Mobile Communications

GSM

Manuel P. Ricardo

Faculdade de Engenharia da Universidade do Porto

Acknowledgements

- These slides are based on the slides developed by
  - » Prof. Jochen Schiller
    - – Slides from the book “Mobile Communication: Wireless Telecommunication Systems”
    - – http://www.jochenschiller.de
  - » Prof. Mário Jorge Leitão
    - – http://www.fe.up.pt/~mleitao/

- *What are the main network elements of GSM?*
- *What are the GSM addresses?*
- *How is the data transmitted over the air interface?*
- *What are the main logical channels?*
- *What is the GSM protocol stack for signalling?*
- *How is a Mobile Terminated Call processed?*
- *How is a Mobile Initiated Call processed?*

GSM - Overview

- Formerly: Groupe Spéciale Mobile (founded 1982)
- Now: Global System for Mobile Communication
- Pan-European standard
  - » ETSI, European Telecommunications Standardisation Institute
- Seamless roaming within Europe possible
- Many providers all over the world

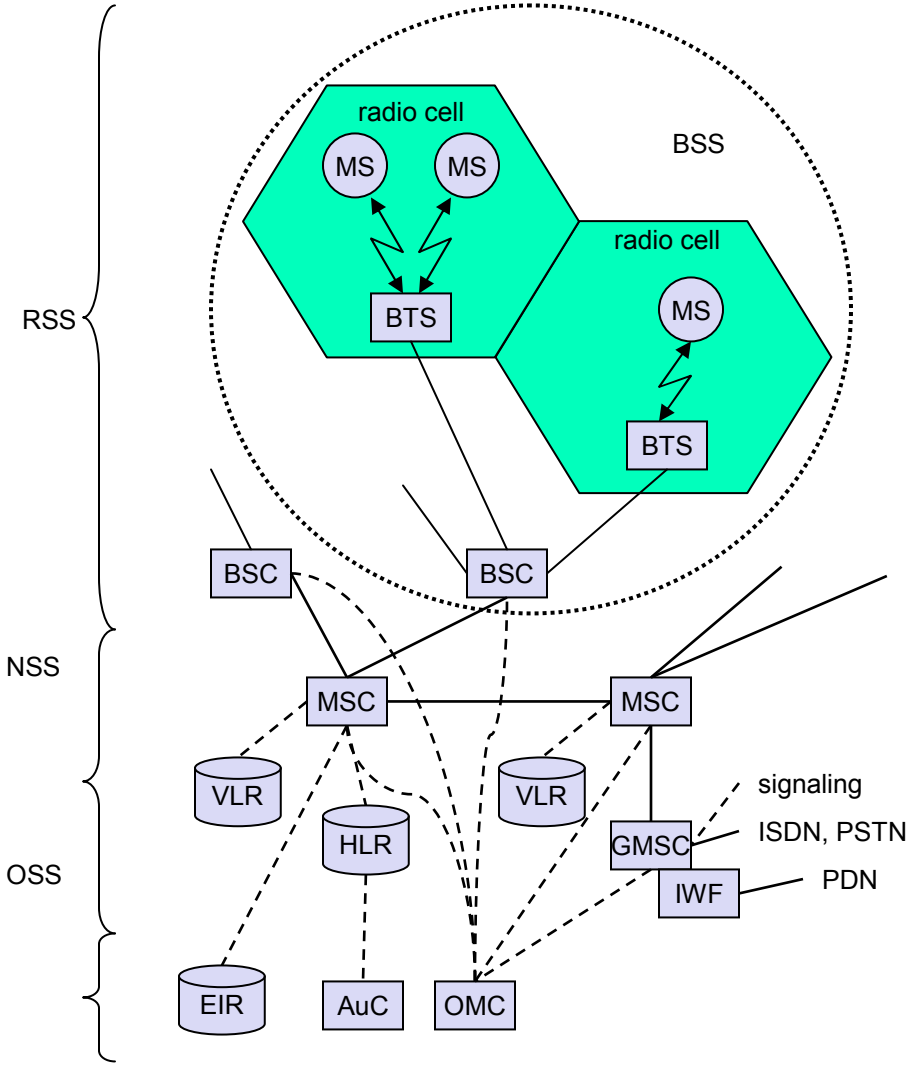
Services

- Basic services
  - » voice services, data services, short message service
- Additional services
  - » emergency number, group 3 fax
- Supplementary services
  - » identification: forwarding of caller number
  - » suppression of number forwarding
  - » automatic call-back

Basic Services

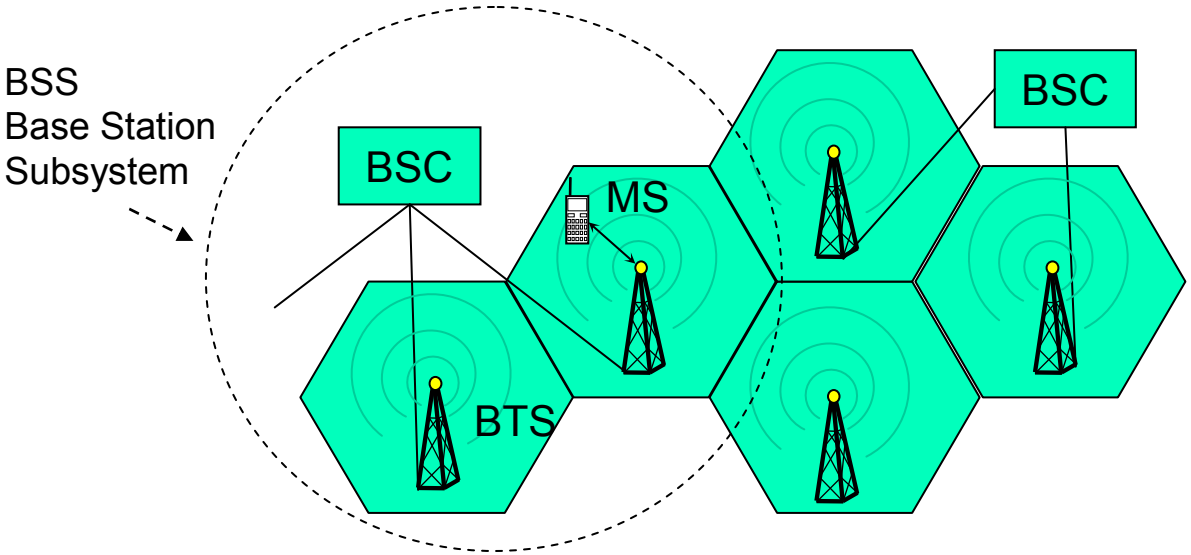
- Voice services (speech coding with protection)
  - » full rate: 13 / 12.2 kbit/s (original coder / enhanced full rate coder)
  - » half rate: 5.6 kbit/s (enhanced half rate coder)
- Data services (coding with different levels of protection)
  - » full rate: 9.6 / 4.8 / 2.4 kbit/s
  - » half rate: 4.8 / 2.4 kbit/s
- Enhanced data services → GPRS (General Packet Radio Service)
  - » various rates (typically up to 53.6 kbit/s)

Public Land Mobile Network (PLMN)



