CS 348: Computer Networks

- Mobiles; 5th - 8th Nov 2012

Instructor: Sridhar Iyer
IIT Bombay

Today's class

- Moving on from Ethernet and WiFi to other MAC.

- Suppose

  - Spectrum is not free

    - Network operators have to pay licensing costs.

  - Predominantly voice traffic

- What is the implication of these on MAC design?
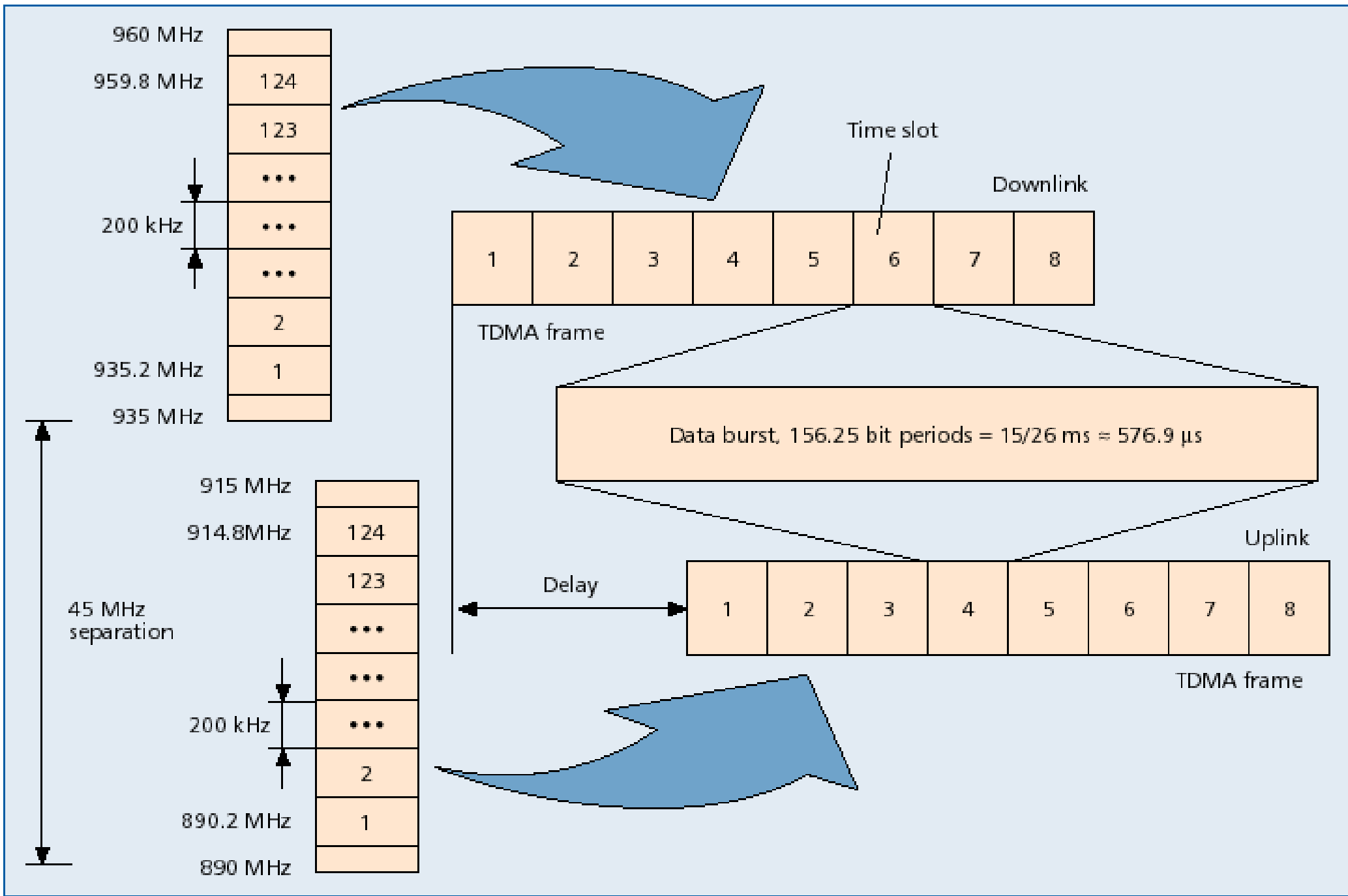
  - Discuss.

Implications

- Efficient utilization of resources is important:

  - Reuse channels; Reduce interference.

  - Spectral Efficiency: No of bits (of useful information) transmitted per second, per Hz.

- Contending for transmission is not suitable:

  - Dedicate resources for the duration of a call.

- So, what is a suitable multiplexing mechanism?

  - Discuss.

GSM MAC (Air Interface)

Communication between mobile and base station.

- Uplink/Downlink of 25 MHz each

    - 890-915 MHz for Up link

    - 935-960 MHz for Down link

- Combination of frequency division and time division multiplexing

    - FDMA: 124 channels of 200 kHz each

    - TDMA: 8 slots per frame

    - Modulation: Gaussian Minimum Shift Keying (GMSK)

960 MHz
959.8 MHz — 124
123
...
200 kHz
...
...
2
935.2 MHz — 1
935 MHz

915 MHz
914.8 MHz — 124
123
...
45 MHz separation
...
200 kHz ...
2
890.2 MHz — 1
890 MHz

Time slot

Downlink

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

TDMA frame

Data burst, 156.25 bit periods = 15/26 ms ≈ 576.9 μs

Uplink

Delay

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

TDMA frame

Activity: Group Discussion

- What is the total number of channels?

- Why 25 MHz? Why not more? Why not less?

- Why separate Uplink and Downlink?

- Why is Uplink band lower than Downlink?

- Why 200 KHz for each channel? Why not less?

- Why 8 time slots per channel? Why not more?

- ...

