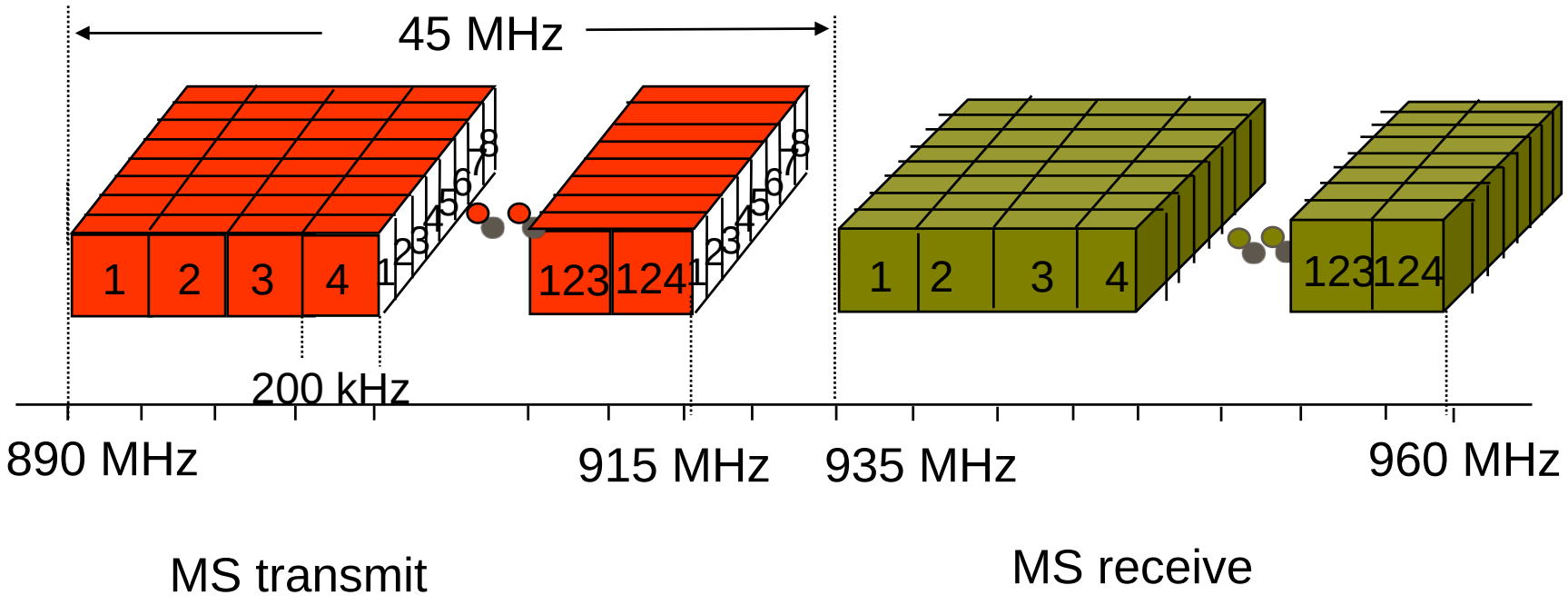
2nd Generation Cellular Systems: GSM - 2

- GSM Logical channels
- GSM Signalling processing
- GMS Operation Handover
- GSM-SMS

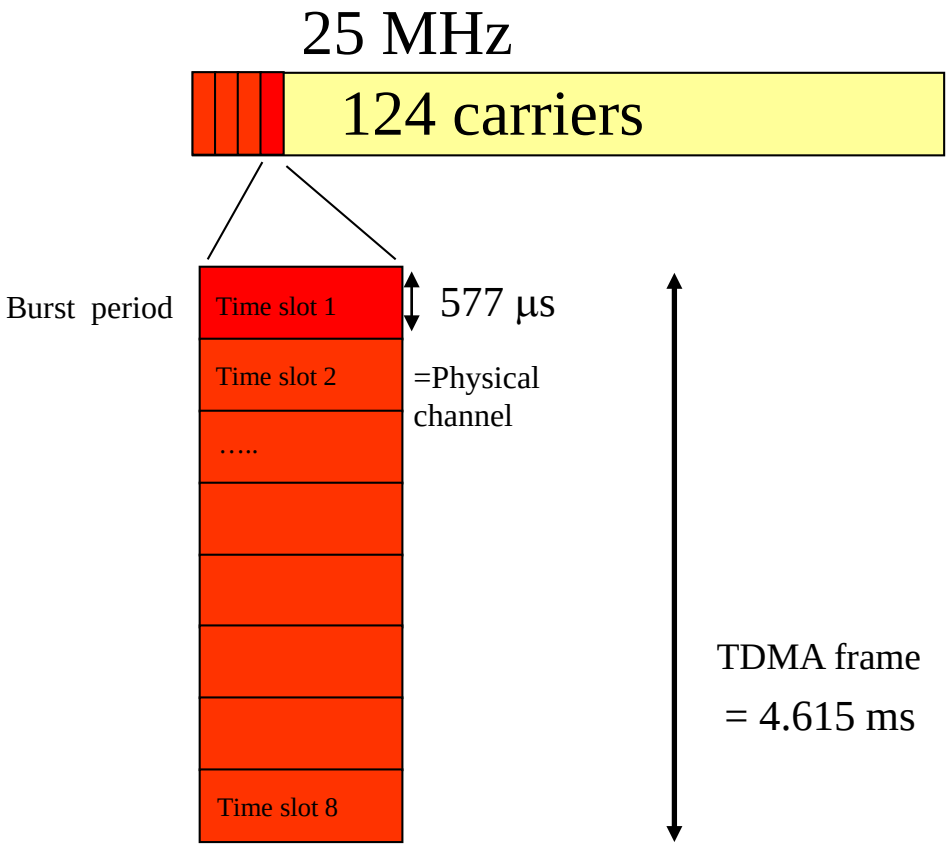
Review

- GSM Architecture
- GSM structure
- GSM Channel structure

Channels in GSM900



GSM Channel structure



- Logical channels is built up of physical channels
  - Control channels
  - Traffic channels