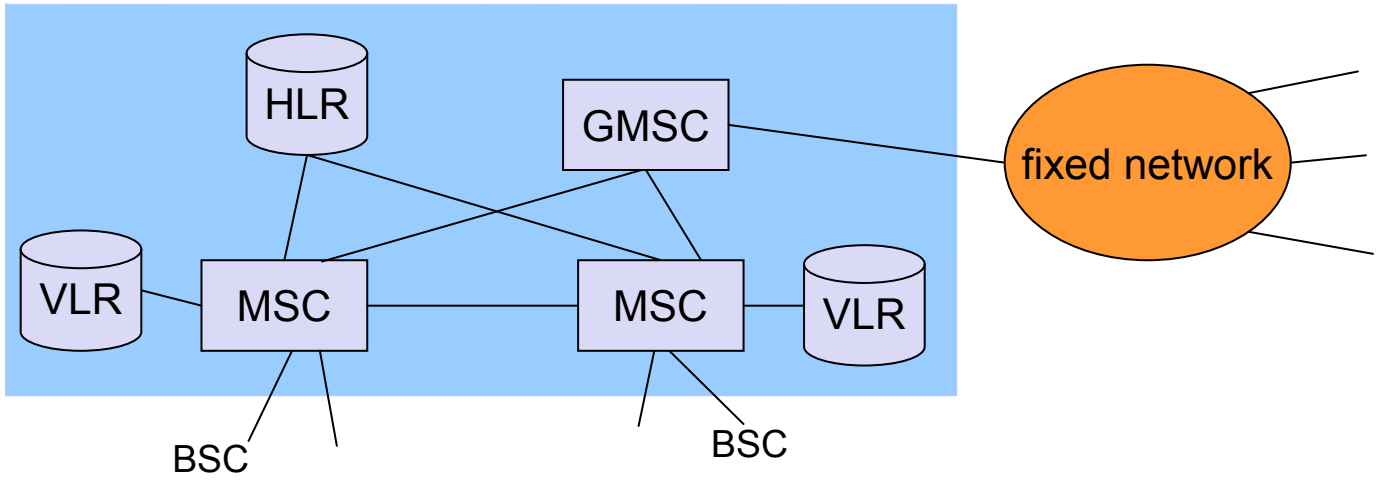
GSM Architecture – Radio Subsystem (RSS)

- MS - Mobile Station
  - Mobile terminal equipment
- BTS- Base Transceiver Station
  - Transmitter, receiver and antennas
- BSC - Base Station Controller
  - Management of several BTS and MS



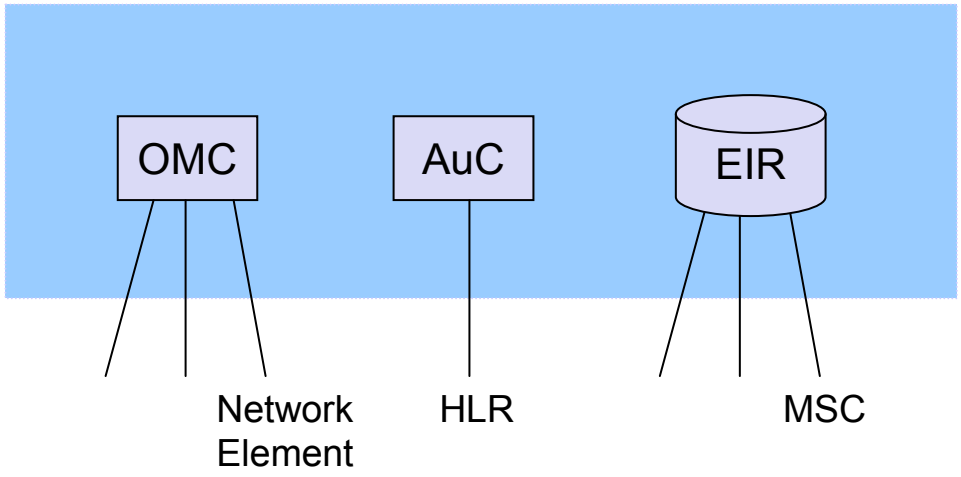
GSM Architecture – Network Subsystem (NSS)

- Switching, mobility management,
- Interconnection to other networks, system control
- MSC - Mobile Switching Centre: Management of connections
- HLR - Home Location Register: Associated to each PLMN
- VLR - Visitor Location Register: Associated to each MSC
- GMSC - Gateway MSC: MSC providing interconnection to other networks

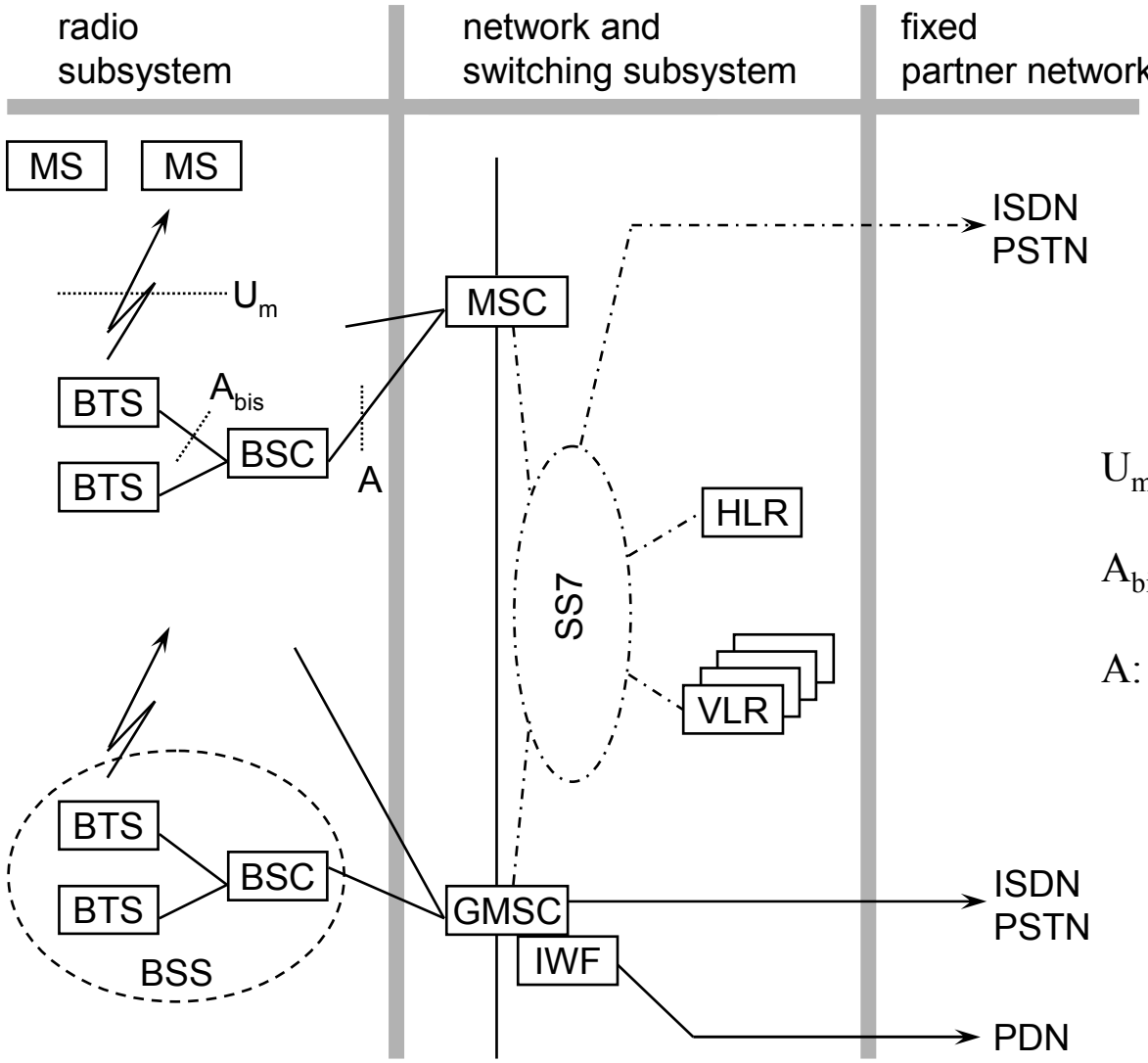


GSM Architecture – Operation Subsystem (OSS)

- Centralized operation, management and maintenance of GSM subsystems
- OMC - Operation and Management
  - Control of the radio and network subsystems
- AuC - Authentication Centre
  - Security functions
- EIR - Equipment Identity Register
  - Mobile station registration



