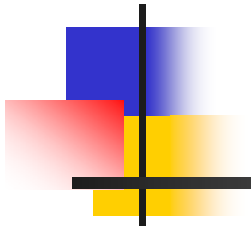
Wireless and Mobile Network Architecture



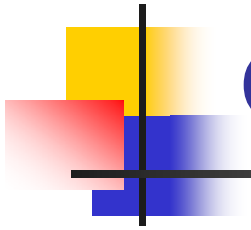
Chapter 6: GSM System Overview

Prof. **Yuh-Shyan Chen**

Department of Computer Science and Information Engineering

National Taipei University

Nov. 2006

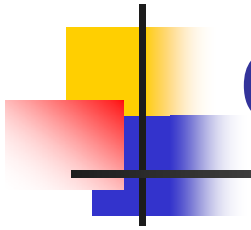


Outline

- Introduction
- GSM Architecture
- Location Tracking and Call Setup
- Security
- Data Services
- Unstructured Supplementary Service Data
- Summary

Introduction

- Global System for Mobile Communications (GSM)
  - A digital wireless network standard.
  - European telecommunications operators and manufactures.
- The basic requirements of GSM
  - Services
    - Providing service protability (roaming), ex: mobile phones
  - Quality of services and security
    - Quality for voice telephony, information encryption



Cont.

- Radio frequency utilization
  - Coexisting with the earlier systems in the same frequency band.
- Network
  - For switching and mobility management.
- Cost
  - Limiting the cost in MSs.

Fig 9.1 GSM Architecture

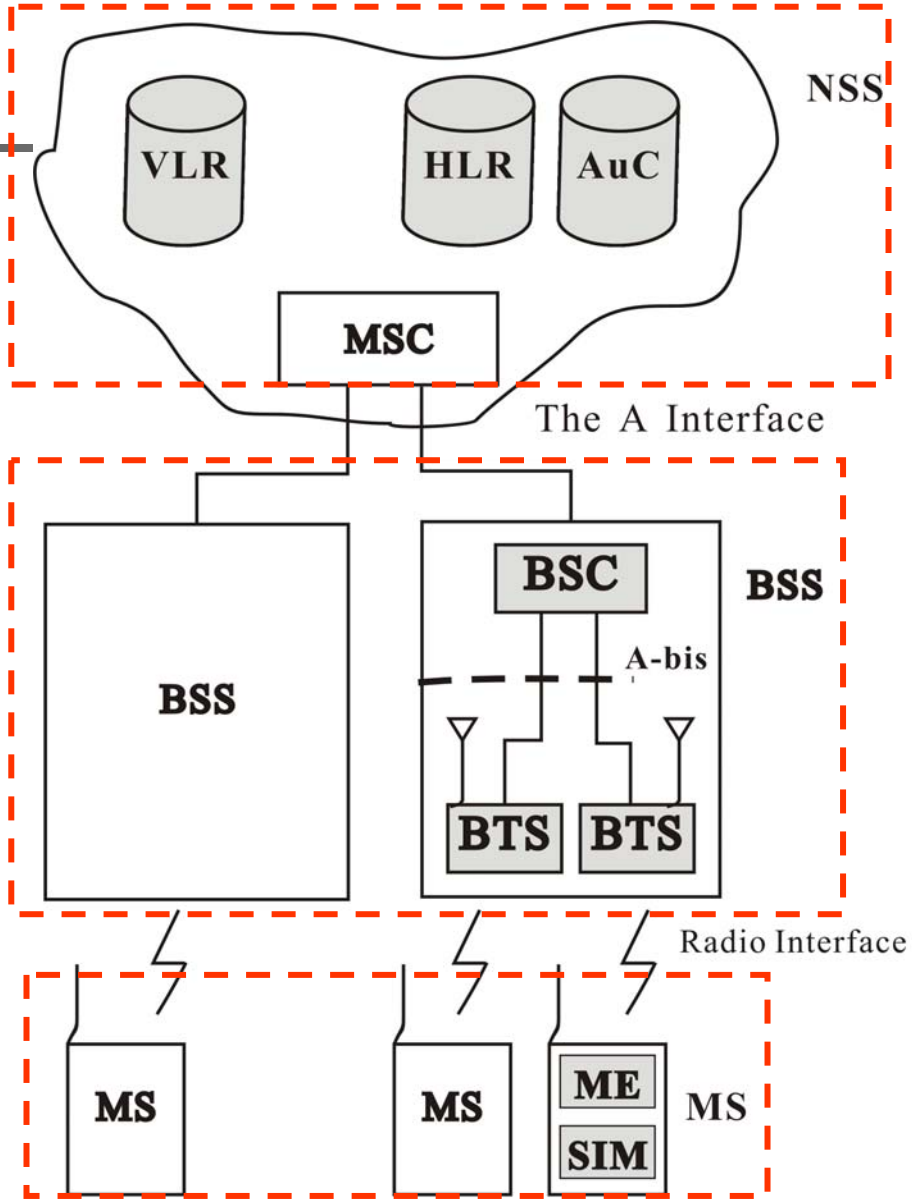
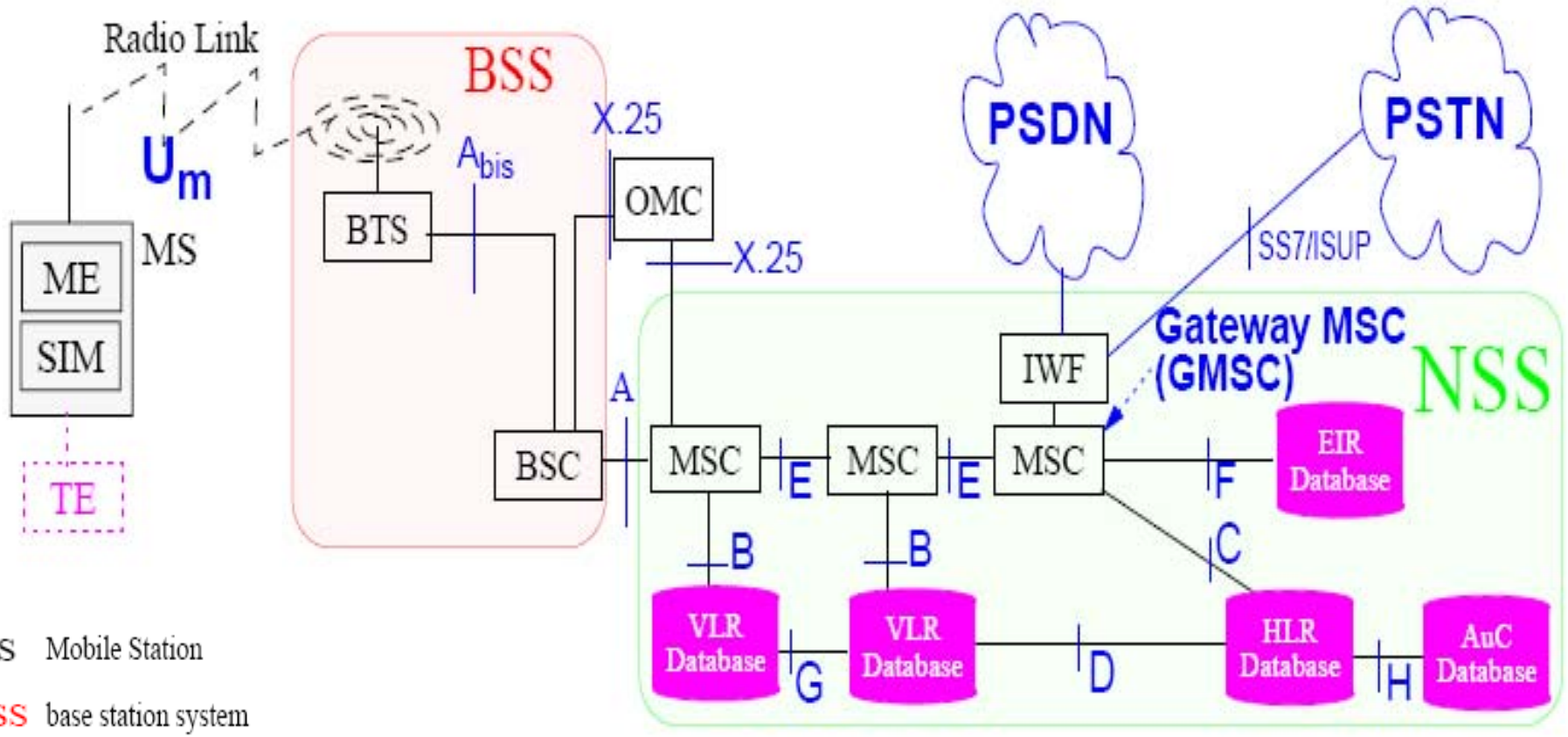


