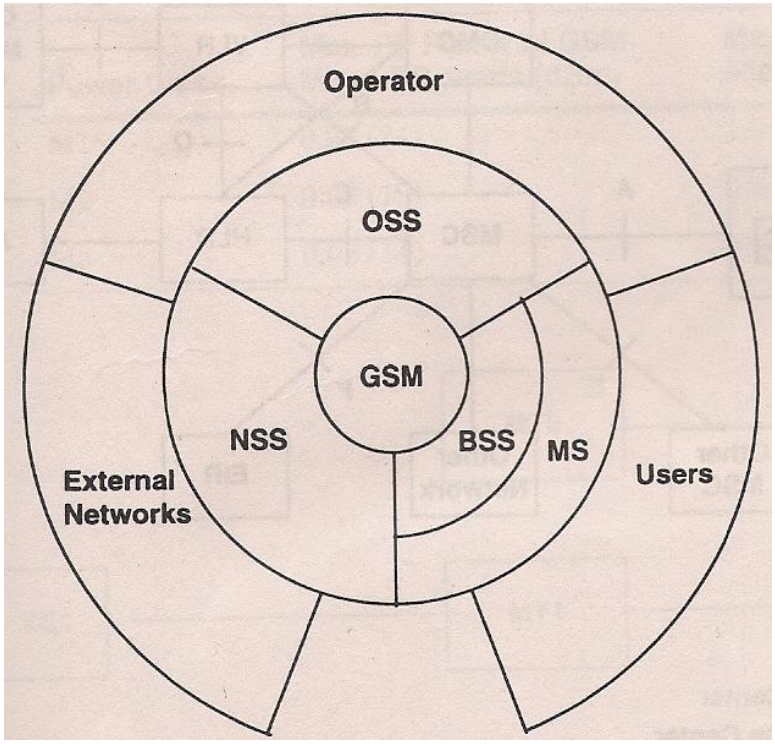
1.



The basic subsystems of the GSM architecture are:

- **BSS** (Base Station Subsystem)
- **NSS** (Network & Switching Subsystem)
- **OSS** (Operational Subsystem)
- **MS** (Mobile Station)

BSS

- Provides and manages transmission paths between the MSs & NSS
- Management of the radio interface between MSs & the rest of the GSM system
- Not in direct contact with the external networks

NSS

- managing communications & connecting MSs to the relevant networks or other MSs
- not in direct contact with the MSs

MS, BSS & NSS form the operational part of the GSM system

OSS

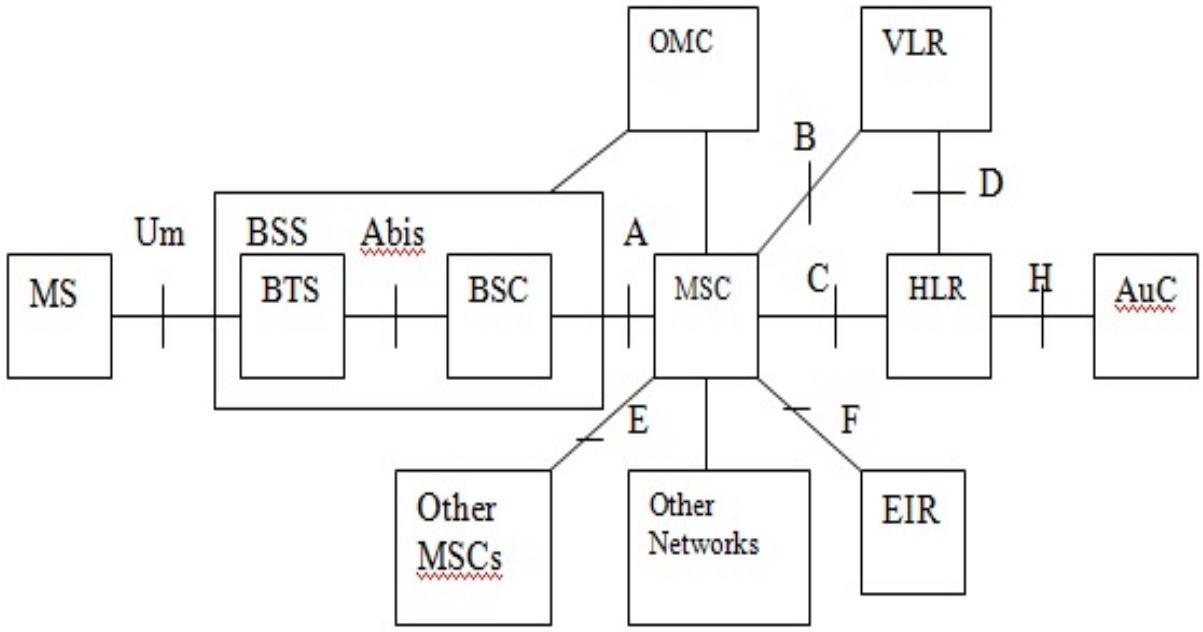
- provides means for a service provider to control & manage the GSM system