GSM Architecture - Interfaces



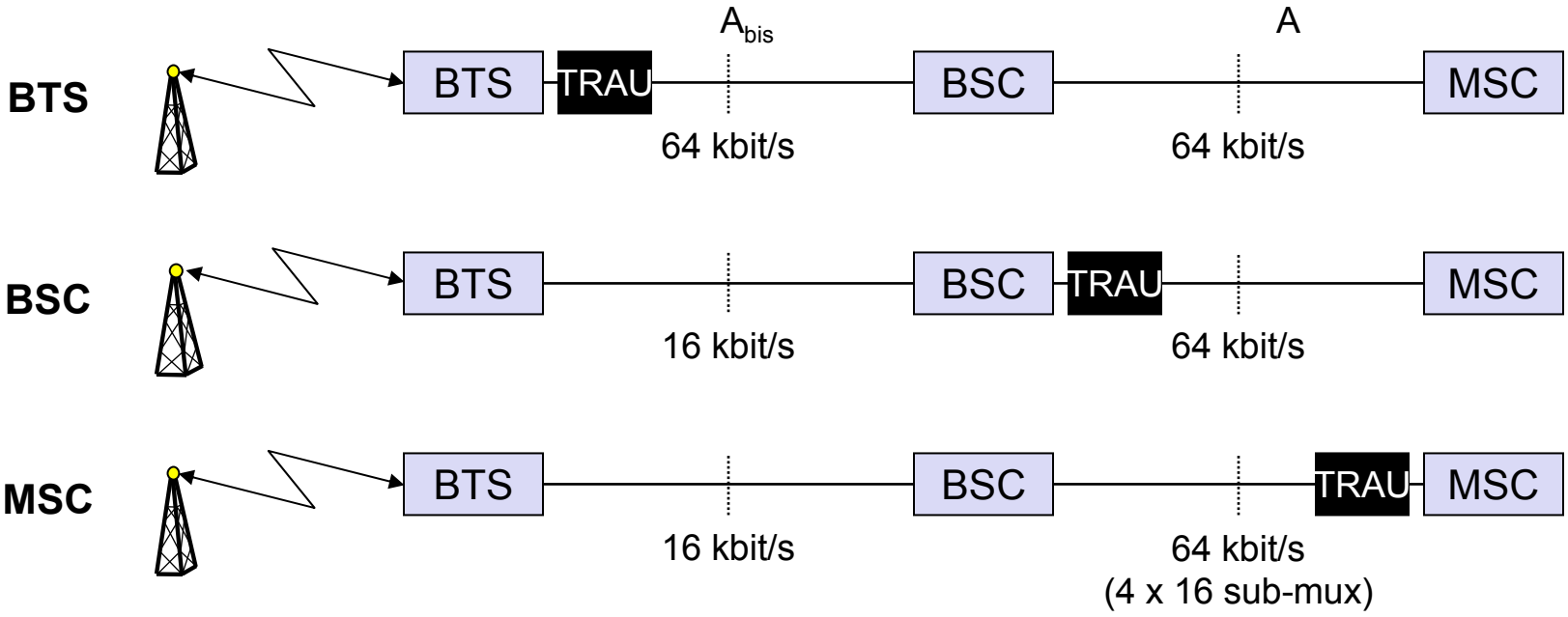
U_m : radio interface

A_{bis} : 16/64 kbit/s user channels

A: 64 kbit/s user channels

Voice Transcoding and Rate Adaptation

- Need for transcoding and rate adaptation
  - » BTS - 13 kbit/s air-interface (original coder)
  - » MSC - 64 kbit/s ISDN type switching (PCM, A-law)
- 3 options for Transcoding and Rate Adapter Unit (TRAU)



Mobile Addresses

- Several mobile numbers are needed
  - » IMSI - International Mobile Subscriber Identity
    - Mobile Country Code (MCC) + Mobile Network Code (MNC) + Mobile Subscriber Identification Number (MSIN)
    - uniquely identifies the user (SIM card)
  - » TMSI - Temporary Mobile Subscriber Identity
    - 32 bits
    - local number allocated by VLR; may be changed periodically
    - hides the IMSI over the air interface; transmitted instead of IMSI
  - » MSRN - Mobile Station Roaming Number
    - Visitor Country Code (VCC) + Visitor National destination Code (VNDC) + Current MSC code + temporary subscriber number
    - generated by VLR for all visiting users
    - helps HLR to determine current location area
    - hides the IMSI inside the network

SIM Card (Subscriber Identity Module)

- Uniquely associated to a user
- Stores user and location addresses
  - IMSI - International Mobile Subscriber Identity
  - TMSI - Temporary Mobile Subscriber Identity
  - LAI - Location Area Identification
- Supports authentication and encryption mechanisms
  - PIN - Personal Identity Number
  - PUK - PIN Unblocking Key
  - Ki - subscriber secret authentication key
  - A3 - authentication algorithm
  - A8 - cipher key generation algorithm
- Contains personal data
  - list of subscribed services
  - RAM for user directory

Base Transceiver Station, Base Station Controller

- BTS comprises radio specific functions
- BSC is the switching center for radio channels: switches calls from MSC to correct BTS

Functions	BTS	BSC
Management of radio channels		X
Frequency hopping (FH)	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption and decryption	X	X
Paging	X	X
Uplink signal measurements	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

Mobile Switching Center - Functions

- Switching of 64 kbit/s channels
- Paging and call forwarding
- Termination of SS7 (signaling system no. 7)
- Mobility specific signaling
- Location registration and forwarding of location information
- Generation/ forwarding of accounting and billing information

Home Location Register (HLR)

- Central master database
  - » data from every user that has subscribed to the operator
  - » one database per operator
  - » may be replicated
- Subscriber data
  - » IMSI - International Mobile Subscriber Identity
  - » List of subscribed services with parameters and restrictions
- Location data
  - » current MSC/VLR address

Visitor Location Register (VLR)

- Local database
  - » data about all users currently in the domain of the VLR
  - » includes roamers and non-roamers
  - » associated to each MSC
- Subscriber identity
  - » IMSI - International Mobile Subscriber Identity
- Temporary location
  - » LAI - Location Area Identification
- Temporary addresses
  - » MSRN - Mobile Station Roaming Number
  - » TMSI - Temporary Mobile Subscriber Identity

GSM Location / Mobile Addresses - Summary

HLR - Home Location Register	
Permanent	IMSI - International Mobile Subscriber Identity
Temporary	MSRN - Mobile Station Roaming Number

VLR - Visitor Location Register	
Permanent	IMSI - International Mobile Subscriber Identity
Temporary	LAI - Location Area Identification MSRN - Mobile Station Roaming Number TMSI - Temporary Mobile Subscriber Identity

