have not been approved by the network vendor

GSM Identifiers and Addresses

- Each MS is identified uniquely by a set of values
  - The country in which the MS resides
  - The mobile network
  - Mobile subscriber
- International Mobile Subscriber Identity (IMSI) or International Mobile Subscriber Number (IMSN)

IMSI

3 digits	2 digits	Up to 10 digits
Mobile Country Code (MCC)	Mobile Network Code (MNC)	Mobile Subscriber ID code (MSIC)

- MCC of 05 identifies Australia, and MCC 234 - UK
- MNC of 01 identifies Telstra

Subscriber Identity Module (SIM)

- IMSI is stored on the SIM, which is located in the subscribers MS
- In addition the SIM contains subscriber specific information
  - phone numbers
  - personal identification number
  - security/authentication parameters
- Can also be used to store short messages

Operation & Support System

- The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC.
- The implementation of OMC is called the operation and support system (OSS).

Operation & Support System

- The OSS is the functional entity from which the network operator monitors and controls the system.
- offers the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network.
- An important function of OSS is to provide network overview and support maintenance activities of different operation and maintenance organizations.

Additional Functional Elements

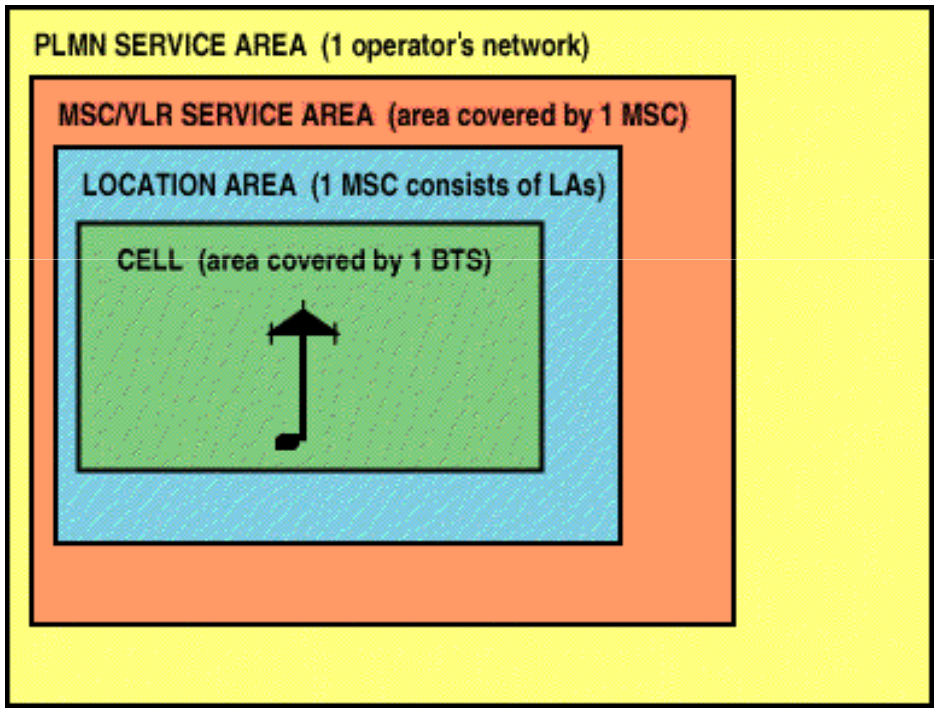
- message center (MXE)
  - The MXE is a node that provides integrated voice, fax, and data messaging. Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, e-mail, and notification.
- mobile service node (MSN)
  - The MSN is the node that handles the mobile intelligent network (IN) services.

Additional Functional Elements

- gateway mobile services switching center (GMSC)
  - A gateway is a node used to interconnect two networks. The gateway is often implemented in an MSC. The MSC is then referred to as the GMSC.
- GSM internetworking unit (GIWU)
  - The GIWU consists of both hardware and software that provides an interface to various networks for data communications. Through the GIWU, users can alternate between speech and data during the same call. The GIWU hardware equipment is physically located at the MSC/VLR.

GSM Network Areas

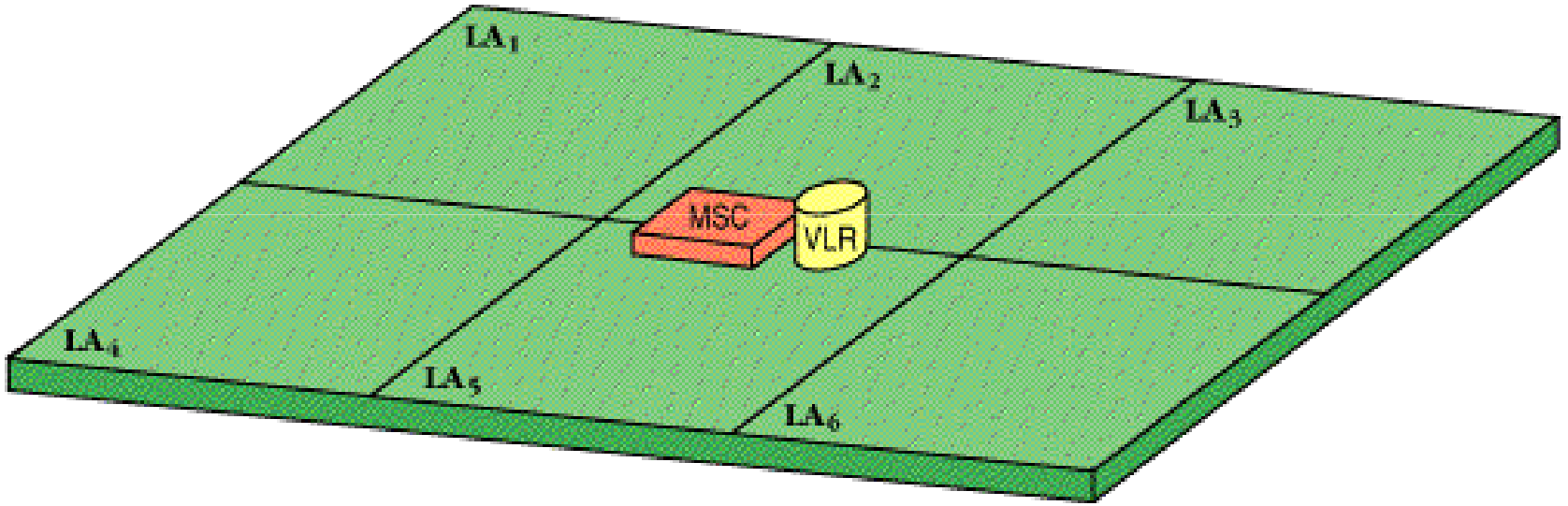
- The GSM network is made up of geographic areas