In the GSM, interaction between the subsystems can be grouped into two main parts:

- Operational
- Control

- Operational – External networks to / from NSS to / from BSS to / from MS to / from Subscriber
- Control – OSS to / from service provider (operator)

The figure shows the functional entities of the GSM & their logical interconnection



2.

- The general objectives of a GSM PLMN network with respect to services to a subscriber are:

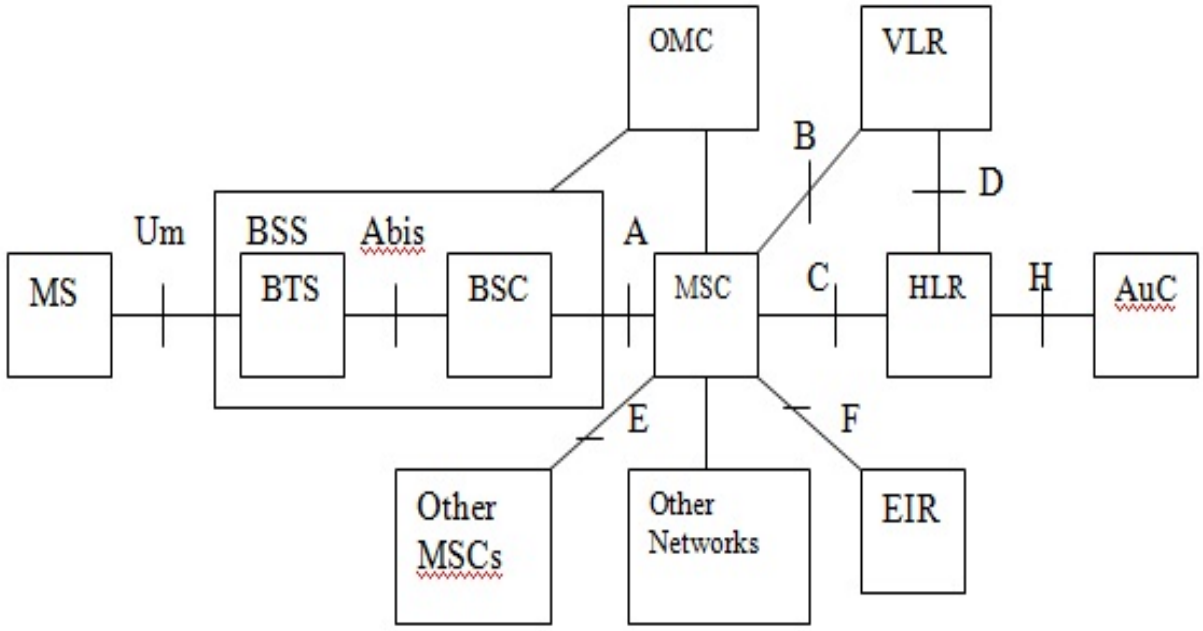
  To provide

  - the subscriber a wide range of services & facilities, (voice & non-voice), that are compatible with those offered by existing networks *[PSTN (Public Switched Telephone Network), ISDN (Integrated Services Digital Network)]*
  - certain services & facilities exclusive to mobile situations
  - access to the GSM network for a mobile subscriber in a country that operates the GSM system
  - facilities for automatic roaming, locating and updating of mobile subscribers
  - service to a wide range of MS's, including vehicle-mounted stations, portable stations, & handheld stations
  - for the efficient use of the frequency spectrum
  - To allow for a low cost infrastructure & terminal & to keep cost of service low

  The basic telecommunication services provided by the GSM PLMN are divided into 3 main groups :

  - Bearer Services
  - Teleservices
  - Supplementary Services

3.