Fig 9.1 GSM Architecture



MS Mobile Station

BSS base station system

NSS network and switching subsystem

9.1 GSM Architecture

- **Mobile Station** (MS)
  - The MS consists of two parts:
    - **Subscriber identity module (SIM)**
      - Containing the subscriber-related information.
      - The SIM is protected by a **persional identity number (PIN)**
      - **PIN unblocking key (PUK)**
        - To unlock the SIM
    - **Mobile equipment (ME)**
      - Containing the noncustomer-related hardware and software specific to the radio interface.

Cont.

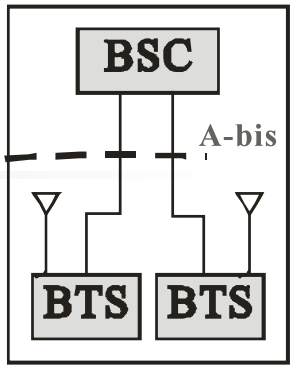
- This SIM-ME design supports portability.
  - The ME is the property of the subscriber.
  - The SIM is the property of the service provider.
  - SIMs may be attached to MEs with different characteristics.
    - The characteristic indication of the the ME is called *classmark*.
  - The ME and SIM are called the **mobile terminal (MT)**.
- In a broader definition, the MS includes a third part called **terminal equipment (TE)**, which can be a PDA or PC connected to the ME.

Fig 9.2 SIM data retrieved from a software tool

SIM Toolkit (Chapter 12)

```
                    GSM SIM SCAN v1.00 by xxxx 1998
*************************************************************
                          Answer To Reset Info
-------------------------------------------------------------
ATR => 3B 82 00 55 19
TS = 3B    Direct convention
T0 = 82    TD = 00
F = 372    Baud rate = Clock * D/F [Hz]
D = 1
I = 50 mA Maximum programming current
P = 5 V    Programming voltage
N = 0      Extra guardtime (Stop bit = 2+N)
T = 0      Protocol type
The Historical Characters: 55 19
*************************************************************
                  Smart Card CLASSES and INSTRUCTIONS Info
-------------------------------------------------------------
CLA:INS  A0:04 => GSM: Invalidate
   P1:P2:P3 00 00 00
   9400  No EF selected
   9804  Access condition not fulfilled!
   CHV (PIN) UNBLOCK-Verification failed
CLA:INS  A0:28 => GSM: Enable  CHV (PIN)
   P1:P2:P3 00 01 08
   6B00  Incorrect parameter P1 or/and P2
   6708  Incorrect parameter P3
CLA:INS  A0:FA => GSM: Sleep
   P1:P2:P3 00 00 00       9000  OK
*************************************************************
                              Files  Info
-------------------------------------------------------------
3F00:              *** GSM Master File ***
-------------------------------------------------------------
Response: 00 00 00 12 3F 00 01 00 00 44 44 ...
-----------------------------------
Allocated memory  :0012      CHV1(PIN1)          :Disabled
File ID           :3F00      CHV1(PIN1) Status   :3 Tries left
Type of file      :MF        CHV1(PUK1) Status   :10 Tries left
Number of DF      :3         CHV2(PIN2) Status   :3 Tries left
Number of EF      :5         CHV2(PUK2) Status   :10 Tries left
Number of CHV's   :4         ...
3F00:7F20:6F07:  IMSI
-------------------------------------------------------------
Response: 00 00 ...
-----------------------------------
File ID           :6F07              Type of file   :EF
Structure of File :Transparent       File Size      :0009
Read Access       :CHV (PIN) 1       Write Access   :CHV (PIN) 4
Increase Access   :CHV (PIN) 15      Rehabilitate   :CHV (PIN) 1
Invalidate        :CHV (PIN) 4       File Status    :Not Invalidated
...
```

Cont.



- **Base Station System** (BSS)
  - The BSS consists of two parts:
    - **Base transceiver station (BTS)**
      - Containing transmitter, receiver, and signaling equipment specific to the radio interface.
      - **Transcoder / rate adapter unit (TRAU)** carries out GSM-specific speech encoding/decoding and rate adaption in data transmission.
    - **Base station controller (BSC)**
      - Providing switching functions connect to an MSC.
      - Supporting radio channel allocation/release and handoff management.
    - The BSC communicates with the BTSs using ISDN protocols via the A-*bis* interface.

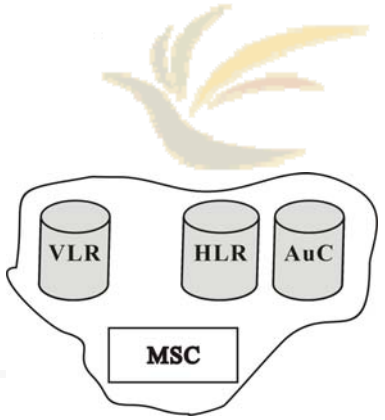
Fig 9.3 & 9.4 GSM BTS and BSC

BTS

BSC

(Nokia - model DE34)

Cont.



- **Network and Switching Subsystem (NSS)**
  - The NSS supports the switching functions, subscriber profiles, and mobility management.
  - The basic switching function is performed by the MSC.
  - The current location of an MS is usually maintained by the **HLR** and **VLR**.
  - The **AuC** is used in the security data management.
  - An incoming call is routed to an MSC, is called the gateway MSC (GMSC), unless the fixed network is able to interrogate the HLR directly.
    - The details will be described in Chapter 11.

Cont.

- Radio Interface
  - The radio link uses both FDMA and TDMA technologies.
  - The 900 MHz frequency bands for the GSM downlink signal and uplink signal are 935-960 MHz and 890-915 MHz.
    - The frequency band is divided into 124 pairs of frequency duplex channels.
  - Saving the power consumption of the MS
    - *Discontinuous transmission*
    - *Discontinuous reception*