Key points to note

- 124 * 8 channels per base station area.

- 25 MHz was decided by Govt regulatory bodies.

  - TRAI: Telecom Regulatory Authority of India.

- Uplink and Downlink are separated to avoid co-channel interference (among neighbouring mobiles).

- Uplink band is lower than Downlink to reduce power requirement at mobile.

- Less than 200 KHz for each channel may lead to adjacent channel interference.

- 8 time slots per channel are suitable for handling voice samples at 20 ms.

Question

- GSM is a F/TDMA system.

  - A major issue any TDMA system is synchronization among the participants.

  - The duration of a slot in GSM is 577 μs.

  - Consider 2 mobiles A and B. A is 10 Km away from the base station, while B is 10m away. Suppose A has been allocated frequency channel 5, time slot 2 [f5,t2], while B has been allocated [f5, t3].

  - Can A's transmission overflow into B's slot?

    – What is the propagation delay for A? for B?

- How does one fix this synchronization problem?
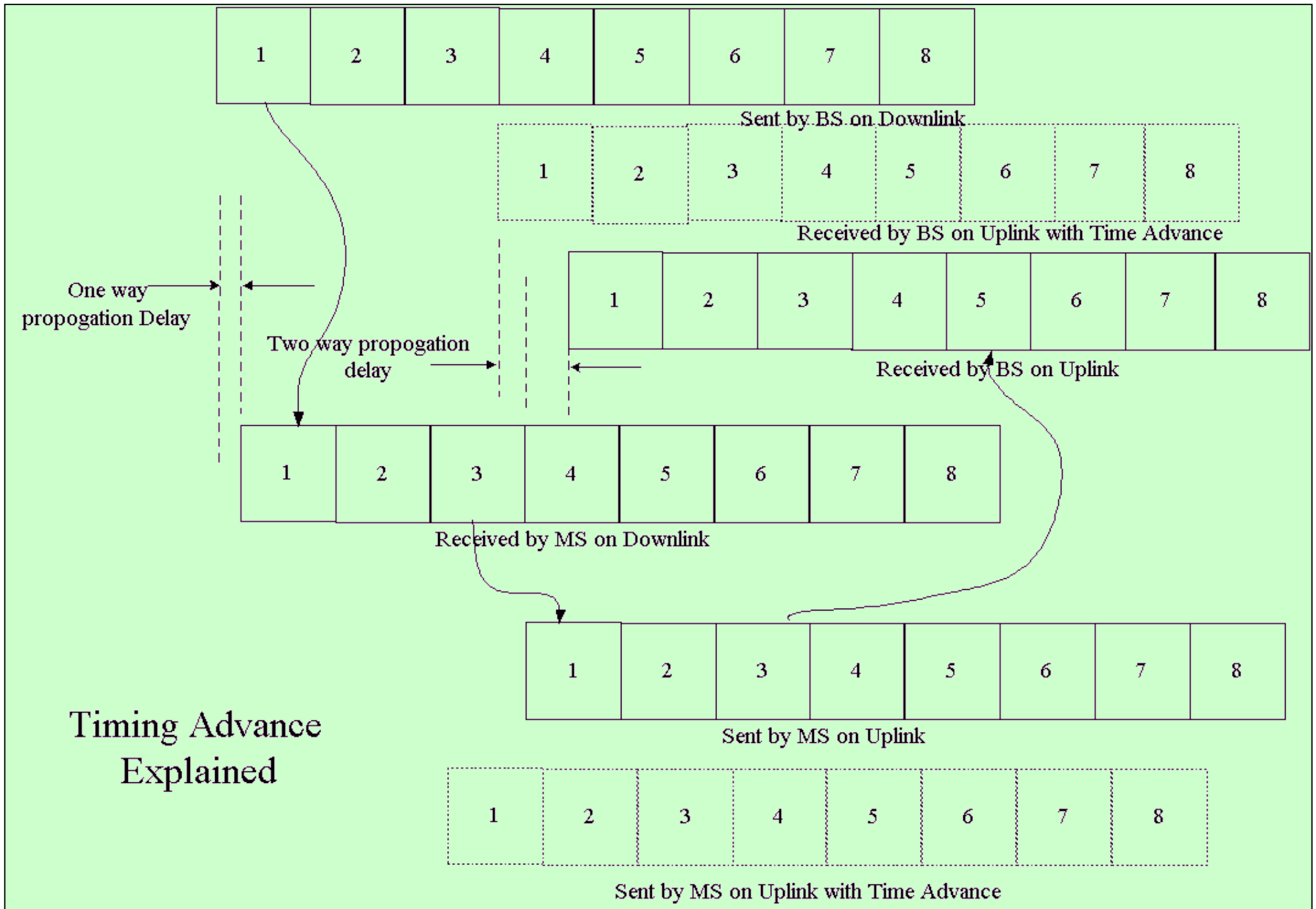
Timing Advance Explained

cs 348 Source: Unknown 9

Adaptive Frame Synchronization

- Also called Timing Advance.

- Advance in Tx time corresponding to propagation delay.

Key idea: Bits should arrive at BS, as per BS's slots.

If A has been allocated [f5, t2], A's first bit should <u>arrive at BS</u> at the start of t2, as per BS's clock.

- 6 bit number used; hence 63 steps.

- 63 bit period = 233 micro seconds (round trip time)

  => 35 Kms is the maximum size of GSM cell.