GSM Interfaces

- The Radio Interface (MS to BTS)
- A_{bis} Interface (BTS to BSC)
- A Interface (BSC to MSC)

The Radio Interface (MS to BTS)

- Also called the U_m Radio Interface
- **Physical layer**

  --transmission of bit streams on the air interface

  -- GSM Recommendation 05 series

- **Data link layer**

  --multiplexing, error detection and correction, flow control, and segmentation to allow for long messages on the upper layers

  -- GSM Recommendation 04.05 and 04.06

- Uses the Link Access Protocol on D_m channel ($LAPD_m$)
- This protocol is based on the ISDN Link Access Protocol on the D channel (LAPD)

The following logical channels are supported:

- **Speech Traffic Channels (TCH)**
  - Full-rate TCH (TCH/F)
  - Half-rate TCH (TCH/H)
- **Broadcast Channels (BCCH)**
  - Frequency Correction Channel (FCCH)
  - Synchronization Channel (SCH)
  - Broadcast Control Channel (BCCH)
- **Common Control Channels (CCCH)**
  - Paging Channel (PCH)
  - Random Access Channel (RACH)
  - Access Grant Channel (AGCH)
- **Cell Broadcast Channel (CBCH)**
  - CBCH uses the same physical channel as the DCCH
- **Dedicated Control Channels (DCCH)**
  - Slow Associated Control Channel (SACCH)
  - Stand-Alone Dedicated Control Channel (SDCCH)
  - Fast Associated Control Channel (FACCH)

- **Radio Resource layer**

--manages the dialog between the MS and BSS concerning the management of the radio connection

- **Mobility management layer**

--location update, authentication, and encryption management

- **Connection Management layer**

--call control entity controls end-to-end call establishment and management

--supplementary service entity supports the management of supplementary services

The A_{bis} Interface (BTS to BSC)

- The interconnection between BTS & BSC
- Primary functions carried out by this interface are
    - Traffic Channel Transmission
    - Terrestrial Channel Management
    - Radio Channel Management
- Supports two types of communication links
    - **Traffic channel** at 64kbps carrying speech or user data
    - **Signaling channels** at 16kbps carrying information for BSC-BTS and BSC-MSC signalling
- There are two types of messages handled by the traffic management part of the signaling interface:
    - **Transparent** (between the MS & BSC-MSC & do not require analysis by the BTS)
    - **Nontransparen**t (do require analysis by the BTS)

The A Interface (BSC to MSC)

- The interconnection between BSS & MSC
- Signaling transport uses
    - **Message Transfer Part (MTP)**

-- Error free transport

- **Signaling Connection Control Part (SCCP)**

-- Logical Connection

- Two types of application part :
    - **BSS Application Part (BSSAP)**

--**Direct Transfer Application Part (DTAP)-** transfer layer3 messages between the MS and the MSC without BSC involvement

--**BSS Management Application Part (BSSMAP)**

--responsible for all aspects of radio resource handling at the BSS.

- **BSS Operation & Maintenance Application Part (BSSOMAP)**

-- supports all the operation and maintenance communications of BSS

Interfaces between other GSM Entities

- Information transfer between GSM PLMN entities uses the MAP
- The MAP contains :
  - Uses the service of the Transaction Capabilities Application Part (TCAP) of SS7
  - Employs the SCCP to offer the necessary signaling functions
- The major procedures supported by MAP are :
  - Location Registration and Cancellation
  - Handover procedures
  - Handling supplementary services
  - Retrieval of subscriber parameters during call setup
  - Authentication procedures

5.

