GSM Overview

Reference:

Wireless Technology,

Michel Daoud Yacoub

CRC Press, 2002

ISBN: 0-8493-0969-7

TABLE 4.1

European Analog Cellular Systems

System	Reverse (MHz)	Forward (MHz)	Channel Width (kHz)	No. of Channels	Countries
TACS	890–915	935–960	25	1000	Austria, Spain
ETACS	872–905	917–950	25	1240	United Kingdom, Italy
NMT–450	435–457.5	463–467.5	25	180	Nordic countries, France, Germany, The Netherlands, Spain
NMT–900	890–915	935–960	12.5	1999	Nordic countries, France, Germany, The Netherlands
C–450	450–455.74	460–465.74	10	573	Austria, Germany, Portugal
RTMS	450–455	460–465	25	200	Italy
Radiocom 2000	192.5–199.5 215.5–233.5 165.2–168.4 414.8–418	200.5–207.5 207.5–215.5 169.8–173 424.8–428	12.5	560 640 256 256	France

TABLE 4.2

GSM Bands

System	Reverse (MHz)	Forward (MHz)	Channel Width (kHz)	Max. No. of Channels
GSM-900	890–915	935–960	200	125
E-GSM	880–915	925–960	200	175
GSM-1800	1710–1785	1805–1880	200	375
GSM-1900	1850–1910	1930–1990	200	300

Service Groups

- Teleservices (TS)
  - Telephony, emergency calls, voice messaging
- Bearer services (BS)
  - SMS and cell broadcast, 9.6kbit/s
- Supplementary Service (SS)

Supplementary Service (SS)

- Advice of charge
- Barring outgoing call, International calls, roaming calls
- Call forwarding under various conditions
- Call hold
- Call waiting
- Call transfer to a third party

Supplementary Service (SS) (cont'd)

- Completion of calls to busy subscribers
- Closed user group ---- only among themselves
- Caller ID and restrictions
- Freephone service (just like 800 numbers)
- Malicious call identification
- Three-party conference calls

Architecture

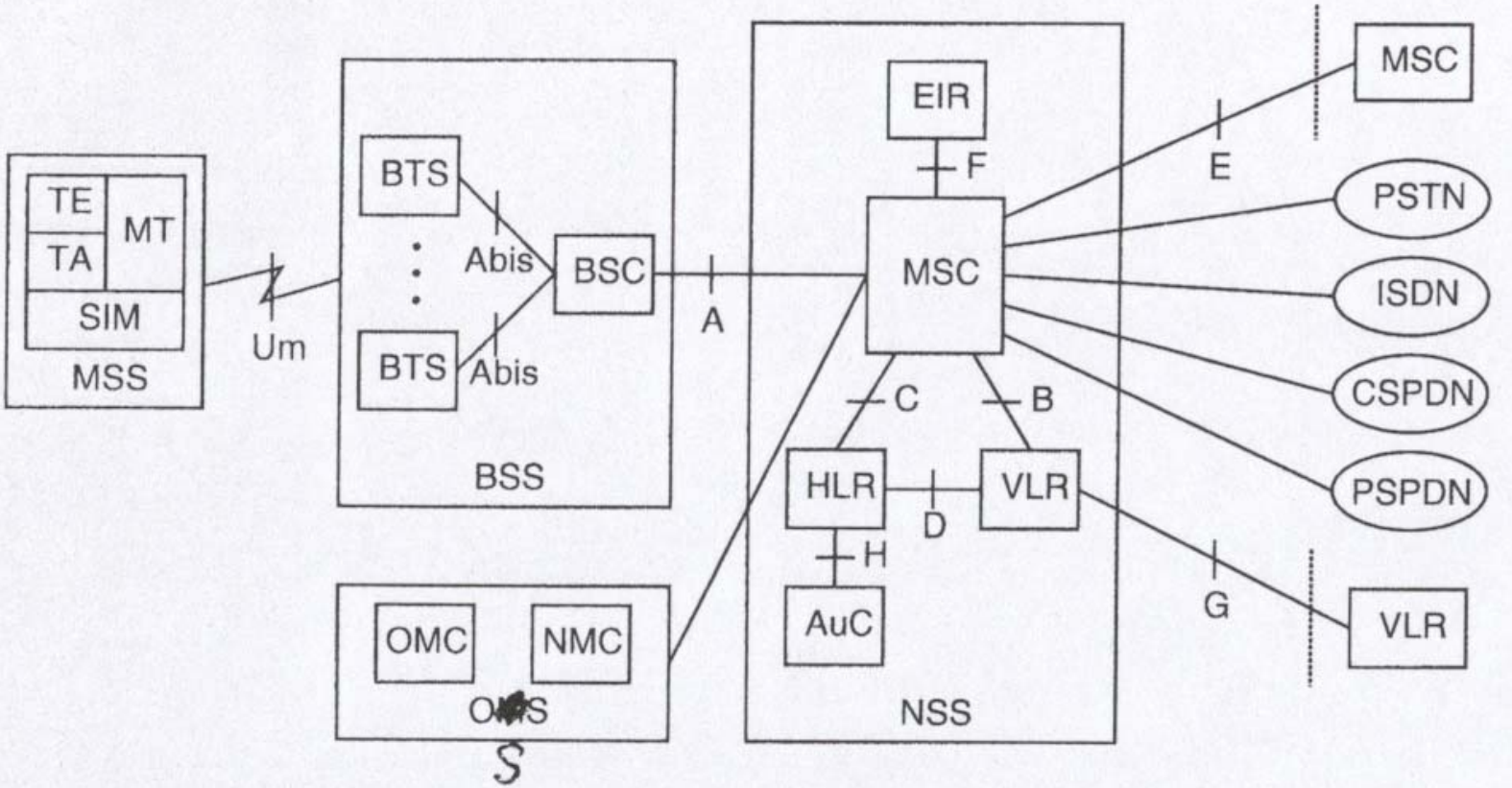


FIGURE 4.1
GSM architecture.