Clicker Question 1

- In a F/TDMA system, co-channel interference can occur because of:

1. 124 channels in 25 MHz	2. Spatial frequency reuse
3. Multiple users per frequency	4. Separate Uplink and downlink bands

- In GSM, co-channel interference is minimized by:

1. Modulation scheme GMSK	2. Using 200 Khz per channel
3. Using time slots	4. Uplink and downlink separation

Clicker Question 2

- In a F/TDMA system, adjacent-channel interference can occur because of:

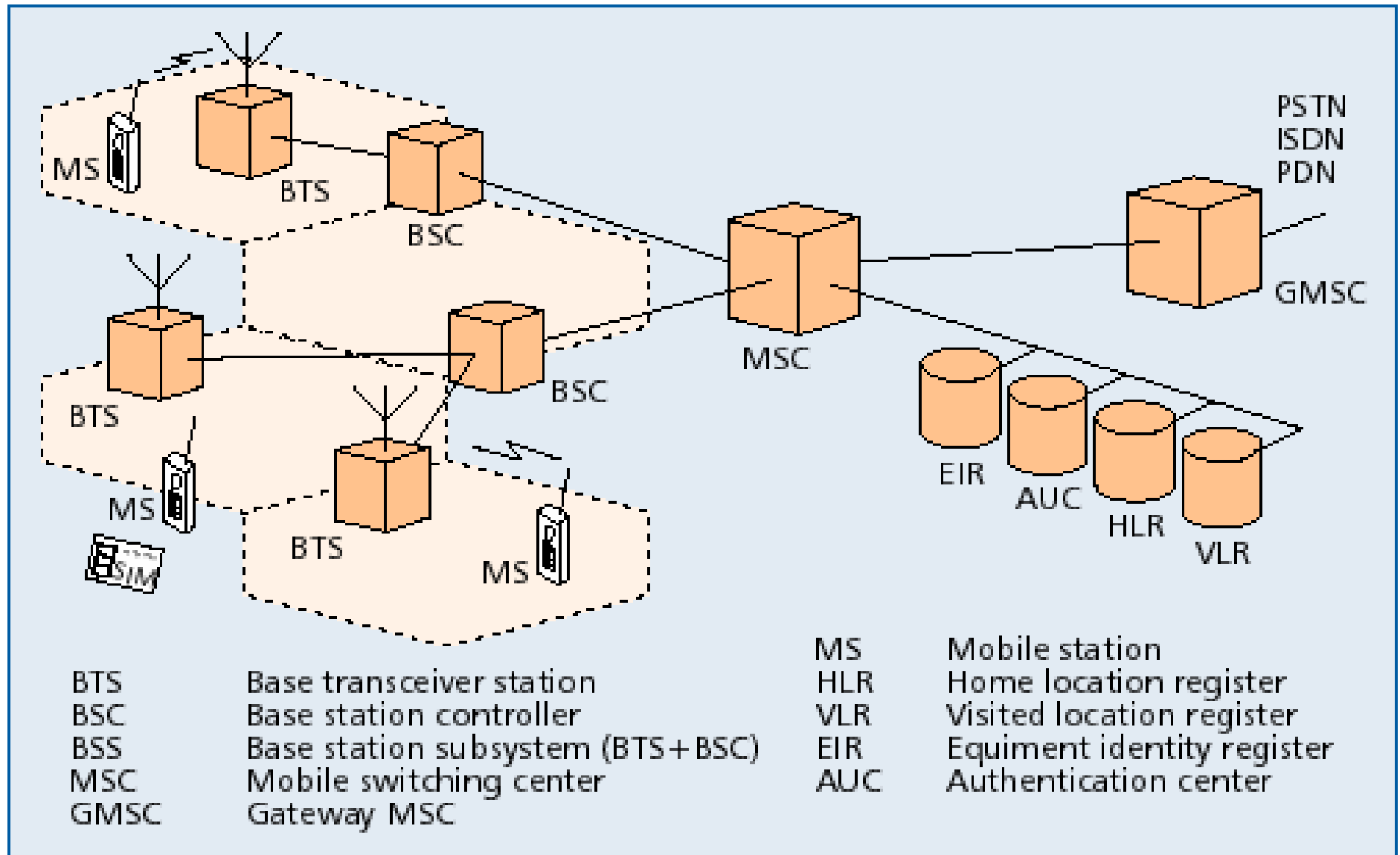| 1. 124 channels in 25 MHz	2. Spatial frequency reuse
3. Multiple users per frequency	4. Separate Uplink and downlink bands

- In GSM, adj-channel interference is minimized by:

1. Modulation scheme GMSK	2. Using 200 Khz per channel
3. Using time slots	4. Uplink and downlink separation

Summary

- GSM is a F/TDMA system:

  - 25 MHz uplink; 25 MHz downlink; 20 MHz separation.

  - 124 channels of 200 KHz each; 8 time slots/channel.

- Co-channel interference:

  - Signals at the same frequencies (co-channel signals) arrive at the receiver from the undesired transmitters (typically in other cells).

- Adjacent-channel interference:

  - Incomplete filtering or poor frequency control leading to unwanted emissions from an adjacent channel.

- Adaptive frame synchronization:

  - Mobiles do timing advance to compensate for 2*T.

GSM Architecture

GSM: System Architecture

PSTN
ISDN
PDN

MS

BTS

BSC

MSC

GMSC

BTS

BSC

BTS

MS

SIM

MS

EIR

AUC

HLR

VLR

BTS	Base transceiver station	MS	Mobile station
BSC	Base station controller	HLR	Home location register
BSS	Base station subsystem (BTS+BSC)	VLR	Visited location register
MSC	Mobile switching center	EIR	Equiment identity register
GMSC	Gateway MSC	AUC	Authentication center

Base Transceiver Station - BTS

- One per cell

- Consists of high speed transmitter and receiver

- Function of BTS

    - Provides two channels

        - Signalling and Data Channel

    - Performs error protection coding for the radio channel

Base Station Controller - BSC

- Controls multiple BTS

- Functions of BSC

  - Performs radio resource management

    - Assigns and releases frequencies and time slots for all the MSs in its area
    - Reallocation of frequencies among cells
    - Hand over protocol is executed here

  - Time and frequency synchronization signals to BTSs

  - Time Delay Measurement and notification of an MS to BTS

  - Power Management of BTS and MS

Mobile Switching Center - MSC

Switching node of a PLMN (Public Land Mobile Network)

- Set up and release of the end-to-end connection.
- Handling mobility and handover during call.
- Charging and account monitoring.

