EE 577 - Wireless and Personal Communications

Introduction to GSM

History of GSM

- 1982: Group Special Mobile was started by CEPT
- Objectives of the group is to come up with a system standard having the following general requirements:
  - Good subjective speech quality
  - Low terminal and service cost
  - Support for international roaming
  - Support for range of new services and facilities
  - Spectral efficiency
  - Efficient inter-operation with ISDN systems

History (Continued)

- 1987: The MoU (Memo of Understanding) Association was formed
- 1989: GSM (Global System for Mobile) became an ETSI technical committee
- 1990: GSM phase 1 recommendations published
- 1990: UK requested DCS 1800 specs., based on GSM
- 1991: DCS 1800 recommendations published
- 1992: First commercial service started (Finland)
- 1993: 1 million subscribers
- 1995 (Middle): 12 million subscribers in 86 countries

History (Continued)

- 1995: PCS-1900 license given in North America
- DCS 1800 now called GSM 1800
- PCS 1900 now called GSM 1900 End of 1997: 55 million subscribers
- In 1995 the GSM MoU expected 100 million subscribers by year 2000
- 100 million subscribers was reached in July 1998 !
- April 1999: about 150 million
- By 2001 there was about 350 million
- Growth 7 million each month (about 3 per second)

GSM Requirements

- User requirements
- Network operator requirements
- Manufacturer requirements

ETSI has established standards that meet these requirements

User Requirements

- Good speech quality
- Call privacy
- Wide network coverage
- Messaging services
- Data services
- Light weight and compact handsets
- High service availability
- Reasonable access cost
- Reasonable usage tariffs

Network Operator Requirements

- Optimum resource utilization
- High availability
- Simple and Efficient operation
- Large number of subscribers
- Standardized equipment
- Several equipment manufacturers
- Reasonable infrastructure cost
- Flexible standards

Manufacturer Requirements

- Stable definition of the product functionality
- Clear definition of the constraints
- Single certification authority
- Wide market

GSM Services

- Telephony and Fax (G3)
- Data (up to 9.6 kbps)
- Access to PSTN, ISDN, PSPDN, CSPDN
- Emergency call and Short Message Service (SMS)
- Supplementary services:
  - Call forwarding
  - Call barring
  - Call waiting
  - Advice of charge
  - Calling line identification

Attractive Features

- It is a purely digital system
- Large number of network interfaces specified by GSM
- Its network specification is based on the well-known Signaling System No. 7 (SS7)
- TDMA/FHMA techniques specify only the air interface
- Open interfaces which give flexibility in procurement