GSM uses 5 different types of bursts :

1. Normal Burst
2. Synchronization Burst
3. Frequency Correction Burst
4. Access Burst
5. Dummy Burst

Normal Burst:

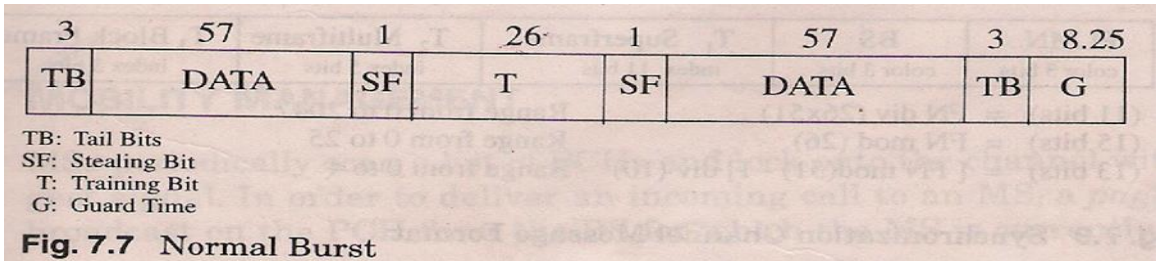


Fig. 7.7 Normal Burst

- It is used to carry information on TCH,CCH except for RACH, SCH &FCCH.
- This burst contains 156.25 bits
- The encrypted bits are 57 bits of data or speech
- 1 bit of “stealing Flag” to indicate whether the burst was stolen for FCCH signaling or not
- The training sequence T is to create a channel model
- The tail bits always equal (0,0,0) and are used to provide start and stop bit patterns
- The guard period is empty space and is used to prevent overlap between adjacent time slots during transmission

Synchronization Bursts:

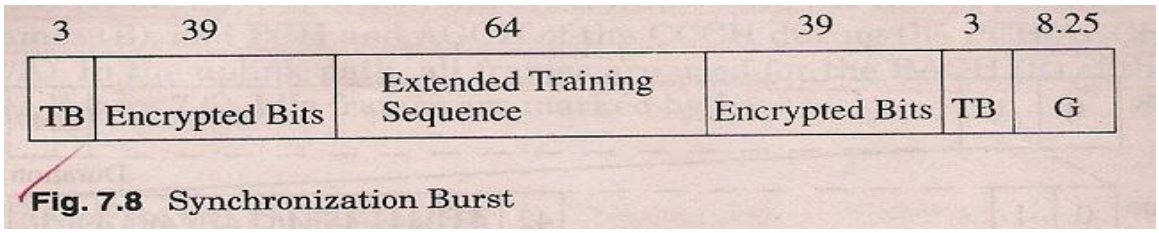


Fig. 7.8 Synchronization Burst

- It is used for time synchronization of the mobile. This burst contains a long synchronization sequence of 64 bits
- The encrypted 78 bits are used to carry information of the TDMA frame number along with the BTS identification code (BSIC)
- The TDMA frame is broadcast over an SCH to protect user information against eavesdropping, this is done by ciphering the information before transmitting
- The algorithm uses TDMA frame number as an important parameter for calculating the ciphering key.
- By knowing the TDMA frame number, the MS will know what type of logical channel is being transmitted on the CCH time slot 0.
- BSIC is also used by MS to check the identity of BTS

Frequency Correction Channel Bursts

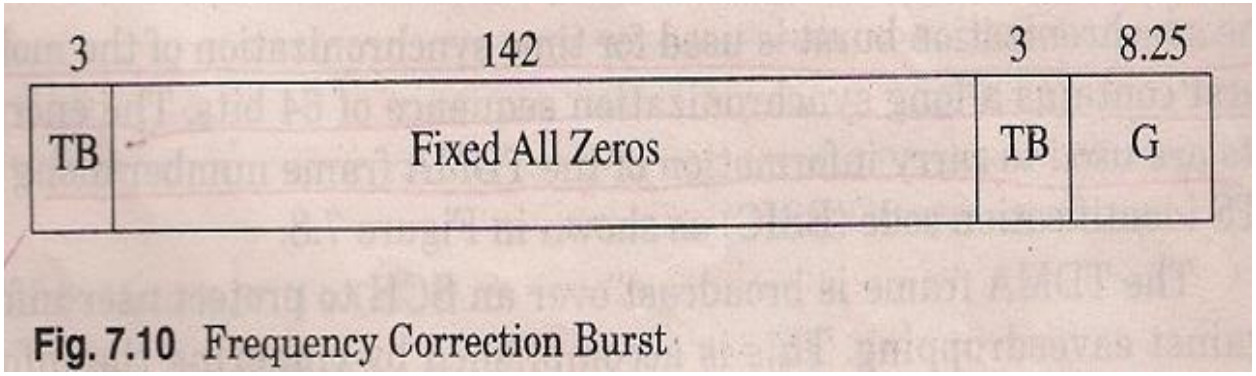


Fig. 7.10 Frequency Correction Burst

- This burst is used for frequency synchronization of the MS
- The fixed input bits are all zeros