- There can be several MSCs in a PLMN

Gateway MSC -GMSC

- Connects mobile network to a fixed network
  - Entry point to a PLMN
- Usually one per PLMN

- Request routing information from the HLR and routes the connection to the local MSC

Home Location Register - HLR

- For all users registered with the network, HLR keeps the user profile.

- HLR stores details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI, which is the primary key to the HLR record.

- HLR (and SIM) also store the MSISDNs, which are the telephone numbers used by mobile phones to make and receive calls.

- The HLR data is stored for as long as a subscriber remains with the mobile phone operator.

- MSCs exchange information with HLR.

- When MS registers with a new GMSC, the HLR sends the user profile to the new MSC.

Vistor Location Register - VLR

- VLR stores information about all the mobiles that are currently under the MSC which it serves. The most important info is the current LAI (Location Area Identity), i.e.,the BSC under which the MS is currently present.

- VLR stores IMSI, authentication data, MSISDN, services available to the user, HLR address of user.

- Whenever an MSC detects a new MS in its network, in addition to creating a new record in the VLR, it also updates the HLR of the mobile subscriber, apprising it of the new location of that MS.

Authentication Centre - AUC

- AUC authenticates each SIM card that attempts to connect to the GSM core network (typically when the phone is powered on).

- Once successful, the HLR is allowed to manage the SIM and services.

- An encryption key is also generated that is subsequently used to encrypt all wireless communications between the mobile phone and the GSM core network.

- Read more about SIM cloning.

Equipment Identity Register - EIR

- EIR is a database that contains information about the identity of the mobile equipment to prevents calls from stolen, unauthorized or defective mobile stations.

- EIR keeps a list of mobile phones (identified by their IMEI) which are to be banned from the network or monitored.

- EIR allows tracking of stolen mobile phones and also logging of call attempts.

Numbers in GSM

- **IMEI**: International Mobile Equipment Identity

  - Number unique to every handset; can be seen by entering *#06# into the keypad.

  - Used to identify valid devices and stop stolen phones.

- **IMSI**: International Mobile Subscriber Identity

  - Unique number associated with GSM mobile phone users. It is stored in the SIM inside the phone and is sent by the phone to the network.

- **MSISDN**: Mobile Subscriber Integrated Services Digital Network Number

  - Telephone number to the SIM card.

  - MSISDN identifies the SIM, while the IMSI is used to route calls to the subscriber.

Numbers in GSM … contd

- **TMSI**: Temporary Mobile Subscriber Identity

  - To prevent eavesdroppers from identifying and tracking the subscriber on the radio interface, the IMSI is sent as rarely as possible. A randomly-generated TMSI is sent instead.

- **MSRN**: Mobile Station Roaming Number

  - used to route telephone calls from a GMSC to the target MSC.

  - a number temporarily assigned for a mobile terminated call. It is another temporary address that hides the identity of a subscriber.

  - The VLR generates this address on request from the MSC.

  - Not an essential feature in most implementations.

Activity

- Consider the following scenario.

- You and your friend are using the same mobile service provider. Both of you are in IIT campus. You call your friend.

- Specify the steps involved in the call setup. You need to include:

  - Actions that take place at your end (outgoing call).

  - Actions that take place in the network (call setup).

  - Actions that take place at your friend's end (incoming call).

Outgoing call setup

- User keys in the number and presses send

- Mobile transmits request on uplink signaling channel

- If network can process the call, BS sends a channel allocation message

- Network proceeds to setup the connection

- Network activity:

  - MSC determines current location of target mobile using HLR, VLR and by communicating with other MSCs