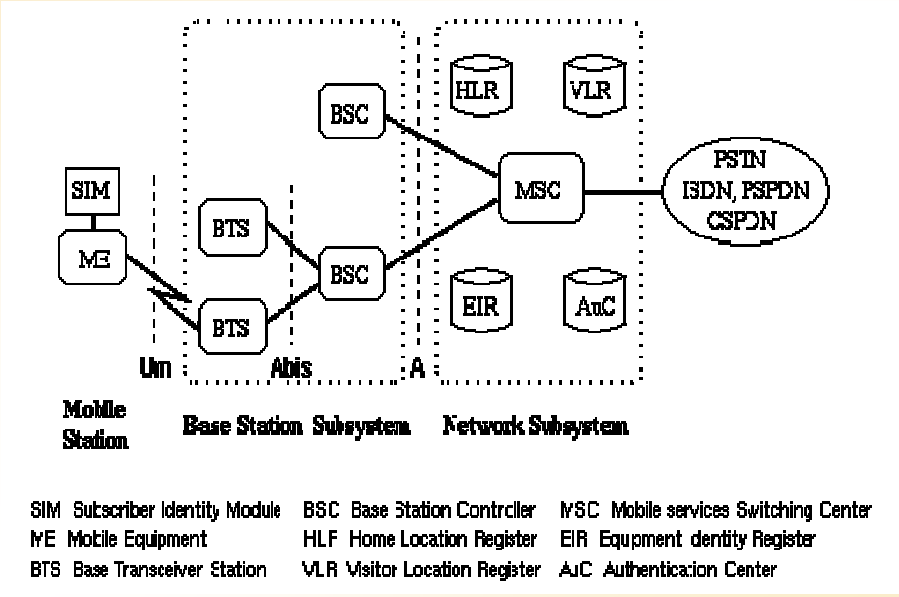
Frequency Bands

- Primary (P-GSM 900, 124 channels)
  - 890-915 MHz (up-link)
  - 935-960 MHz (down-link)
- Extension (E-GSM 900, 50 more channels)
  - 880-890 MHz (up-link)
  - 925-935 MHz (down-link)
- DCS 1800 (GSM 1800) (374 channels)
  - 1710-1785 MHz (up-link)
  - 1805-1880 MHz (down-link)
- PCS 1900 (GSM 1900) (6 bands)

GSM System Architecture

- The Mobile Station (MS) is carried by the subscriber
- The Base Station Subsystem (BSS) controls the radio link with the MS
- The Network Subsystem (NSS) performs the switching of calls between the mobile and other fixed or mobile network users, as well as mobility management.
- Operations and Maintenance Center (OMC) oversees the proper operation and setup.

System Architecture



SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transceiver Station
BSC Base Station Controller
HLR Home Location Register
VLR Visitor Location Register
MSC Mobile services Switching Center
EIR Equipment identity Register
AuC Authentication Center

Mobile Station Components

- Subscriber Identity Module (SIM):
  - Implemented as a smart card
  - Contains the IMSI
  - Contains secret key for authentication
  - Implements personal mobility
- Mobile Equipment (ME):
  - Uniquely identified by IMEI
  - Operational only with SIM card, except for emergency calls

Base Station Subsystem

- Base Transceiver Station (BTS):
  - Contains the radio transceivers for a given cell
  - Handles the radio-link protocols with the Mobile Station
- Base Station Controller (BSC):
  - Manages radio resources for one or more BTS's
  - Provides the connection between the MS and the Mobile service Switching Center (MSC)
  - Manages radio resources, such as channel setup, handoffs, frequency hopping
  - Manages inter-cell handover
  - controls transmitted power

Network Subsystem

- Mobile Services Switching Center (MSC)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)

Mobile Services Switching Center

- Associated with one geographical location
- Responsible for one or more BSCs
- Controls the traffic among all the BSC's
- Provides the connection to the fixed networks (such as the PSTN or ISDN)
- Manages registration, authentication, call establishment and routing
- Provides (together with the HLR and VLR) roaming service

Home Location Register (HLR)

- Stores subscription information and current location of all subscribers in the network
- The location of the mobile is typically in the form of the signaling address of the VLR associated with the MS
- There is logically one HLR per GSM network, although it may be implemented as a distributed database.

Visitor Location Register (VLR)

- Contains selected administrative information from HLR
- Only necessary info. for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR.

Equipment Identity Register (EIR)

- Each mobile station is identified by its International Mobile Equipment Identity (IMEI)
- The EIR is a database that contains the IMEI of all registered mobile equipment

Authentication Center (AuC)

- The AuC protects the network against all unauthorized users.
- It is a protected database which contains all the authentication and encryption information, needed for every mobile user.
- It also stores the secret key held in SIM card that is used in data encryption

Operations and Maintenance Center (OMC)

- The control center for the operation and configuration of the network

- Major activities:
  - Supervision of equipment alarms
  - Rectification of mis-operations
  - Control of software versions
  - Performance management
  - Security management