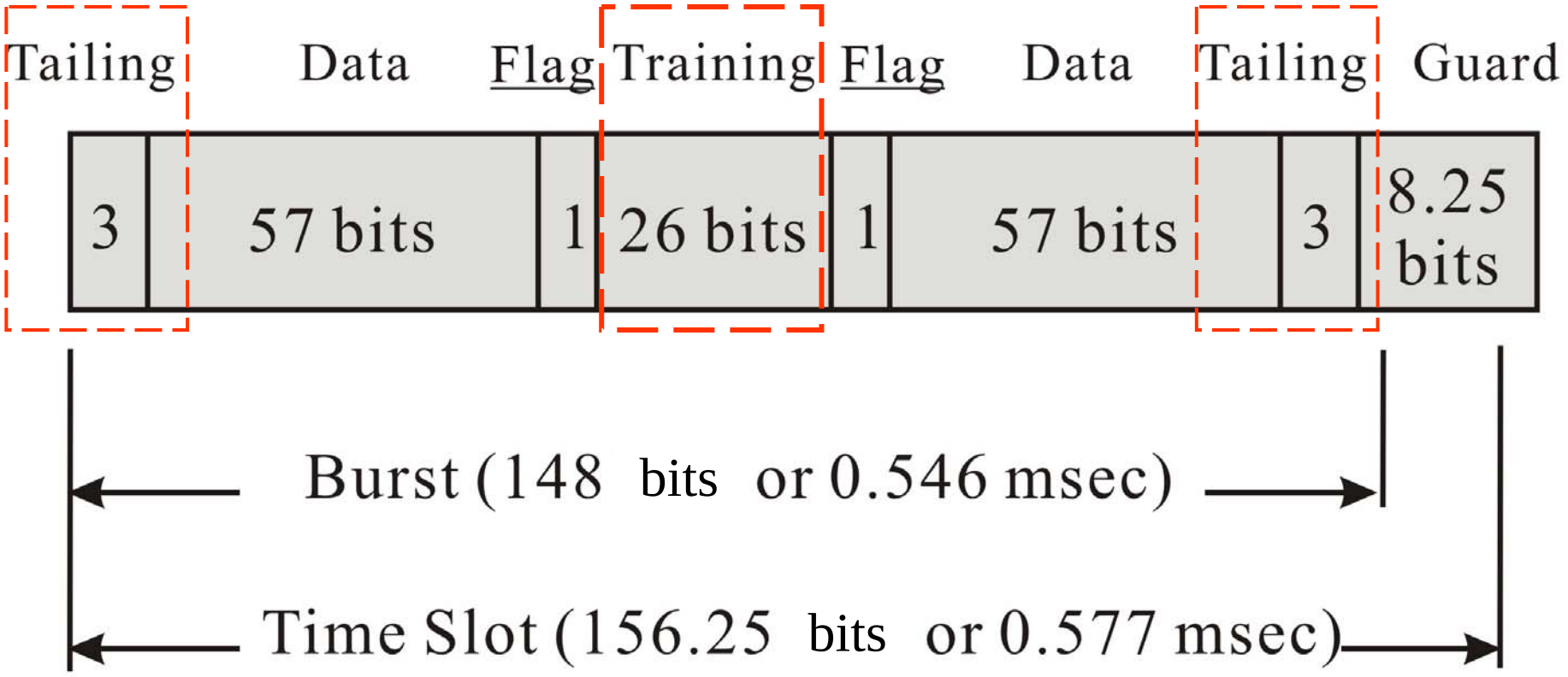
Power saving

- Note that, for a given distance, less power is required to transmit signal over a lower frequency
- To save MS power, uplink frequencies in mobile systems are always the lower band of frequencies.

Cont.

- The GSM frame
  - A GSM frame in a frequency channel is 4.615 msec.
  - The frame is divided into eight bursts (time slots) of length 0.577 msec.
  - By a delay of three time slots prevents an MS from transimtting and receiving at the same time.
    - *Timeing advance value* is calculated by the BSS and signaled to the MS twice per second.

Fig 9.5 GSM burst structure



Cont.

- The burst begins with three head bits, and ends with three tail bits, all of which are logical zeros.
- Two groups of data bits are separated by an equalizer training sequence of 26 bits.
- Each data group consists of 57 information bits and one flag.
  - The flag indicates whether the information bits are for user speech/data or signaling.

Cont.

- Two types of logical channels
  - **Traffic channels (TCHs)**
    - Carry user information (speech or data)
      - Full-rate TCH (TCH/F)
        - Enhanced full-rate (EFR) speech coders
        - Provides transmission speed of 13 Kbps for speech or 9.6, 4.8, 2.4 Kbps for data
      - Half-rate TCH (TCH/F)
        - Allows transmissions of 6.5 Kbps speech, or 4.8 or 2.4 Kbps of data
  - **Control channels (CCHs)**
    - Carry signaling information
      - Common control channels (CCCHs)
      - Dedicated control channels
      - Broadcast channels (BCHs)

Cont.

- **Common control channels** (CCCHs)
  - **Downlink**
    - Paging channel (PCH)
      - Used by the network to page the destination MS in call termination.
    - Access grant channel (AGCH)
      - Used by the network to indicate radio link allocation upon prime access of an MS.
  - **Uplink**
    - Random access channel (RACH)
      - Used by the MSs for initial access to the network.

Cont.

- **Dedicated control channels**
  - **Downlink and uplink**
    - Standalone dedicated control channel (SDCCH)
      - Used only for signaling and short messages.
    - Slow associated control channel (SACCH)
      - Transmission of power and time alignment control information reports from the MS.
    - Fast associated control channel (FACCH)
      - Used for time-critical signaling, such as call-establishing progress, authentication of subscriber, or handoff.
  - **Downlink**
    - Cell broadcast channel (CBCH)
      - Carries only the short message service cell broadcast messages.

Cont.

- Broadcast channels (BCHs)
  - Frequency correction channel (**FCCH**) and synchronization channel (**SCH**)
    - Carry synchronization information from the BSS to the MS.
  - Broadcast control channel (**BCCH**)
    - Provides system information to support cell selection and location registration procedures in an MS.

Common control channels (CCCHs)	Paging channel (**PCH**)	Used by the network to page the destination MS in call termination.
	Access grant channel (**AGCH**)	Used by the network to indicate radio link allocation upon prime access of an MS.
	Random access channel (**RACH**)	Used by the MSs for initial access to the network.
Dedicated control channels	Standalone dedicated control channel (**SDCCH**)	Used only for signaling and short messages.
	Slow associated control channel (**SACCH**)	Transmission of power and time alignment control information reports from the MS.
	Fast associated control channel (**FACCH**)	Used for time-critical signaling, such as call-establishing progress, authentication of subscriber, or handoff.
	Cell broadcast channel (**CBCH**)	Carries only the short message service cell broadcast messages.
Broadcast channels (BCHs)	Frequency correction channel (**FCCH**) and synchronization channel (**SCH**)	Carry synchronization information from the BSS to the MS.
	Broadcast control channel (**BCCH**)	Provides system information to support cell selection and location registration procedures in an MS.