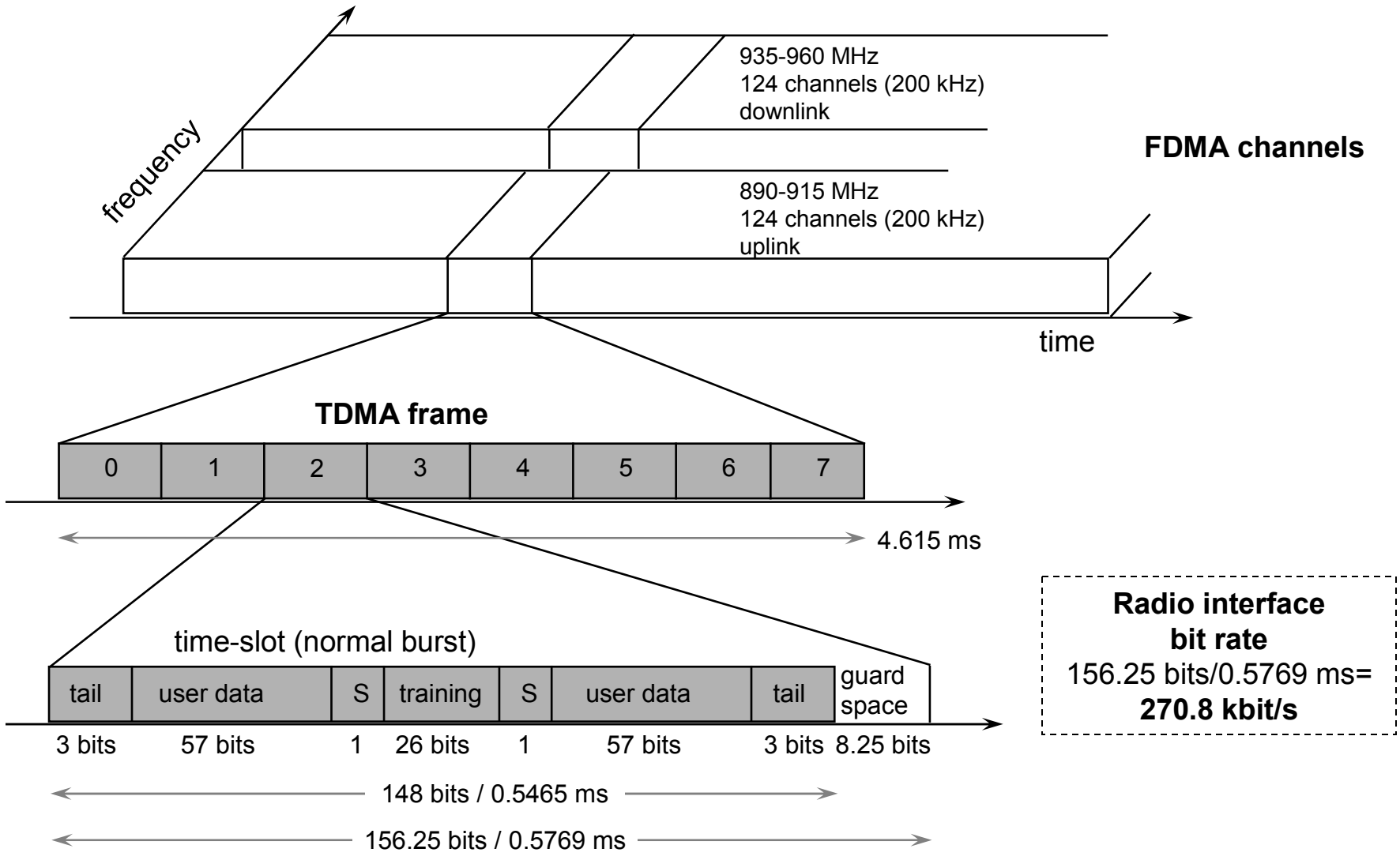
SIM - Subscriber Identity Module	
Permanent	IMSI - International Mobile Subscriber Identity
Temporary	LAI - Location Area Identification TMSI - Temporary Mobile Subscriber Identity

AuC, EIR

- Authentication Center (AuC)
  - associated to HLR
  - search key: IMSI
  - supports authentication and encryption mechanisms
    - Ki - subscriber secret authentication key
    - A3 - authentication algorithm
    - A8 - cipher key generation algorithm

- Equipment Identity Register (EIR)
  - stores mobile stations IMEI (International Mobile Equipment Identity)
  - white list - mobile stations allowed to connect without restrictions
  - black list - mobile stations locked (stolen or not type approved)
  - gray list - mobile stations under observation for possible problems

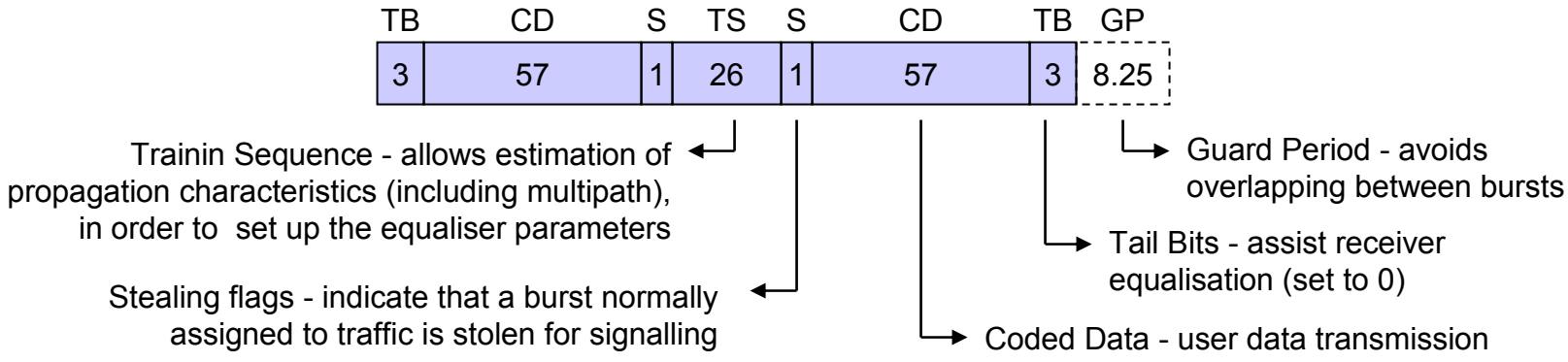
GSM - TDMA/FDMA



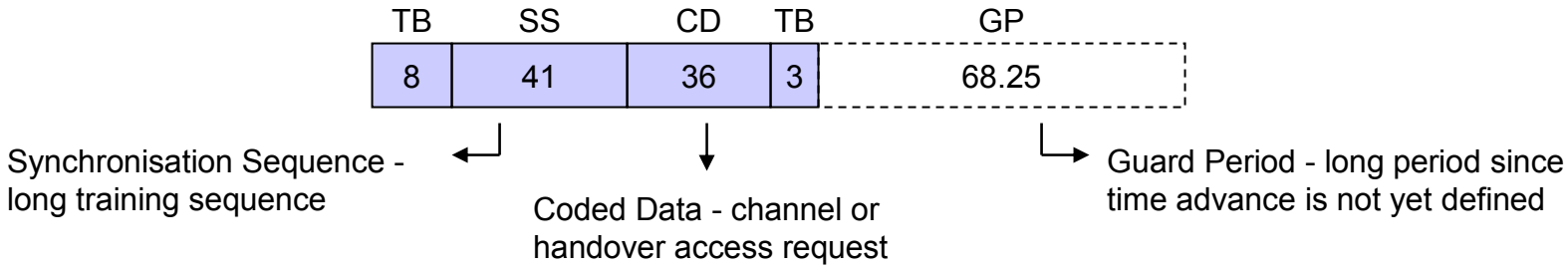
Radio interface bit rate
156.25 bits/0.5769 ms=
270.8 kbit/s