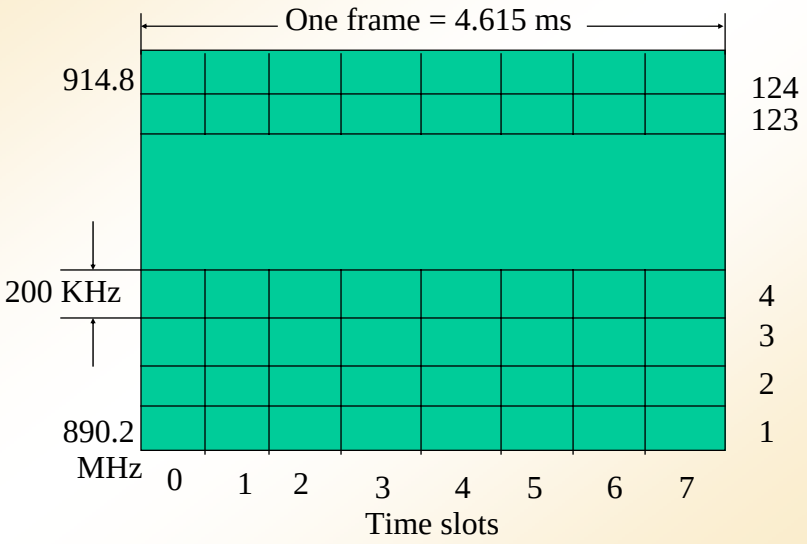
Summary of Radio Characteristics

❑ Access mode	TDMA/FDMA
❑ Radio channel spacing	200 kHz
❑ Uplink/downlink frequency spacing	45 MHz
❑ Uplink/downlink time spacing	3 slots
❑ Number of channels/direction	124 channels
❑ Overall bit rate	270.833 kbps
❑ Overall bit rate per telephony channel	22.8 kbps
❑ Full-rate codec bit rate	13 kbps
❑ Speech codec type	RPE-LTP

Summary of Radio Characteristics

❑ Modulation type	GMSK (BT = 0.3)
❑ Maximum cell radius	30 km
❑ Minimum cell radius	350 m
❑ Maximum date rate	9.6 Kbps
❑ Automatic Cell handover	yes
❑ Roaming	yes
❑ Subscriber identity card	yes
❑ Authentication	yes
❑ Radio interface encryption	yes
❑ Transmitter power control	yes

Physical Channels



Channel Structure

- Each eight burst periods are grouped into a **TDMA frame** (120/26 = 4.615 ms), which forms the basic unit for the definition of logical channels
- One physical channel is one burst period (time slot) per TDMA frame
- Channels are defined by the number and position of their corresponding burst periods.
- Channels can be divided into:
  - **Dedicated Channels**: allocated to a mobile station
  - **Common Channels:** used by mobile stations in idle mode

Logical Channels vs. Physical Channels

- A logical channel is formed by a given slot in the sequence of frames
- A logical channel may be formed by the same slot number in successive frames
- It is not necessary that the same slot in successive frames belong to the same logical channel

Types of Channels

- **Traffic Channels (TCH):** Carry encoded speech or user data
- **Control Channels (CCH):** Carry signaling and synchronization information.
  - Broadcast Control Channels (BCCH)
  - Common Control Channels (CCCH)
  - Associated Control Channels (ACCH)
  - Stand-alone Dedicated Control Channels (SDCCH)

Traffic Channels

- A traffic channel (TCH) is used to carry speech and data traffic
- It is either a full-rate or half-rate
- They have identical formats for both uplink and downlink
- TCH's for the uplink and downlink are separated in time by 3 burst periods
- For this, the MS does not have to transmit and receive simultaneously => simplifying the electronics

Traffic Channels

- Traffic channels are defined using a **26-frame multi-frame**, or a group of 26 TDMA frames
- 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
- **Half-rate** TCHs are also defined
- Eighth-rate TCHs are also specified, and are used for signaling to setup a service. They are called Stand-alone Dedicated Control Channels (SDCCH).