Access Burst:

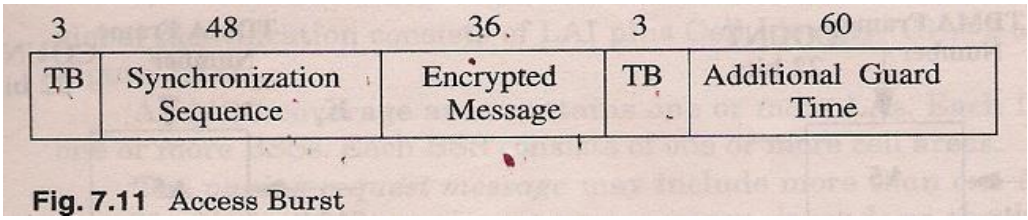


Fig. 7.11 Access Burst

- This is used for random access
- has a longer guard period to protect for burst transmission from an MS that does not know the timing advance when it first accesses the system

Dummy Bursts:

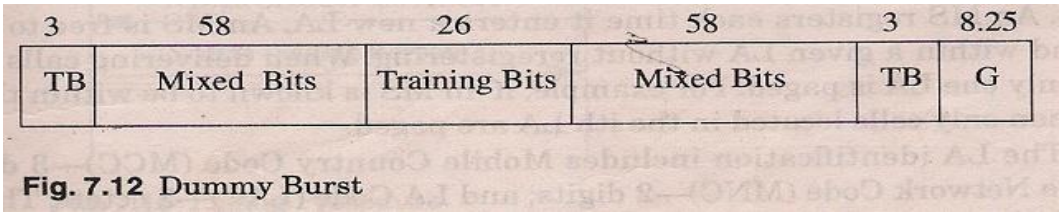


Fig. 7.12 Dummy Burst

- It carries no information
- sent from BTS on some occasions.
- The mixed bits are defined as modulating bit states.

6(a);

Mobility management

- MS periodically scan a list of PCH and lock onto the channel with strongest signal.
- To deliver an incoming call to MS a page message is broadcast on PCH from BS
- If MS hears its identification code it responds with a page response message.
- It is difficult to know which cell area should be paged and how many cell areas should be paged.
- Involving too many cells in the paging preoces for call delivery can affect performance of the system.
- Performance related problems arise when too many cells are paged when attempting to deliver a call to an MS.
- As the page attempt rate increases to a given BS, a resource becomes a bottleneck.

- BS real-time might become a bottleneck if a BS is unable to perform other call-handling functions because of the volumes of pages it is being required to broadcast
- To keep paging performance within a safe range it is necessary to form clusters of cells and page only the cluster of cells for which the MS is known to be situated
- These cell clusters are referred to as location area-LA

Functions of LA:

- The GPA (GSM PLMN Area) is divided into LAs. Each LA is made up of one or more cell areas.
- An MS registers as soon as it enters into a new LA. An MS is free to move around within a given LA without re-registering.
- When delivering calls to an MS only one LA is paged.

The LAI (Location Area Identification) includes :

1. MCC [Mobile Country Code-3 digits]
2. MNC [Mobile Network Code-2 digits]
3. LAC [Location Area Code-2 octets]

   The cell global identification consists of LAI + Cell Identity(CI) of 2 octets.