GSM Network Areas

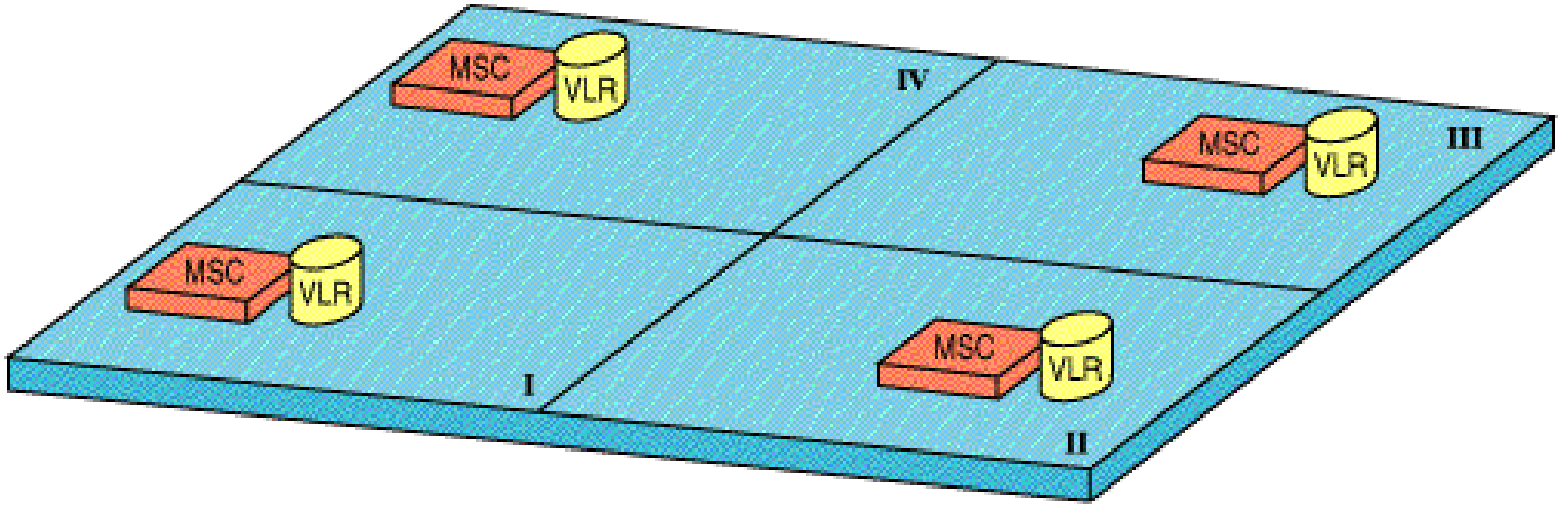
- Cell
  - Area given radio coverage by one base transceiver station.
  - The GSM network identifies each cell via the cell global identity (CGI) number assigned to each cell.
- Location area
  - A group of cells.
  - It is the area in which the subscriber is paged
  - Each LA is
    - served by one or more base station controllers, yet only by a single MSC
    - assigned a location area identity (LAI) number.

Location Areas



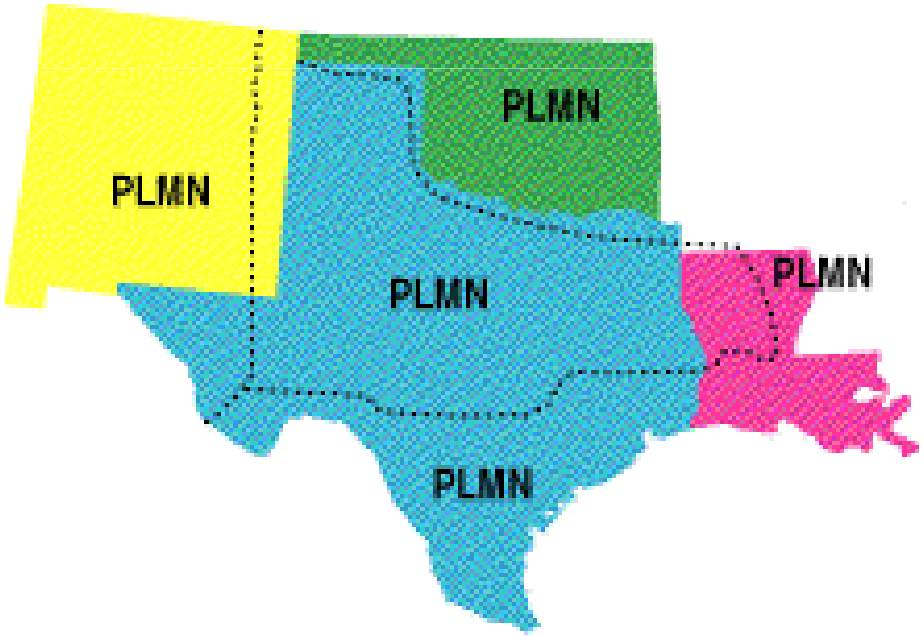
MSC/VLR Service Area

- Represents the part of the GSM network that is covered by one MSC and which is reachable, as it is registered in the VLR of the MSC



PLMN Network Areas

- The PLMN (public land mobile network) service area is an area served by one network operator



Operation Overview

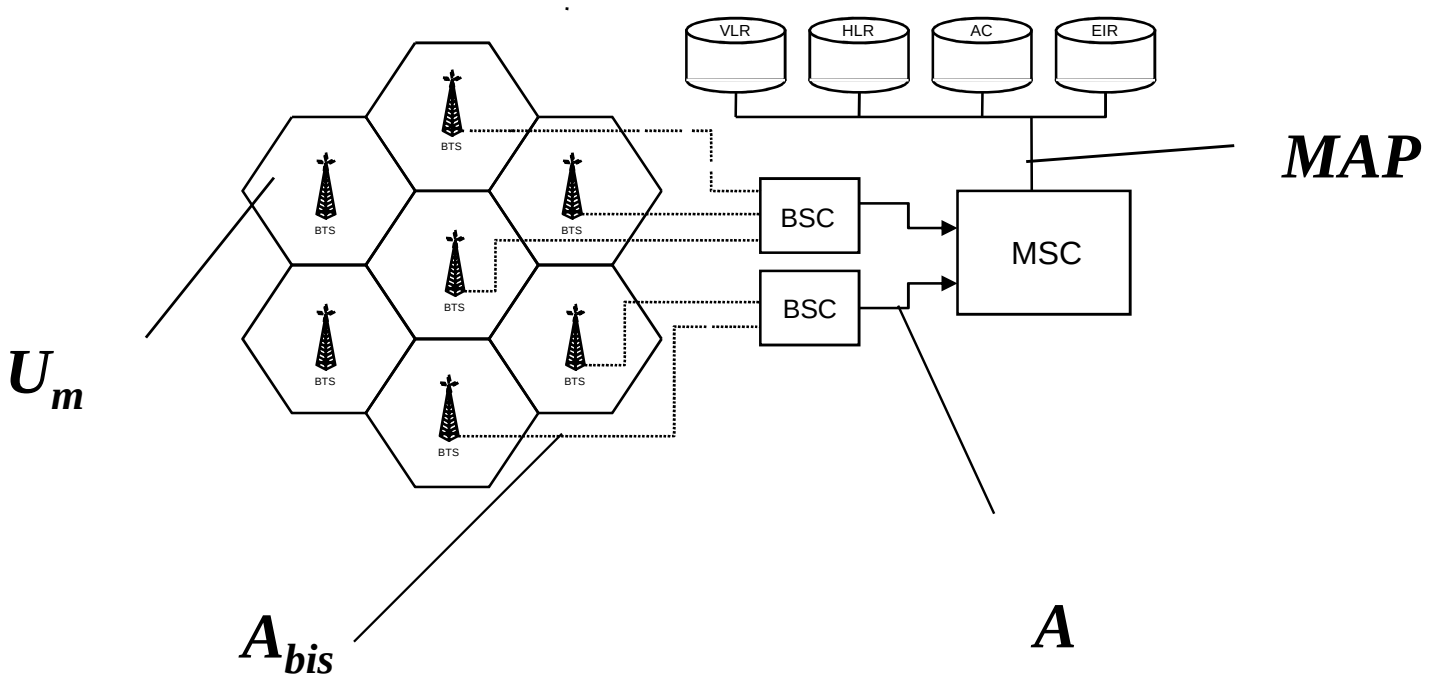
- Consists of three phases
  - Registration
  - Call Establishment
  - Roaming

Registration(1)

- After an MS is turned on, it scans the GSM frequency bands and locks on to a forward (base) channel (broadcasting case)
- At this point the MS knows the area it is in
- If it is in a different area to when it was last used, registration takes place

GSM Interfaces

- Four interfaces are defined in the GSM structure



The Air Interface U_m

- Uses a combination of FDM and TDMA
- The original GSM system operated at 900 MHz range with 890 - 915 MHz - MS to BTS, and 935 - 960 MHz BTS to MS
- DCS now uses space from 1710 - 1785 MHz& 1805 - 1880 MHz
- 124 channel pairs operate at full duplex (FDX) with 200 kHz spacing

Multiple Access & Channel Structure

- The method chosen by GSM is a combination of Time- and Frequency-Division Multiple Access (TDMA/FDMA).
- The FDMA part involves the division by frequency of the (maximum) 25 MHz bandwidth into 124 carrier frequencies spaced 200 kHz apart.
- One or more carrier frequencies are assigned to each base station.
- Each of these carrier frequencies is then divided in time, using a TDMA scheme.