Four blocks

- Mobile Station Subsystem (MSS)
- Base Station Subsystem (BSS)
- Network and Switching Subsystem (NSS)
- Operation and Support Subsystem (OSS)

MSS ---- (Mobile Termination MT)

- Mobile Termination (MT) including Terminal Equipment (TE) and Terminal Adapter (TA)

MSS ---- (Mobile Termination MT) (cont'd)

- TE identities and classmark
  - International Mobile Equipment ID (IMEI) --- IEEE 48 bit hardware address
  - Revision level ---- GSM version implemented
  - Encryption capability
  - Frequency capability --- dual-band tri-band
  - Short message capability
  - RF power capability

TABLE 4.3

Equipment Class and Their Maximum Power

Class	GSM-900 (watt)	GSM-1800 (watt)	GSM-1900 (watt)
I	20	1	1
II	8	0.25	0.25
II	5	4	2
IV	2	—	—
V	0.8	—	—

MSS ---- (Mobile Termination MT) (cont'd)

- Subscriber Identity Module (SIM)
  - Subscriber and equipment ID's are independent elements. A major reason of the success of GSM over that of DAMPS.
  - International Mobile Subscriber ID(IMSI)
    - 15 digit = 3 for country code, 3 for mobile network code and 9 for mobile ID number.
  - Temporary Mobile Subscriber ID(TMSI)
    - per-call basis ID for security reason to avoid sending IMSI over the air
  - Mobile Station ISDN Number (MS-ISDN)

MSS ---- (Mobile Termination MT) (cont'd)

- Subscriber Identity Module (SIM) (cont'd)
  - Mobile Station Roaming Number
    - Temporary ID for roamers
  - International Mobile Equipment ID (IMEI)
    - (IMEI, IMSI) pair ensures only authorized users are granted access to the system.
  - Location Area Identity (LAI)
    - Identifies the particular group of cells the MT has most recently visited
  - Subscriber Authentication Key (Ki)
    - A secret assigned by the operating company to a subscriber

Base Station Subsystem --- 1

Consists of

- Base Transceiver Station (BTS)
  - radio equipments responsible for radio coverage
- Base Station Controller
  - Controls a few BTS
  - Manage radio resource management, signaling transmission, power control, handover control, frequency hopping control etc.

Base Station Subsystem --- 2

- Transcoder/Rate Adapter Unit
  - A device placed between GSM elements (BTS, BSC and MSC) to conserve bandwidth resources.
  - Combines four 13 kbps speech channels to one 64 kbps data stream. Thirty 64 kbps channels can then be multiplexed to a E1 channel. Located at BTS, BSC (more often) or MSC.

Network and Switching Subsystem (NSS)

- Perform functions such as call setup, paging, resource allocation, location registration, encryption, interfacing with other networks, handoff control, billing, synchronization, echo canceling and interface with external networks.
- Consist of 4 elements
  - MSC, HLR, VLR, AuC and EIR
  - MSC is the processor, the others are database units.

NSS --- Home Location Register (HLR)

- HLR contains a list of subscribers belonging to one or more MSC areas.
- Permanent subscriber data including IMSI, MS-ISDN, roaming restriction, permitted supplementary services and authentication key.
- Temporary subscriber data consist of MSRN, data related to encryption, VLR address, MSC address and roaming restriction.
- HLR is usually centralized within a network.

NSS --- Visitor Location Register (VLR)

- Data of visitors that is similar to HLR
- When a roamer appears, his HLR is transferred to the local VLR.
- VLR is usually co-located with MSC.

NSS --- Authentication Center (AuC)

- Performs authentication function for each subscriber within the system.
- A key kept in SIM and AuC is never transmitted over air.
- Authenticate by using a random challenge.
- Vulnerability is present when encrypted authentication keys must be transmitted from HLR to VLR.

NSS --- Equipment Identity Register (EIR)

- Records the IMEI of all subscribers in three lists.
- White list ---- clean equipment
- Black list ---- stolen equipment
- Gray list ---- equipment with minor problems

Operation and Support Subsystem (OSS)

- OSS consists of two entities not fully specified in GSM. They are
  - Operation and Maintenance Center (OMC)
  - Network Management Center (NMC)
- Performs alarm handling, fault management, performance management, configuration management, traffic data acquisition, activate and deactivate functions, and long term planning.
- Normally centralized in a network.

Open Interfaces

- A-Interface ---- between BSC and MSC, E1 link.
- Abis-Interface ---- between BTS and BSC using LADP (Link Access Data Protocol) protocol.
- B-Interface ---- between MSC and VLR
- C-Interface ---- between MSC and HLR
- D-Interface ---- between HLR and VLR
- E-Interface ---- between MSCs
- F-Interface ---- between MSC and EIR
- Um-Interface ---- between MSS and BSS.

Multiple Access

- FDMA/TDMA/FDD
- GSM 900 uses 50 MHz is two 25 MHz bands for up and down link.
- Provides a maximum 125 carriers at 200 kHz spacing in each band.
- EGSM adds 10 MHz or 50 carriers to each band.
- GSM-1800 uses two 75 MHz bands with a maximum of 375 carriers at 200 kHz spacing.
- Each carrier is divided into 8 TDMA channels.