Full-Rate Traffic Channels

- All Full-Rate traffic channels have an overall rate of 22.8 kbps (including channel coding)
- **Full-Rate Speech Channel:** Sends voice at a raw data rate of 13 kbps
- **Full-Rate Data Channel for 9.6 kbps:** Sends data at a raw data rate of 9.6 kbps
- **Full-Rate Data Channel for 4.8 kbps:** Sends data at a raw data rate of 4.8 kbps
- **Full-Rate Data Channel for 2.4 kbps:** Sends data at a raw data rate of 2.4 kbps

Half-Rate Traffic Channels

- Half-Rate TCHs were designed under the expectation of having speech codecs that can provide half the initial rate
- All Half-Rate TCHs have an overall rate of 11.4 kbps
- **Half-Rate Speech Channel:** Sends voice at a raw data rate of 6.5 kbps
- **Half-Rate Data Channel for 4.8 kbps:** Sends data at a raw data rate of 4.8 kbps
- **Half-Rate Data Channel for 2.4 kbps:** Sends data at a raw data rate of 2.4 kbps

Control Channels

Three types of control channels

- Broadcast Channels (BCH)
- Common Control Channels (CCCH)
- Dedicated Control Channels (DCCH)

Broadcast Channels

- Unidirectional (BS to MS)
- Broadcast Control Channel (BCCH): Continually broadcasts, on the downlink, information including BS identity, frequency allocations, and frequency-hopping sequences
- Frequency Correction Channel (FCCH): Carries information used by the MS to synchronize the carrier
- Synchronization Channel (SCH): Used to synchronize the mobile to the time slot structure of a cell.

Common Control Channels

- Unidirectional
- Paging Channel (PCH): Used to alert the mobile station of incoming call (downlink)
- Random Access Channel (RACH): Carries SDCCH allocation requests (uplink)
- Access Grant Channel (AGCH): Used to allocate a frequency, a time burst and a SDCCH following a request on the RACH (downlink).

Stand-Alone Dedicated Control Channel (SDCCH)

- Bidirectional
- Used to negotiate authentication and services requested by the MS before assigning a traffic channel to the MS

Associated Control Channels

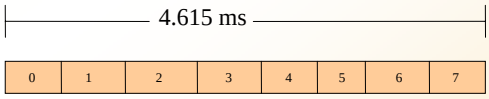
- Bidirectional
- Fast Associated Control Channel (FACCH): Handles urgent massages such as handover and frequency reassignment requests. Assigned if no SDCCH exists by stealing frames from TCH
- Slow Associated Control Channel (SACCH): Carries power control commands on the downlink and signal strength measurements on the uplink. Associated with the TCHs or SDCCH (on the same physical channel)

Call Setup in GSM

- The MS receives information from BS on BCH
- He will be locked to frequency and synchronized to BS through FCCH, SCH and BCCH
- MS requests a call by sending a burst of RACH data using the physical channel the BS is using for broadcast
- BS responds over AGCH and assigns the MS frequency and burst numbers for a SDCCH
- MS and BS exchange info over the SDCCH regarding authentication and services requested
- Meanwhile, MSC starts routing the call to PSTN
- BS assigns a new channel for starting the call

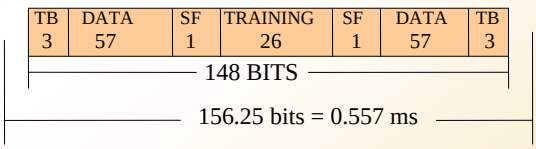
Slot Structure within a TDMA Frame

- Each frame consists of 8 time slots (bursts)
- Duration of a frame is 120/26 ms (approx. 4.614 ms)
- Duration of a time slot is 4.614/8 (approx. 0.577 ms)



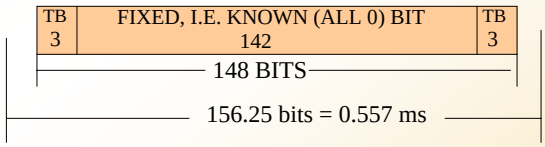
Normal Burst

- Tail Bits (TB): Used to help equalize data bits towards either end of the data stream
- Stealing Flag (SF): Used to indicate a stolen data stream for control channels
- Normal burst could be on any slot



