GSM Network Architecture, Channelisation, Signalling and Call Processing

Dr Bhaskar Ramamurthi
Professor
Department of Electrical Engineering
IIT Madras
Call Routing in Wireline Network

- location of exchange port corresponding to each number fixed
  ⇒ incoming calls to a number have to be routed to a particular exchange
- routing based on number analysis by originating exchange and intermediate exchanges
  ⇒ call routed hop by hop
Call Routing To and From Mobile Network

- Location of mobile telephone not fixed
  - tracked by mobile network (MN)
    - MN must accept incoming calls at one (or more) fixed exchanges (called gateway)
    - routing of call to mobile handled by MN
    - subsequent routing due to movement of mobile handled entirely by MN
      - handovers

- all calls to mobiles with a particular prefix routed to one interconnect point

- outgoing calls can be routed to Interconnect Point nearest the called subscriber
GSM Subsystem Functions

- **MS**: voice, short messages, terminal adapter for fax/modem
  - **Subscriber Identity Module** is the subscriber’s personality
    - handset is “faceless”

- **BTS**: radio endpoint
  - may, or may not, have 13/5.6 kbps ↔ 64 kbps transcoders
    - transcoders may be at BSC or MSC

- **BSC**: controls one or more BTSs
  - channel assignment, handover, power control

- **MSC**: controls BSCs, interface to PSTN, databases
Physical vs Logical Channels on Air Interface

- **Physical Channels**: 
  - one or more time slots in every TDMA frame (e.g. speech data)
  - periodic frames (e.g. signalling)
  - random frames (e.g. call set up)

- can be
  - dedicated to one mobile
  - shared by many mobiles

- **Logical Channels**: pathways created on physical channel for data flow between mobile and other entities of MN
  - **traffic** channel (carries user payload - speech, data)
    - broadcast
    - common control
    - dedicated control
  - **signalling** channel
Multiframe Structure

• 8 time slots per carrier: $576.92 \, \mu s \times 8 = 4.615 \, ms$ frame duration
  
  – slot 0 on one carrier (called **beacon**) is for control
  
  – 156.25 bits/slot

• control slot multiframe = 51 frames

• traffic slot multiframe = 26 frames (120 msec)

• superframe = 26 x 51 frames (6.12 sec)

• hyperframe = 2048 superframes (~ 3.5 hours)
Multiframe Structure (Contd.)

1 hyperframe = 2048 superframes (3h 28m 53s 760 mussec)

1 superframe = 51 traffic multiframes
= 26 control multiframes (6.12 sec)

traffic multiframe = 26 frames

Control multiframe = 51 frames

1 frame = 8 slots

TB: Tail Bits
F: Flag
G: Guard

576.92 μsec
Traffic Channels: Full Rate/Half Rate (TCH/F and TCH/H)

- One slot in every frame of 26-multiframe except in frame numbers (FN) 12 and 25
  \[ \Rightarrow 24 \text{ slots in 120 msec} \Rightarrow 4 \times 57 \times 2 = 456 \text{ bits every 20 msec} \]

- 13 kbps speech coder: 260 bits/20 msec \( \Rightarrow 456 \text{ bits with FEC} \)

<table>
<thead>
<tr>
<th>FN</th>
<th>0</th>
<th>1</th>
<th>. . .</th>
<th>12</th>
<th>13</th>
<th>25</th>
</tr>
</thead>
</table>

- half-rate: use alternate frames for one user
  \[ \Rightarrow \text{second user uses FN 25 for signalling (FN 25 is idle for first)} \]

- 5.6 kbps coder: 112 bits/20 msec \( \Rightarrow 228 \text{ bits with FEC} \)
- downlink frames offset by 3 slots to avoid simultaneous Tx/Rx in MS
Associated Control Channel (ACCH)

- 114 bits every 120 msec for signalling (in FN 12)
- [184 bits (23 bytes) message + 40 parity bits] × 2 due to convolutional code
  \[\rightarrow\] 456 bits \[\rightarrow\] 480 msec, or four 26 - multiframes
  - Slow ACCH ( \[\approx\] 380 bits/sec)