Signal Processing

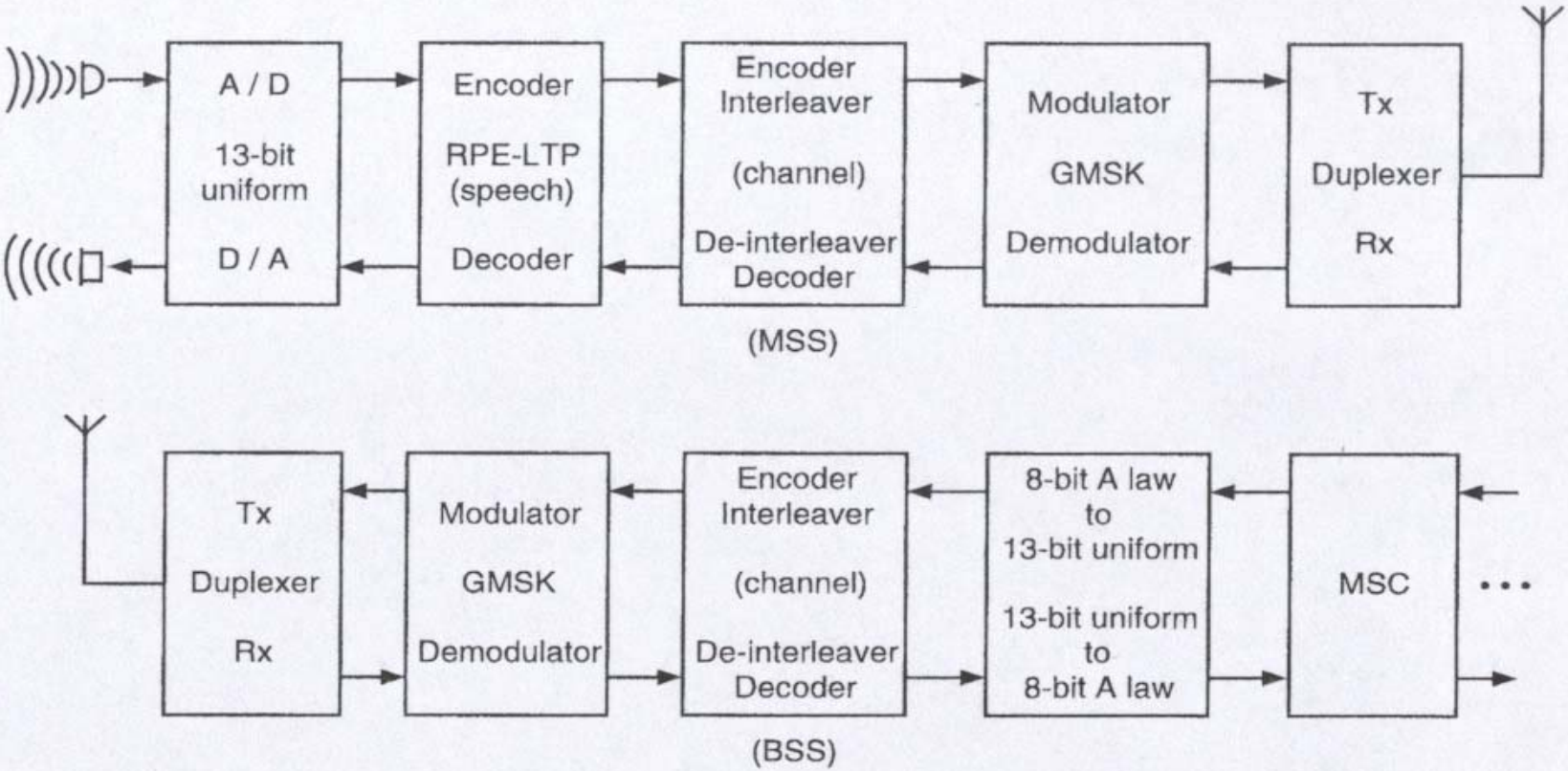


FIGURE 4.2
GSM transmission/reception chain.

MSS Signal Processing

- The voice input is sampled at 8 kHz using 13 bits/sample.
- The resulting 104 kbits/s is reduced to 13 kb/s using Regular Pulse Excitation-Long-Term Prediction Linear Prediction Coding (RPE-LTP-LPC)
- FEC and interleaver
- GMSK modulation

BSS Signal Processing

- Demodulate
- Deinterleave
- FEC
- Decode into 13 bits/sample uniform code
- Convert to A-Law-PCM code and send to MSC

Speech Coding and Processing --- 1

- Take 20 ms speech or 160 samples.
- Represent it by 260 bits divided as follows
  - 36 bits for LPC coefficients
  - 36 bits for long-term prediction
  - 188 bits for excitations
- The coding rate is (260 bit)/(0.02 seconds) = 13 kb/s.
- Bits are classified as
  - Class 1a: 50 bits are essential.
  - Class 1b: 132 bits are important.
  - Class 2: 78 bits are less important.

Speech Coding and Processing --- 2

- 3 parity bits are added to the Class 1a bits to give 53 bits.
- These 53 bits are added to the132 bits Class 1b bits and appended by “0000” to give 189 bits. After rate 1/2 convolutional encoding gives 378 bits.
- Adding the 78 Class 2 bits gives 456 bits in 20 ms, or 456/0.02=22.8 kb/s.
- Two 456 bit blocks are interleaved and transmitted over 8 frames, i.e. spread out to 114 bits per frame.

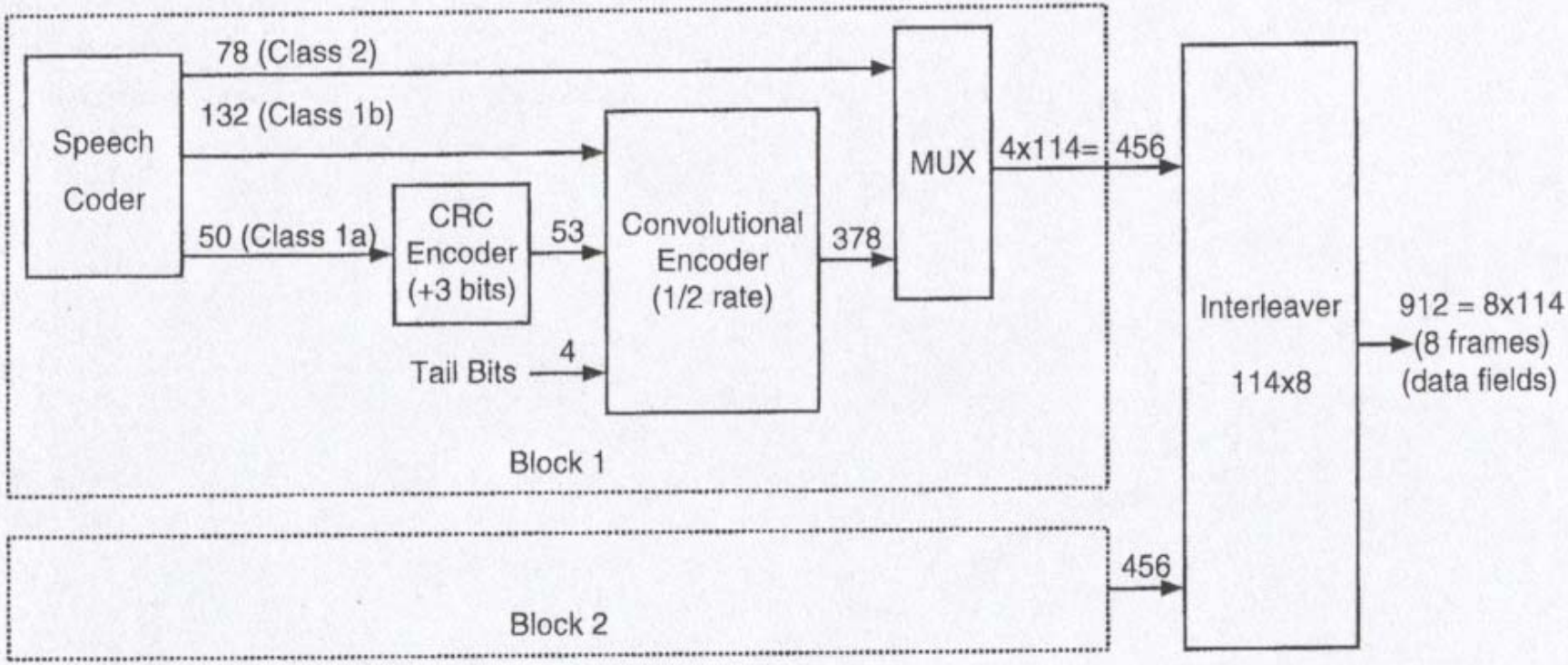


FIGURE 4.8
Traffic channel structure.