GSM Logical Channels

- Traffic Channels
  - The full-rate traffic channel (TCH/F)
    - uses a 13 kbps speech-coding scheme and 9,600 bps, 4,800 bps, and 2,400 bps data
    - 8 slots per TDMA frame, gross rate of 22.8kbps
  - The half-rate traffic channel (TCH/H)
    - uses 16 slots per frame that has a gross bit rate of 11.4 kbps
    - supports 4.8 kbps and 2.4 kbps for data
    - It can support half rate speech coding
- Control Channels (three classes) :
  - broadcast channels (BCH)
  - common control channels (CCCH)
  - dedicated control channels (DCCH)

Broadcast channels

- The frequency control channel (FCCH)
  - BTS broadcasts and the MS (in the coverage area) uses the FCCH to synchronize its carrier frequency and bit timing
- The synchronization channel (SCH)
  - BTS broadcasts and the MSs will synchronize their counters to specify the location of arriving packets in the TDMA hierarchy (frame synchronization)
- The broadcast control channel (BCCH)
  - used by the BTS to broadcast synchronization parameters, available services, and cell ID
  - Once the carrier, bit, and frame synchronization between the BTS and MS are established, the BCCH informs the MS about the environment parameters associated with the BTS covering that area
  - The BCCH is physically implemented over the NB(Normal Burst)s
  - The BCCH is also used for signal strength measurements for handoff

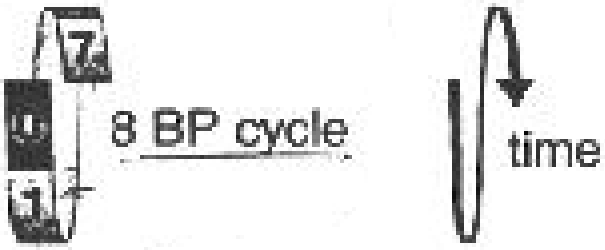
Common control channels (CCCH)

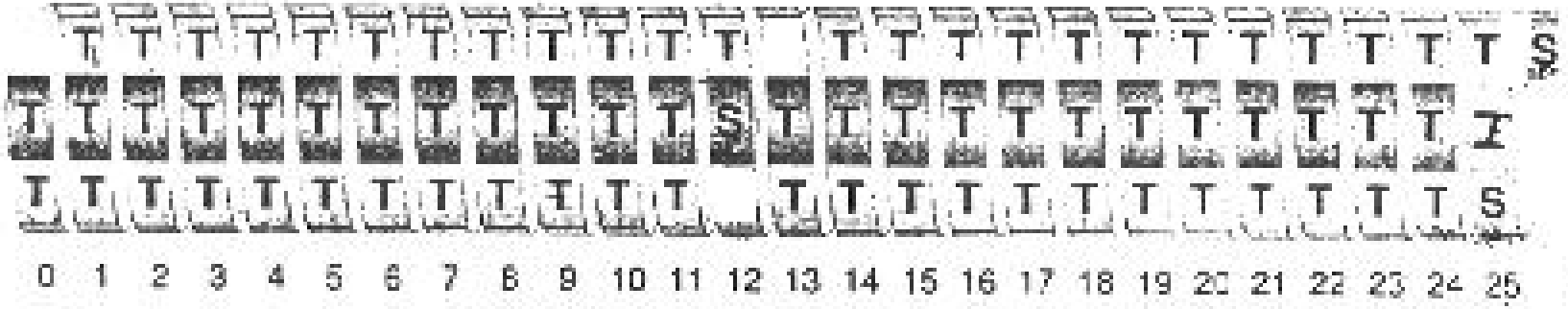
- The paging channel (PCH)
  - used by the BTS to page the MS for an incoming call
  - It is a broadcast channel implemented on a NB
- The random access channel (RACH)
  - used by the MS to access the BTS for call establishment
  - The RACH is used for the implementation of the slotted-ALOHA protocol, the random access control used by mobile stations
- The access grant channel (AGCH)
  - used for implementation of the acknowledgement from the BTS to the MS after a successful attempt by the MS using RACH
  - This channel is implemented on an NB and indicates the TCH for access to the GSM network

Dedicated control channels (DCCH)

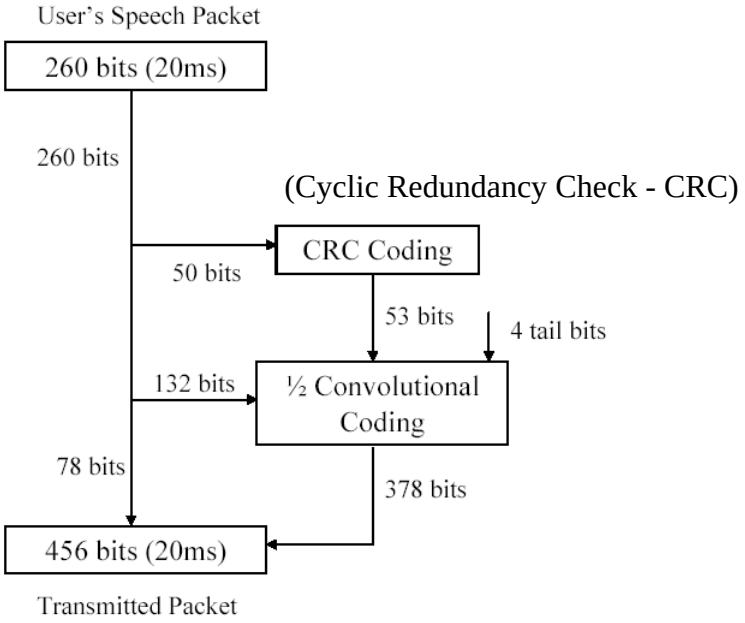
- The DCCH are two-way channels supporting signaling and control for individual users
- The stand-alone dedicated control channel (SDCCH)
  - It is a two-way channel assigned to each terminal to transfer network control information for call establishment and mobility management
- The slow associated control channel (SACCH)
  - It is a two-way channel assigned to each TCH and SDCCH channels
  - The SACCH is used to exchange the necessary parameters between the BTS and the MS to maintain the link
    - Example: the MS sends its report on RSS of neighbouring BTSs
- The fast associated control channel (FACCH)
  - It is used during call initialization and release phases when user data is not being yet/still transmitting
  - also used for handoff orders
  - Stealing bit tells when the FACCH is being used instead of TCH
  - The FACCH is physically multiplexed with the TCH or SDCCH to provide additional support to the SACCH