Fig 9.6 GSM call origination

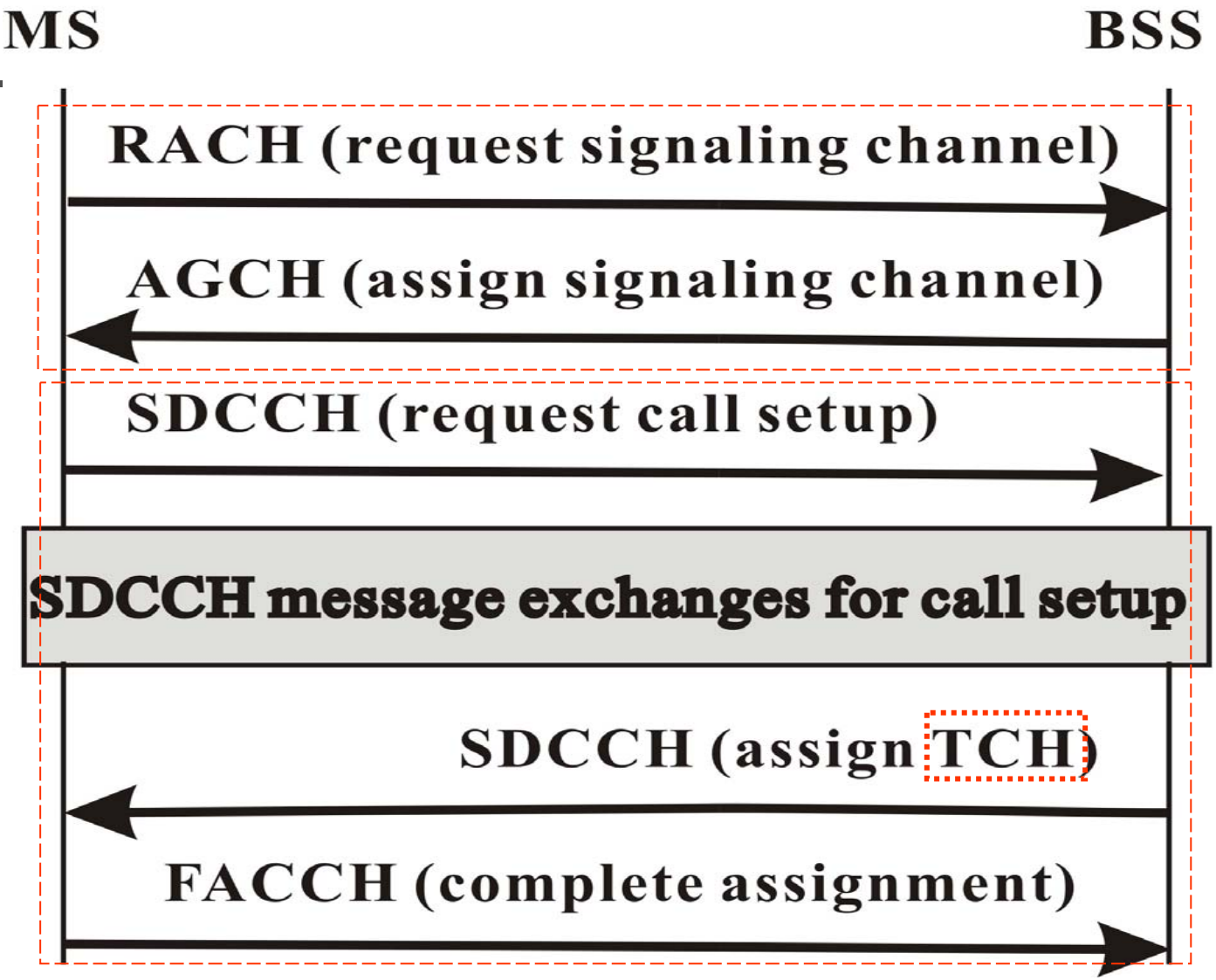
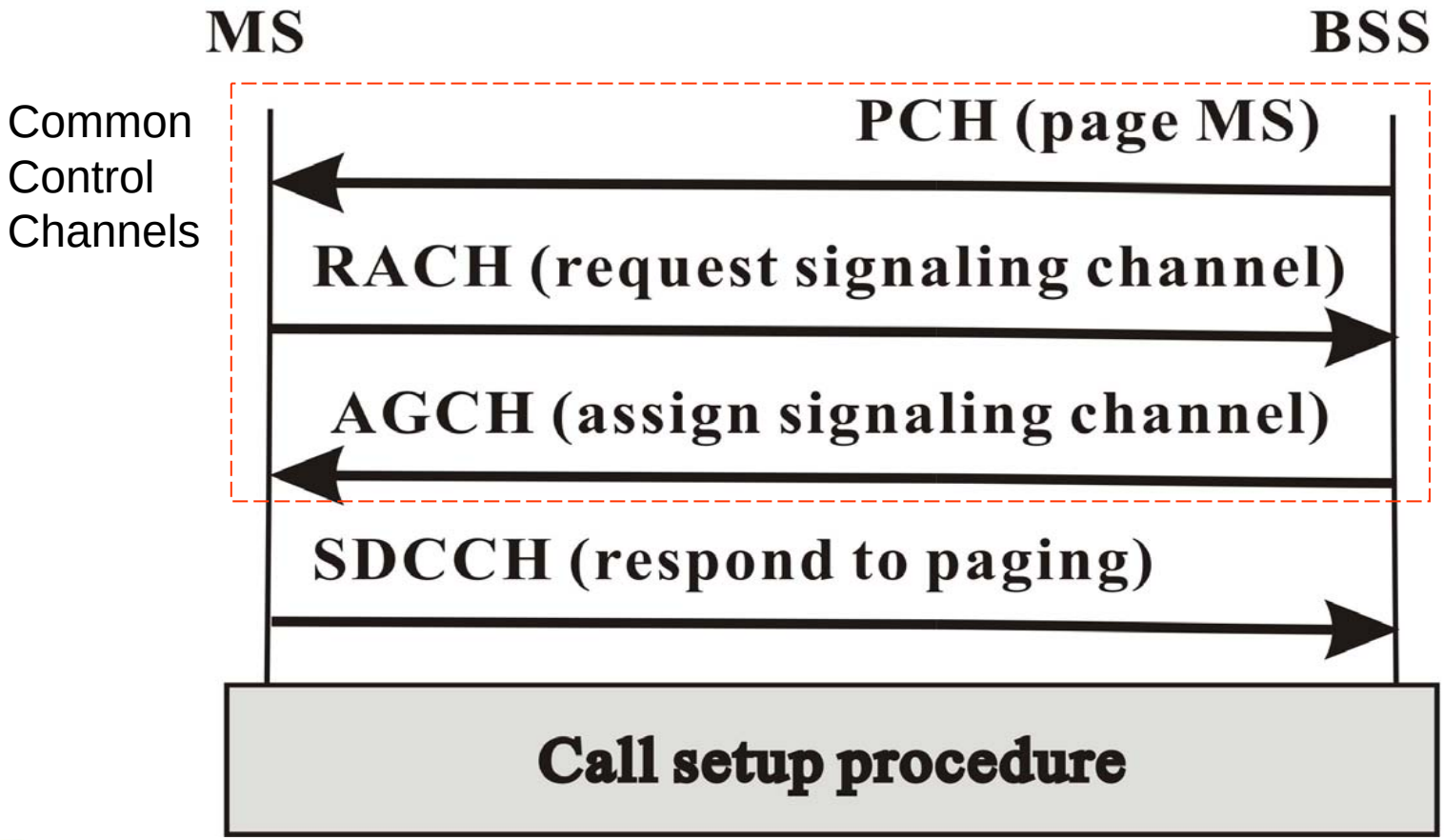