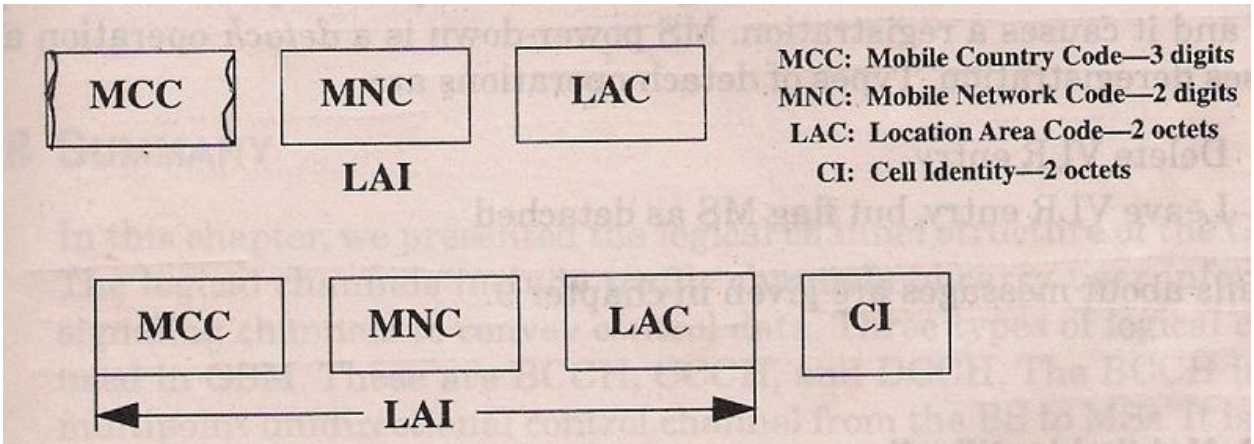


Fig. 7.14 GSM Location Area and Cell Area Identification

GSM supports following types of location registration

- Geographic based
- Time based
- On/off based

In geographic based , BSS broad cast LAC information. The MS compared the new LAC with last LAC. Registration takes place if LAC is detected.

In time based,the MS registers periodically. A minimum registration interval is 6min and maximum registration interval is 25.5hr. A timer is reset when MS activity has taken place. The timer value is kept in memory when MS turned off.

In on/off based, MS powers up is an attach operation and it causes a registration. MS power down is a detach operation and it causes deregistration