Multiple Access & Channel Structure

- The fundamental unit of time in this TDMA scheme is called a *burst period* and it lasts 15/26 ms (or approx. 0.577 ms).
- Eight burst periods are grouped into a *TDMA frame* (120/26 ms, or approx. 4.615 ms), which forms the basic unit for the definition of logical channels.
- One physical channel is one burst period per TDMA frame.

Channels

- Channels are defined by the number and position of their corresponding burst periods.
- All these definitions are cyclic, and the entire pattern repeats approximately every 3 hours.
- Channels can be divided into *dedicated channels*, which are allocated to a mobile station, and *common channels*, which are used by mobile stations in idle mode.

Channels

- TCH - traffic channel
- CCH - control channel
- SACCH- Slow Associated Control Channel
- SDCCH - Dedicated Control Channels
- BCCH- Broadcast Control Channel
- FCCH - Frequency Correction Channel
- SCH - Synchronization Channel
- RACH - Random Access Channel
- PCH - Paging Channel
- AGCH - Access Grant Channel

Traffic channels

- A traffic channel (TCH) is used to carry speech and data traffic.
- Traffic channels are defined using a 26-frame multi-frame, or group of 26 TDMA frames.
- The length of a 26-frame multi-frame is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame).

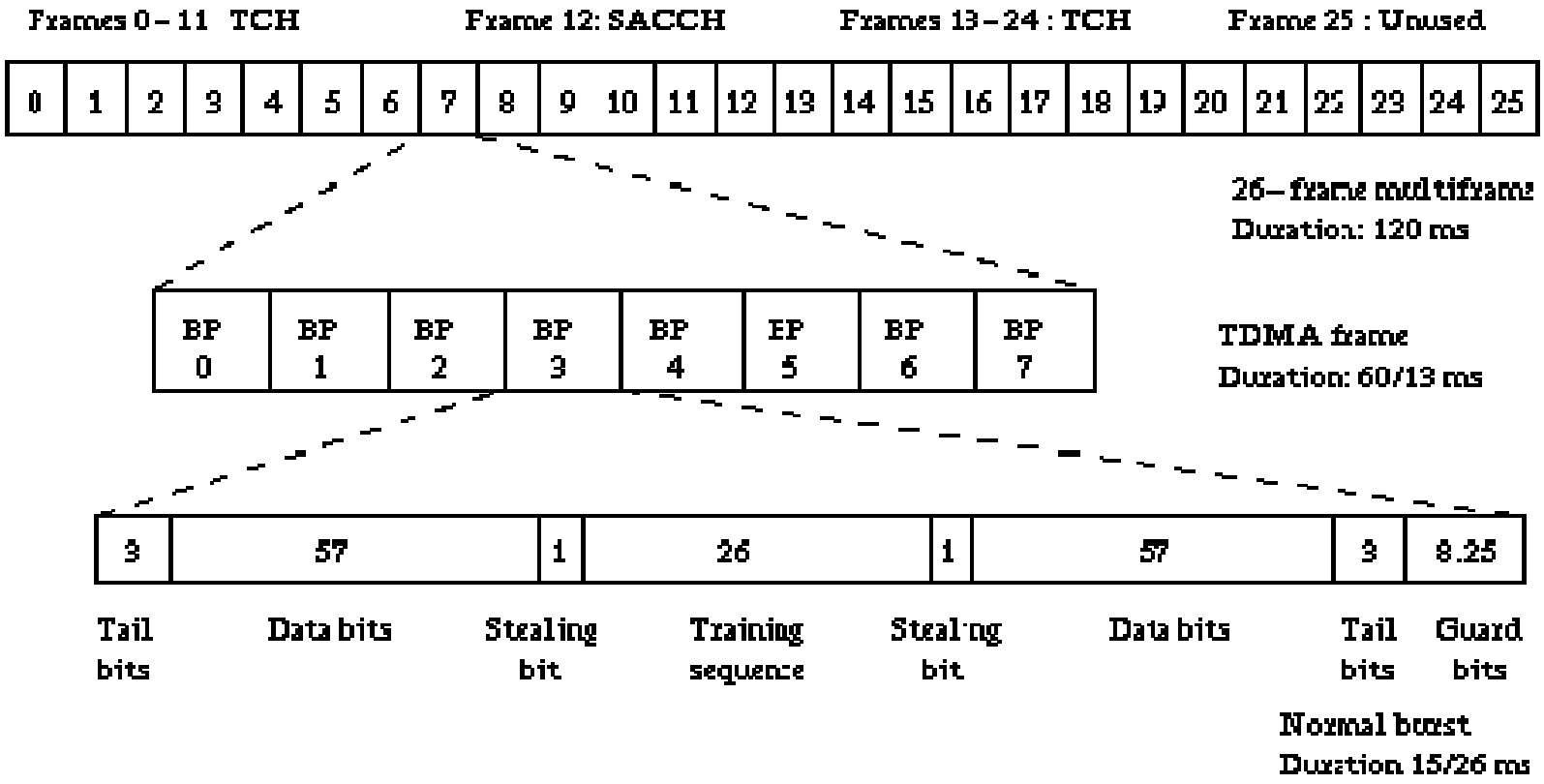
Traffic channels

- Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated Control Channel (SACCH) and 1 is currently unused
- TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thus simplifying the electronics
- In addition to these *full-rate* TCHs, there are also *half-rate* TCHs defined

Traffic channels

- Half-rate TCHs will effectively double the capacity of a system once half-rate speech coders are specified (i.e., speech coding at around 7 kbps, instead of 13 kbps).
- Eighth-rate TCHs are also specified, and are used for signaling.
  - In the recommendations, they are called Stand-alone Dedicated Control Channels (SDCCH).

Structure


Frames 0 – 11 TCH
Frame 12: SACCH
Frames 13 – 24 : TCH
Frame 25 : Unused
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26–frame multiframe
Duration: 120 ms
BP 0
BP 1
BP 2
BP 3
BP 4
EP 5
BP 6
BP 7
TDMA frame
Duration: 60/13 ms
3
57
1
26
1
57
3
8.25
Tail bits
Data bits
Stealing bit
Training sequence
Stealing bit
Data bits
Tail bits
Guard bits
Normal burst
Duration 15/26 ms

Control channels

- There are three types of control channels in GSM:
  - BCH – broadcast channels
  - CCCH – common control channels
  - DCCH – dedicated control channels
- The common channels are used by idle mode mobiles to exchange the signaling information required to change to dedicated mode.
- Mobiles already in dedicated mode monitor the surrounding base stations for handover and other information.

Control Channels

- The common channels are defined within a 51-frame multi-frame, so that dedicated mobiles using the 26-frame multi-frame TCH structure can still monitor control channels.
- Broadcast Control Channel (BCCH)
  - Continually broadcasts, on the downlink, information including base station identity, frequency allocations, and frequency-hopping sequences.

Control Channels

- Frequency Correction Channel (FCCH) and Synchronization Channel (SCH)
  - Used to synchronize the mobile to the time slot structure of a cell by defining the boundaries of burst periods, and the time slot numbering. Every cell in a GSM network broadcasts exactly one FCCH and one SCH, which are by definition on time slot number 0 (within a TDMA frame).
- Random Access Channel (RACH)
  - Slotted Aloha channel used by the mobile to request access to the network.

Control Channels

- Paging Channel (PCH)
  - Used to alert the mobile station of an incoming call.
- Access Grant Channel (AGCH)
  - Used to allocate an SDCCH to a mobile for signaling (in order to obtain a dedicated channel), following a request on the RACH.

Burst structure

- There are four different types of bursts used for transmission in GSM
- The normal burst is used to carry data and most signaling.
- It has a total length of 156.25 bits, made up of two 57 bit information bits, a 26 bit training sequence used for equalization, 1 stealing bit for each information block (used for FACCH), 3 tail bits at each end, and an 8.25 bit guard sequence.

Burst structure

- The 156.25 bits are transmitted in 0.577 ms, giving a gross bit rate of 270.833 kbps.
- The F burst, used on the FCCH, and the S burst, used on the SCH, have the same length as a normal burst, but a different internal structure, which differentiates them from normal bursts
  - allowing synchronization
- The access burst is shorter than the normal burst, and is used only on the RACH.