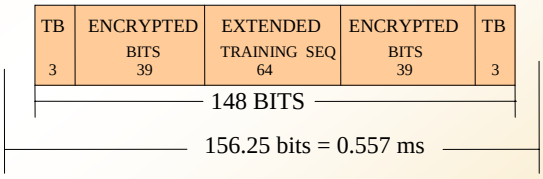
Frequency Correction Burst

- Frequency correction burst must be on slot ‘0’
- Fixed bits (all 0’s) convey no information
- They are used by the MS to acquire RF synchronization (of the carrier)



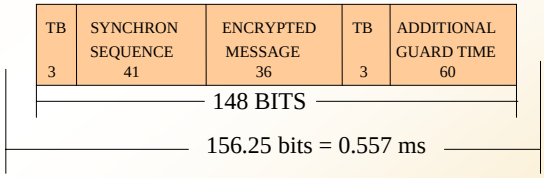
Synchronization Burst

- Synchronization burst must be on slot ‘0’
- ENCRYPTED BITS are used to:
  - Identify the BS
  - Obtain synchronization within the frame/multiframe/superframe structure



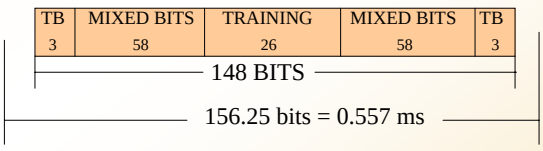
Access Burst

- Access burst must be on slot ‘0’
- Additional (large) guard time for slotted ALOHA related problems
- Additional tail bits for better equalization

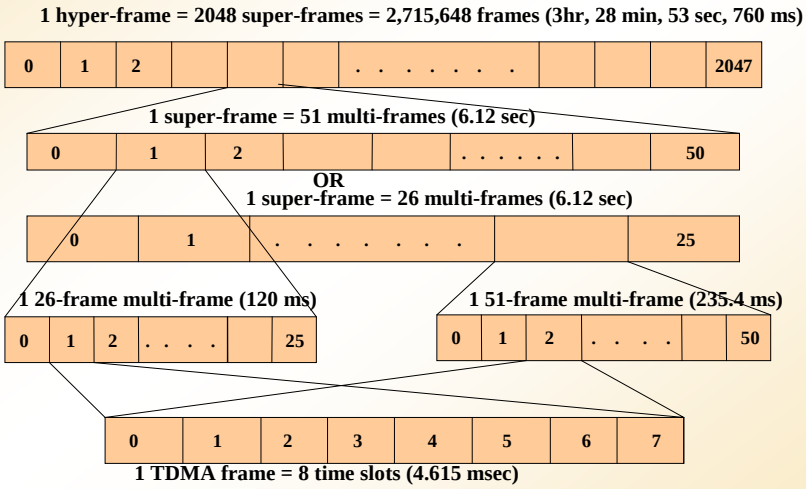


Dummy Burst

Used to fill bursts that are not used in a TDMA frame



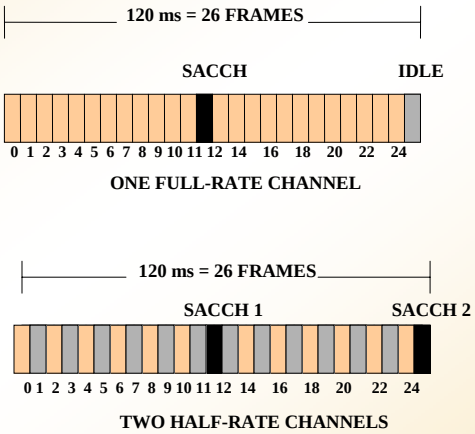
Frame Hierarchy



Multi-frames

- Traffic channels and the SACCH are defined using the 26-frame multi-frame
- Control channels are defined using the 51-fame multi-frame
- The grouping of 26 or 51 frames into one Multi-frame is only a logical grouping
- 26-frame multi-frame duration is exactly 120 ms
- 51-frame multi-frame duration is 235 ms
- Only slot “0” is considered for the 51-frame Multi-frame