Burst Structures

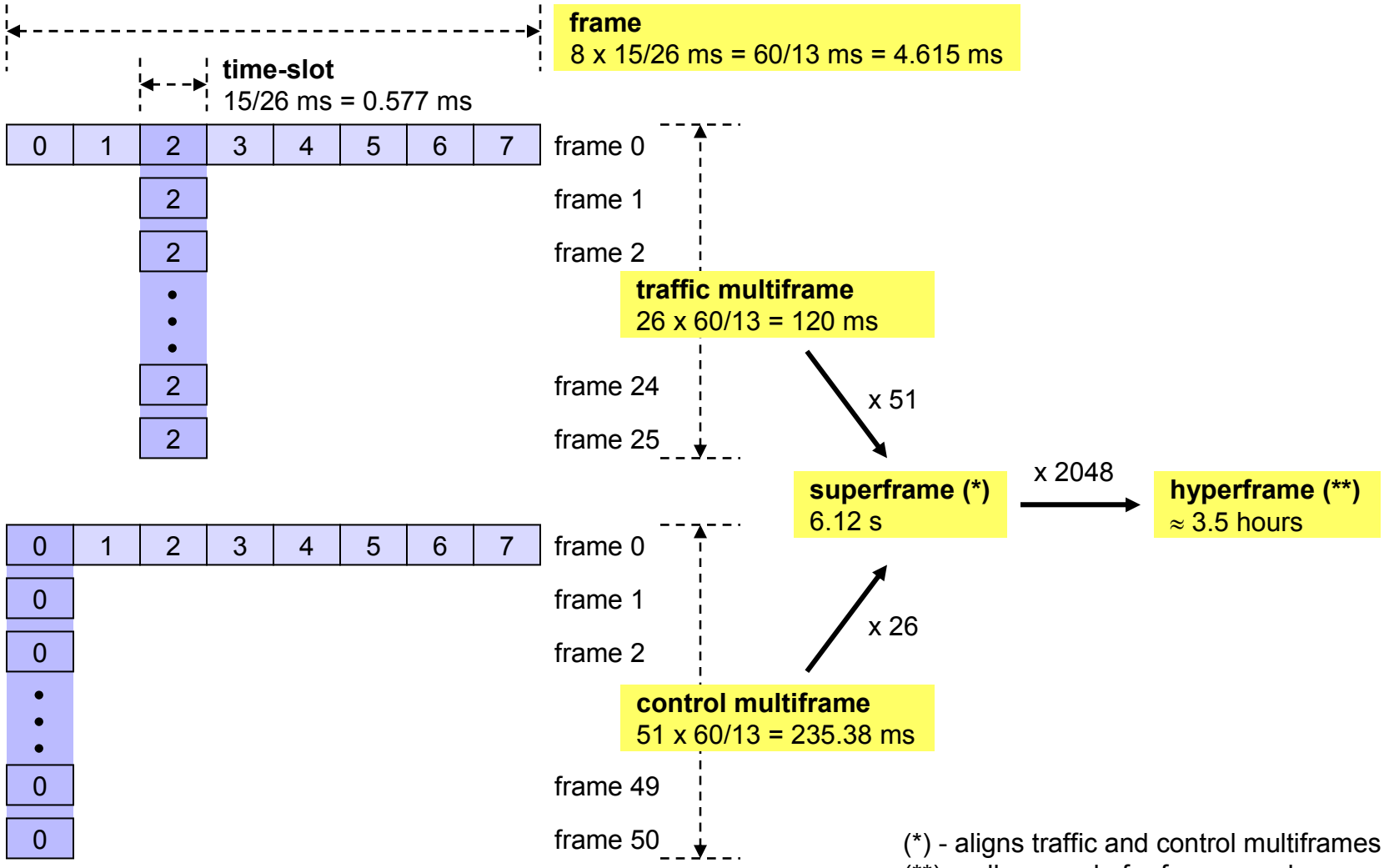
- Normal Burst: normal data transmission



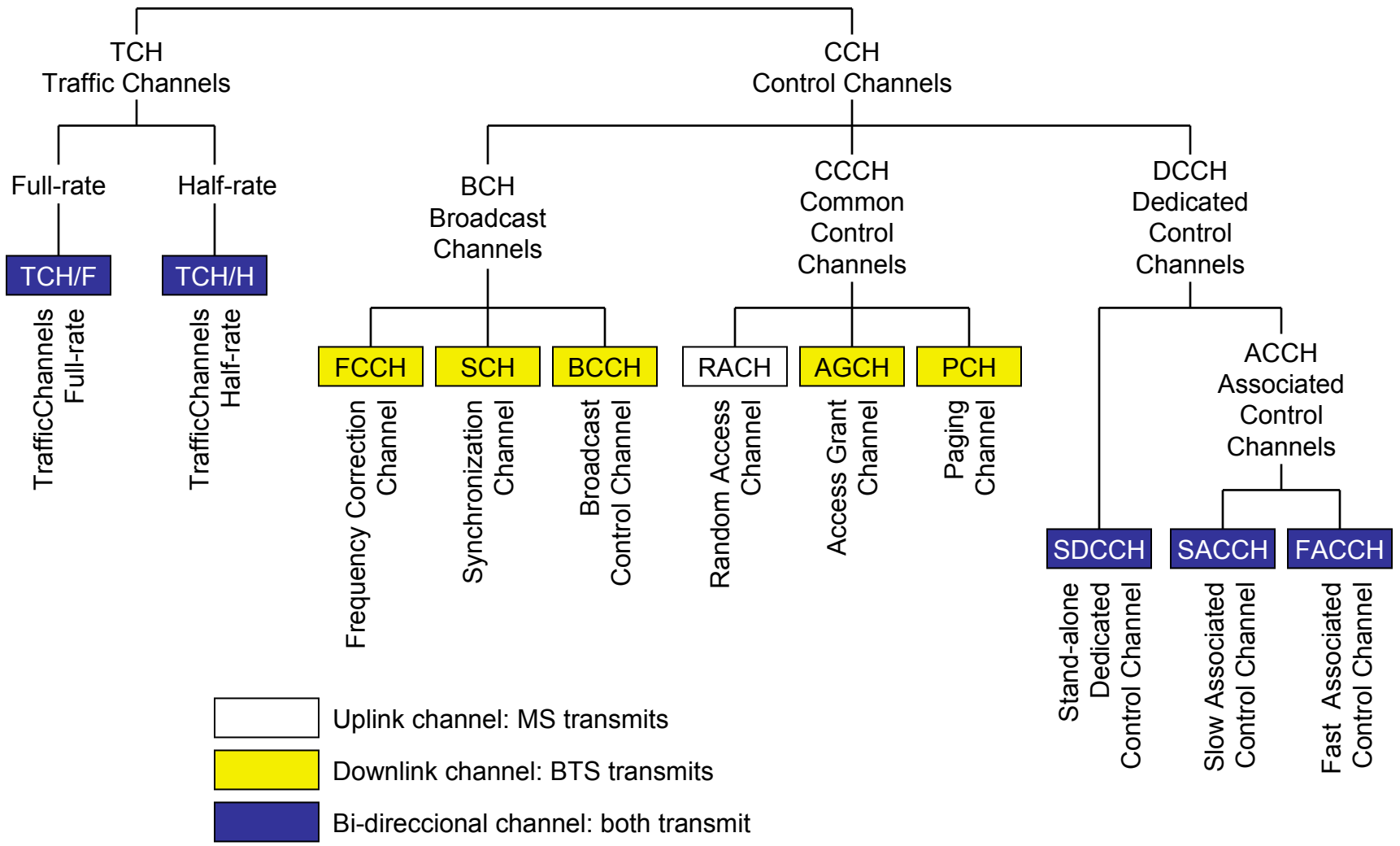
- Access Burst: MS first time access



Frame Hierarchy



Logical Channels



Logical Channels

Channel		Direction	Application	Allocation
TCH Traffic Channels	TCH/H	BTS ↔ MS	User data	Allocated by network on demand by MS
	TCH/F			
BCH Broadcast Channels	FCCH	BTS → MS	Carrier synchronization	Permanent
	SCH		Frame synchronisation	
	BCCH		General network information Cell information (present and adjacent)	
CCCH Common Control Channels	RACH	BTS ← MS	Request SDCCH for signalling Request TCH for handover	Multiple access with slotted Alhoa contention between MS
	AGCH	BTS → MS	Confirmation of SDCCH or TCH request	Permanent
	PCH		Allert MS to a call originated in the network	
DCCH Dedicated Control Channels	SDCCH	BTS ↔ MS	Registration / location updating Call control procedures	Allocated by network on demand
	SACCH		Control information between MS and BTS during the progress of a call or call set up	Associated to a specific TCH or SDCCH
	FACCH		Exchange of time critical control information during the progress of a call	Allocated by network or MS (*)