Speech coding

- Pulse Coded Modulation (PCM) output stream is 64 kbps
- Too high a rate to be feasible over a radio link.
- The GSM group studied several speech coding algorithms on the basis of subjective speech quality and complexity (which is related to cost, processing delay, and power consumption once implemented)
- Choice - Regular Pulse Excited -- Linear Predictive Coder (RPE--LPC) with a Long Term Predictor loop.

RPE-LPC

- Basically, information from previous samples, which does not change very quickly, is used to predict the current sample.
- The coefficients of the linear combination of the previous samples, plus an encoded form of the residual, the difference between the predicted and actual sample, represent the signal.
- Speech is divided into 20 millisecond samples, each of which is encoded as 260 bits, giving a total bit rate of 13 kbps.

Speech coding

- This is the so-called Full-Rate speech coding.
- Recently, an Enhanced Full-Rate (EFR) speech coding algorithm has been implemented by some North American GSM1900 operators.
- This is said to provide improved speech quality using the existing 13 kbps bit rate.

Channel Coding

- GSM uses convolutional encoding and block interleaving to achieve protection.
- The exact algorithms used differ for speech and for different data rates.
- Example speech blocks:
- Speech codec produces a 260 bit block for every 20 ms speech sample.
- From subjective testing, it was found that some bits of this block were more important for perceived speech quality than others.

Channel Coding

- The bits are thus divided into three classes:
  - Class Ia 50 bits - most sensitive to bit errors
  - Class Ib 132 bits - moderately sensitive to bit errors
  - Class II 78 bits - least sensitive to bit errors
- Class Ia bits have a 3 bit Cyclic Redundancy Code added for error detection.
- If an error is detected, the frame is judged too damaged to be comprehensible and it is discarded.
- It is replaced by a slightly attenuated version of the previous correctly received frame.

Channel Coding

- These 53 bits, together with the 132 Class Ib bits and a 4 bit tail sequence (a total of 189 bits), are input into a 1/2 rate convolutional encoder of constraint length 4.
- Each input bit is encoded as two output bits, based on a combination of the previous 4 input bits. The convolutional encoder thus outputs 378 bits, to which are added the 78 remaining Class II bits, which are unprotected.

Channel Coding

- Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps.
- To further protect against the burst errors common to the radio interface, each sample is interleaved.
- The 456 bits output by the convolutional encoder are divided into 8 blocks of 57 bits, and these blocks are transmitted in eight consecutive time-slot bursts.
- Since each time-slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.

Modulation

- GSM digital signal is modulated onto the analog carrier frequency using Gaussian-filtered Minimum Shift Keying (GMSK).
- GMSK was selected over other modulation schemes as a compromise between spectral efficiency, complexity of the transmitter, and limited spurious emissions.

Modulation

- The complexity of the transmitter is related to power consumption, which should be minimized for the mobile station.
- The spurious radio emissions, outside of the allotted bandwidth, must be strictly controlled
  - so as to limit adjacent channel interference, and allow for the co-existence of GSM and the older analog systems (at least for the time being).

Multi-path Equalization

- At the 900 MHz range, radio waves bounce off everything - buildings, hills, cars, airplanes, etc.
- Equalization is used to extract the desired signal from the unwanted reflections.
- It works by finding out how a *known* transmitted signal is modified by multi-path fading, and constructing an inverse filter to extract the rest of the desired signal.

Multi-path Equalization

- This ***known*** signal is the 26-bit training sequence transmitted in the middle of every time-slot burst.
- The actual implementation of the equalizer is not specified in the GSM specifications.

Frequency Hopping

- The mobile station already has to be frequency agile, meaning it can move between a transmit, receive, and monitor time slot within one TDMA frame, which normally are on different frequencies.
- GSM makes use of this inherent frequency agility to implement slow frequency hopping,
  - the mobile and BTS transmit each TDMA frame on a different carrier frequency.

Frequency Hopping

- The frequency hopping algorithm is broadcast on the Broadcast Control Channel.
- Since multi-path fading is dependent on carrier frequency, slow frequency hopping helps alleviate the problem.
- In addition, co-channel interference is in effect randomized.

Discontinuous Transmission

- Minimizing co-channel interference is a goal in any cellular system,
  - it allows better service for a given cell size, or the use of smaller cells,
    - increasing the overall capacity of the system.
- Discontinuous transmission (DTX) is a method that takes advantage of the fact that a person speaks less that 40 percent of the time
  - turning the transmitter off during silence periods.

Discontinuous Transmission

- An added benefit of DTX is that power is conserved at the mobile unit.
- The most important component of DTX is, of course, Voice Activity Detection.
- It must distinguish between voice and noise inputs, a task that is not as trivial as it appears, considering background noise.
- If a voice signal is misinterpreted as noise, the transmitter is turned off and a very annoying effect called clipping is heard at the receiving end.

Discontinuous Transmission

- If, on the other hand, noise is misinterpreted as a voice signal too often, the efficiency of DTX is dramatically decreased.
- Another factor to consider is that when the transmitter is turned off, there is total silence heard at the receiving end, due to the digital nature of GSM.
- To assure the receiver that the connection is not dead, *comfort noise* is created at the receiving end by trying to match the characteristics of the transmitting end's background noise.

Discontinuous reception

- Another method used to conserve power at the mobile station is discontinuous reception.
- The paging channel, used by the base station to signal an incoming call, is structured into sub-channels.
- Each mobile station needs to listen only to its own sub-channel. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used.

Power control

- There are five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts.
- 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 Control

- Power levels can be stepped up or down in steps of 2 dB from the peak power for the class, down to a minimum of 13 dBm (20 milliwatts).
- The mobile station measures the signal strength or signal quality (based on the Bit Error Ratio)
  - The information is passed to the Base Station Controller
  - Base Station Controller decides if and when the power level should be changed.

Power Control

- Power control should be handled carefully, since there is the possibility of instability.
- This arises from having mobiles in co-channel cells alternatively increase their power in response to increased co-channel interference caused by the other mobile increasing its power.