26-Frame Multi-Frame Structure (Traffic Channels and SACCH)

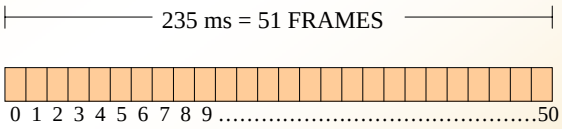


Data Rates

- For Traffic Channels (22.8 Kbps):
  - 114 bits/slot
  - 1 slot / frame
  - 24 frames / 26-frame multiframe
  - 26-frame multiframe / 120 ms
- For SACCH (950 bps)
  - 114 bits/slot
  - 1 slot / frame
  - 1 frame / 26-frame multiframe
  - 26-frame multiframe / 120 ms

51-Frame Multi-Frame Structure (uplink)

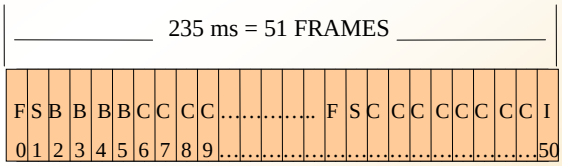
Slot 0 of all frames are random access frames



51-Frame Multi-Frame Structure (downlink)

Slot 0 of all the 51 frames are assigned as:

- F: FCCH
- S: SCH
- B: BCCH
- C: AGCH/PCH
- I: Idle slot



Remarks

- The 51-fames are grouped into 5 sets of ten frames each, with one frame remaining idle
- Each of these sets starts with a FCCH followed by a SCH
- The remaining 8 frames in each set form two blocks of 4
- The first block of the first set is for BCCH while the other 9 blocks are for the PCH and AGCH

Speech Coding

- Traditional speech coding is at 64 Kbps (too high)
- Initially over 20 different proposals from 9 European countries
- Four speech codecs were evaluated:
  - RPE-LPC: Regular-Pulse Excited with Linear Predictive Coding (Germany/Philips)
  - MPE-LTP: Multi-Pulse Excitation with Long Term Prediction (France/IBM)
  - SBC-APCM: Sub-Band Coding/Adaptice PCM (14 sub-bands) (Sweden/Ellemtel)
  - SBC-ADPCM: Sub-Band Coding/ Adaptive Differential PCM (6 sub-bands) (England/British Telecom)

Speech Codec Comparisons

Codec Type	Quality (MOS)	Bit Rate	Complexity (MOPS)
RPE-LPC	3.54	14.77	1.5
MPE-LTP	3.27	13.2	4.9
SBC-APCM	3.14	13.0	1.5
SBC-ADPCM	2.92	15.0	1.9
Analog FM	1.95	NA	NA

Summary of the Codec Aspects

- All codecs have better quality than analog FM
- RPE-LPC had the best quality (15.77 Kbps)
- Modified to be RPE-LTP (13 Kbps)
- Voice activity detection is used to minimize unnecessary transmissions
- Segments of 160 samples are formed every 20 ms
- The codec delivers a block of 260 bits/segment
- The code bit rate is 260 bits / 20 ms = 13 kbps
- Not all bits has the same significance on the voice quality
- Total delay is about 70-80 ms

Discontinuous Transmission

- Speech transmission is suspended in time intervals during a call when the user is not speaking
- This results in:
  - Reduced power consumption at the MS
  - Reduced interference
- A Voice Activity Detector (VAD) is needed to differentiate between speech and noise segments
- **Drawback:** Silent periods are annoying to the listener
- Therefore, comfort noise is introduced at the receiver

Discontinuous Reception

- It is another method used to conserve power at the MS
- The paging channel, used by the BS to signal an incoming call, is structured into sub-channels.
- Each MS 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.