Physical Channel

- After deducting 100 kHz as guard band at both ends of the spectrum, only 124 carriers are used.
- Radio frequency channel number N $\in$ {1, 2, …, 124} is defined and corresponds to center frequency in MHz as follows for GSM-900

$$f_{up} = 0.2N + 890$$

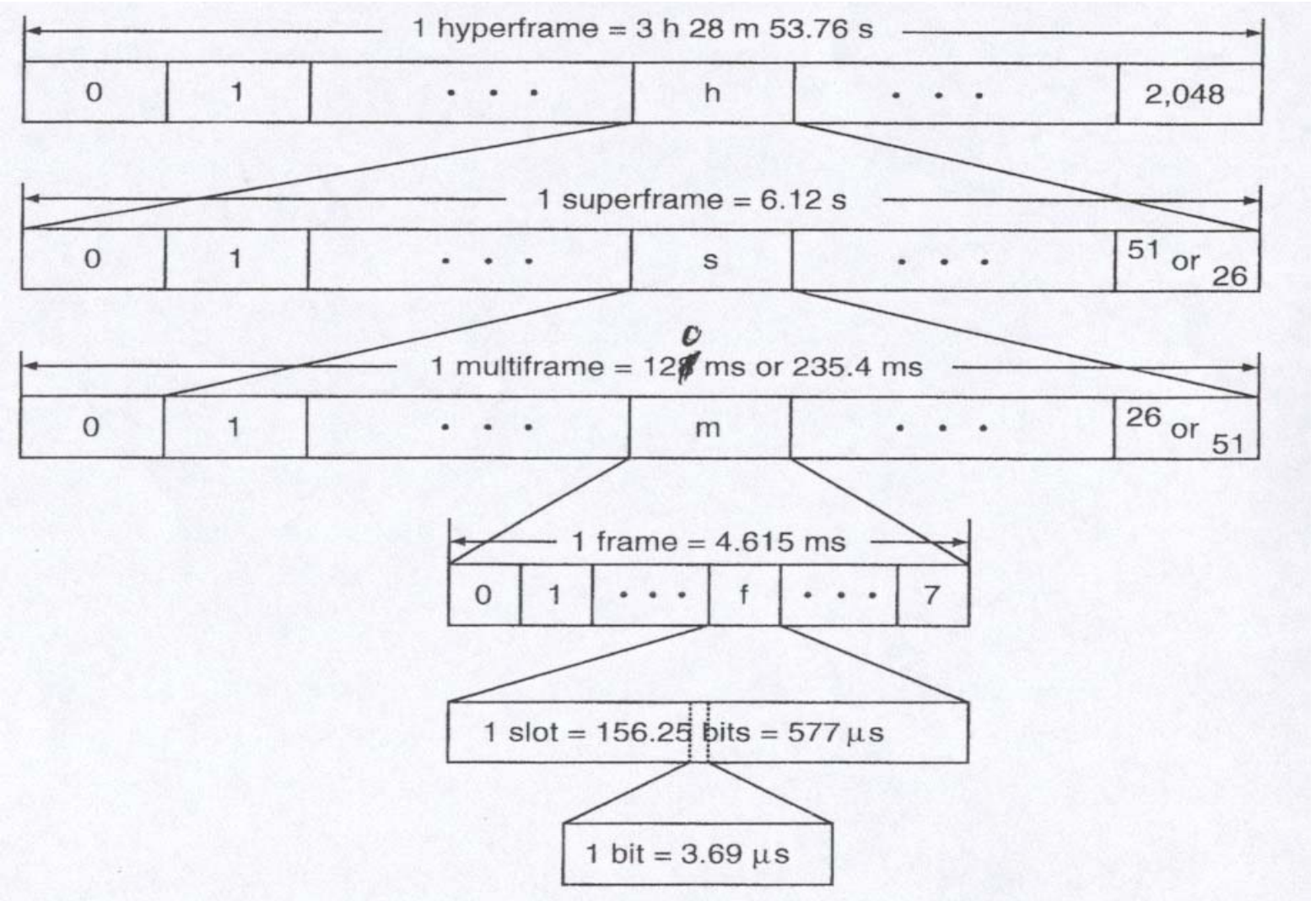
$$f_{down} = 0.2N + 935$$

- For GSM-1800, N $\in$ {512, 513, …, 855}

$$f_{up} = 0.2N + 1607.8$$

$$f_{down} = 0.2N + 1702.8$$

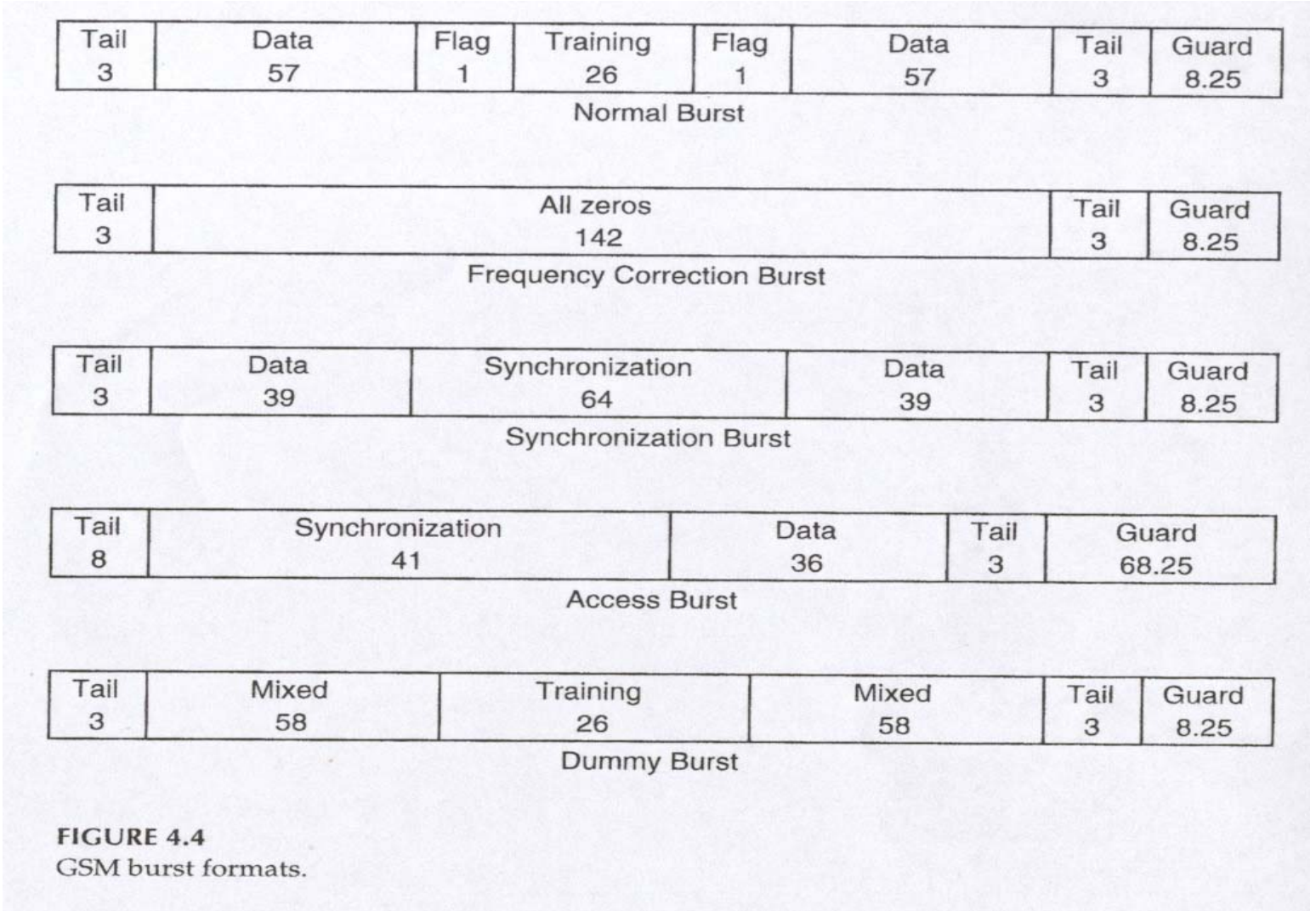
GSM Framing Structure



GSM Framing Structure

- A frame has duration 4.615 ms. Consists of 8 slots. Each slot can accommodate one burst of duration 577 micro-second.
- Two kinds of multiframe:
  - traffic MF = 26 frames(120ms),
  - control MF = 51 frames.
- Superframe --- same structure as multiframe.
- 2048 superframes form a hyperframe of duration 3 h 28 m 53.76 s.

GSM Burst Format



Tail	Data	Flag	Training	Flag	Data	Tail	Guard
3	57	1	26	1	57	3	8.25

Normal Burst

Tail	All zeros	Tail	Guard
3	142	3	8.25

Frequency Correction Burst

Tail	Data	Synchronization	Data	Tail	Guard
3	39	64	39	3	8.25

Synchronization Burst

Tail	Synchronization	Data	Tail	Guard
8	41	36	3	68.25

Access Burst

Tail	Mixed	Training	Mixed	Tail	Guard
3	58	26	58	3	8.25

Dummy Burst

FIGURE 4.4