Week 15

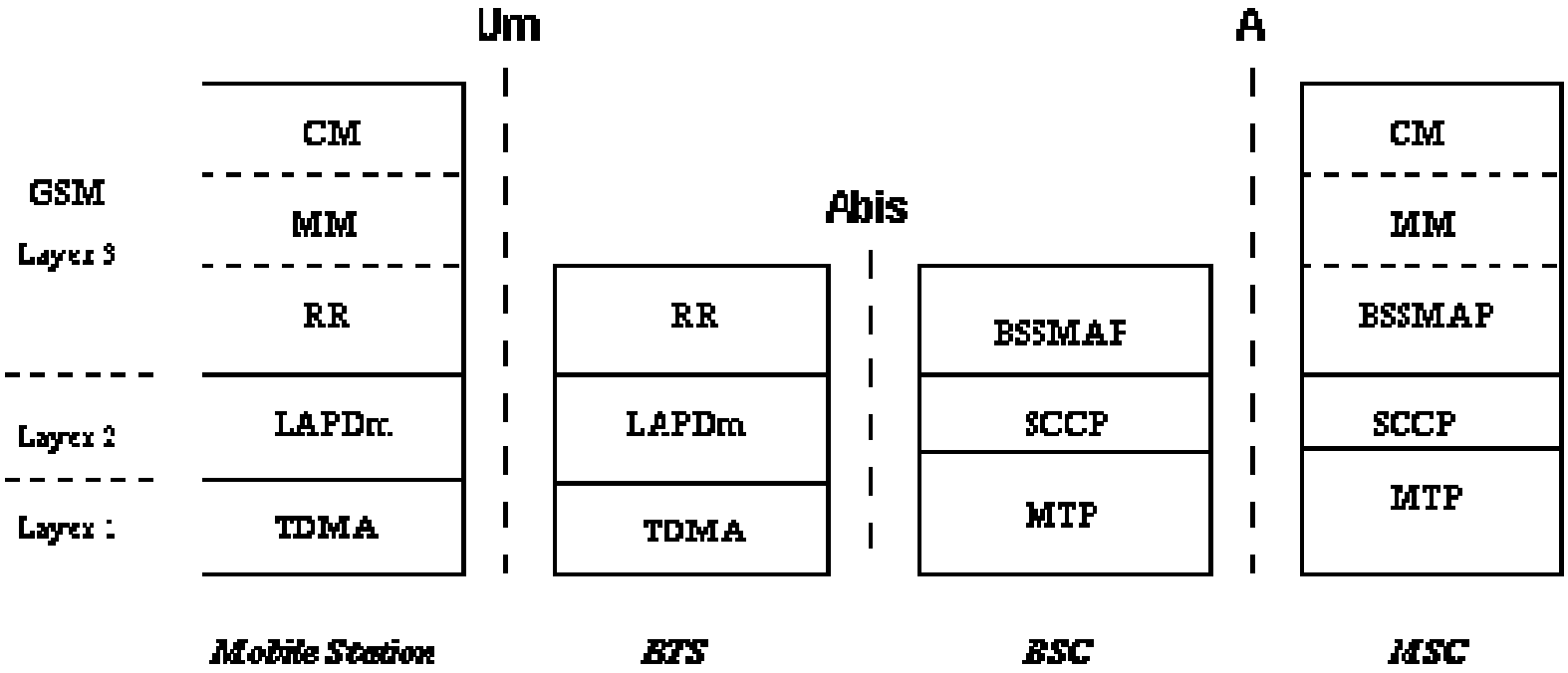
Network Aspects

- Ensuring the transmission of voice or data of a given quality over the radio link is only a part of the function of a cellular mobile network.
- A GSM mobile can seamlessly roam nationally and internationally,
- Roaming requires that
  - Registration and authentication,
  - Call routing and location updating functions are standardized in GSM networks.

Network Aspects

- In addition, the fact that the geographical area covered by the network is divided into cells necessitates the implementation of a handover mechanism.
- These functions are performed by the Network Subsystem, mainly using the **Mobile Application Part (MAP)** built on top of the Signaling System No. 7 protocol.

Network Aspects



Network Aspects

- The signaling protocol in GSM is structured into three general layers depending on the interface
  - **Layer 1** is the physical layer, which uses the channel structures discussed above over the air interface.
  - **Layer 2** is the data link layer. Across the Um interface, the data link layer is a modified version of the LAPD protocol used in ISDN, - LAPDm.
  - Across the A interface, the Message Transfer Part layer 2 of Signaling System Number 7 is used.
  - **Layer 3** of the GSM signaling protocol is itself divided into 3 sub-layers.

Layer 3 Sublayers

- Radio Resources Management
  - Controls the setup, maintenance, and termination of radio and fixed channels, including handovers.
- Mobility Management
  - Manages the location updating and registration procedures, as well as security and authentication.
- Connection Management
  - Handles general call control, similar to CCITT Recommendation Q.931, and manages Supplementary Services and the Short Message Service.

Network Aspects

- Signaling between the different entities in the fixed part of the network, such as between the HLR and VLR, is accomplished through the Mobile Application Part (MAP).
- MAP is built on top of the Transaction Capabilities Application Part (TCAP, the top layer of Signaling System Number 7.

Radio resources management

- The radio resources management (RR) layer oversees the establishment of a link, both radio and fixed, between the mobile station and the MSC.
- The main functional components involved are the mobile station, and the Base Station Subsystem, as well as the MSC.

Radio resources management

- The RR layer is concerned with the management of an RR-session, which is the time that a mobile is in dedicated mode, as well as the configuration of radio channels including the allocation of dedicated channels.
- An RR-session is always initiated by a mobile station through the access procedure, either for an outgoing call, or in response to a paging message.

Radio resources management

- The details of the access and paging procedures, such as when a dedicated channel is actually assigned to the mobile, and the paging sub-channel structure, are handled in the RR layer.
- In addition, it handles the management of radio features such as power control, discontinuous transmission and reception, and timing advance.

Handover

- The execution & measurements for handover are one of the basic functions of the RR layer.
- There are four different types of handover, which involve transferring a call between:
  1. Channels (time slots) in the same cell
  2. Cells (Base Transceiver Stations) under the control of the same Base Station Controller (BSC),
  3. Cells under the control of different BSCs, but belonging to the same Mobile services Switching Center (MSC)
  4. Cells under the control of different MSCs.

Handover

- The first two types of handover, called **internal handovers**, involve only one Base Station Controller (BSC).
- To save signaling bandwidth, they are managed by the BSC without involving the Mobile services Switching Center (MSC), except to notify it at the completion of the handover.
- The last two types of handover, called **external handovers**, are handled by the MSCs involved.

Handover

- An important aspect of GSM is that the original MSC, the *anchor MSC*, remains responsible for most call-related functions, with the exception of subsequent inter-BSC handovers under the control of the new MSC, called the *relay MSC*.
- Handovers can be initiated by either the mobile or the MSC (as a means of traffic load balancing).

Handover

- During its idle time slots, the mobile scans the Broadcast Control Channel of up to 16 neighboring cells, and forms a list of the *six* best candidates for possible handover, based on the received signal strength.
- This information is passed to the BSC and MSC, at least once per second, and is used by the handover algorithm.

Handover

- The algorithm for when a handover decision should be taken is *not* specified in the GSM recommendations.
- There are two basic algorithms used, both closely tied in with power control.
- This is because the BSC usually does not know whether the poor signal quality is due to multi-path fading or to the mobile having moved too far to another cell.

Handover

- This is especially true in small urban cells.
- The *'minimum acceptable performance'* algorithm gives precedence to power control over handover, so that when the signal degrades beyond a certain point, the power level of the mobile is increased.
- If further power increases do not improve the signal, then a handover is considered.

Handover

- This is the simpler and more common method, but it creates 'smeared' cell boundaries when a mobile transmitting at peak power goes some distance beyond its original cell boundaries into another cell.
- The *'power budget'* method uses handover to try to maintain or improve a certain level of signal quality at the same or lower power level.

Handover

- It thus gives precedence to handover over power control.
- It avoids the 'smeared' cell boundary problem and reduces co-channel interference, but it is quite complicated.

Mobility management

- The Mobility Management layer (MM) is built on top of the RR layer, and handles
  - the functions that arise from the mobility of the subscriber - ***Location Management***
  - the ***Authentication and Security*** aspects.
- Location management
  - procedures that enable the system to know the current location of a powered-on mobile station so that incoming call routing can be completed.

Location updating

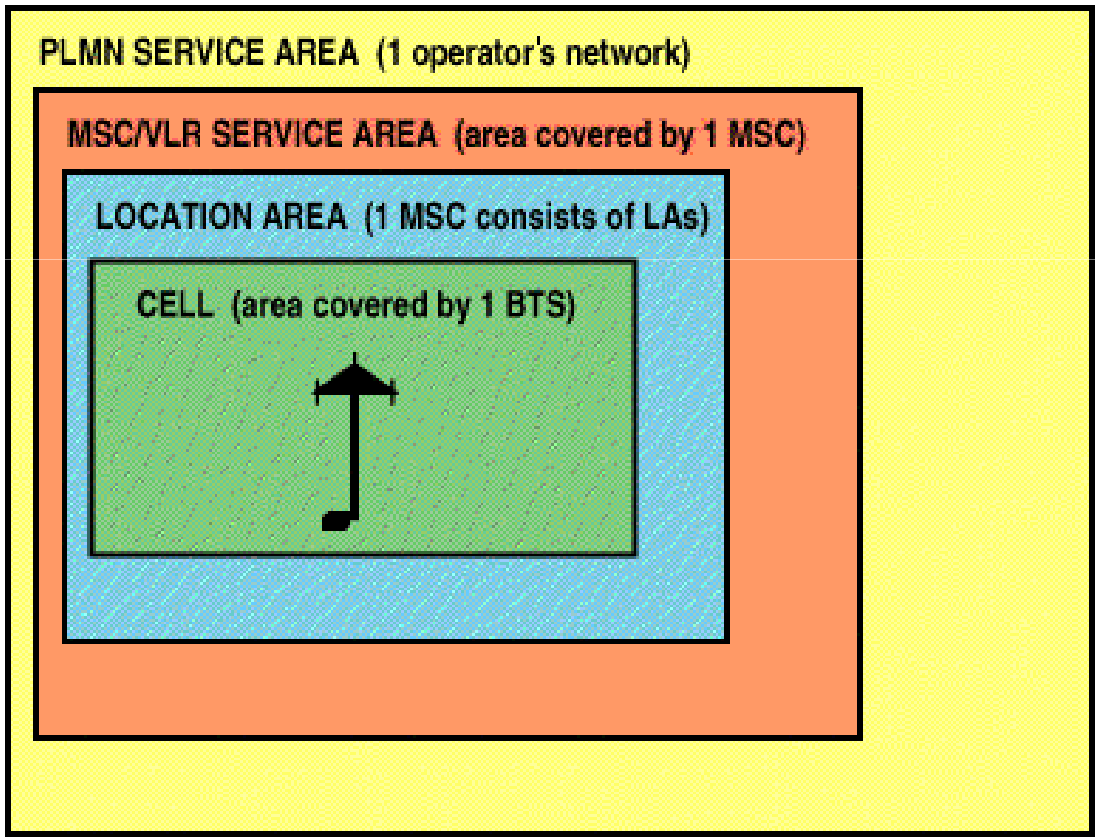
- A powered-on mobile is informed of an incoming call by a paging message sent over the PAGCH channel of a cell.
- Two possibilities
  - Page every cell in the network for each call
  - Mobile notify the system, via location updating messages, of its current location at the individual cell level.
- Both wasteful due to the large number of location updating messages.