Channel Coding for Speech

- GSM uses convolutional encoding and block interleaving
- The exact algorithms used differ for speech and for different data rates
- The speech codec produces a 260-bit block for every 20 ms speech sample (rate = 13 kbps).
- The bits are 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

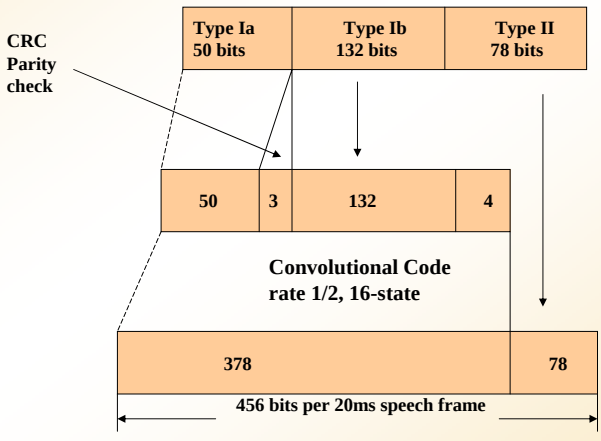
Speech Bits Channel Coding

- Class Ia bits have a 3 bit Cyclic Redundancy Code (CRC) added for error detection.
- 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 rate 1/2 16-state convolutional encode.
- The convolutional encoder thus outputs 378 bits, to which are added the 78 remaining Class II bits, which are unprotected.
- Thus every 20 ms speech sample is encoded as 456 bits, giving a bit rate of 22.8 kbps

Speech Bits Channel Coding

- The 456 bits output by the convolutional encoder are divided into 8 blocks of 57 bits.
- These blocks are transmitted in 8 bursts within 8 consecutive frames
- Since each time-slot burst can carry two 57 bit blocks, each burst carries traffic from two different speech samples.
- This means that two 20-ms speech samples are transmitted over 8 consecutive frames

Speech Bits Channel Coding Scheme



User Data Channel Coding

- User data is encoded using convolutional codes only
- 60 bits of user data are handled every 5 ms
- 240 bits are applied with 4 tailing bits to a rate 1/2 16-state convolutional encoder
- The 488 bits are reduced to 456 bits through puncturing
- Interleaving degrees of up to 19
- The 456 bits are divided into 4 groups each having 114 bits, which are sent over 8 consecutive frames

Channel Coding for Control Channels

- 184 bits are transmitted every 20 ms
- Concatenated codes are used to provide more protection to control data
- The 184 bits are encoded first using a shortened binary cyclic fire code which produces 40 parity-check bits
- The 224 bits from the fire code are applied with 4 tailing bits to a rate 1/2 16-state convolutional code resulting in a total number of 456 bits
- The 456 bits are interleaved onto 8 consecutive frames

Modulation

- Binary transmission is used
- Gaussian Minimum Shift Keying (GMSK) is used for modulation
- GMSK is robust to signal fading and has good spectral efficiency
- The Gaussian filter has $BT = 0.3$
- Separation between frequencies representing 0s and 1s is the minimum
- Δf =135.5 kHz = $1/2T_b = R_b/2$
  => R_b = 270.833/2 kbps

Equalization

- The channel impulse response spreads over a duration greater than one symbol time => ISI
- Adaptive equalization is needed to overcome ISI
- Maximum likelihood sequence estimation (MLSE) is implemented using the Viterbi Algorithm (VA)
- A 16-state VA is used (tradeoff between complexity and performance)
- 26-bit training sequence is used to estimate the channel impulse response

Frequency Hopping

- Successive TDMA frames are transmitted over different RF channels
- Hopping rate = 217 hops/sec = # TDMA frames /sec
- As many as 64 different channels may be used before a hopping sequence is repeated
- Frequency hopping makes use of two types of diversity:
  - frequency diversity (effective for slow mobiles)
  - Interference diversity (randomizes CCI and ACI)

Power Control

- Use of power control reduces power consumption
- It also reduces interference to co-channel cells
- Average hand-held terminal power is 250 mW
- Average vehicle-mounted terminal power is 1 W
- MS's and BTS's operate at the lowest power level that will maintain an acceptable signal quality.