Fig 9.7 GSM call termination



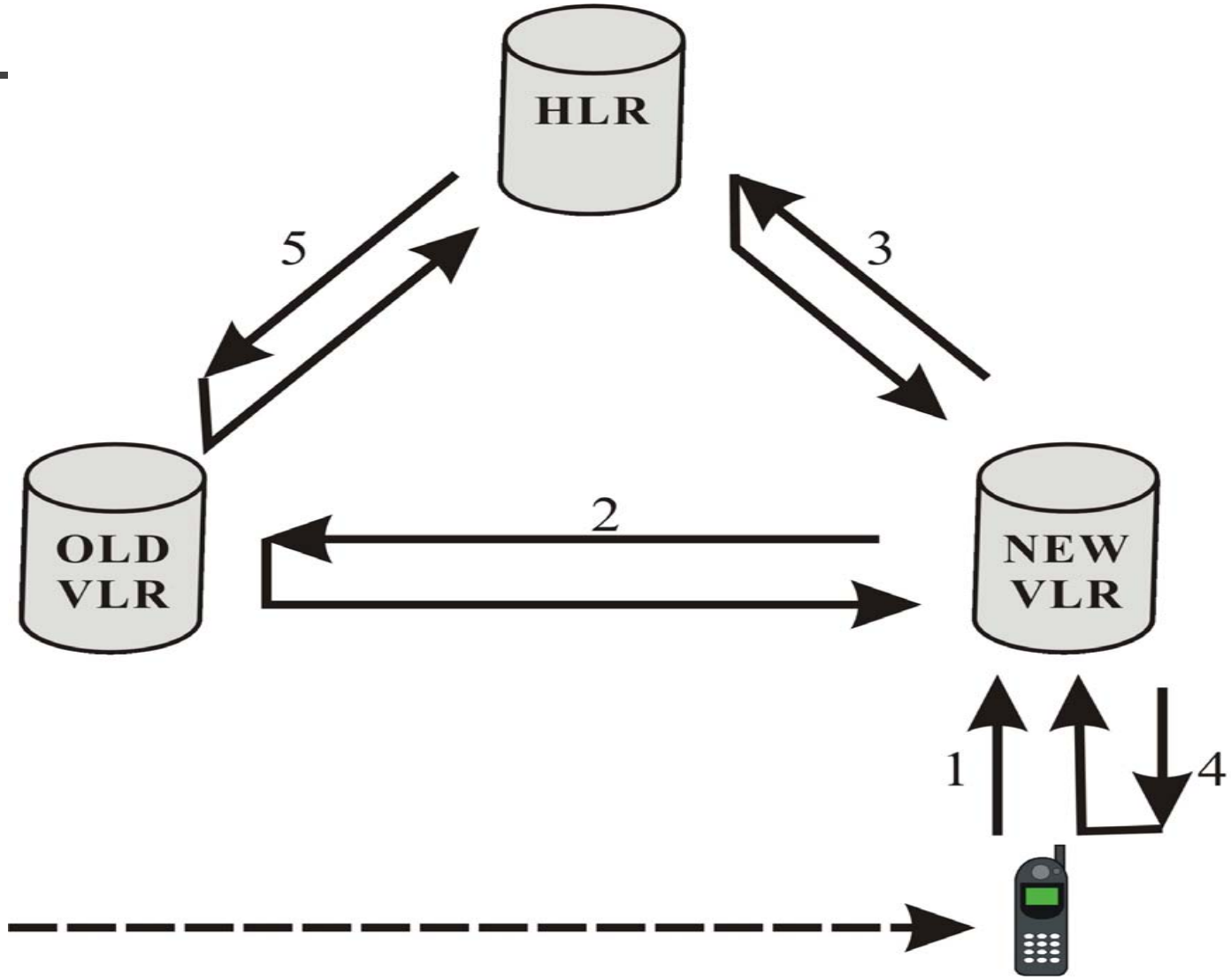
9.2 Location Tracking and Call Setup

- The current location of an MS is maintained by a two-level hierarchical strategy with the HLR and the VLR.
- For example, the registration process of the MS moving from one VLR to another VLR is illustrated in Figure 9.8.

Fig 9.8 The MS registration process

- **Step 1.** The MS periodically listens to the BCCH broadcast from the BSS.
  - If the MS enters a new location area, it sends a registration message (SDCCH) to the new VLR.
- **Step 2.** The new VLR communicates with the old VLR to find the HLR of the MS. (chapter 11)

Fig 9.8 The MS registration process



Cont.

- **Step 3.** The new VLR sends a registration message to the HLR.
  - If the registration request is accepted, the HLR provides the new VLR with all information for call handling.
- **Step 4.** The new VLR informs the MS of the successful registration.
- **Step 5.** The HLR sends a deregistration message to the old VLR.

Fig 9.9 The mobile call termination (delivery) procedure

- **Step 1.** When the MSISDN is dialed, the call is forwarded to the GMSC, a switch that has the capability to interrogate the HLR for routing information.
  - The HLR requests the VLR of the MS to provide the routable address, called a **mobile station roaming number (MSRN).**
- **Step 2.** The VLR returns the MSRN to the GMSC through the HLR.
- **Step 3.** The GMSC uses the MSRN to route the call to the MS through the visited MSC.

Fig 9.9 The mobile call termination (delivery) procedure

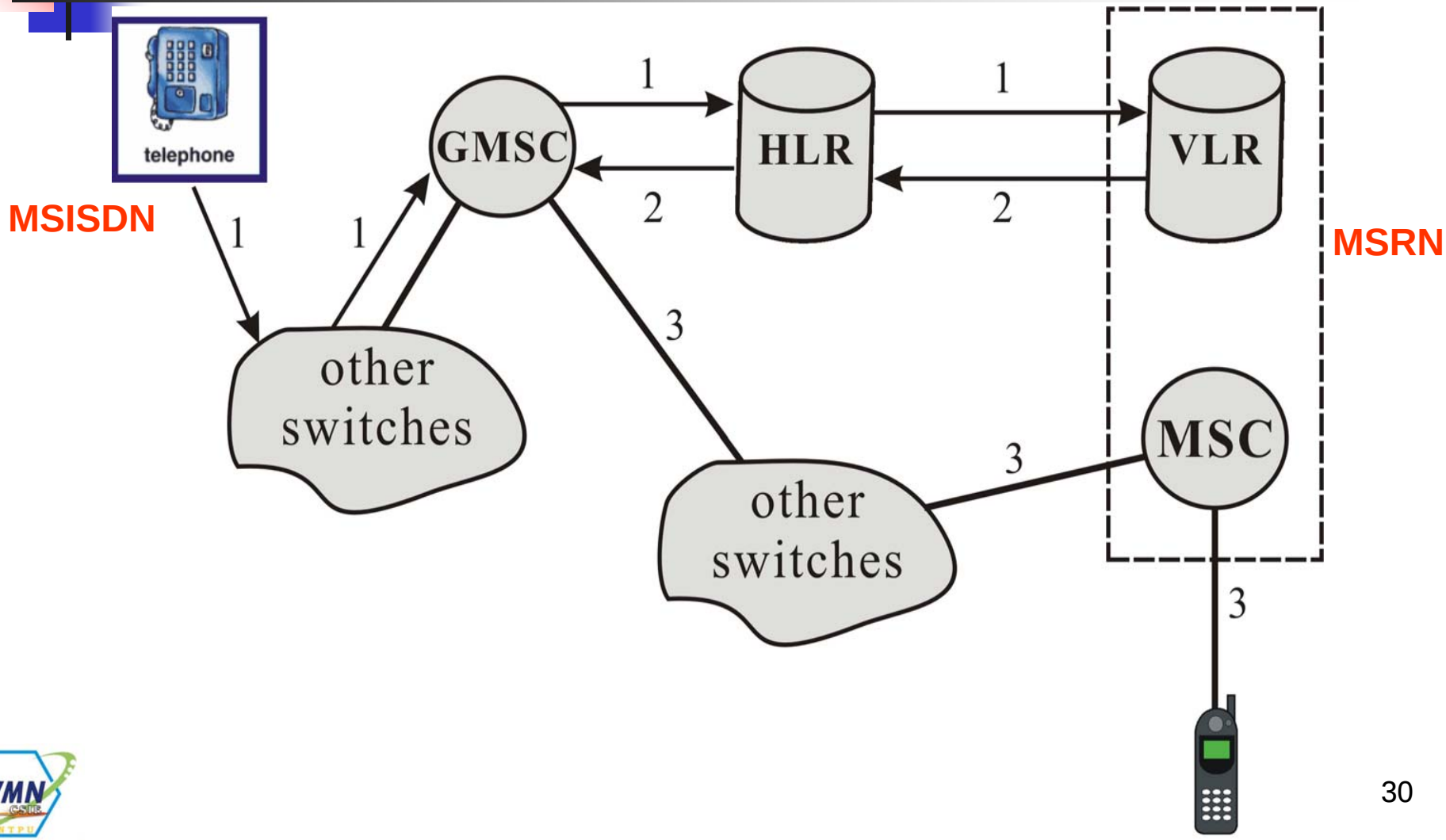
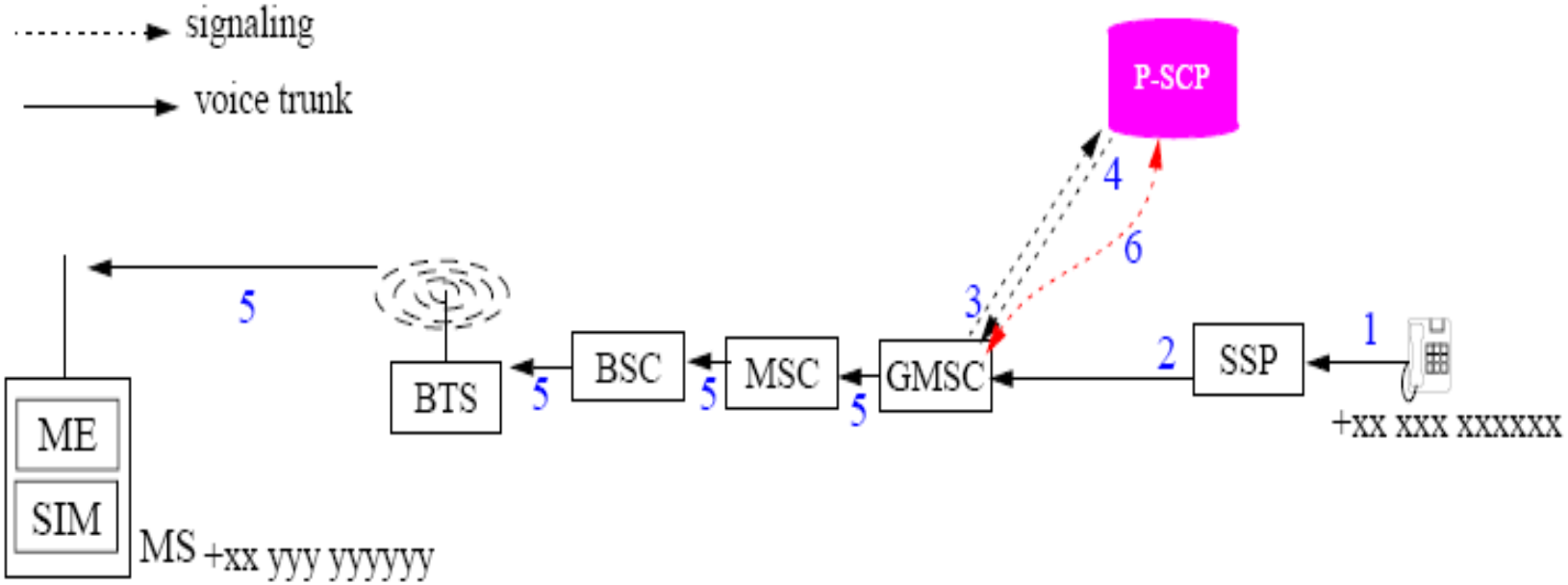