GSM burst formats.

GSM Bursts

- For carrying traffic, network control data, frequency correction, synchronization and random access data.
- Flag ---- indicate the type of information, traffic or network control.
- Training ---- for channel adaptive equalization.
- Tail ---- all-zero bits to indicate the start and the end of the burst.
- Guard ---- ramping time for transmitter ON/OFF, to avoid overlapping between adjacent time slots. Necessarily much longer for Access Burst.
- Synchronization ---- a known sequence for time synchronization.

Logical Channels

- Traffic Channels (TCH)
  - TCH/F and TCH/H for full and half rate speech channels.
  - TCH/9.6, TCH/4.8 and TCH/2.4 for 9.6, 4.8 and 2.4 kb/s data channels.
- Broadcast Channels (BCH)
  - frequency correction channel (FCCH),
  - synchronization channel (SCH),
  - broadcast control channel (BCCH).

Logical Channels (cont'd)

- Common control channels
  - paging channel (PCH),
  - access grant channel (AGCH),
  - random access channel (RACH).
- Dedicated control channels
  - stand-alone dedicated control channel (SDCCH),
  - slow associated control channel (SACCH),
  - fast associated control channel (FACCH).

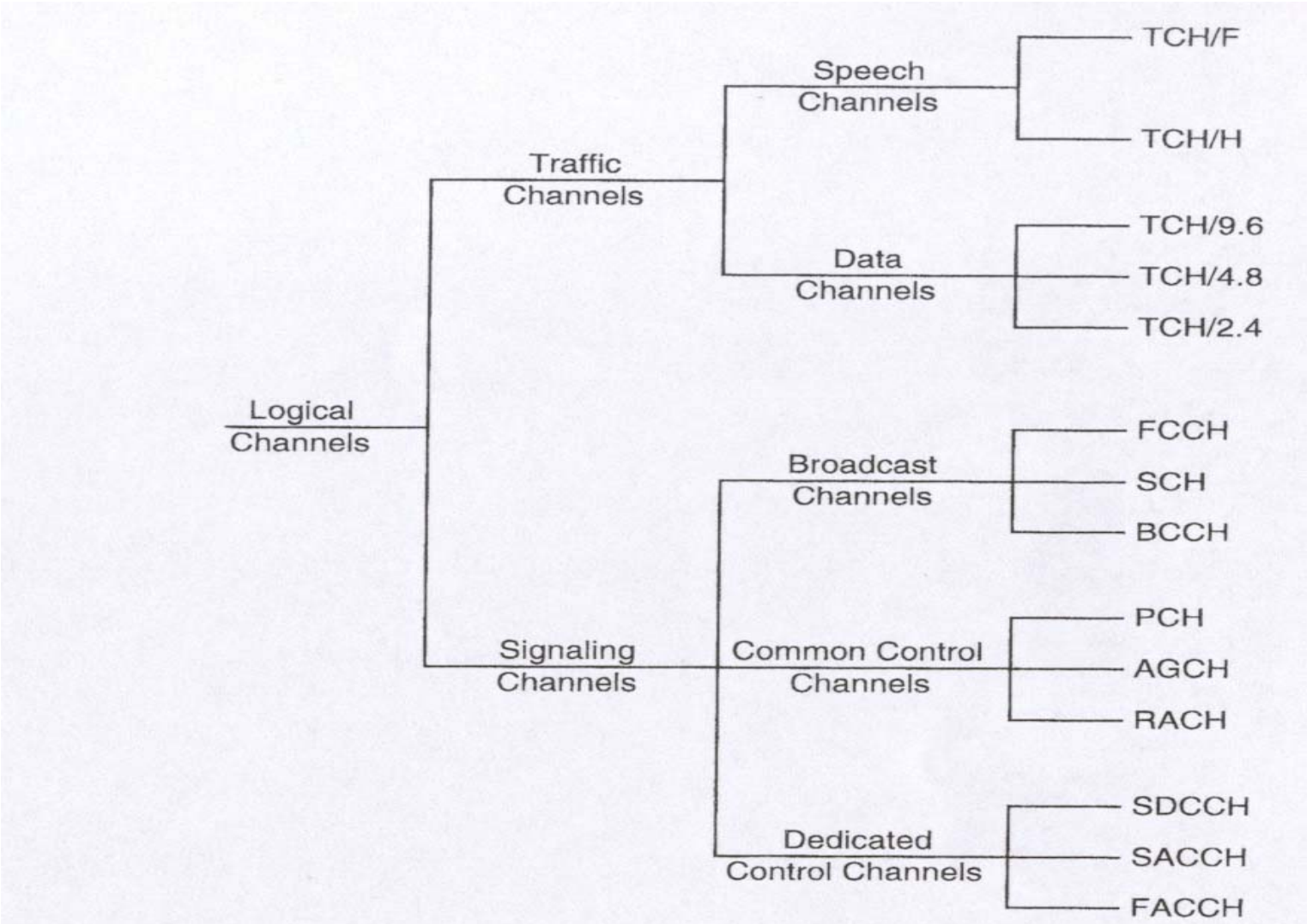


FIGURE 4.5
GSM logical channels.