Location Areas

- A compromise solution used in GSM is to use *location areas*.
  - Updating messages are required when moving between location areas, and
  - mobile stations are paged in the cells of their current location area
- The location updating procedures, and subsequent call routing, use the MSC and two location registers: HLR & VLR

GSM Network Areas

- The GSM network is made up of geographic areas



HLR & VLR

- When a mobile station is switched on in a new location area, or it moves to a new location area or different operator's PLMN, it must register with the network to indicate its current location.
- In the normal case, a location update message is sent to the new MSC/VLR, which records the location area information, and then sends the location information to the subscriber's HLR.

HLR & VLR

- The information sent to the HLR is normally the SS7 address of the new VLR, although it may be a routing number.
- The reason a routing number is not normally assigned, even though it would reduce signalling, is that there is only a limited number of routing numbers available in the new MSC/VLR and they are allocated on demand for incoming calls.

HLR & VLR

- If the subscriber is entitled to the service, the HLR sends a subset of the subscriber information, needed for call control, to the new MSC/VLR, and sends a message to the old MSC/VLR to cancel the old registration.
- For reliability reasons, GSM also has a periodic location updating procedure.
  - If an HLR or MSC/VLR fails, to have each mobile register simultaneously to bring the database up to date would cause overloading.

HLR & VLR

- Therefore, the database is updated as location updating events occur.
- The enabling of periodic updating, and the time period between periodic updates, is controlled by the operator, and is a trade-off between signaling traffic and speed of recovery.
- If a mobile does not register after the updating time period, it is deregistered.

HLR & VLR

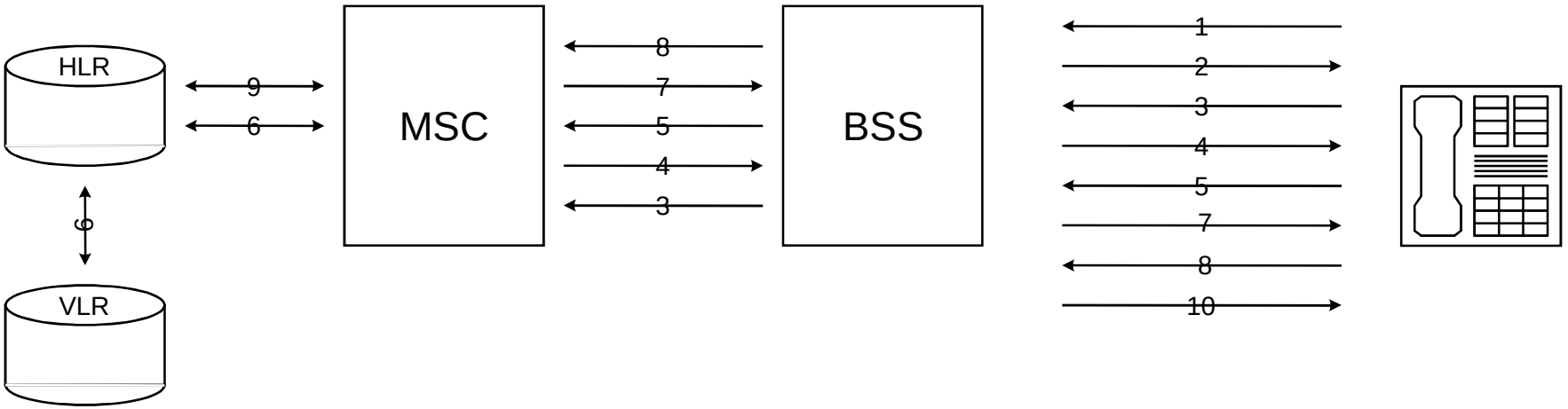
- A procedure related to location updating is the IMSI attach and detach.
- A detach lets the network know that the mobile station is unreachable, and avoids having to needlessly allocate channels and send paging messages.
- An attach is similar to a location update, and informs the system that the mobile is reachable again.

HLR & VLR

- The activation of IMSI attach/detach is up to the operator on an individual cell basis.

Registration (2)

1 - Channel Request
2 - Channel Assignment
3 - Location Update Request
4 - Authentication Request
5 - Authentication Response
6 - Process Authentication Parameters
7 - Assignment of New Area and TMSI
8 - Acknowledgment
9 - VLR and HLR Updates
10 - Channel Release



Authentication and Security Aspects Background Private Key Encryption

- Sender and receiver use one value (key) to scramble and unscramble
- Called private keys
- Example: Data Encryption Standard (DES) specified by the US Government in 1977

Data Encryption Standard

- Based on an encryption algorithm that changes plain text with so many combinations it will be impossible to figure out the plain-text
- Uses a permutation function and a substitution function
  - P-functions changes bit positions
  - S-function, a 5-bit input (decoder) selects one of 8 possible inputs and does line substitution

Data Encryption Standard

- Idea is to use P and S functions to provide for several stages
- Problems !

•This distribution of private keys - need to be fully meshed

•Gave rise to public key encryption

Public Key Encryption

- Uses two (or more) keys
- The keys are generated during the same invocation of an algorithm
- Because of this relationship, it allows the sharing of the public key without compromising security.

RSA Algorithm

- Best known public key algorithm, named after its inventors: Ron Rivest, Adi Shamir and Len Adleman
- Party A selects two large prime numbers p and q and calculates n=p *x* q
- Part A then chooses a random integer e, 1<e>n, and must not have integer divisors >1 that are common with p-1 and q-1.

RSA

- Party A publishes the (n,e) but not the (p,q) pair
- Party B encrypts a message m into cipher c to send to A
  - $c = m^e \pmod n$ $0 < c < n$
- Party A decrypts the ciphered message c as follows:
  - $m = C^d \pmod n$