Fig 9.9 The mobile call termination (delivery) procedure



1. Caller dials prepaid mobile customer +xx yyy yyyyyy
2. Call forwarded to gateway GMSC
3. GMSC get a WIN call setup trigger, suspends call processing, sends message to P-SCP
4. P-SCP determines if mobile is allowed to receive this call, if so instructs GMSC to resume call setup procedure
5. GMSC connects the call
6. P-SCP monitors called party's balance and can terminate the call if there is no credit (just as per call origination case)

Cont.

- MS ISDN number (MSISDN) is part of the ISDN numbering plan defined in ITU-T Recommendation E.164.
  - The number points to the subscriber's record in the HLR.
- Different communication sessions that are distinguished by their *transcation identifiers* may be associated with an MS at the same time.
- Details of the information fields maintained in the HLR are described in Chapter 11.

9.3 Security

- Two aspects:
  - Authentication
    - Avoiding fraudulent access by a cloned MS.
    - Input: K_i, 128-bit random number (RAND)
    - Algorithm: A3 (depend on the GSM service provider)
    - Output: *Signed result* (SRES)
  - Encryption
    - Avoiding unauthorized listening.
    - Input: K_i, RAND, K_c, and TDMA frame number
    - Algorithm: A8, A5
    - Output: Cipher and decipher data

Fig 9.10 Authentication and encryption

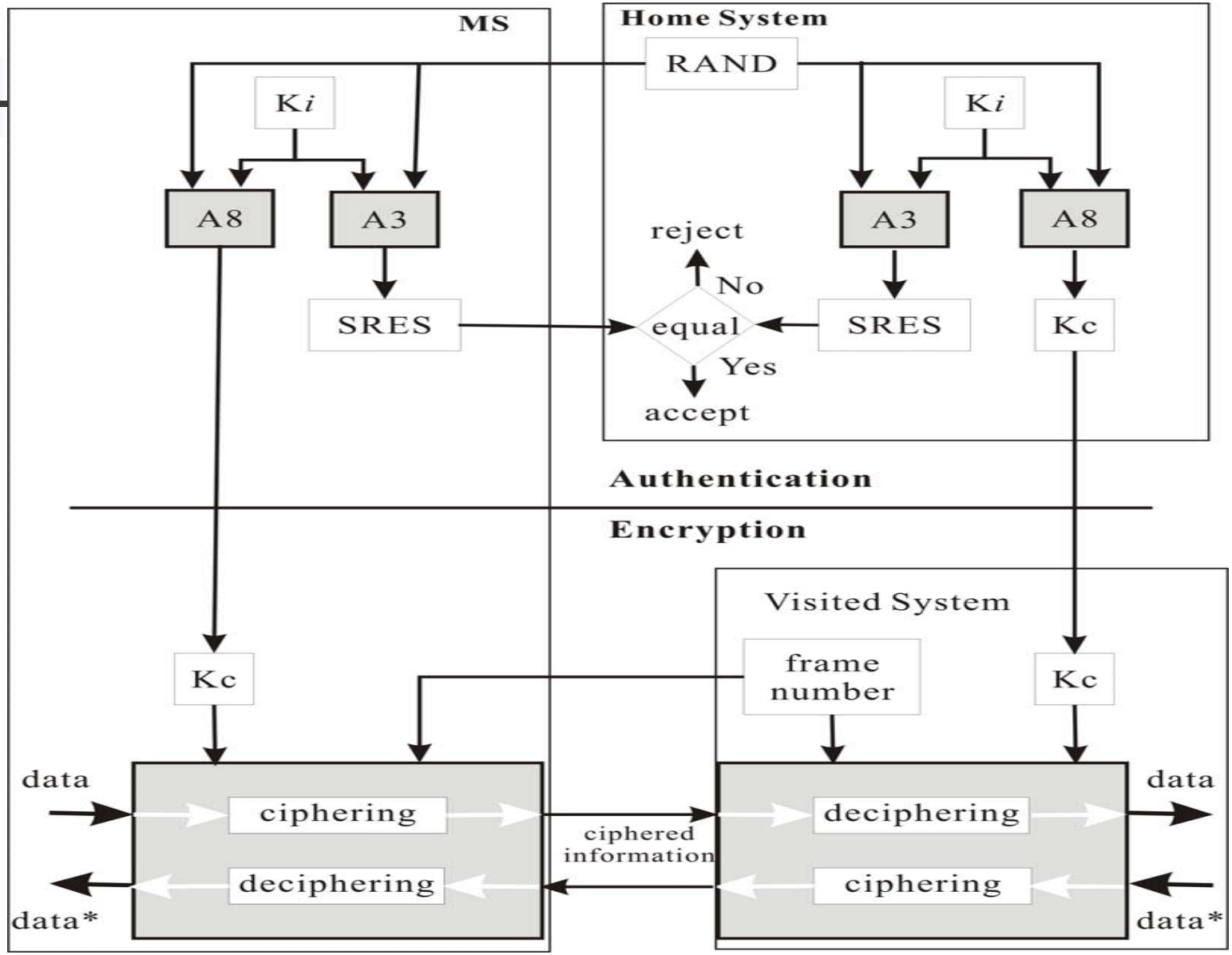
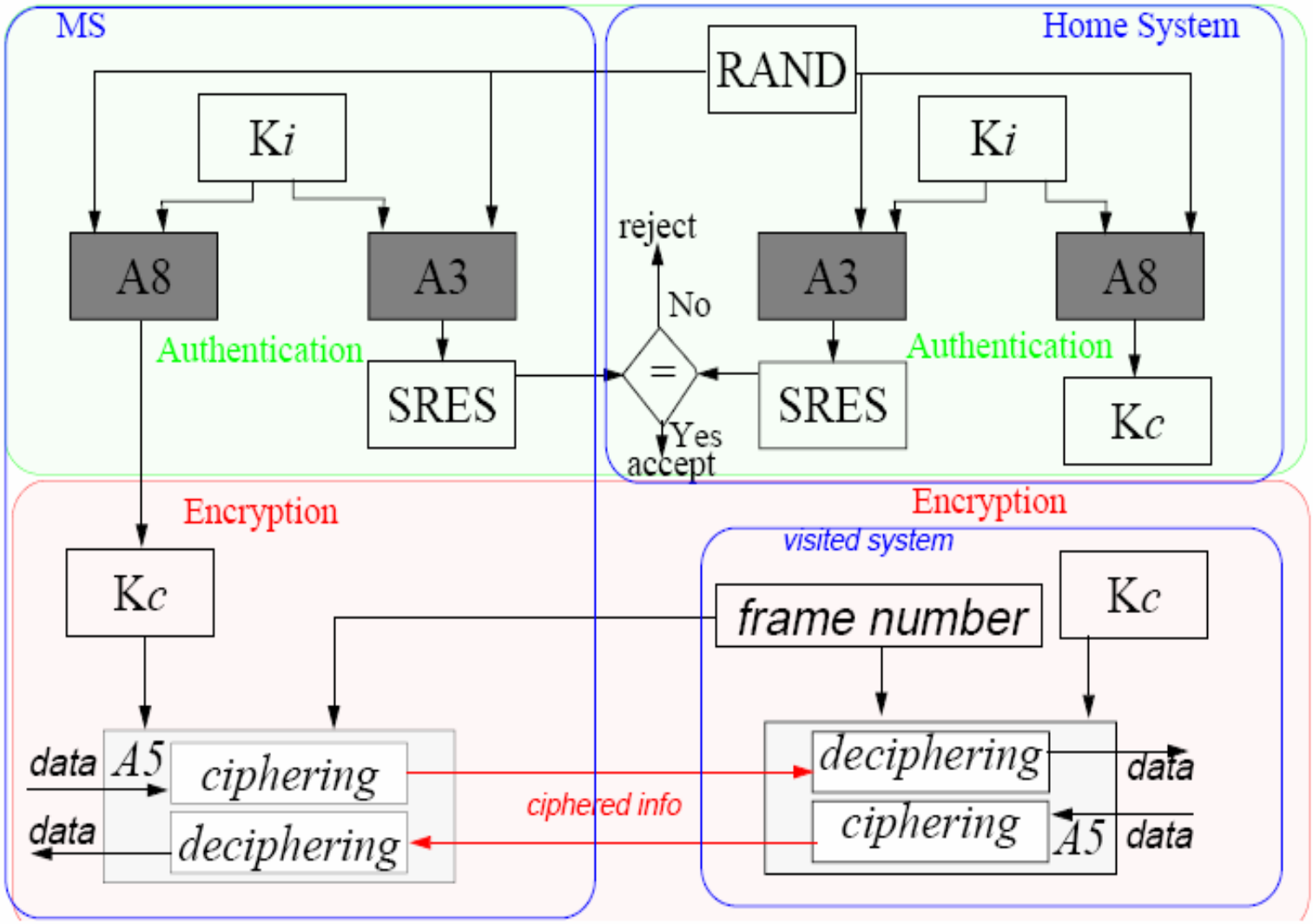
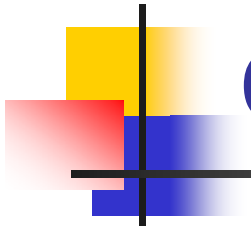