- SACCH is associated with TCH
  \[\rightarrow\] useful after TCH assigned to MS

- SACCH multiframes for different time slots are offset
  \[\rightarrow\] load balancing at BSC

- for fast signalling (e.g. for handover), use FACCH
  - steal 57 bits from TCH in 8 slots
  \[\rightarrow\] set stealing Flag F to indicate this
Simplex Control Channels: Downlink

- in slot 0 of specific beacon carriers (frequencies stored in SIM)
- 51-multiframe : 51 and 26 are mutually prime!
  \[ \Rightarrow \] slots of 51-multiframe will “file past” \textbf{idle slot} of 26-multiframe even when TCH is present
  \[ \Rightarrow \] MS can tune to control slot during idle slots

- slot 0 of beacon is transmitted continuously by BTS
  \[ \Rightarrow \] “empty” bursts are filled with dummy data
Frequency Correction Channel (FCH)

- slot 0 in frames 0, 10, ..........40 of control multiframe (x 51) are for frequency offset estimation and correction

- all-zero data $\rightarrow$ constant frequency
- when MS is turned on, it can hunt continuously for FCH on beacon all carriers in its SIM list
  - when found, look in slot 0 of next frame for Synchronisation Burst
- One beacon per cell
Synchronisation Channel (SCH)

- first data reception after turning MS on
  - long training sequence (64 bits)

- 78 bits containing frame number and **BSIC**
  - can determine slot number (SCH is slot no.1), multiframe, superframe and hyperframe numbers

- **BSIC** is 6 bit “colour code” for the beacon frequency
  - adjacent cells will have different “colours” (BSICs)
Broadcast Paging and Access Grant Channels

- **Broadcast CHannel**
  - used for transmitting IDs of network, BTS (i.e., cell), RACH parameters

- **Paging CHannel**
  - for paging MS during incoming calls
  - paging channel divided into sub-channels (one out of every ‘n’ PCH slots)
    - $\Rightarrow$ MS wakes up less often in idle mode

- **Access Grant CHannel**
  - used to grant access after MS sends its ID on RACH
  - dedicated duplex signalling channel assigned to avoid RACH thereafter for the call
Uplink Simplex Channel: Random Access Channel

- time slot 0 (control slot) of beacon on all frames
- shorter than normal burst: 60 guard bits extra
  - even a burst from distant MS, without timing adjustment for propagation delay, will not overlap into next slot
- first burst from MS to be detected
  - longer training sequence
- 36 bits for encrypted data
- slotted ALOHA random access protocol
  - parameters obtained from BCCH
Dedicated Signalling Channels

• need these when TCH is not (yet) assigned, or, for user service (like messaging) not requiring TCH
  – like TCH, but of lower capacity

• Standalone Dedicated Control CHannel obtained by dividing TCH/F into 8 parts
  – a time slot in four contiguous frames (for 23 bytes message), but a gap of ‘n’ frames before next such occurrence

• SDCCH/8 typically de-allocated if TCH is assigned
  ↦ SACCH becomes available
Cell Broadcast Channel

- **CBCH** consists of 4 occurrence of time slot 0 in 4 contiguous frames in eight 51-multiframes (~ 2 secs)

- 80 byte message can be broadcast to all MS once every 2 sec
GSM Logical Channels : Summary

Traffic channels
- Full-rate TCH/F
- Half-rate TCH/F

Broadcast channels
- Broadcast control BCCH
- Frequency correction FCCH
- Synchronization SCH
- Cell broadcast CBCH
- Paging PCH
- Access grant AGCH
- Random access RACH

Signalling channels
Common control channels
Dedicated control channels

- Broadcast control BCCH
- Frequency correction FCCH
- Synchronization SCH
- Cell broadcast CBCH
- Paging PCH
- Access grant AGCH
- Random access RACH

- Stand alone dedicated control SDCCH
- Fast associated control FACCH
- Slow associated control SACCH
Combining Channels on Carriers