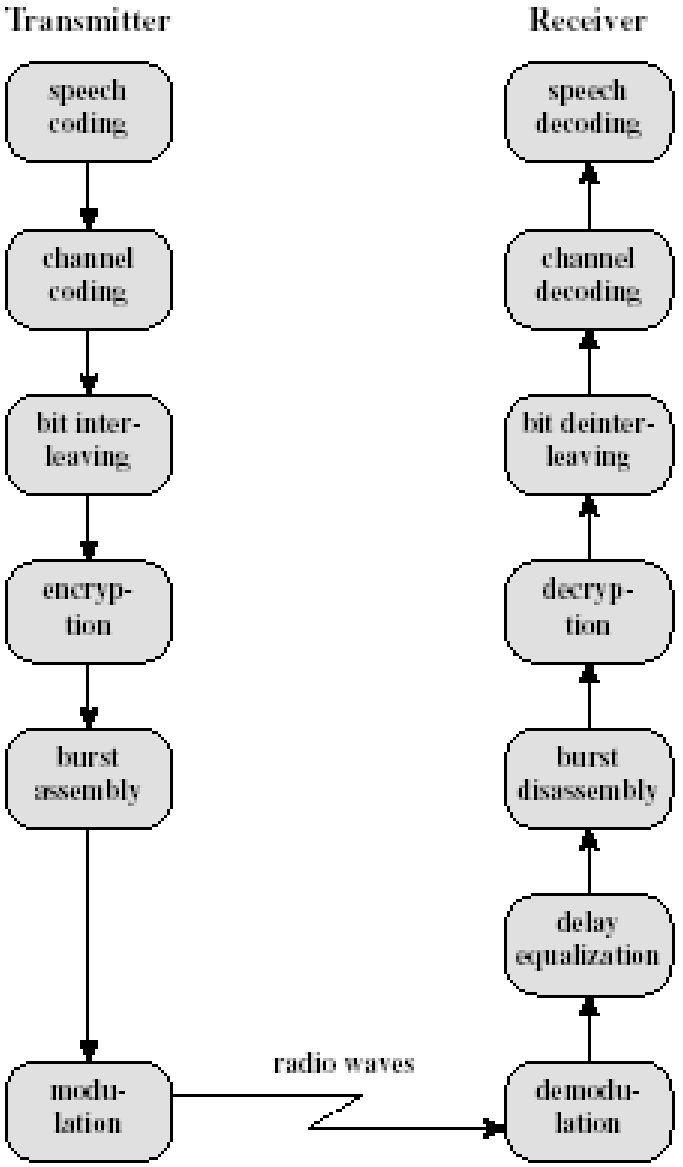
GSM Channel Structure [MP 92]





GSM Signal Processing





GMSK (*Gaussian Minimum Shift Keying*)

[Stallings 02]

Mechanisms to Support a Mobile Environment

- Random Access in GSM
- Registration Procedure
- Call Establishment
- Handoff or Handover
- Security

Random Access in GSM

- GSM uses the slotted ALOHA protocol
  - An MS that wants to access the GSM system sends the request message in the beginning of a time slot
  - The BTS checks if the message arrived without error, i.e. without collision with another MS's message
  - If the transmission is correct, the BTS sends an acknowledgment back to the MS
  - The MS can continue its requested procedure (registration, traffic channel allocation …)
  - If there was collision, the BTS does not send the acknowledgement
  - If the MS does not receive the acknowledgment in a specified period of time, it assumes that a collision took place and reschedules the access within a randomly selected delay to avoid repeated collisions

Registration Procedure

- When the MS is turned on, it synchronizes to the frequency, bit, and frame timings of the closest BS
- After this, the MS reads the system and cell identity to determine its location in the network
- If the current location is not the same as before, the MS initiates a registration procedure
- During a registration procedure, network provides the MS with a channel for preliminary signaling
- The MS provides its identity and finally the network authenticates the MS
- The simplest connection takes place if the MS is turned on in the previous area
- The most complex registration process occurs when the mobile is turned on in a new MSC area which needs changes in the entries of the VLR and HLR

Registration Procedure [PK 02]

Steps	MS	BTS	BSC	MSC	VLR	HLR
1. Channel request	←	←	←			
2. Activation Response		→	→			
3. Activation ACK			←			
4. Channel Assigned	→	→				
5. Location Update request	←	←	←	←		
6. Authentication Request	→	→	→	→		
7. Authentication Response				↔	↔	
8. Authentication Check						
9. Assigning TMSI	→	→	→	→		
10. ACK for TMSI	←	←	←	←		
11. Entry to VLR and HLR				↔		↔
12. Channel Release	→	→	→			