Fig 9.10 Authentication and encryption



9.4 Data Services

- GSM Phase 2 standard supports two data service groups (9.6Kbps)
  - Short message services
    - **Chapter 12**
  - Bearer services
    - **A circuit-switched connection**
      - The wireline circuit and radio channel resources are reserved even if the data are not transferred.



Cont.

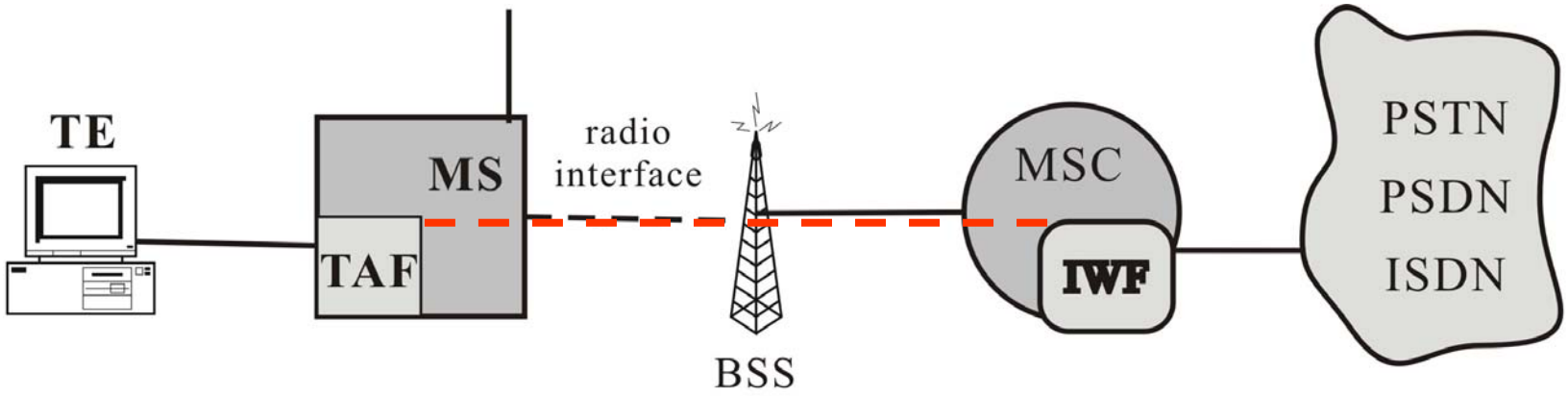
- GSM Phase 2+ standared (28.8Kbps or higher)
  - European Telecommunications Standard Institute (ETSI)
  - Support fast access to radio resources on demand and packet-switched transmission.
    - **High-Speed Circuit-Switched Data** (HSCSD)
    - **General Packet Radio Service** (GPRS)

9.4.1 HSCSD

- High-Speed Circuit-Switched Data (HSCSD)
  - Circuit-switched protocol
  - For high-speed file transfers and mobile video applications.
  - *Radio link protocol* (RLP)
    - Using multiple TDMA time slots (up to eight).
    - The protocol may not recover the frame errors.
    - The blocking rate of the system will be increased.

Fig 9.11 HSCSD architecture

- IWF supports adaption between GSM and the external networks.