  - Source MSC initiates a call setup message to MSC covering target area

Incoming call setup

- Target MSC initiates a paging message

- BSs forward the paging message on downlink channel in coverage area

- If mobile is on (monitoring the signaling channel), it responds to BS

- BS sends a channel allocation message and informs MSC

- Network activity:
  - Network completes the two halves of the connection

GSM call routing
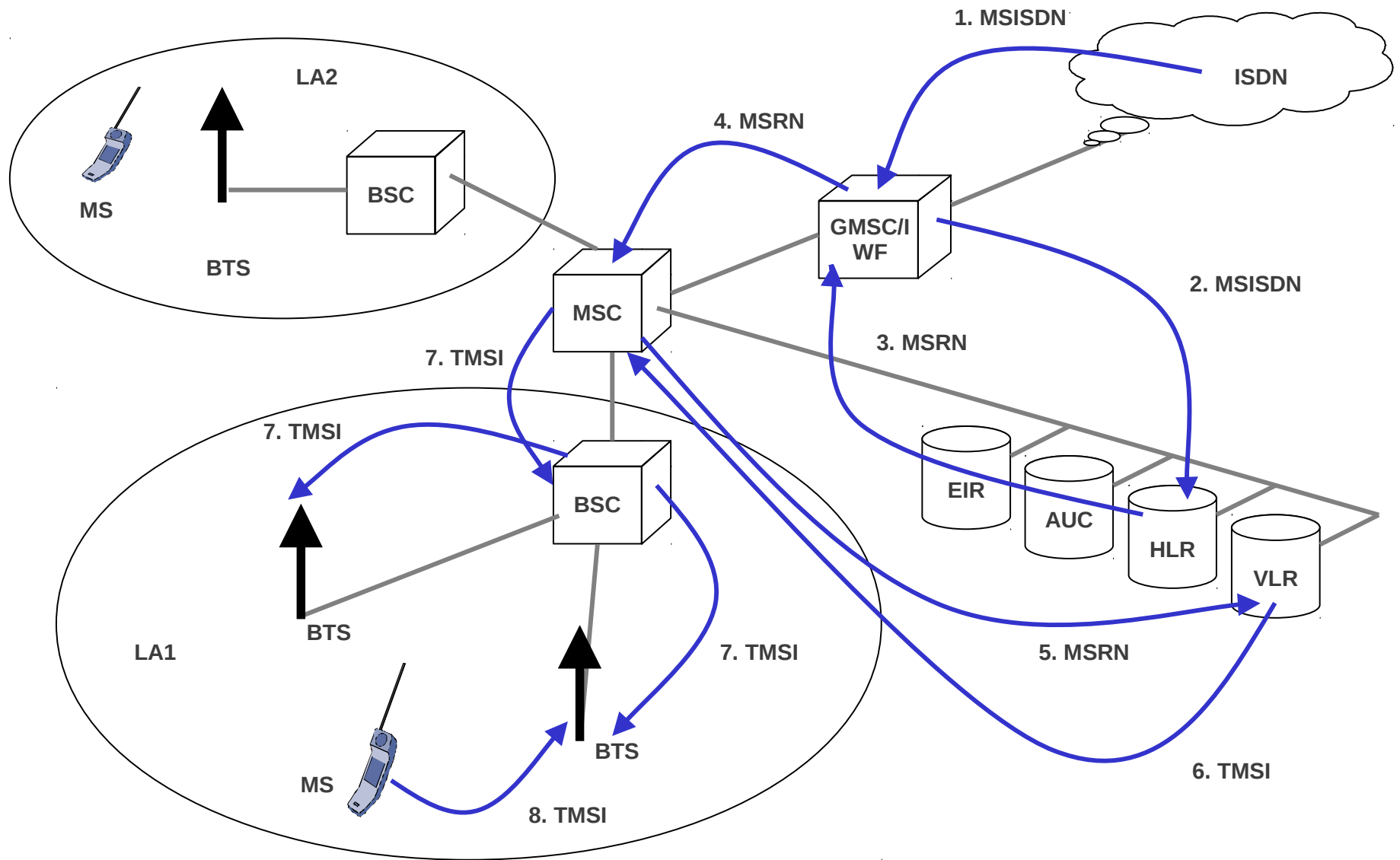
Roaming

- Assume that your mobile is registered in Mumbai. You are currently on roaming in Delhi.

1. What are the HLR/VLR lookup actions when your friend in Mumbai (having a mobile registered in Mumbai) calls you?

2. What are the actions when you want to call your friend?

3. What happens if your friend is also in Delhi?

GSM Air Interface Details

GSM Logical Channels

- Traffic Channel (TCH)

- Signalling Channels
  - Broadcast Channel (BCCH)
  - Common Control Channel (CCH)
  - Random Access Channel (RACCH)
  - Dedicated Control Channel (DCCH)
  - Associated Control Channel (ACCH)
  - Access Grant Channel (AGCH)
  - Paging Channel (PGCH)

Questions

- Why does GSM have/need so many channels?

  - Hint: When should we allocate a traffic channel? Immediately upon request? Just before talk?

- Consider a power-on scenario, when the mobile is just switched on.

  - How does it come to know about BS?

  - How does it let BS know about its presence?

  - How does it initiate a call? etc

- Discuss in groups

```
┌─────────────┐      ┌──────────────────┐      ┌─────────────────────────┐
│  Power On   │─────▶│  Scan Channels,  │─────▶│ Select the channel with │
│             │      │ monitor RF levels│      │ highest RF level among  │
└─────────────┘      └──────────────────┘      │ the control channels    │
                                               └─────────────────────────┘
                                                            │
                          ┌──────────────▶                 ▼
                          │                    ┌─────────────────────────┐
                          │                    │ Scan the channel for the│
                          │                    │ FCCH                    │
                          │                    └─────────────────────────┘
                                                            │
  ┌──────────────────────┐         NO                       ▼
  │ Select the channel   │◀────────────────    ◇ Is FCCH detected? ◇
  │ with next highest Rf  │
  │ level from the        │                              │ YES
  │ control list.         │                              ▼
  └──────────────────────┘                    ┌─────────────────────────┐
             ▲                                 │   Scan channel for SCH  │
             │                                 └─────────────────────────┘
             │               NO                            │
             │◀────────────────────────       ◇ Is SCH detected? ◇
             │                                            │ YES
             │                                            ▼
             │                                 ┌─────────────────────────┐
             │                                 │ Read data from BCCH     │
             │                                 │ and determine is it BCCH?│
             │                                 └─────────────────────────┘
             │                                            │
  ┌──────────────────────┐        NO                      ▼
  │ From the channel data │◀──────────────   ◇ Is the current BCCH ◇
  │ update the control    │                   ◇ channel included?  ◇
  │ channel list          │                              │ YES
  └──────────────────────┘                              ▼
                                                ┌─────────────────────────┐
                                                │ Camp on BCCH and        │
                                                │ start decoding          │
                                                └─────────────────────────┘
```

BCCH

- Broadcast Control Channel (BCCH)↓

  – BTS (Base Station) to MS (Mobile)

  – Radio channel configuration

      ☐ Current cell + Neighbouring cells

  – Synchronizing information

      ☐ Frequencies + frame numbering

  – Registration Identifiers

      ☐ LA + Cell Identification (CI) + Base Station Identity Code (BSIC)

FCCH & SCH

- Frequency Correction Channel
  - Repeated broadcast of Frequency Bursts

- Synchronization Channel
  - Repeated broadcast of Synchronization Bursts
  - Message format of SCH

RACH & SDCCH

- Random Access Channel (RACH)
  - MS to BTS
  - Slotted Aloha
  - Request for dedicated SDCCH