• Half-rate RACH/H, SDCCH/4 possible

• similarly one-third rate PCH/3 and AGCH/3 possible

⇒ allows traffic, common and dedicated control channels on one carrier

Example: small capacity cell with 1 carrier (also the beacon)
slot 0: FCCH, SCH, BCCH, PCH/3, AGCH/3, RACH/H, SDCCH/4
slot 1-7: TCH/F

Example: large capacity cell with 12 carriers (96 slots)
slot 0 of beacon: FCCH, SCH, BCCH, PCH, AGCH, RACH
slot 2,4,6: BCCH, PCH, AGCH (additional)
  5 slots: SDCCH/8
  87 slots: TCH/F
Timing Advance

- Propagation delay: \( \sim 1 \mu s \) per 300 m

- MS synchronised to BTS clock as received by MS \( d \) meters away
  \[ d / 300 \mu s \text{ offset} \]

- Transmission from MS in slot \( n \) received by BTS \( d / 150 \mu s \) late
  \[ \text{can exceed guard time of 8.25 bit durations} \ (8 \times 3.7 \mu s) \]

- BTS measures delay in reception on RACH
  - 68.5 guard bits available in RACH \( \sim 250 \mu \text{sec} \)

- BTS informs MS on SACCH about a delay value \( 0-233 \mu \text{sec} \equiv 0-35 \text{ km} \)
  - sent as number of bit periods \( n \) \([0 - 63]\) \( \equiv \) requires 6 bits to code
Location Area

• should a paging message go on PCH channels of all BTSs?
  ⇒ heavy load on PCH

• can reduce load if MN knows approximate location of MS
  ⇒ concept of Location Area (LA)

• LA is a group of cells
  – all cells must belong to same MSC

• MS listers to LA ID from BCCH
  ⇒ MS (i.e., SIM) registers itself in the LA with MSC

• LA updation also helps MSC determine if call restrictions apply; e.g., in case of roaming
Locking to a BTS (i.e., Cell)

• search beacon frequency (ies) for FCH, SCH and BCCH
  – list of beacons for a LA stored in SIM (from previous locked state)
  – search all frequencies if in new LA when MS is tuned ON

• periodically lock to beacons of neighbouring cells also, i.e., listen to FCH, SCH, BCCH
  – estimate cell quality parameter
  – based on received power level, and some parameters on BCCH related to max Tx power of BTS, etc

• if better cell found in same LA, lock to new cell

• if sufficiently better (with “handicap”) cell found in another LA, lock to it
  ⇒ perform LA update
GSM Signalling Protocol Layers

ISO Layers

Appln.
CM
MM
RRM

Network
LAPD

Datalink
LAPDm

Phy
Radio

MS

Um interface

Abis interface

A interface

CM: call management
MM: mobility management
RRM: radio resource management
SCCP: signal connection control part (SS7)
MTP: message transfer part (SS7)
LAPD: link access protocol -D channel (ISDN)
LAPDm: modified LAPD (GSM)

CM
MM
RRM
SCCP
MTP

CM
MM
RRM
SCCP
MTP

CM
MM
RRM

Radio

64 kb/s

64 kb/s

64 kb/s

64 kb/s
Data Link Layer Protocols

- All protocols are HDLC-like
- LAPD: as in ISDN D-channel link layer
  - 260 byte payload
- LAPm: GSM physical layer provides framing
  \(\Rightarrow\) no need for framing, bit stuffing, etc.
  - 23 byte packets
- MTP: as in SS7
  - 272 byte payload
Signalling

- **MS-BSC**: radio resource management
  - channel assignment, timing advance, power control, handover (MS-BTS only for handover)

- **MS-MSC**: call management

- **BSC-MSC**: handover co-ordination

- **MSC-HLR + Auc**: interrogation of MS location, authentication

- **MS-VLR**: LA update
Circuit-Switched User Data

- for user data between Terminal Adapter of MS and Inter Working Unit of MSC
- Radio Link Protocol provides for ARQ between TA and IWU
- uses the framing provided by GSM physical layer to reduce overhead
- frame size is 240 hits
  - 200 bits of user data
Radio Resource Management