Mobile identification

Used to identify the MS when VLR does not recognize the TMSI sent by the MS

This may result from the change of LAC

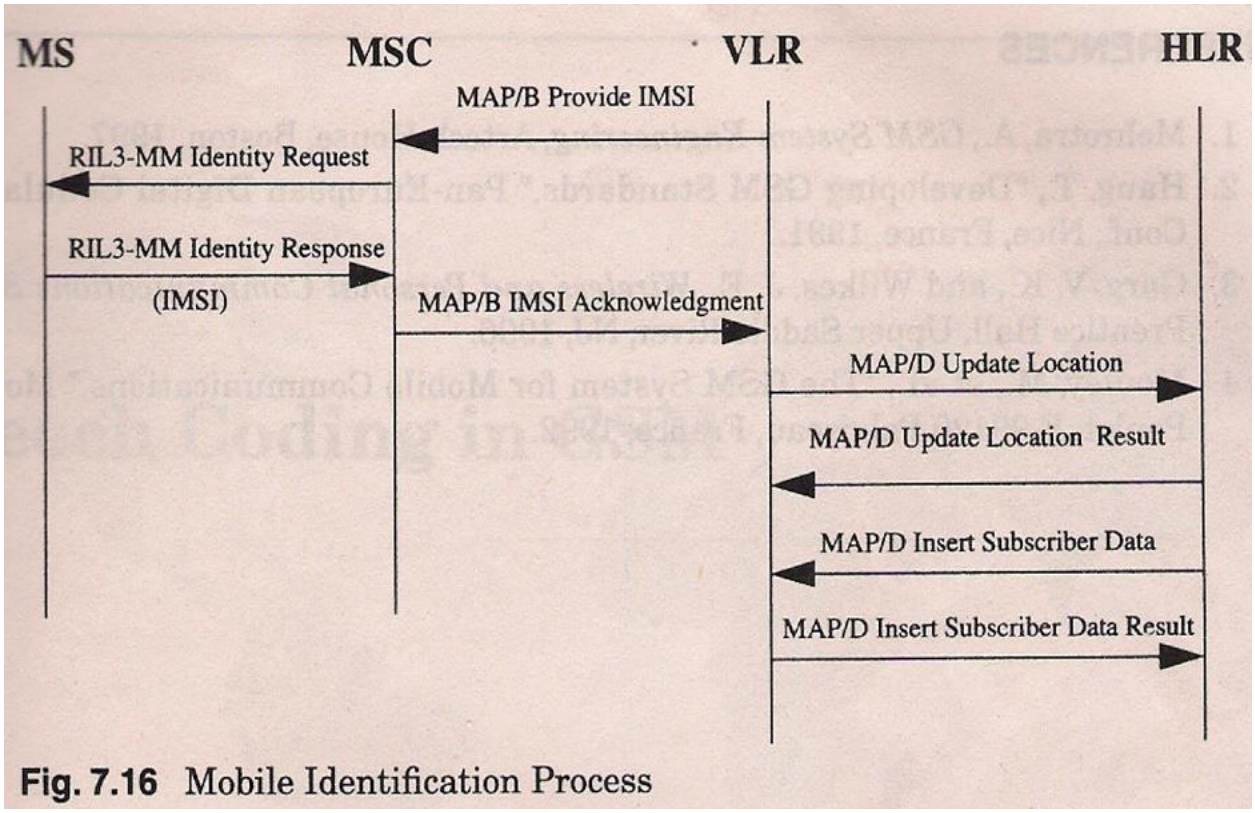


Fig. 7.16 Mobile Identification Process

6(b)

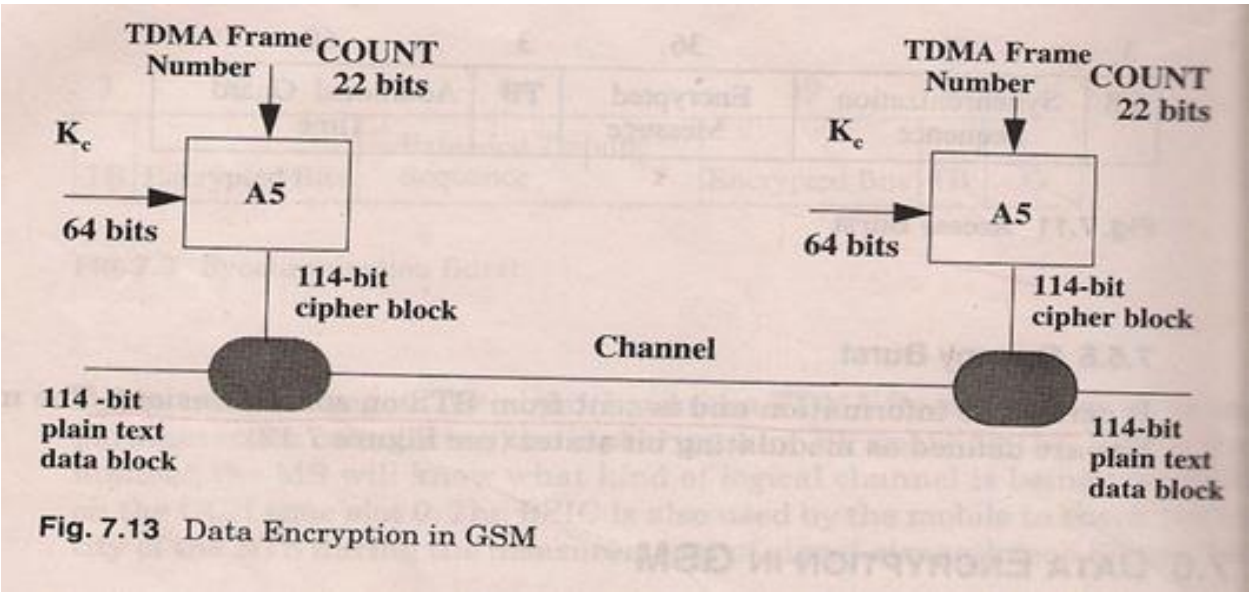


Fig. 7.13 Data Encryption in GSM

- Data is encrypted at the transmitter in blocks of 114 bits by taking 114-bit plain text data burst and performing an "EX-OR" logical function operation with a 114-bit cipher block
- The decrypting function at the receiver is performed by taking the encrypted data block of 114 bits and performing the same "EX-OR" operation using the same 114-bit cipher block that was used at the transmitter