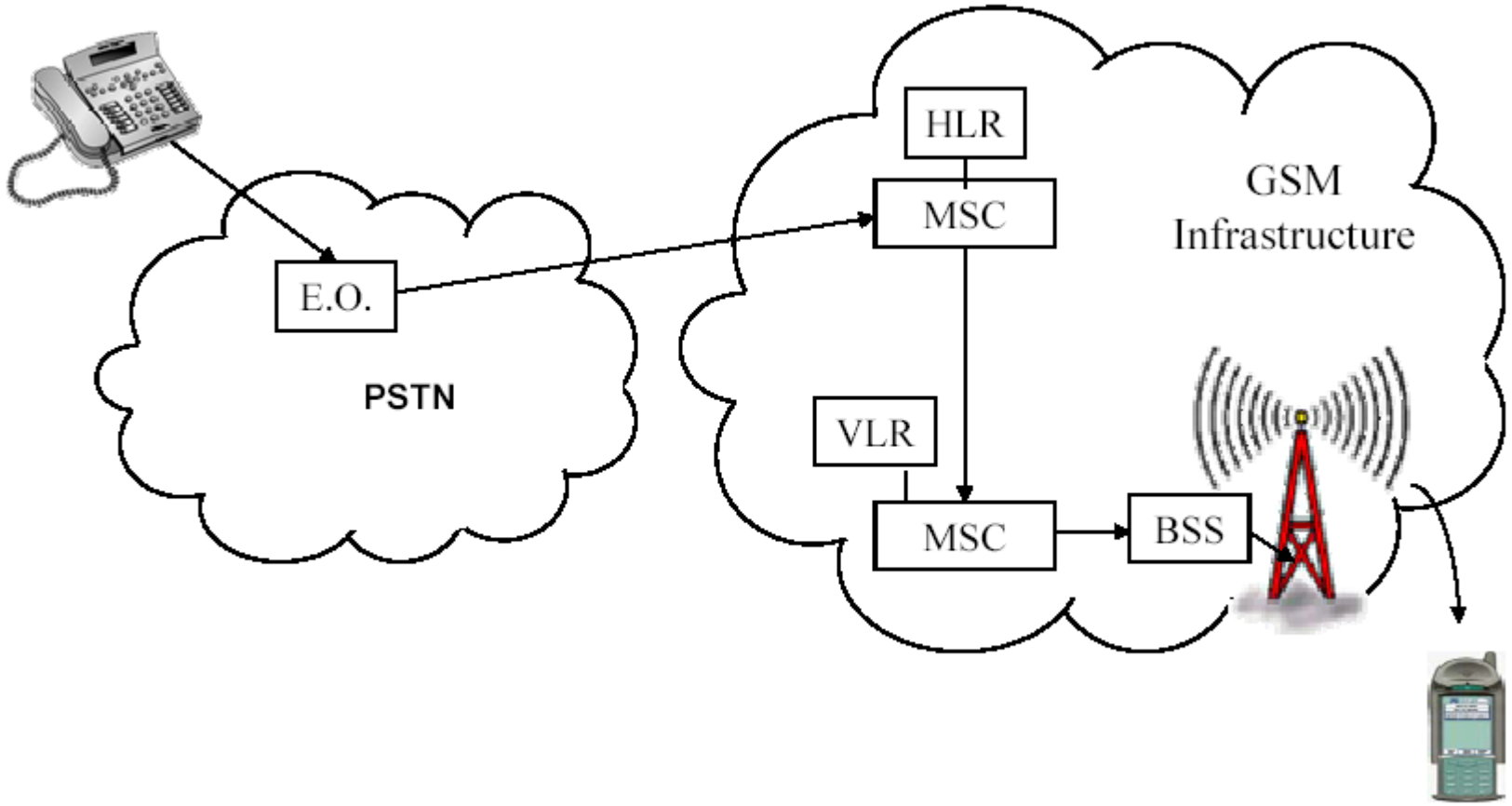
Mobile Originated Call in GSM [PK 02]

Steps	MS	BTS	BSC	MSC
1. Channel request (RACH)				
2. Channel Assigned (AGCH)				
3. Call Establishment Request (SDCCH)				
4. Authentication Request (SDCCH)				
5. Authentication Response (SDCCH)				
6. Ciphering Command (SDCCH)				
7. Ciphering Ready (SDCCH)				
8. Send Destination Address (SDCCH)				
9. Routing Response (SDCCH)				
10. Assign Traffic Channel (SDCCH)				
11. Traffic Channel Established (FACCH)				
12. Available/Busy Signal (FACCH)				
13. Call Accepted (FACCH)				
14. Connection Established (FACCH)				
15. Information Exchange (TCH)				

Call Establishment

- Mobile Originated Call
  - 15-step mobile originated call establishment procedure in the GSM
  - The first five steps are similar to the registration process in GSM
  - The next two steps start ciphering (encryption) to provide a protection against eavesdropping.
  - The rest of the steps are similar to those in wired networks except that we have an additional traffic channel assignment procedure

Mobile Terminated Call [PK 02]