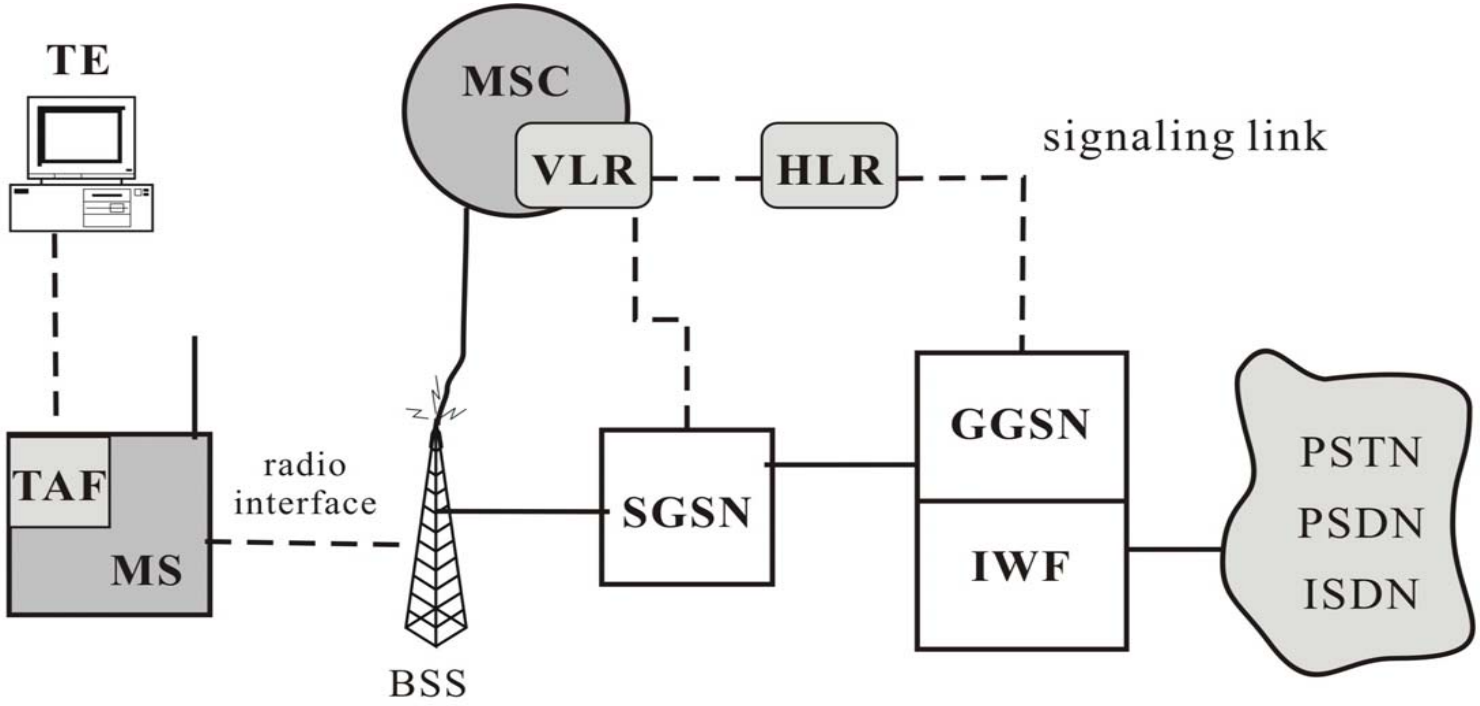


MSC: Mobile Switching Center
MS: Mobile Station (Handset)
BSS: Base Station Subsystem
TAF: Terminal Adaption Funtions
TE: Terminal Equipment
IWF: Interworking Functions
PSTN: Public Switched Telephone Network
PSDN: Public Switched Data Network

9.4.2 GPRS

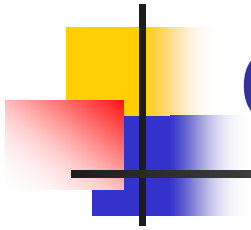
- General Packet Radio Service (GPRS)
  - Packet-switched protocol
  - For bursty data applications such as e-mail and WWW.
  - Two new entities
    - *Serving GPRS support node* (SGSN)
      - SGSN receives and transmits packets between the MSs and their counterparts in the *public-switched data network* (PSDN).
    - *Gateway GPRS support node* (GGSN)
      - Connectionless network protocols, such as internet protocol.
      - Connection-oriented protocols, such as X.25

Fig 9.12 GPRS architecture



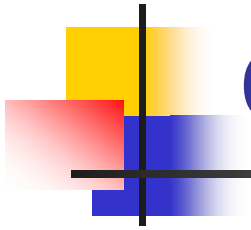
HLR: Home Location Register
VLR: Visitor Location Register
MSC: Mobile Switching Center
MS: Mobile Station (Handset)
BSS: Base Station Subsystem
TAF: Terminal Adaption Funtions

SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
TE: Terminal Equipment
IWF: Interworking Functions
PSTN: Public Switched Telephone Network
PSDN: Public Switched Data Network



Cont.

- SGSN and GGSN interact with the HLR and the VLR, to track the location of the MSs.
- GPRS needs to implement a *packet radio media access control* (MAC) for packet switching to guarantee fast call setup procedure and low-bit error rate. (Chapter 18)



Cont.

- Difference between HSCSD and GPRS
  - GPRS
    - Supports up to 100 users with one to eight channels.
    - Supports broadcast and multisessions.
    - Requires an investment in new infrastructure.
  - HSCSD
    - Supports fewer users, where a user may utilize two to eight channels.
    - Supports point-to-point session.
    - Needs to address handoff issues.

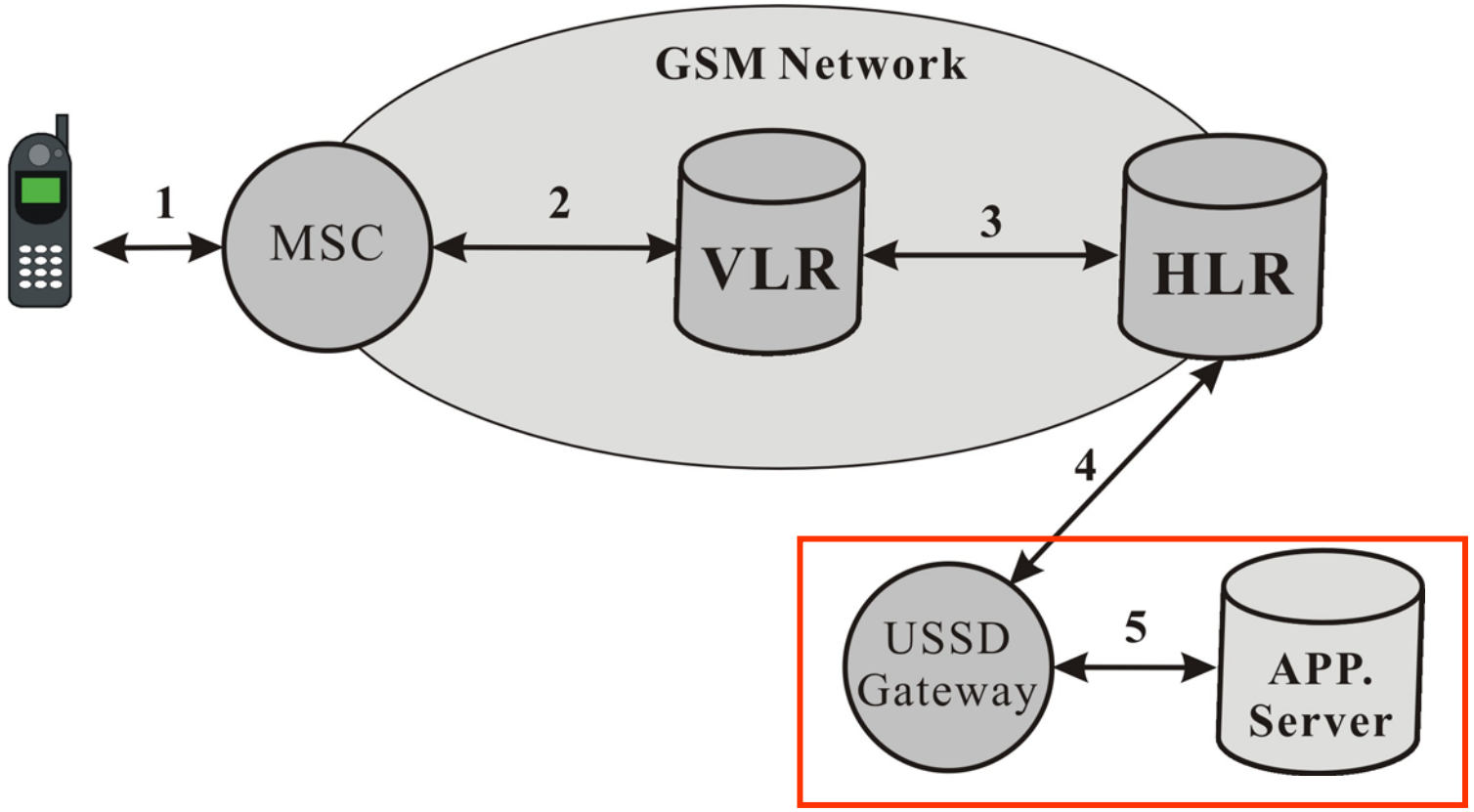
9.5 Unstructured Supplementary Service Data

- To support new service in old MSs, *unstructured supplementary service data* (USSD) was introduced.
  - USSD is used as a GSM transparent bearer for old MSs.
  - Chapter 19 will describe in detail.

Cont.

- A USSD string is a command code followed by several parameters that are separated by an asterisk (*) and ends with the pound symbol (#).
  - Ex: *159*5288128#
    - Specify command code 159
    - Phone number 528-8128

Fig 9.13 USSD architecture



Cont.

- If the USSD service node is an MSC, the USSD messages are exchanged through path (1).
- If the service node is a VLR (or HLR), the messages are exchanged through path (1)⇔(2) (or (1)⇔(2)⇔(3)).
- The HLR is expensive to modify, maintain, and test to handle additional services.
  - USSD gateway
    - Connecting to the application server.

9.6 Summary

- This chapter provides an overview of the GSM system.
  - GSM architecture
  - How the locations of the MSs are tracked.
  - How phone calls are delivered to those MSs in a GSM network.
  - The security and data service aspects of GSM.
- Details of the GSM network signaling will be discussed in subsequent chapters.