• paging, access request and access grant
  – access always initiated by MS

• allocation and teardown of dedicated signalling and traffic channels
  – dynamic re-configuration of channel pool

• handover management
  – channel quality and adjacent cell measurements by MS
  – co-ordination with MSC

• ciphering/encryption control
  – access initiation always in clear mode
    transition to encrypted mode occurs later

• orchestrated by BSC
  – MSC involved only in handover, due to traffic considerations
Handover Management

- handovers can be due to
  - movement out of cell, i.e., *rescue*, even call break and re-establishment can occur
  - reduction of interference, i.e., *confinement*, or good civic behaviour
  - *traffic* congestion in a cell

- **downlink** measurements by MS on neighbouring cell beacons reported to BSC
  - reports made 1-2 times per second

- BTS makes measurement of MS **uplink** transmission

- MSC + BSC decide handover based on measurements and traffic levels
  - cells involved may be managed by same BSC, different BSCs, even different MSCs.

- MS **pre-synchronised** to neighbouring cells by listening to their SCH

- MS sent handover command with BSIC channel ID, and other parameters (power level, etc)
Mobility Management

• Location area updation and paging control
• HLR contains user registration information
• VLR knows LA of each MS
  – VLR obtains subscriber information from HLR

incoming call to MS always involve a query to HLR

International Mobile Subscriber Identity: a world-wide unique ID
  – MS roaming into new GSM MN provides IMSI to visited MSC/VLR
  query sent to home HLR (whose SS7 address is known, given IMSI)

• Authentication and Encryption involve keys stored in SIM
  – new key computed each time and stored
  – Temporary MSI assigned by VLR in lieu of IMSI
    minimises transmission of IMSI in clear mode
Call Management

• manages call establishment and teardown
  – treats MS-MSC (visited) link as fixed link

• Gateway MSC (GMSC) plays central role for incoming calls to GSM MN

• GSM subscriber’s directory number part of country’s PSTN numbering plan
  – country code+STD code+subscriber number
    \[ \Rightarrow \text{gives SS7 address of GMSC (where HLR is present)} \]

• HLR maps directory number to IMSI and sends query to VLR where MS is registered
  \[ \Rightarrow \text{VLR sends routing information of visited MSC} \]

• GMSC establishes incoming call to visited MSC
  \[ \Rightarrow \text{caller pays till GMSC} \]
  \[ \Rightarrow \text{GSM subscriber pays for call from GMSC to MS} \]
  – could involve a terrestrial link through PSTN
Call Setup by a MS

1. **Setup** (dialed digits + encryption)
2. **Call Proceed** (on SDCCH)
3. **Assignment of TCH (SDCCH)**
4. **Assignment Complete**
5. **Assignment of trunk on A channel**
6. **Assignment Complete** (voice path from MS to MSC)
7. **Alerting**
8. **ringback heard by MS**
9. **Connect**
10. **Connect Acknowledge**
11. **Send info for Outgoing Call (call restriction query)**
12. **Complete Call**
13. **Call Establishment to PSTN no.**
14. **Route Establishment**
15. **Answer**
16. **Set up (dialed digits)**
Intra - MSC Handover

1. Periodic Measurement Report
2. Handover Request with ranking of target BTSs
3. Handover Command + new BSIC, TCH
4. Handover Access (on new TCH)
5. Physical Information
6. Handover Command
7. Handover Request Acknowledge new TCH ID
8. Handover Detected
9. Handover Completed (after timing advance, power control)
10. Release
11. Handover Detected
12. Release Complete
13. Handover Completed
GSM 2G Services

- circuit-switched services
  - voice: full rate (13 kbps) and half-rate (5.6 kbps)
  - data: fax, modem, X.25.....
    - terminal adapter needed at MS, modem/fax/PAD needed at MSC
  - supplementary services common in PSTN (CLIP, call barring, call waiting,......)

- short messages
  - broadcast messages on CBCH
  - 2-way paging on SACCH or SDCCH using Short Message Transport Protocol between MS and SMC-Service Centre at MSC
References

1. *GSM: A System for Mobile Communications*, M. Mouly, and M-B. Pautet, Palaiseau, 1992