Mobile Terminated Call

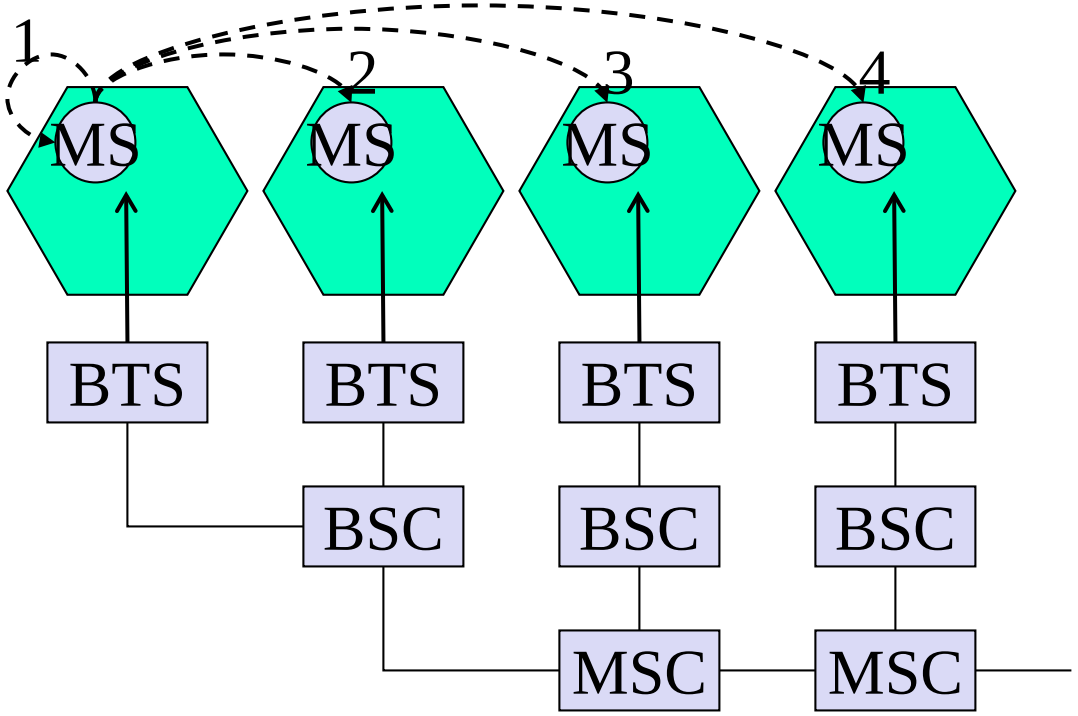
- A fixed telephone dials a mobile to a MSC
- After dialing, the PSTN directs the call to the MSC identified by the destination address
- The MSC requests routing information from the HLR
- In the worse case, the mobile is roaming in the area of a different MSC, the address of the new MSC is given to the MSC, and it contacts the new MSC
- At the destination MSC, the VLR initiates a paging procedure in the LA (location area) the MS have registered last time
- After a reply from the MS, the VLR sends the necessary parameters to the MSC to establish the link to the MS

Types of handover

- Intra cell (to another channel in the same cell) (1)
- Inter cell, intra BSC (2)
- Inter BSC, intra MSC (3)
- Inter MSC (4)

- In addition inter system handover can sometimes be performed, e.g. GSM to UMTS
  - Complicated, special rules apply

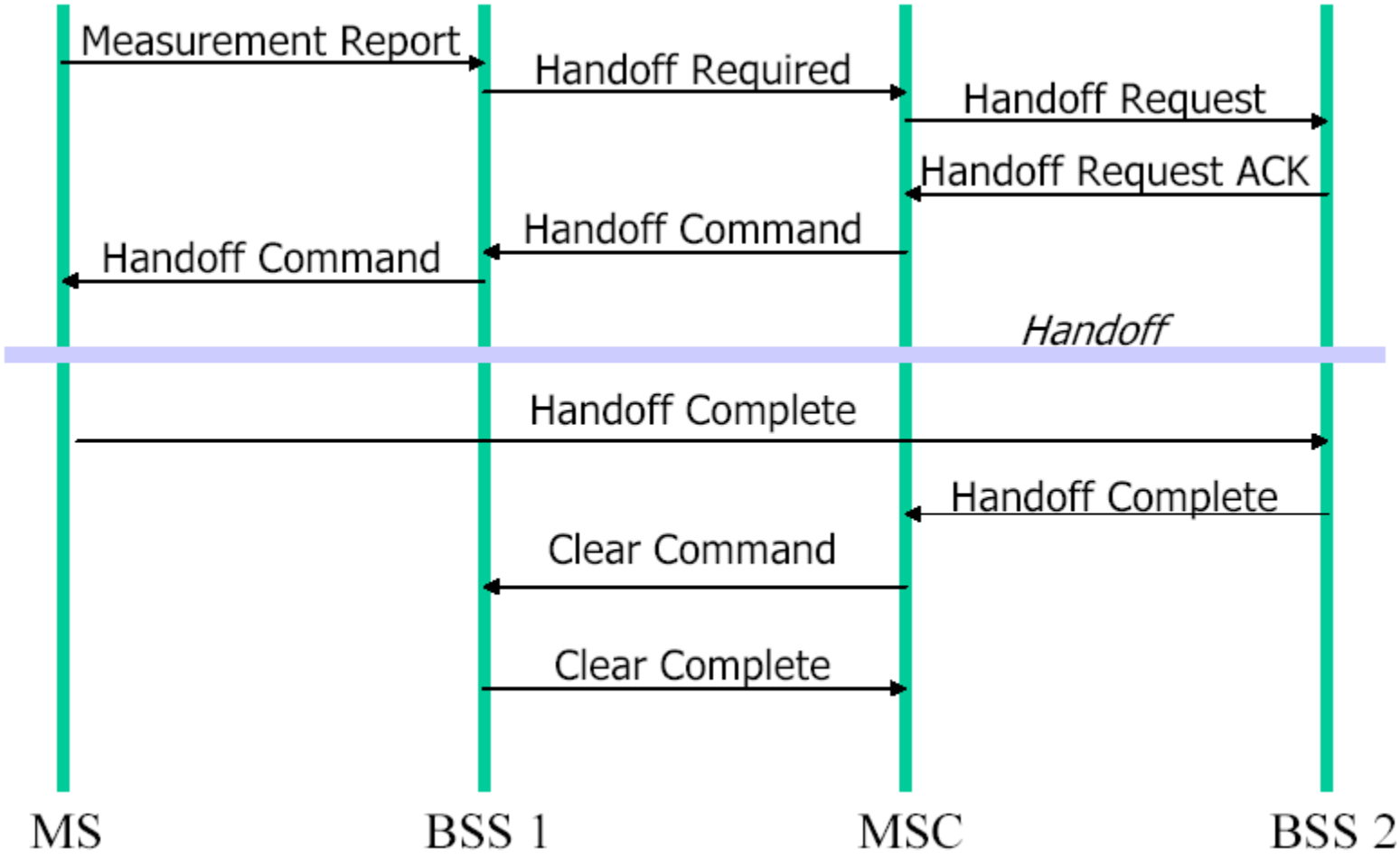
- Type of handover has network implications, but the algorithms to decide handover are the same