- Standalone Dedicated Control Channel (SDCCH)
  - MS □ BTS
  - Standalone; Independent of Traffic Channel

AGCH & PCH

- Access Grant Channel (AGCH)
  - BTS to MS
  - Assign an SDCCH/TCH to MS

- Paging Channel (PCH)
  - BTS to MS
  - Page MS

SACCH & FACCH

- Slow Associated Control Channel (SACCH)
  - MS BTS
  - Always associated with either TCH or SDCCH
  - Information
    - Optimal radio operation; Commands for synchronization
    - Transmitter power control; Channel measurement
  - Should always be active; as proof of existence of physical radio connection
- Fast Associated Control Channel (FACCH)
  - MS BTS
    - Handover
    - Pre-emptive multiplexing on a TCH, Stealing Flag (SF)

Example: Incoming Call Setup

MS ↓ BSS/MSC	------	Paging request	(PCH)
MS ↑ BSS/MSC	------	Channel request	(RACH)
MS ↓ BSS/MSC	------	Immediate Assignment	(AGCH)
MS ↑ BSS/MSC	------	Paging Response	(SDCCH)
MS ↓ BSS/MSC	------	Authentication Request	(SDCCH)
MS ↑ BSS/MSC	------	Authentication Response	(SDCCH)
MS ↓ BSS/MSC	------	Cipher Mode Command	(SDCCH)
MS ↑ BSS/MSC	------	Cipher Mode Compl.	(SDCCH)
MS ↓ BSS/MSC	------	Setup	(SDCCH)
MS ↑ BSS/MSC	------	Call Confirmation	(SDCCH)
MS ↓ BSS/MSC	------	Assignment Command	(SDCCH)
MS ↑ BSS/MSC	------	Assignment Compl.	(FACCH)
MS ↑ BSS/MSC	------	Alert	(FACCH)
MS ↑ BSS/MSC	------	Connect	(FACCH)
MS ↓ BSS/MSC	------	Connect Acknowledge	(FACCH)
MS ⬍ BSS/MSC	------	Data	(TCH)

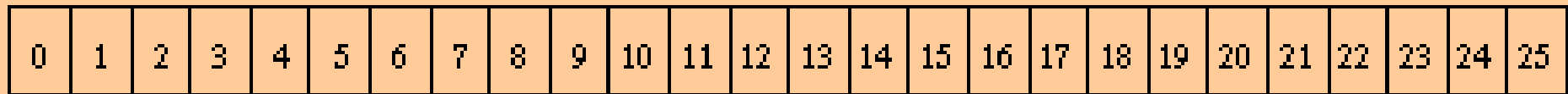# Air Interface: Physical Channel

- Transmission of a frame is called a Burst
  - It is the building unit of a physical channel
  - Types of bursts: Normal, Synchronization, Frequency Correction, Access, Dummy.

- Normal Burst
  - 2*(3 head bit + 57 data bits + 1 signaling bit) + 26 training sequence bit + 8.25 guard bit

  - Used for all except RACH, FSCH & SCH

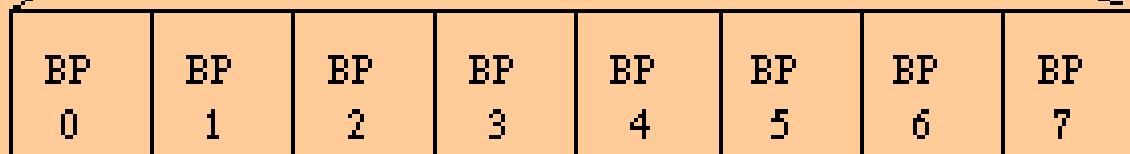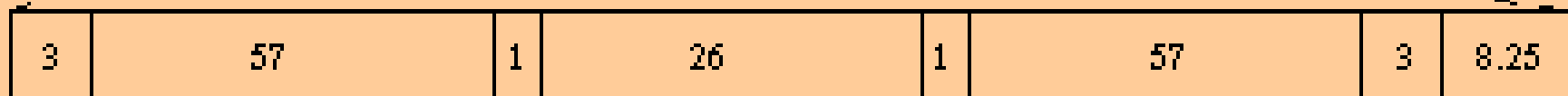Frames 0 – 11 : TCH   Frame 12 : SACCH   Frames 13 – 24 : TCH   Frame 25 : Unused