Traffic Multiframe -- 1

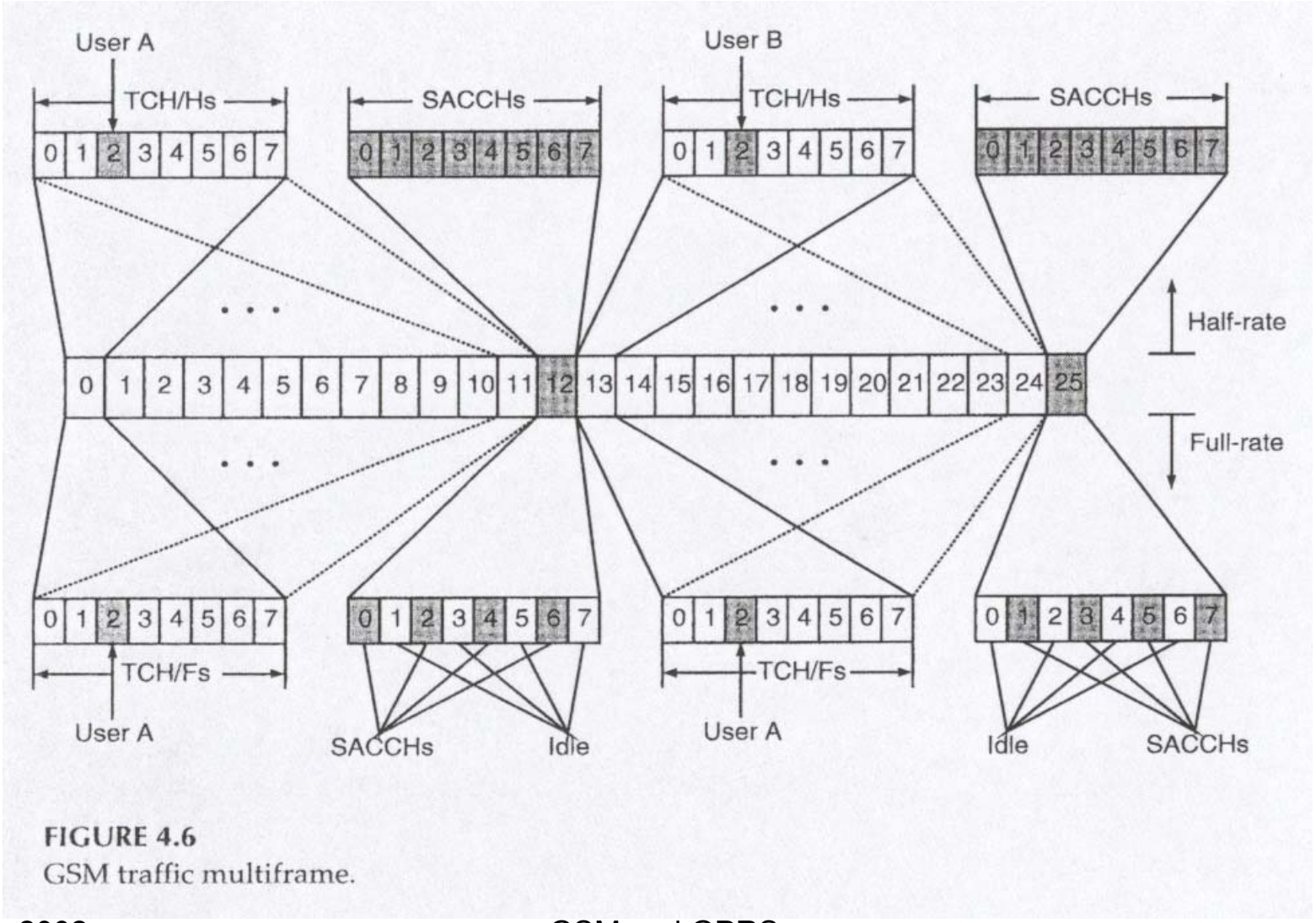
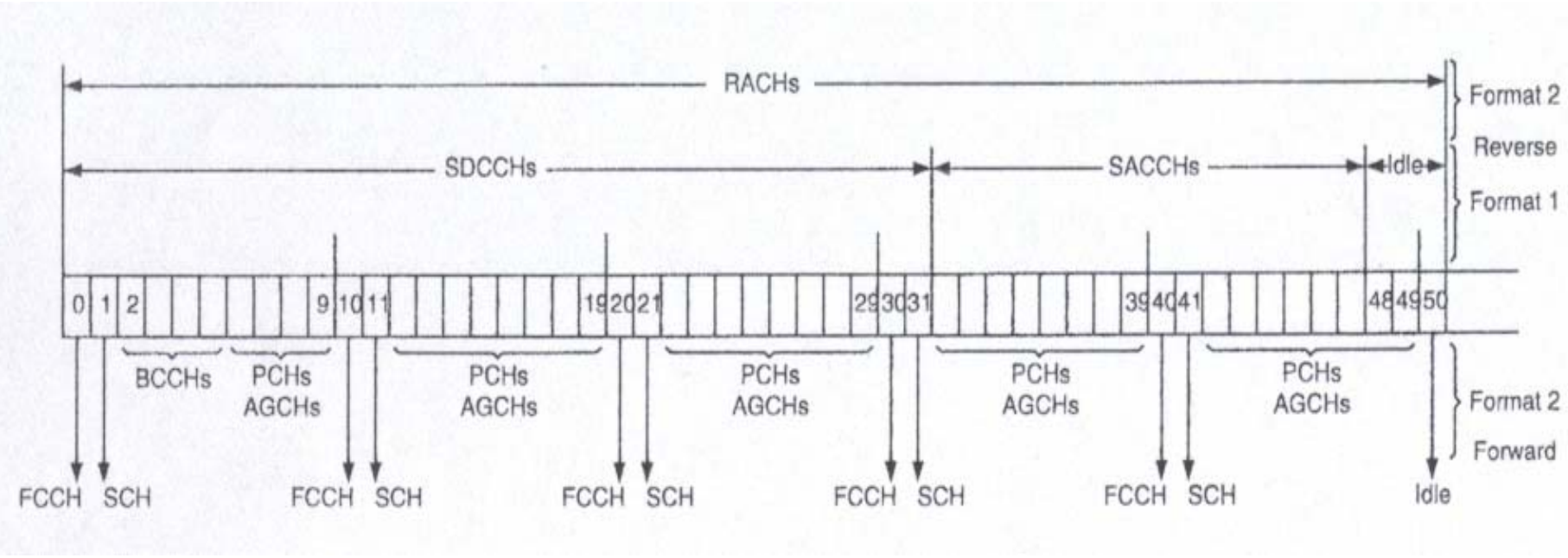


FIGURE 4.6
GSM traffic multiframe.