Handover

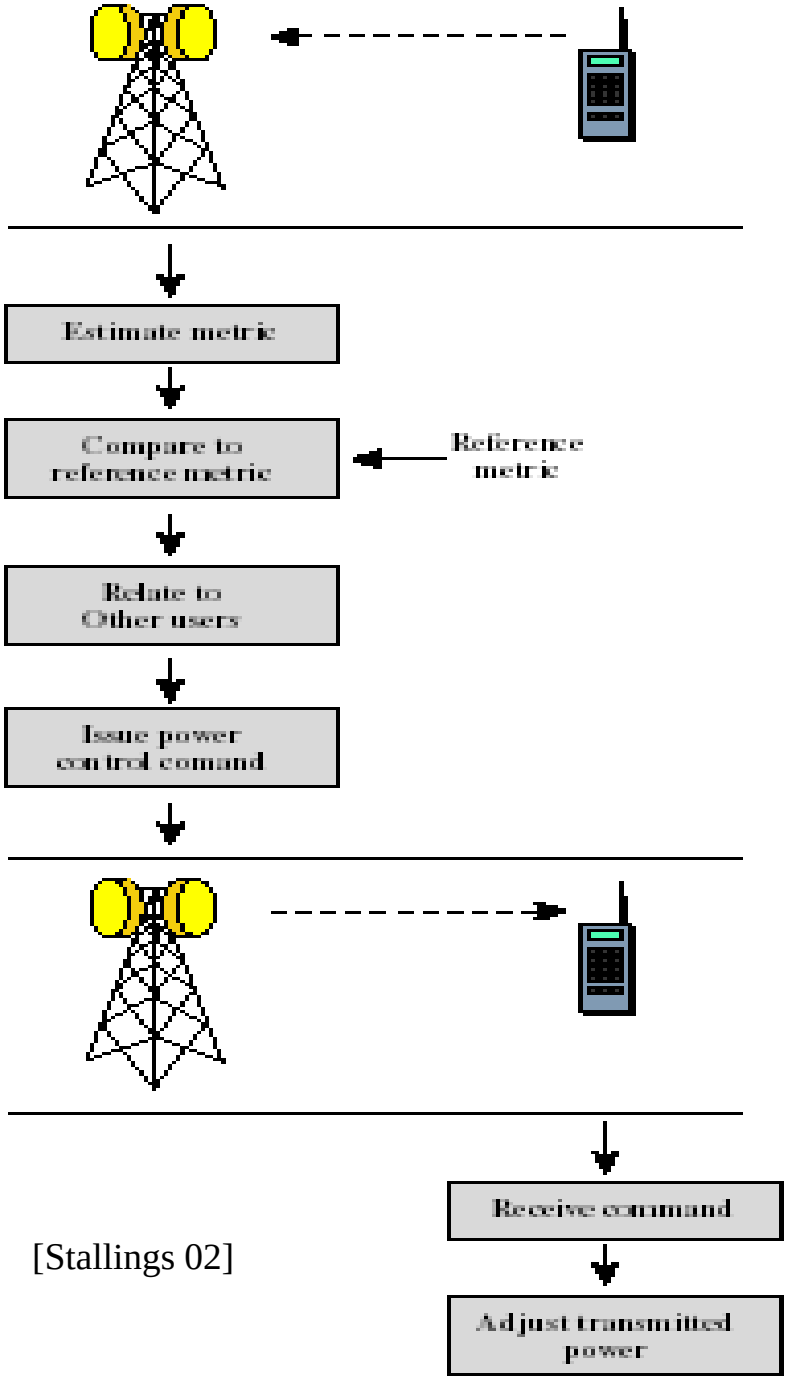
- Between BTSs that belong to the same BSS (Internal)
- Between two different BSSs belonging to the same MSC (External)
- Between BSSs that are controlled by two different MSCs (Inter Systems)
  - the old MSC continues to handle call management
- Reasons
  - mainly Signal strength deterioration
  - sometimes traffic balancing
- Handoff procedure between two BSSs that are controlled by one MSC
  - The BTS provides the MS with a list of available channels in neighboring cells via the BCCH.
  - The MS monitors the RSS from the BCCHs of these neighboring cells and reports these values to the MSC using the SACCH (mobile-assisted handoff)
  - The BTS also monitors the RSS from the MS to make a handoff decision
  - The MSC negotiates a new channel with the new BSS and indicates to the MS that a handoff should be made using a handoff command.
  - Upon completion of the handoff, the MS indicates this with a handoff complete message to the MSC

Handover [PK 02]



Closed-loop power control

- Used in GSM
- Eliminates the disadvantages of the open loop power control by implementing a feedback mechanism between the BS and the MS
- The BS measures the quality of the signal received from the MS and adjusts (based on metric of performance - RSS, SIR or BER) the signal strength that the reverse channel should apply
- Base station makes the power adjustment decision and communicates to mobile on control channel



[Stallings 02]