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

26 – frame multiframe
Duration: 120 ms

| BP 0 | BP 1 | BP 2 | BP 3 | BP 4 | BP 5 | BP 6 | BP 7 |

TDMA frame
Duration: 60/13 ms

| 3 | 57 | 1 | 26 | 1 | 57 | 3 | 8.25 |

Tail bits | Data bits | Stealing bit | Training sequence | Stealing bit | Data bits | Tail bits | Guard bits
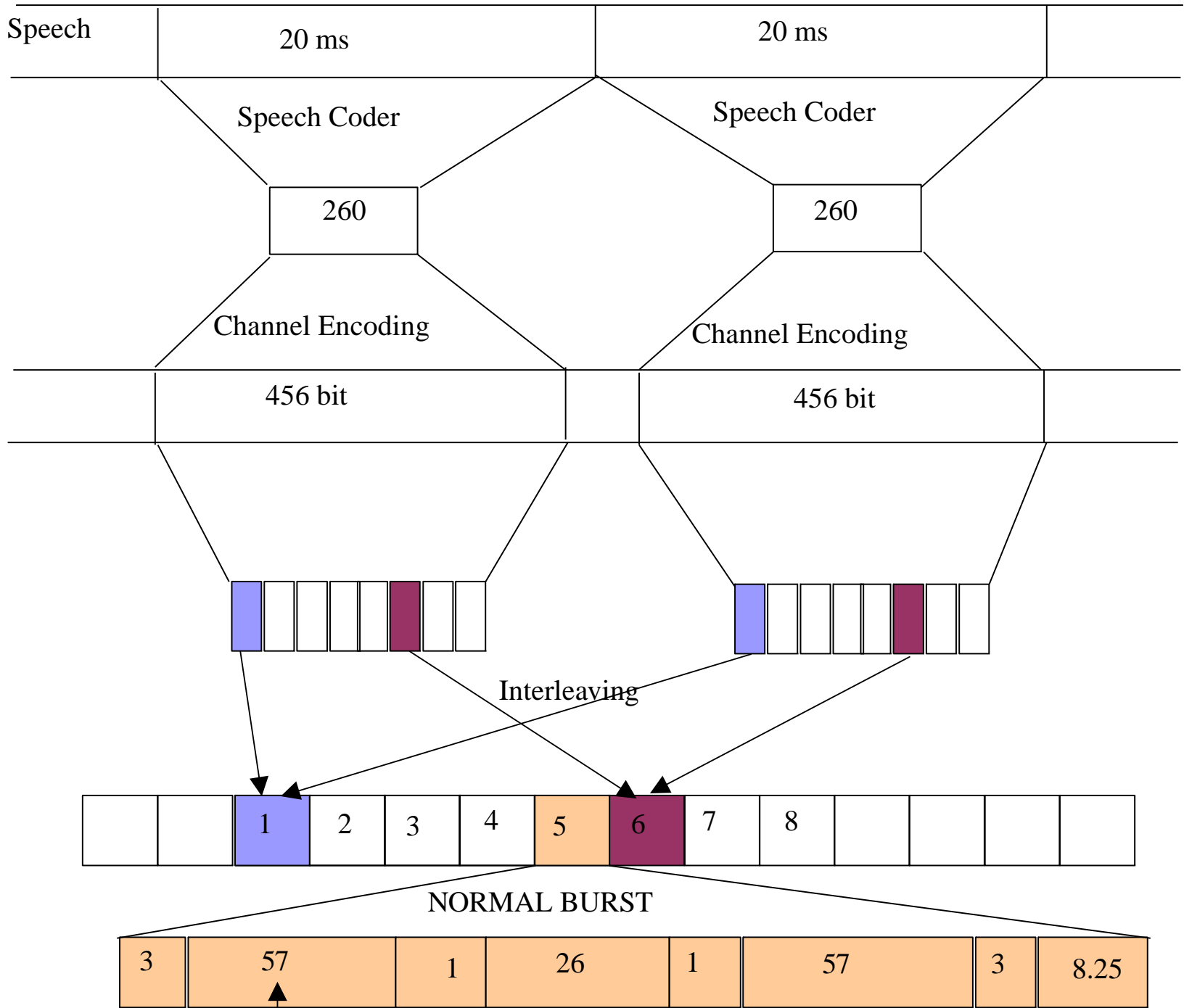
Normal burst
Duration 15/26 ms

Source: Unknown
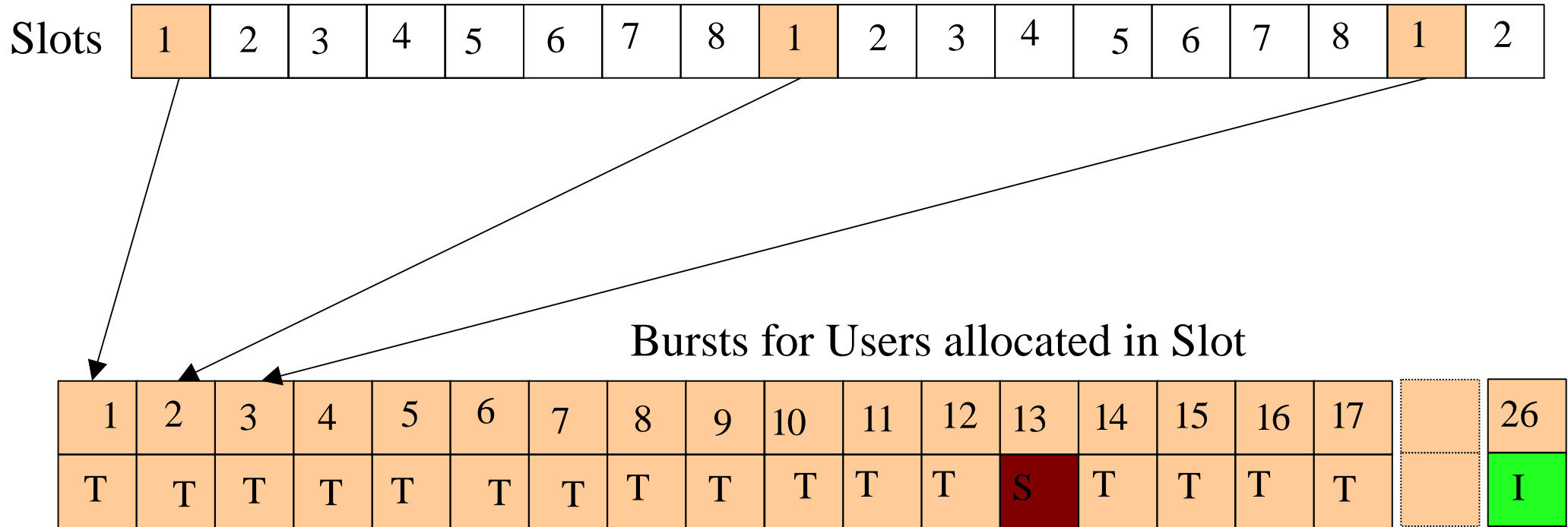
Traffic Channel

- Transfer either encoded speech or user data
- Bidirectional

- Full Rate TCH
  - Rate 22.4 kbps

- Half Rate TCH
  - Rate 11.2 kbps

Full Rate Speech Coding

- Speech Coding for 20ms segments
  - 260 bits at the output ; Effective data rate 13kbps
- Unequal error protection
  - 182 bits are protected
  - 78 bits unprotected
- Channel Encoding
  - Codes 260 bits into (8 x 57 bit blocks) 456 bits
- Interleaving
  - 2 blocks of different set interleaved on a normal burst (save damages by error bursts)