7. **TCH Multiframe**

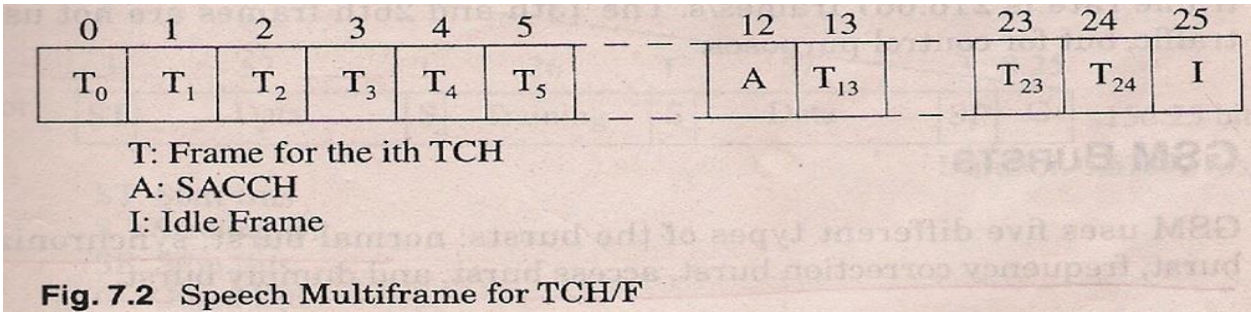


Fig. 7.2 Speech Multiframe for TCH/F

With one TCH/F

--user information is send in 24 out of 26 TDMA frames

--with an SACCH frame & an idle frame occurring every 26 TDMA frames

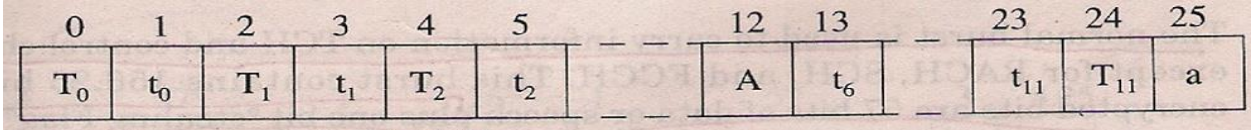


Fig. 7.3 Speech Multiframe for TCH/H

- With 2 TCH/H channels, user information requires only 12 out of 26 TDMA frames per TCH.
- In addition there are 2 SACCH frames, one per user TCH.
- Two users can share the same physical channel

- **CCH Multiframe**

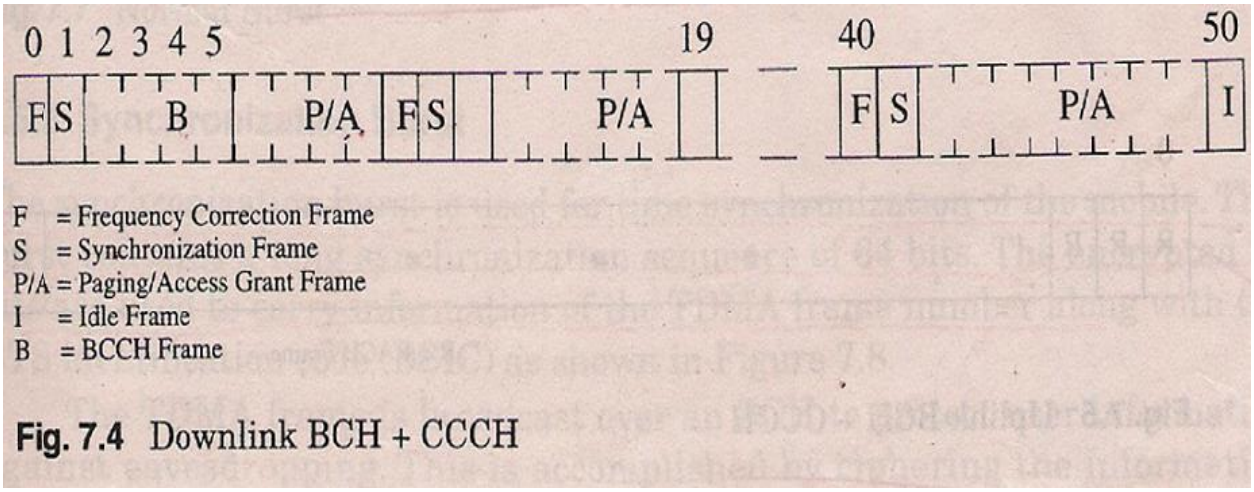


Fig. 7.4 Downlink BCH + CCCH

- The BCH & CCCH forward control channels are implemented only on certain Absolute Radio Frequency Channel Number (ARFCN) channels & are allocated time slots in a specific manner

- Uplink BCH+CCCH