Power Control

- Five classes of mobile stations defined, according to their peak transmitter power, rated at 20, 8, 5, 2, and 0.8 watts.
- Power levels can be stepped up or down in steps of 2 dB (minimum power = 13 dBm = 20 mW).
- The MS measures the signal strength or signal quality and passes the information to the BSC.
- The BSC ultimately decides if and when the power level should be changed

Handoffs

- A Handover is the switching of an on-going call to a different channel or cell.
- Handovers can be initiated by either the MS or the MSC.
- During its idle time slots, the MS scans the BCH 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 Algorithms

- 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.
- The **minimum acceptable performance** algorithm gives precedence to power control over handover
- The **power budget** method gives precedence to handover over power control. It is quite complicated.

Handover Types

- Internal handovers (involves only the BSC):
  - Channels (time slots) in the same cell
  - Cells (BTS's) under the control of the same BSC
- External Handovers (handled by the MSC):
  - Cells under the control of different BSC's, but belonging to the same Mobile services Switching Center (MSC)
  - Cells under the control of different MSC's.

Security Aspects

- Security features address the confidentiality of the subscriber's signaling and data
- Three types of security measures exist in the standard:
  - The SIM is authenticated by the system (against non-registered users)
  - The subscriber identity is protected and never conveyed openly on the network
  - The radio link can be encrypted to avoid eavesdropping

Subscriber Authentication

- A personal IMSI number uniquely identifies subscribers in all GSM networks
- The IMSI number is universal in all PLMNs
- The IMSI has the following information
  - Country
  - Home network in the country
  - HLR
  - address of the subscriber details in the HLR

Subscriber Identity Protection

- Transmission of the subscriber's IMSI openly on the radio channel is strictly limited
- A TMSI number is substituted where possible
- The TMSI number is held in the SIM card and the VLR

Mobile Equipment Security

- Another level of security is performed on the mobile equipment itself, as opposed to the mobile subscriber.
- A list of IMEIs in the network is stored in the Equipment Identity Register (EIR). 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 is not allowed to connect to the network (stolen or not approved)

Security: Based on GSM

- Authentication
  - SGSN uses same principle as MSC/VLR:
  - Get triplet, send RAND to MS, wait for SRES from MS, use Kc
  - MS can't authenticate the network
- Key management in MS
  - Kc generated same way from RAND using Ki as in GSM
- Ciphering
  - Ciphering algorithm is optimized for GPRS traffic ('GPRS - A5')
  - Ciphering is done between MS and SGSN
- User confidentiality
  - IMSI is only used if a temporary identity is not available
  - Temporary identity (TLLI) is exchanged over ciphered link

Data Services in GSM

- Circuit-Switched operation:
  - Uplink and downlink channels allocated for a user for the entire call
  - The user pays for the connection time not for the amout of data
  - Connection establishment time ~ 20 seconds
  - Connection to any modem service in PSTN

Data Services in GSM

- Data transmission rate standardized with only 9.6kbit/s
  - advanced coding allows 14.4 kbit/s
  - not enough for Internet and multimedia applications
- Circuit switched data is not good for:
  - Packet-based protocols such as IP
  - Bursty traffic
  - Unbalanced traffic

HSCSD (High-Speed Circuit Switched Data)

- Bundles several time-slots to get higher AIUR (Air Interface User Rate)
  (e.g., 57.6 kbit/s using 4 slots, 14.4 each)
- Advantage: ready to use, constant quality, simple
- Disadvantage: channels blocked for voice transmission

Packet Service Main Requirements

- Operators:
  - Better utilization of radio resources
  - Simple access to data networks
  - More users can be accommodated
- Users:
  - Lower cost
  - Higher transfer data rates
  - shorter setup time