Speech

20 ms

20 ms
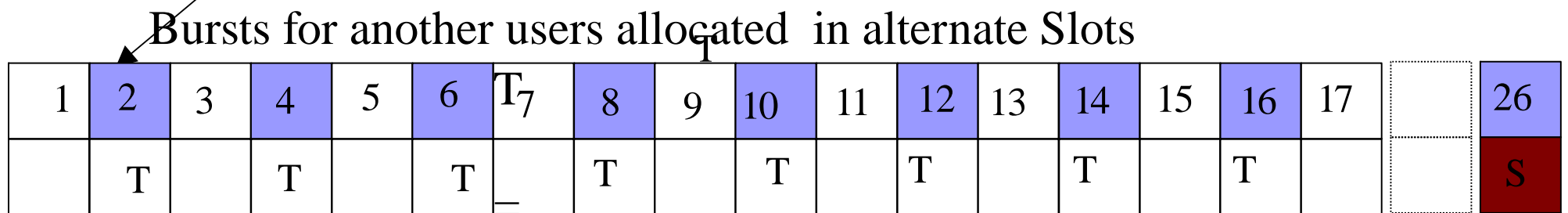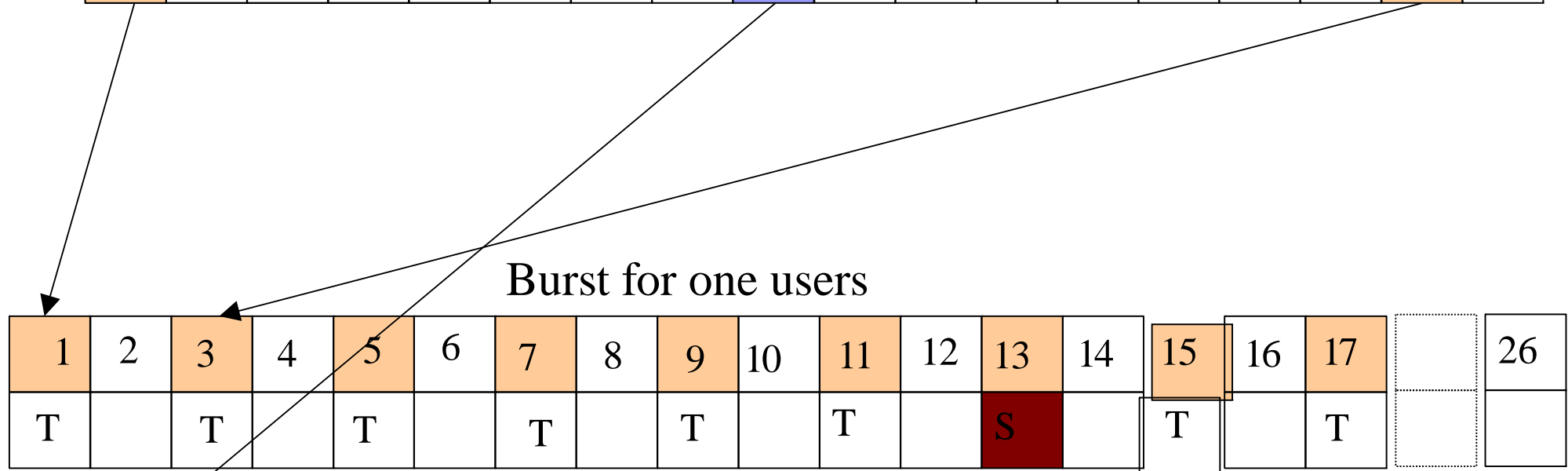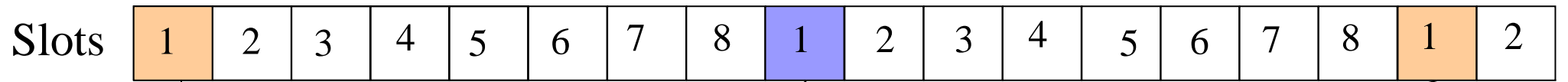
Speech Coder

Speech Coder

260

260

Channel Encoding

Channel Encoding

456 bit

456 bit

Interleaving

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | | | |

NORMAL BURST

| 3 | 57 | 1 | 26 | 1 | 57 | 3 | 8.25 |

Out of first 20 ms

Out of second 20ms

Traffic Channel Structure for Full Rate Coding

Slots

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 |

Bursts for Users allocated in Slot

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17		26
T	T	T	T	T	T	T	T	T	T	T	T	S	T	T	T	T		I

T = Traffic
S = Signal(contains information about the signal strength in neighboring cells)

Slots

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 1 | 2 |

Burst for one users

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | | 26 |
| T | | T | | T | | T | | T | | T | | S | | T | | T | | |

Bursts for another users allocated in alternate Slots

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | | 26 |
| | T | | T | | T | | T | | T | | T | | T | | T | | | S |

Traffic Channel Structure for Half Rate Coding

Note on error protection mechanism

- Error protection – happens at 3 levels
  - Redundancy – 260 bits coded into 456 bits.
  - 456 bits (57*8): create row-wise; transmit column-wise => burst errors look like random errors
  - Block interleaving for further protection (slide 20).

- Why is this done?
  - Spectrum is a scarce resource!
  - No re-transmission schemes.

GSM: Vocoders

- Ever noticed that your friend's voice sounds different on a landline versus a mobile?

- Why does this happen?

- vocoders; speech synthesis; comfort noise

- Your mobile is doing a lot of work!