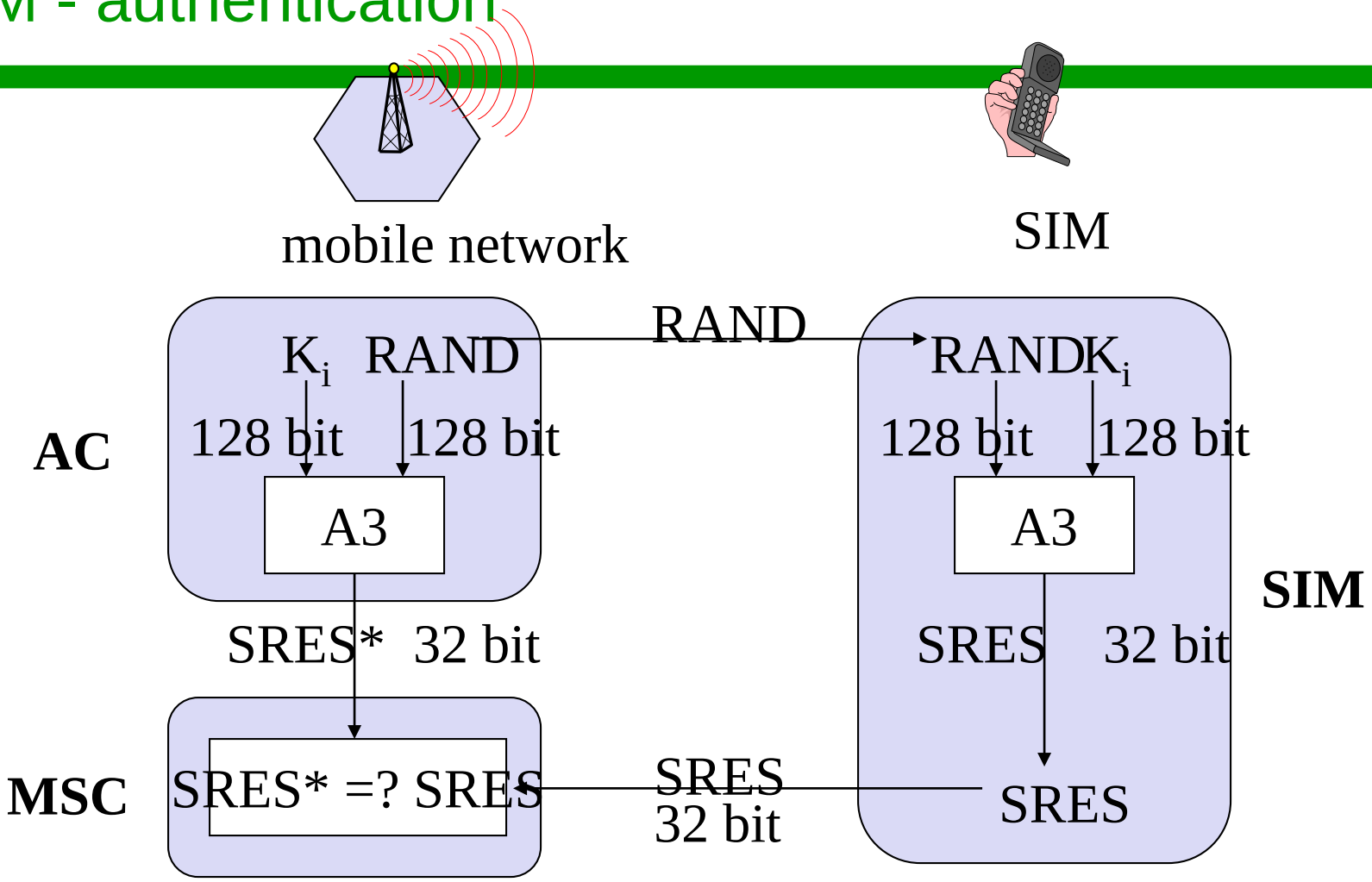
Closed Loop Power Control in GSM

- The MS measures the RSS and the signal quality of up to six neighbouring BSs and reports to its BTS (base transceiver station)
- The BTS also measures the RSS, signal quality and the distance to each MS in its serving area.
- From these measurements, the BTS determines the minimum required transmit power and inform the MS in a five-bit field in the slow associate control channel

Security

- Implemented to prevent fraud via authentication, avoid revealing the subscriber number over the air, and encrypt conversations
- The SIM cards have a microprocessor chip that can perform the computations required for security purposes
- A secret key K_i is stored on the SIM card, and it is unique to the card
- This key is used in two proprietary algorithms A3 (authentication) and A8 (confidentiality)
- For authentication, the secret key K_i is used in a challenge response protocol using the A3 algorithm between the BSS and the MS
- The secret key K_i is used to generate a privacy key K_c that is used to encrypt messages (voice or data) using the A8 algorithm

GSM - authentication



K_i: individual subscriber authentication key SRES: signed response

Security

- One example of challenge-response protocol
  - The MS is registered with the HLR via IMSI and secret key Ki
  - The MSC sends a random number (challenge) to the MS
  - The MS replies with an encrypted value of the random number where the encryption is done by using the secret key Ki (response)
  - The VLR verifies if the response generated by the MS is the same
- The secret key information is not shared between systems
- Instead a triple consisting of the random number used in the challenge, the response to the challenge, and the data encryption key K_c is exchanged between the VLR and the HLR
- An eavesdropper cannot replay the response because the challenge is different if he tries to contact the MSC
- The eavesdropper cannot determine the key because the encryption scheme is sufficiently safe and the K_i is not revealed