(*) Fast allocation by setting S bit; bits are stolen from TCH

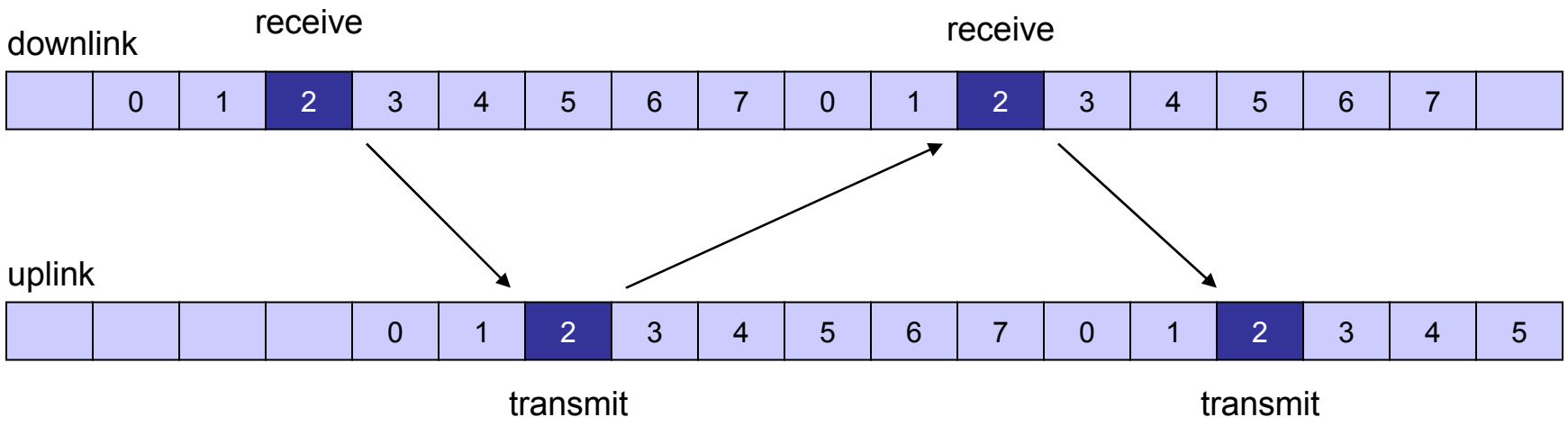
Logical channels

Channel		Burst type	Time-slot	Mulitiframe	Bursts / Multiframe	Capacity
TCH Traffic Channels	TCH/H	Normal (114 data bits)	Any	26 frames (120 ms)	24	24 x 114 / 120 = 22.8 kbit/s
	TCH/F				12	12 x 114 / 120 = 11.4 kbit/s
BCH Broadcast Channels	FCCH	Frequency correction	TS0 - base channel (*) TS0/TS2/TS4/TS6 (**)	51 frames (235.38 ms)	5	
	SCH	Synchronisation			5	
	BCCH	Normal (114 data bits)			4	4 x 114 / 235.38 = 1.94 kbit/s
CCCH Common Control Channels	RACH	Random access	TS0 - base channel (*) TS2/TS4/TS6 (**)	51 frames (235.38 ms)	27 minimum 51 typical	
	AGCH	Normal (114 data bits)			12 minimum	12 x 114 / 235.38 = 5.81 kbit/s minimum
	PCH					
DCCH Dedicated Control Channels	SDCCH	Normal (114 data bits)	TS0 - base channel (*) TS0/TS2/TS4/TS6 (**)	51 frames (235.38 ms)	4	4 x 114 / 120 = 3.8 kbit/s
	SACCH		Same TS as SDCCH		2 (***)	2 x 114 / 120 = 1.9 kbit/s
			Same TS as TCH	26 frames (120 ms)	1	1 x 114 / 120 = 0.95 kbit/s
	FACCH		Same TS as TCH (bits stolen from TCH)		Same as TCH	Same as TCH

(*) Low capacity cells
(**) High capacity cells
(***) 4 bursts in 2 multiframes equivalent to 2 bursts/ multiframe

Transmission / Reception Timing

- Transmit / receive frame staggering
  - » transmitter and receiver never operate at the same time
    - – to simplify hardware design
  - » transmission becomes half-duplex
  - » the numbering scheme is staggered by 3 time-slots



Transmit Time Advance

- Principle of operation
  - correct timing of uplink bursts at the BTS is required to avoid overlapping
  - different path delays (MS-BTS distances) must be compensated
  - transmission from the MS is advanced 0-63 bits under BTS control
  - maximum time advance of 63 bits allows 0.233 ms round trip delay
  - maximum cell radius is approximately 35 km
- Initial ranging
  - Access Burst is transmitted without time advance
  - Guard Period of 68.25 bits allows for a path delay due to 37 km distance
  - BTS measures path delay and sends required time advance on SACCH
  - MS introduces time advance on all bursts
- Adaptive control
  - BTS monitors burst and measures delays with specified time advance
  - if path delay varies more than 1 bit period, the new value is signalled on SACCH

Frequency hopping

» Application of frequency hoping
  – optional, but usually implemented
  – channels with no frequency hopping: BCH and CCCH

» Hoping sequence
  – several possible hoping algorithms
  – selected algorithm broadcast on BCCH

» Slow frequency hopping characteristics
  – in a given time-slot, successive TDMA frame are transmitted on different carriers
  – main hoping parameters
    ◆ period: 4.615 ms
    ◆ frequency: 217 hops/s
    ◆ number of bits: 1250 bits/hop

Transmission power

- Mobile station power classes

GSM 900			GSM 1800		
8 W	39 dBm	vehicular	4 W	36 dBm	vehicular
5 W	37 dBm	portable	1 W	30 dBm	portable
2 W	33 dBm	portable	0.25 W	24 dBm	portable
0.8 W	29 dBm	portable			

usual classes

- Discontinuous transmission (DTX) for voice
  - » no data transmission during periods of silence (approx. 60% of time)
    - – Voice Activity Detector (VAD) algorithm suppresses TCH transmission
  - » silent frames are sent to synthesise comfort noise at the receiver
  - » several advantages
    - – reduces interference, on average, by 3 dB
    - – Increases MS battery life