Traffic Multiframe -- 2

- Each multiframe consists of 26 frames, 24 for traffic and 2 for control (frame 12 and 25).
- Frames 12 and 25 carry 8 SACCH, one for each TCH/F.

Control Multiframe --1



Control Multiframe -- 2

- Consists of 51 frames in two formats
- Format 1 is occupied by SDCCH and SACCH
- Format 2 is occupied by FCCH, SCH, BCCH, PCH, AGCH and RACH and are different for up and down links. Uplink is for RACH only.

Frequency Control Channel

- FCCH is a forward channel using frequency correct burst format. The 142 all zero bits causes GMSK to deliver an unmodulated carrier for the entire slot.

Synchronization Channel

- One-way forward channel using synchronization burst format.
- Of the 89 bits raw message, 64 bits are for frame synchronization and 25 are for identifications.
- The identification bits consists of the followings:
  - 6 bits are for BTS identifications,
  - 11 bits to identify the superframe within the hyperframe,
  - 5 bits specify the multiframe within the superframe and
  - 3 bits identify the control block within the control multiframe.
- The 64 bit frame synchronization is put in the synchronization field in synchronization burst.
- The 25 identification bits are apended by 10 parity bits 4 tail bits to yield 39 bits. This is in turn rate ½ convolutional encoded to give 78 bits and is placed in the two 39 bit data fields in the synchronization burst.
- SCH bursts are located at slot 0 of some specific carriers.

Synchronization Channel (cont'd)

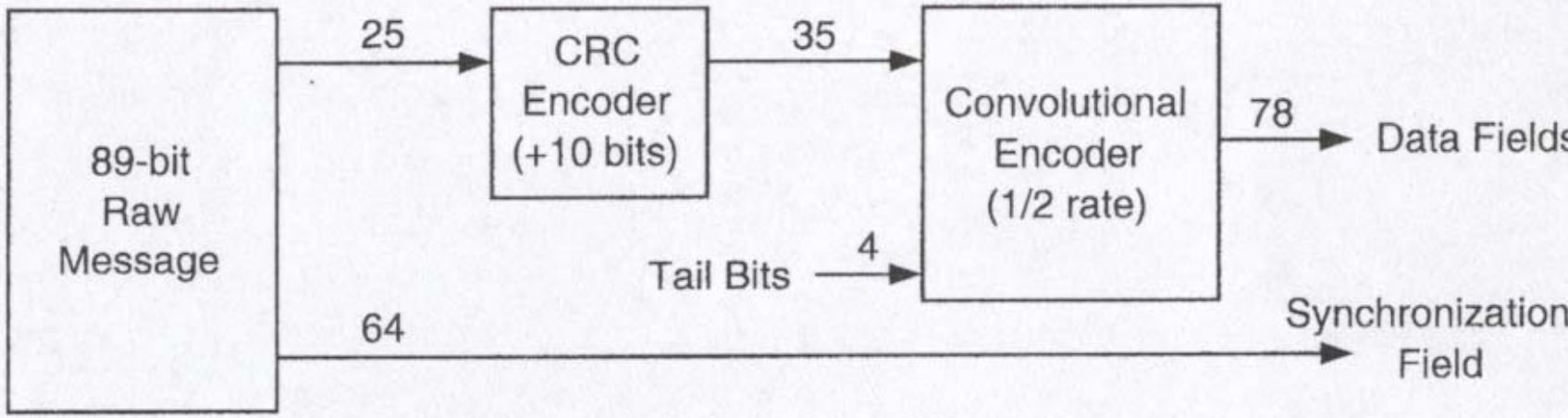


FIGURE 4.9
Synchronization channel structure.

Broadcast Control Channel

- Bears information for call setup purpose
- One-way forward channel using normal burst format
- Information includes cell identity, network identity, control channel structure, list of channels in use, congestion status, details of access protocol
- Raw message is 184 bits protected by a 40 bit fire code (FEC)
- 184 + 40 + 4(tail bits) = 228 bits are rate ½ convolutionally coded to yield 456 bits
- Divide into 4×114 bits and sent in 4 time slots
- Located at slot 0 of some specific carriers

Paging Channel and Access Grant Channel

- One way forward channel using normal burst format
- Use same coding scheme as BCH
- 36 paging (AG) channels per control multiframe gives 36/4 = 9 paging (AG) messages per multiframe
- Paging and AG channels share the slots. Blocks of 4 frames are assigned to paging or AG as informed on the BCCH.
- PCH blocks are divided into groups. Terminals need only to monitor the group it belongs to save power. This is the principle of sleeping-mode operation.

Random Access Channel -- 1

- Use access burst format
- For call origination, short message transmission, ack to paging message, location registration, IMSI (International Mobile Subscriber Identity) attachment, IMSI detachment
- Slotted ALOHA with a maximum number of trials as specified on BCCH
- All successfully received RACH bursts are ack'ed to indicate the time slot number of the SDCCH. In other words, RACH is for establishing SDCCH.

Random Access Channel -- 2

- 68.25-bit time is used as guard time. This guard time corresponds to a propagation distance of 75 km, or a maximum cell radius of 37.5km.
- Base station use arrival time to determine the timing advance. It is sent to the terminal for subsequent transmission.
- 8 bit raw access message
  - 3 bits for type of access such as call origination, paging acknowledgment, etc.
  - 5 bits of random color code for distinguishing messages from different terminals transmitting in the same time slot.
- 8 bits are CRC encoded to 14 bits. Add 4 tail bits and rate 1/2 convolutional encoded to produce 36 bits of data.

Stand-Alone Dedicated Control Channel (SDCCH)

- A 2-way channel using normal burst format for signaling purpose related to registration, authentication and location update.

- Established by using RACH and before the allocation of a TCH (traffic channel).
- Uses 4 slots within the 51-frame control multiframe.

Slow Associated Control Channel (SACCH)

- A continuous 2-way data channel (using normal burst format) between BS and Terminal.
- Associated with a TCH or an SDCCH.
- Forward link: For power level command and timing adjustment directives.
- Reverse link: convey measurement reports on signal quality of the serving BS and of the neighboring cells.
- For TCH, SACCH occupies 1 slot (114 bits) per multiframe (120 ms). ∴ the data rate is 114/0.12 = 950 bits/s.
- Each message comprises 456 bits, or takes 4 multiframe to transmit.
- Same coding scheme for BCCH is used for SACCH.

Fast Associated Control Channel (FACCH)

- For time sensitive signaling such as handover request.
- Setting a 2-bit flag to convert a TCH or an SDCCH burst into a FACCH burst.
- This is an example of in-band signaling.