Trivia - Breaking the RSA Code

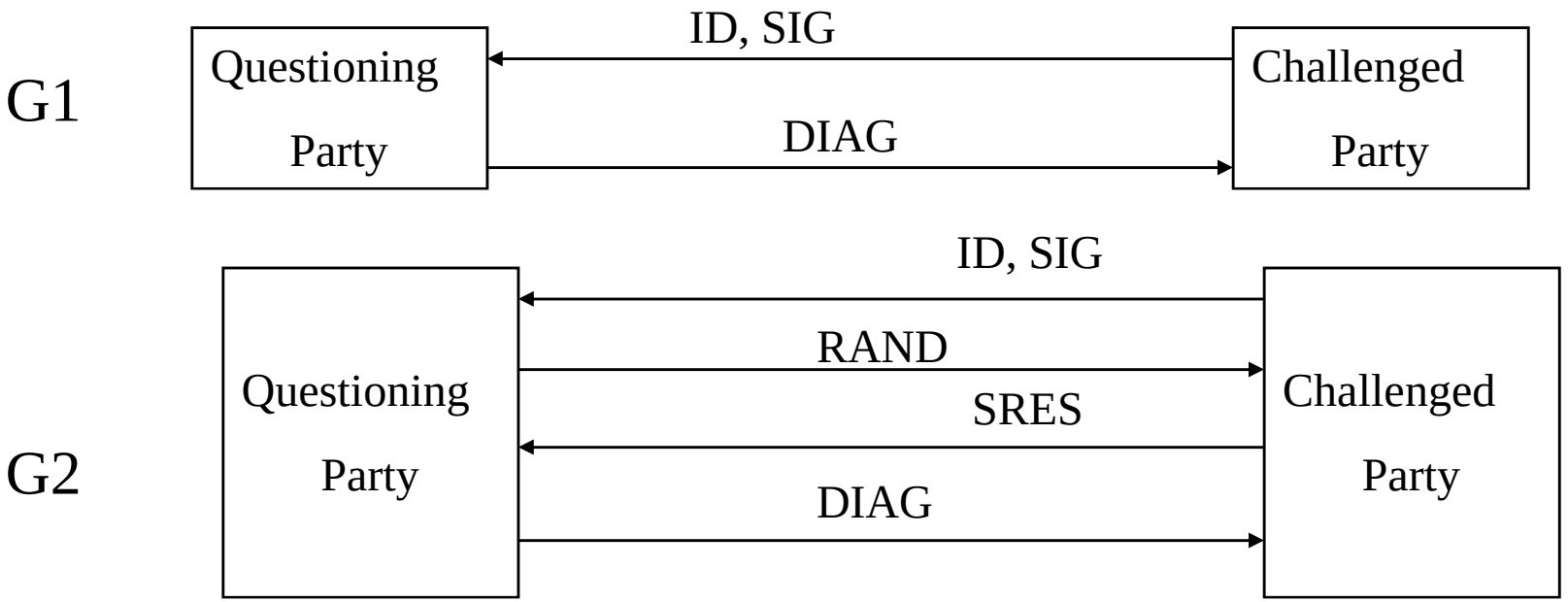
- In 1977 challenged was issues to break the RSA 129-digit code
- In 1994, task force organized by Bellcore broke the code - find two prime numbers multiplied together that resulted in the 129-digit key
- Claims are being made that 155-digit code is close to being broken

Authentication Model

- Based on a challenge
  - ID - a string of octets representing the identity of the challenge party
  - SIG - a string of octets representing the ID - password or result of an encryption process
  - RAND - An unpredictable range of octets
  - SRES - The reply of the challenged party
  - DIAG - The result of the identification process

Authentication Model

- Defines two security options: grade 1 and 2



GSM - Authentication and Security

- Authentication involves two functional entities:
  - the SIM card in the mobile, and
  - the Authentication Center (AuC).
- Each subscriber is given a secret key, one copy of which is stored in the SIM card and the other in the AuC.
- During authentication, the AuC generates a random number that it sends to the mobile.

Authentication and security

- Both the mobile and the AuC then use the random number, in conjuction with the subscriber's secret key and a ciphering algorithm called A3, to generate a signed response (SRES) that is sent back to the AuC.
- If the number sent by the mobile is the same as the one calculated by the AuC, the subscriber is authenticated.

Authentication and security

- The same initial random number and subscriber key are also used to compute the ciphering key using an algorithm called A8.
- This ciphering key, together with the TDMA frame number, use the A5 algorithm to create a 114 bit sequence that is XORed with the 114 bits of a burst (the two 57 bit blocks).

Authentication and security

- Enciphering is an option for the fairly paranoid, since the signal is already coded, interleaved, and transmitted in a TDMA manner, thus providing protection from all but the most persistent and dedicated eavesdroppers.
- Another level of security is performed on the mobile equipment itself, as opposed to the mobile subscriber.

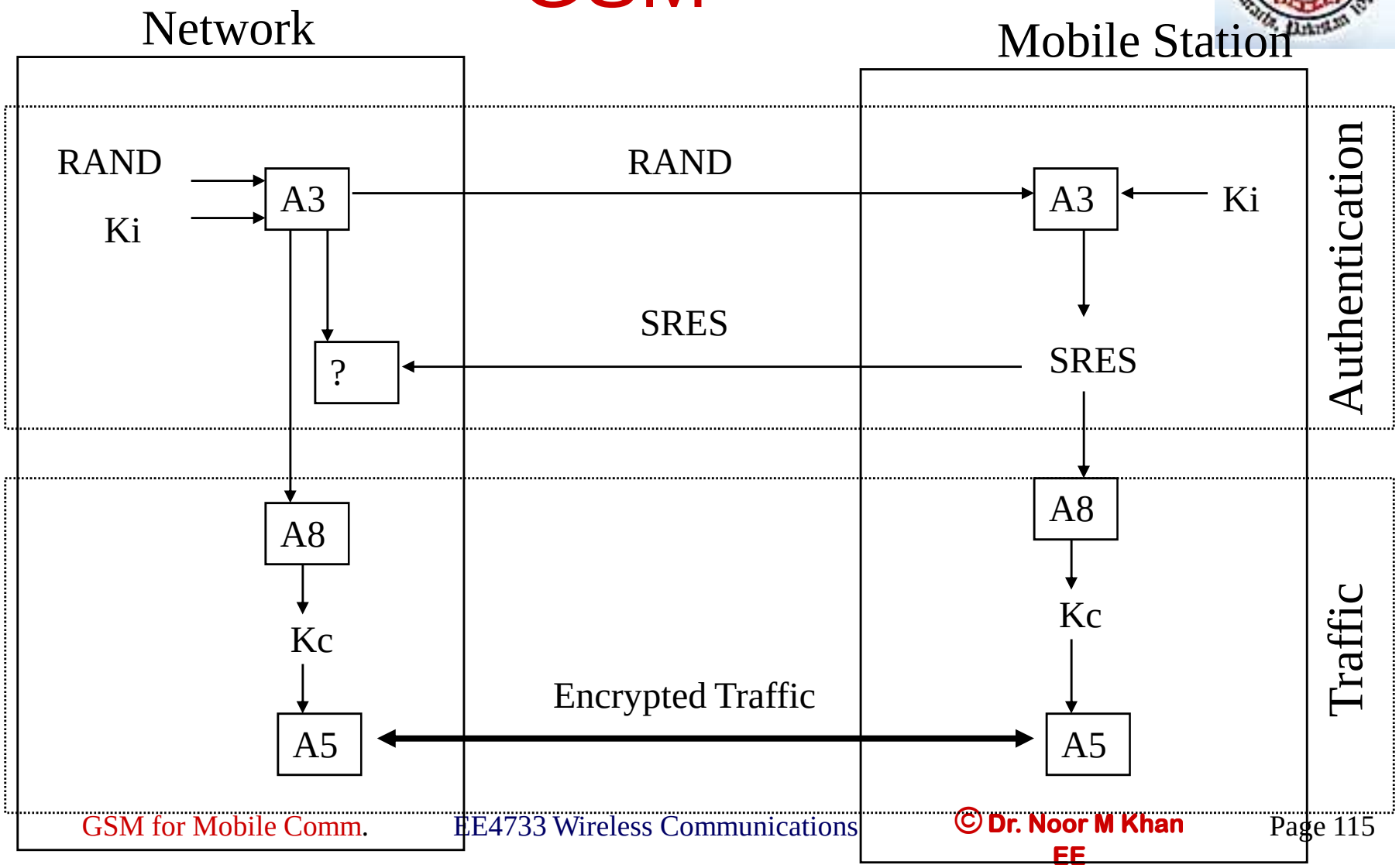
Authentication and security

- As mentioned earlier, each GSM terminal is identified by a unique International Mobile Equipment Identity (IMEI) number.
- A list of IMEIs in the network is stored in the Equipment Identity Register (EIR).

Authentication and security

- The status returned in response to an IMEI query to the EIR is one of the following:
  - White-listed: The terminal is allowed to connect to the network.
  - Grey-listed: The terminal is under observation from the network for possible problems.
  - Black-listed: The terminal has either been reported stolen, or is not type approved (the correct type of terminal for a GSM network). The terminal is not allowed to connect to the network.