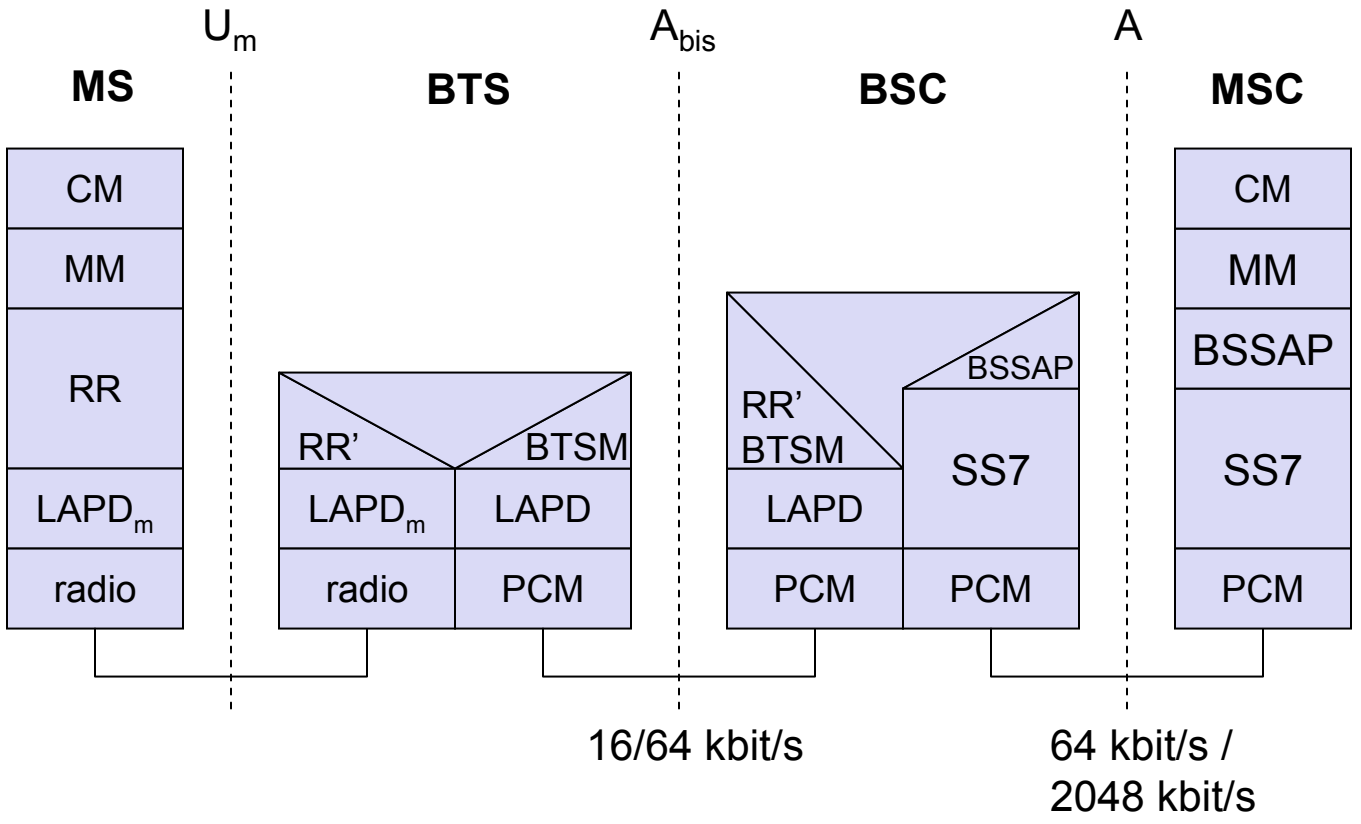
Power Control

- Implemented on both links
- Objective: lowest power level which provides desired quality (BER)
- Procedure
  - MS measures power received and BER and sends result on SACCH
  - BTS sends new power level on SACCH, if and when necessary
- control range

GSM 900	GSM 1800	Comments
5 - 39 dBm	0 - 36 dBm	effective maxima depend on cell size and MS capability control steps of 2 dB

- channels with no power control - use maximum power for the cell
  - downlink BCH and CCCH: power set by BTS
  - uplink RACH
    - BCCH broadcasts maximum power level for the cell
    - MS uses this value to set RACH transmission power

GSM Protocol Layers for Signaling

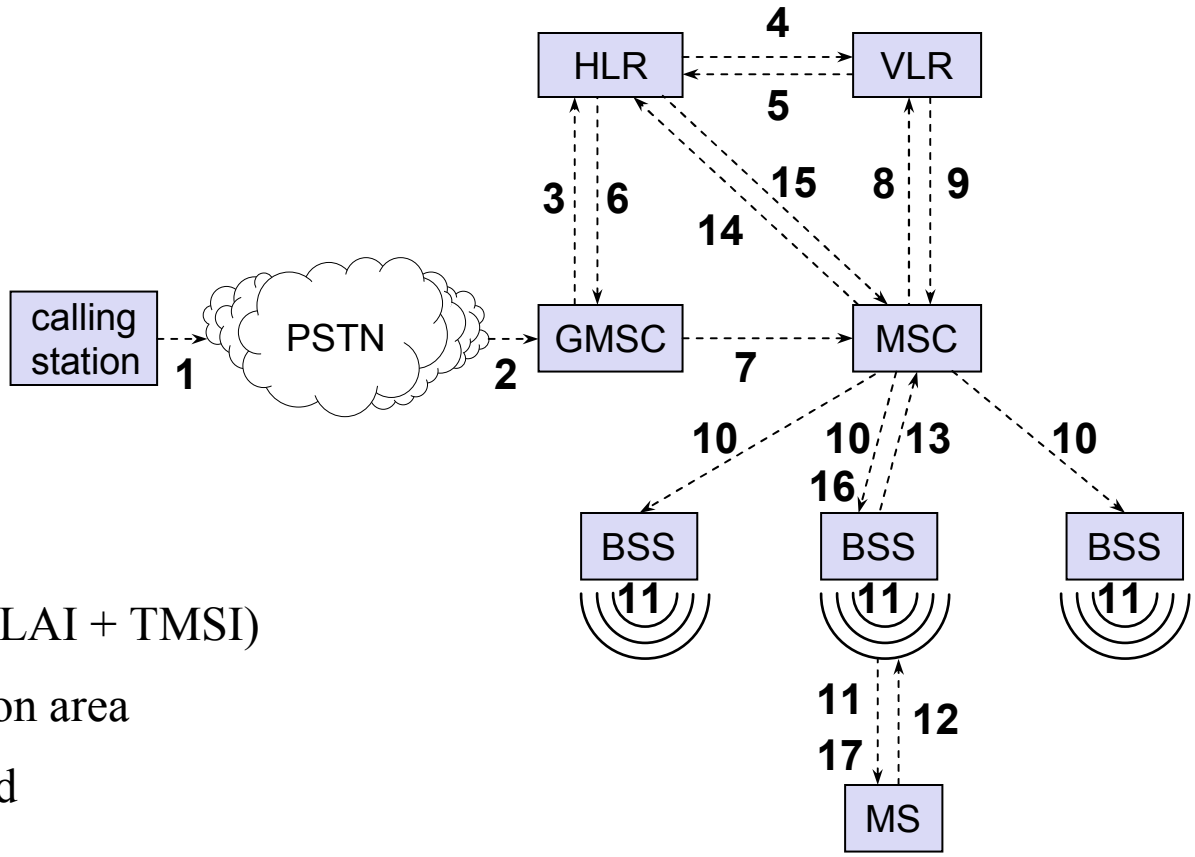


GSM Protocol Layers for Signaling

- CM (Connection Management)
  - call control, short message service and supplementary service
- MM (Mobility Management)
  - registration, authentication, location and handover management
- RR (Radio Resource Management)
  - setup, maintenance and release of radio channels
  - control of radio transmission quality
- LAPDm ("Link Access Protocol D-channel" modified)
  - modified version of ISDN LAPD protocol
- BTSM (Base Transceiver Station Management)
  - radio resources control messages between BSC and BTS
- BSSAP (Base Station System Application Part)
  - control of BSC by MSC