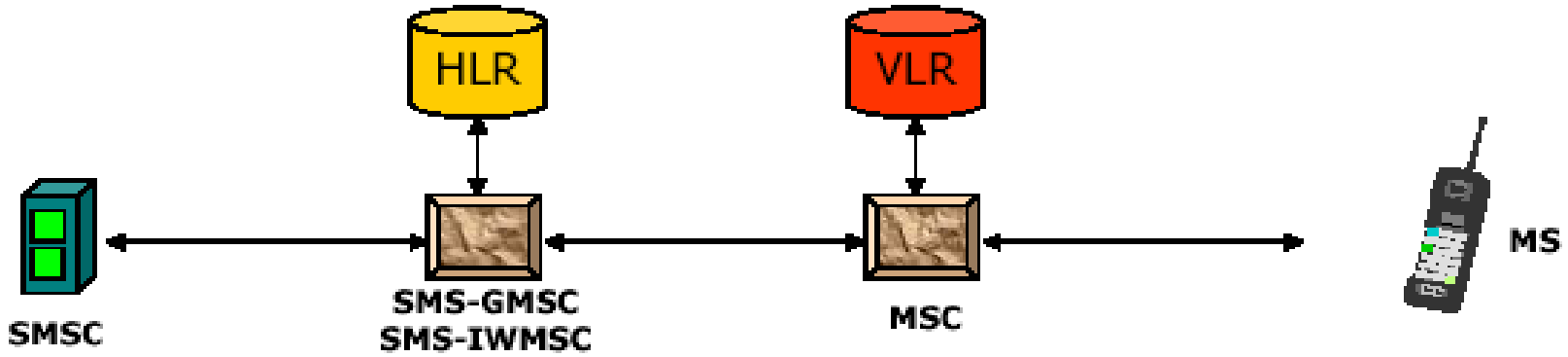
Security

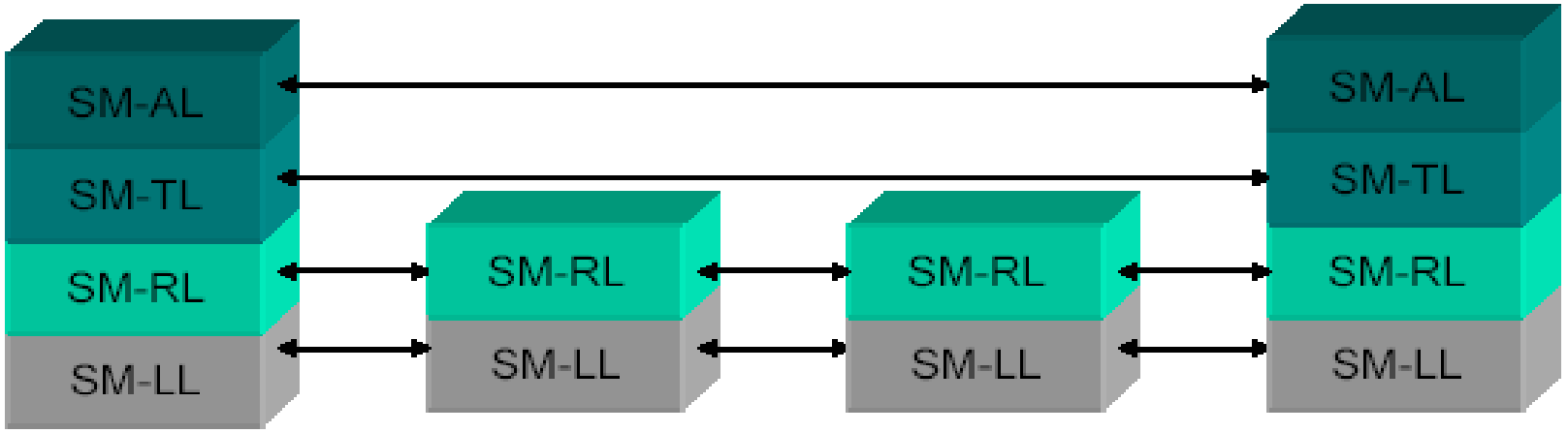
- The control channel signals are encrypted using a third encryption algorithm called A5
- The size of the secret key K is 128 bits, and the response to the challenge is 32 bits long (not very secure)
- The algorithms A8 and A3 are secret and not shared between different systems
- More details [PK 02] chapter 6 section 6.4

Short Messaging Services (SMS)

- A Short Message (SM) is an alphanumeric message of up to 160 characters
- Available wherever GSM exists
- SMS makes use of the GSM infrastructure with the addition of a SMS center - SMSC
- The SM is delivered almost instantly if the destination MS is active
- The SM is stored and forwarded later if the MS is inactive
- Two types of services are specified:
  - Cell broadcast service
    - the message is transmitted to all MSs that are active in a cell and that are subscribed to the service
    - This is an unconfirmed, one-way service used to send weather forecasts, stock quotes, and so on
  - PTP service
    - An MS may send a message to another MS using a handset or by calling a paging center
    - A sender may request acknowledgment of message receipt

SMS- Reference Architecture and Protocol Layers [PK 02]





Short Messaging Services (SMS)

- Each SM is maintained and transmitted by the SMSC
  - The SMSC sorts and routes the messages
- SS-7 (signalling system) is used through the GSM infrastructure
- Two cases of SMS:
  - A mobile originated SM:
    - A SM from an MS reaches an MSC for processing
    - It is delivered to the service centre through SMS-interworking MSC (SMS-IWMSC) function in the MSC
      - forwards the SM to the SMSC using a global SMSC ID
  - A mobile terminated SM:
    - An SM is forwarded by the SMSC to the SMS-gateway MSC (SMS GMSC) function in an MSC
    - It either queries the HLR or sends it to the SMS-GMSC function at the home MSC of the recipient
    - The SM is forwarded to the destination MSC, querying the VLR for MS details, then to the BSC controlling the BTS providing coverage to the MS, and so on

SMS Protocol Layers

- The application layer (AL)
  - can generate and display the alphanumeric message.
- The Transfer Layer (TL)
  - services the SMS-AL to exchange SMs and receive confirmation of receipt of SMs
  - It can obtain a delivery report or status of the SM sent in either direction
- The relay layer (RL) and Link Layer (LL)
  - relays the SMS PDUs through the LL
- In the air interface
  - MS in idle state
    - the short messages are sent over the SDCCH
  - MS is in active state
    - the SACCH has to be used for delivering the SM
  - Cell broadcast
    - On the cell broadcast channel (CBCH)
    - The broadcasts contain the data and identities of destination MSs

Class Quizzes

- What are the logical channels in GSM?
- How is handover organised in GSM?
- How is the SMS operated in GSM?

References

- [Meht 97] Asha Mehrotra. GSM System Engineering. Mobile Communications Series. Artech House Publishers.1997.
- [MP 92] Michel Mouly, Marie-Bernadette Pautet. GSM Systems for Mobile Communications, Telecom Publishing, 1992.
- [PK 02] Kaveh Pahlavan and Prashant Krishnamurthy. Principles of Wireless Networks. Prentice Hall Communications Engineering and Emerging Technologies Series. 2002.
- [Stallings 02] William Stallings. Wireless Communications and Networks. *Prentice Hall*. ISBN 0-13-040864-6, 2002.