GSM


Network
Mobile Station
RAND
Ki
A3
RAND
A3
Ki
SRES
?
SRES
Authentication
A8
Kc
A5
Encrypted Traffic
A8
Kc
A5
Traffic

Communication management

- The Communication Management layer (CM) is responsible for Call Control (CC), supplementary service management, and short message service management.
- Each of these may be considered as a separate sublayer within the CM layer.

Communication management

- Call control attempts to follow the ISDN procedures specified in Q.931, although routing to a roaming mobile subscriber is obviously unique to GSM.
- Other functions of the CC sublayer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

Call routing

- Unlike routing in the fixed network, where a terminal is semi-permanently wired to a central office, a GSM user can roam nationally and even internationally.
- The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the E.164 numbering plan.

Communication management

- This number includes a country code and a National Destination Code which identifies the subscriber's operator.
- The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN.
- An incoming mobile terminating call is directed to the Gateway MSC (GMSC) function.
- The GMSC is basically a switch which is able to interrogate the subscriber's HLR to obtain routing information, and thus contains a table linking MSISDNs to their corresponding HLR.

Communication management

- A simplification is to have a GSMC handle one specific PLMN.
  - GMSC function is distinct from the MSC function, but is usually implemented in an MSC.
- The routing information that is returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is also defined by the E.164 numbering plan.

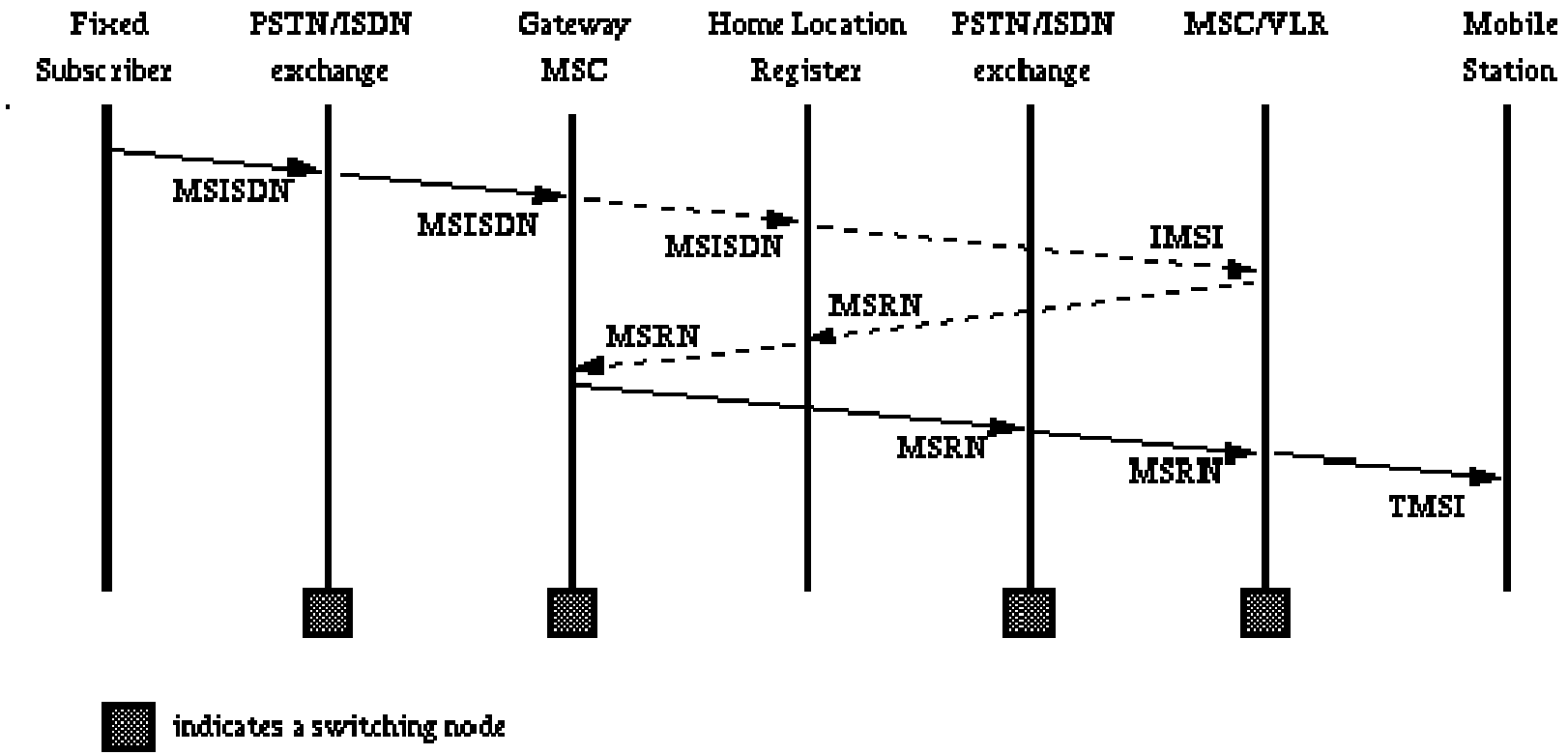
Communication management

- MSRNs are related to the geographical numbering plan, and not assigned to subscribers, nor are they visible to subscribers.
- The most general routing procedure begins with the GMSC querying the called subscriber's HLR for an MSRN.
- The HLR typically stores only the SS7 address of the subscriber's current VLR, and does not have the MSRN.

Communication management

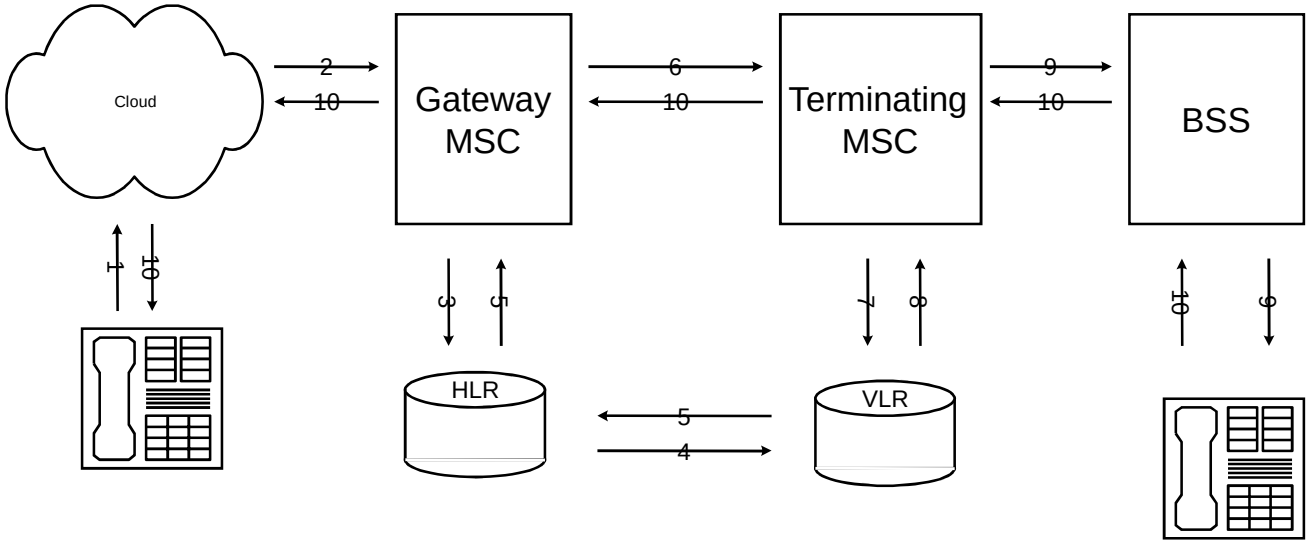
- The HLR must therefore query the subscriber's current VLR, which will temporarily allocate an MSRN from its pool for the call.
- This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC.
- At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area

Call Routing



Call Establishment

1 - Call made to MS
2 - PSTN recognized and passes to GMSC
3 - MSC cannot route - asks HLR
4 - Asks VLR serving user
5 - Routing number to HLR & then to GMSC
6 - Call routed to terminating MSC
7 - requests VLR to correlate call to subscriber
8 - VLR complies
9 - Mobile unit paged
10 - Mobile unit responds



Roaming

1 - Location update request
2 - Location update message
3 - subscription data return
4 - Location update ACK
5 - Location cancellation message