GSM Message -- 1

- For signaling purpose and uses LAPDm (mobile) protocol.
- A 184-bit message segment is processed to yield 456 bits and transmitted in 4 slots.
- Structure: Address (8), Control (8), Length Indicator (8), Information (I bits), Fill (F bits).
- 3 types of messages: supervisory (S), unnumbered (U) and information (I).

GSM Message -- 2

- S and U messages precede or follow the I messages to control the flow of messages.
- S is for requesting (re) transmissions or suspending transmission. U is for initiating or terminating transmission.
- In other words, S and U are Layer 2 messages, I is a Layer 3 message.
- They serve 4 network management functions :
  - Data Link Control (DCL)
  - Radio Resource Management (RRM)
  - Mobility Management (MM)
  - Call Management (CM)

DLC Messages

- Set Asychronous Balanced Mode (U) – initiate a transfer of I message
- Disconnect (U) -- terminate transfer
- Unnumbered Acknowledgment (U)
- Receive Ready (S) – request transmission
- Receive Not Ready (S) – request retransmission
- Reject (S) – suspend transmission

RRM Messages

- *Sync Channel Information* -- downlink message running on SCH. Conveys BS identifier and the frame number for terminals to achieve time synchronization.
- *System Information* -- downlink on BCCH. Contains location area identifier, number of physical channels carrying signaling information, parameters of RACH protocols, radio frequency carriers active in the neighboring cells.

RRM Messages -- 2

- *Channel request*.
- *Paging request*.
- *Immediate Assignment* -- downlink on AGCH. For assigning an SDCCH to a terminal for call set up.
- *Handover command*
- *Ciphering mode*.
- All together 22 message types.

Call Management (CM) and Mobility Management (MM) messages

- CM consists of setup, emergency setup, call proceeding, progress, call confirm, alerting, connect, user information, disconnect, release, status, congestion control, etc all together 18 messages.
- MM consists of authentication request, authentication response, identify request, location update request, etc all together 13 messages.

GSM Call Management

1. Mobile Initialization
2. Location Update
3. Authentication
4. Ciphering
5. Mobile station termination
6. Mobile station origination
7. Handover
8. Call clearing

CM 1: Mobile Initialization

- Three goals:
  - Frequency synchronization,
  - Time synchronization,
  - and Overhead information acquisition.
- Frequency synchronization -- When switched on, terminal scans the GSM RF channels, and identifies the one with strongest signal strength. Search for the frequency correlation burst on the BCCH. If frequency correlation burst is not found, search the next strongest signal strength channel. Frequency synchronize with the BS transceiver.
- Time synchronization -- search for synchronization burst on SCH.

CM 1: Mobile Initialization (cont'd)

- Overhead Information Acquisition ---- search for overhead information on BCCH including the following:
  - Country code
  - Network code
  - Location area code
  - Cell identity
  - Adjacent cell list
  - BCCH location
  - Minimum received signal strength
- Verify the codes with that in the SIM card.
- IF Okay, maintain the link and monitor the PCH.

CM 2: Location Update

- Update when:
  - Terminal is switched on
  - Terminal moves to a different location
  - After long idling -- for speeding up the paging procedure. Update period indicated on BCCH and varies according to network loading.
- Procedure:
  - Terminal sends uplink channel request on RACH.
  - Network assigns a SDCCH channel via the AGCH message.
  - Send location update request with its ID (IMSI or TMSI) on SDCCH.
  - After authentication and ciphering, send a new TMSI to the terminal.
  - Terminal acknowledge and the SDCCH channel is released.

CM 3: Authentication

- Network sends an Au request message consisting of a 128-bit RAND to terminal.
- Terminal uses RAND, secret key Ki, stored in SIM and the A3 encryption algorithm to compute a 32 bit signed response called SRES.
- Another 64-bit ciphering key Kc is computed using the A8 encryption algorithm. This is used later fro cyphering.
- Terminal sends an Au response message containing SRES.
- Network computes its SRES. If it matches with the received SRES, Authentication is successful.

CM 4: Ciphering

- For encrypting data after Authentication.
- Network sends a ciphering mode message to tell terminal if encryption is to be used.
- Terminal uses Kc, the frame number and the A5 encryption algorithm to compute a 114-bit encryption mask.
- Mask is mod-2 added to the 114-bit data in the burst.
- The BS performs the reverse for decryption.
- Ciphering changes from frame to frame.

CM 5-6: Mobile Station Termination and Origination

- Termination: A call to the terminal
- Origination: A call that starts from the terminal
- Follows the normal call set up procedures in SS7.

CM 7: Handover

- Mobile monitors the signal levels of all RF channels in its own and neighboring cells.
- Report to BS on SACCH.
- Intercell and Intracell handover.
- Synchronous HO ---- The original and destination cells are synchronized. The time difference between time slots and the timing advance are calculated for adjusting the transmission on the new channel. Takes 100 ms on the average.
- Asynchronous HO ---- perform the full synchronous process at the destination cell. Takes 200 ms.

CM 8: Call Clearing

- BS sends a release message on BCCH to terminal.
- Terminal sends release message back.
- BS replies with a release complete message.

Frequency Hopping

- Slow FH at each frame (4.615 ms interval) is implemented in all GSM terminals.
- To hop or not is decided by operator.
- Cyclic hopping mode ---- hop sequentially over the set of frequencies.
- Random hopping mode ---- hop in one of the 63 pseudorandom sequences.
- The broadcast carrier, known as the base channel, contains FCCH, SCH and BCCH is the network beacon and is not hopped.
- All carriers within a cell and within a group of cells hop in a coordinated manner so that frequency overlapping is avoided.
- Up and down links use the same FH sequence.
- Terminal is informed about the set of hopping channels and the sequence number.

Discontinuous Transmission (DTx)

- For power saving using voice activity detector (VAD).
- A synthetic comfort noise signal is inserted during the “voice off” period.
- When a badly corrupted speech frame occurs, it is replaced by the preceding uncorrupted speech frame. Due to correlation, this speech frame extrapolation (SFE) can significantly reduce CNR.

Power Control

- For power conservation and co-channel interference reduction.
- Terminals power can range over 30 dB in steps of 2 dB. (i.e. 16 power levels).
- Power control interval is 60 ms or 13 frames.

Spectral Efficiency

- GSM allows a reuse factor of 3 to 4 cells per cluster
- Spectral efficiency parameter η

$$\eta = \frac{(conversations)}{(cells)(spectrum)}$$

- The number of physical channels in a 50 MHz GSM-900 is 124 carriers $\times$ 8 channel/carrier = 992.

Therefore

$$\eta = \begin{cases} \dfrac{992}{4 \times 50} = 4.96 & f = 4 \\ \dfrac{992}{3 \times 50} = 6.61 & f = 3 \end{cases}$$

Or, 5 to 6 calls per cell per MHz