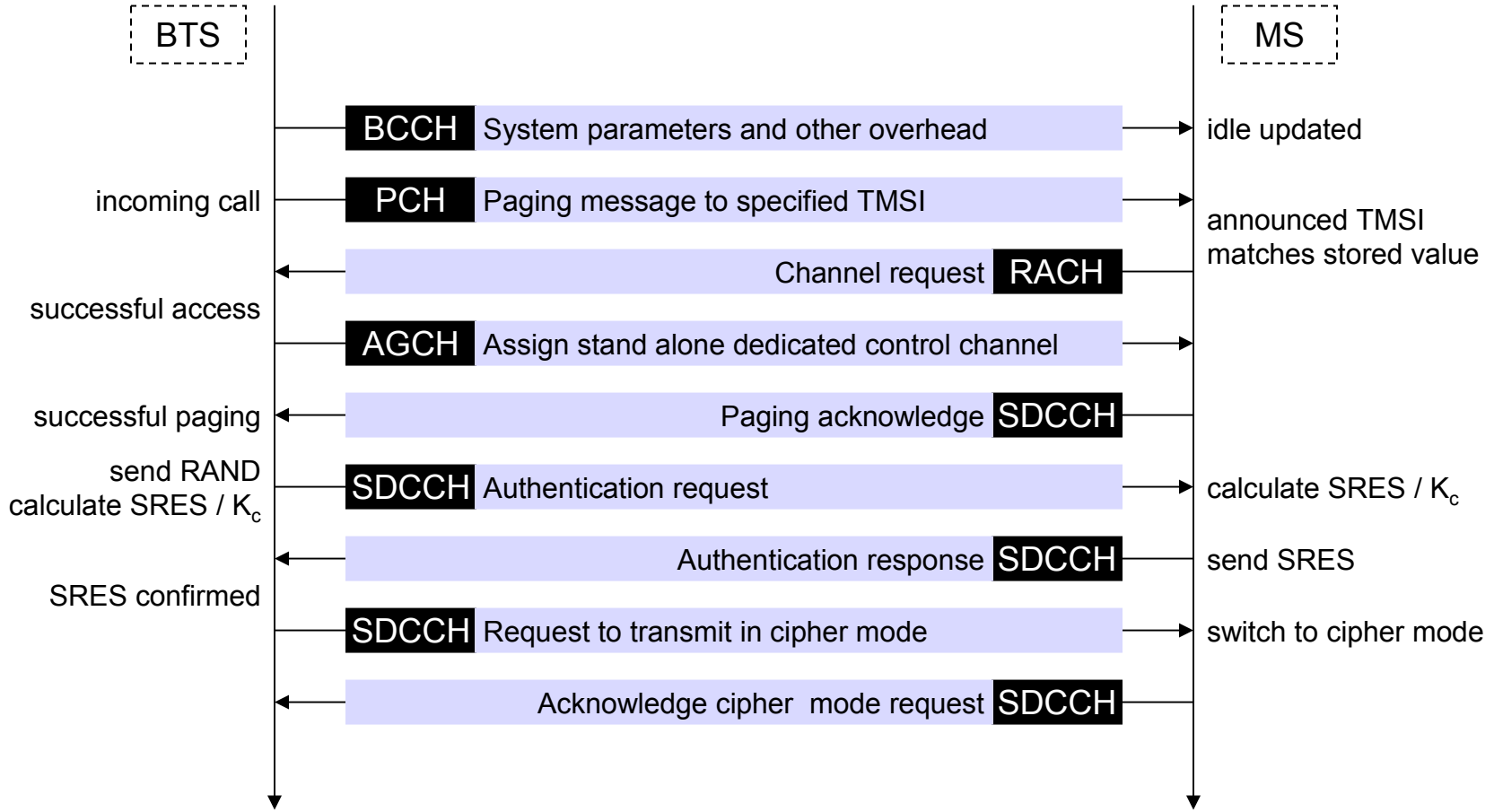
Mobile Terminated Call

- 1: calling a GSM subscriber
- 2: forwarding call to GMSC
- 3: signal call setup to HLR
- 4, 5: get routing info (MSRN) from VLR
- 6: forward routing info to GMSC
- 7: route call to current MSC
- 8, 9: get current status of MS (LAI + TMSI)
- 10, 11: paging of MS in location area
- 12, 13: MS answers paging and authentication request
- 14, 15: security checks
- 16, 17: set up connection



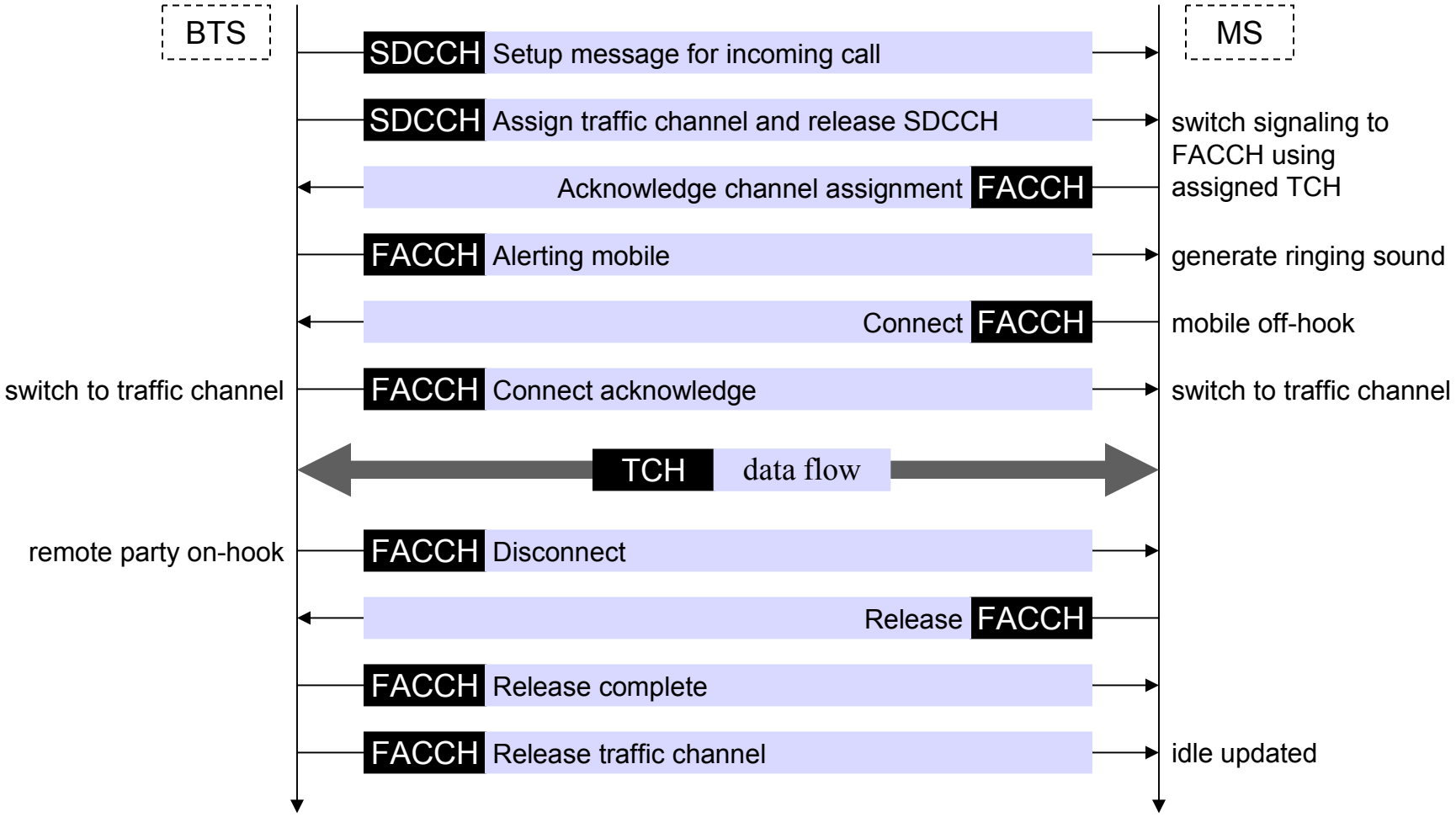
Mobile Terminated Call

Channel activity at radio interface



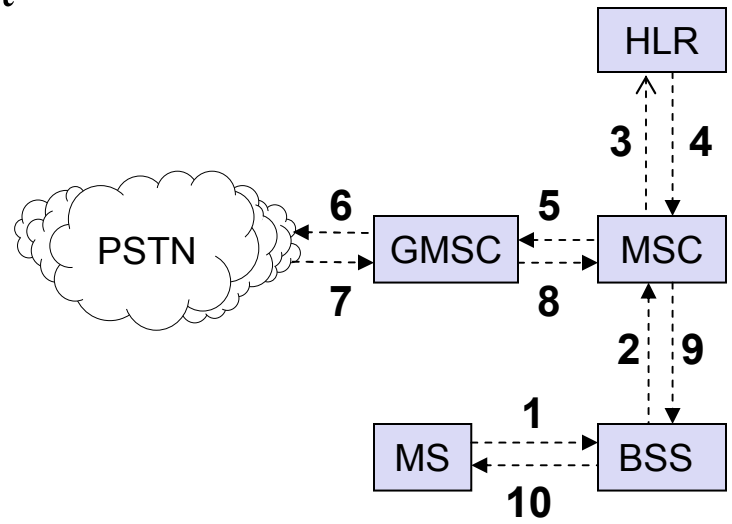
Mobile Terminated Call

Channel activity at radio interface (cont.)



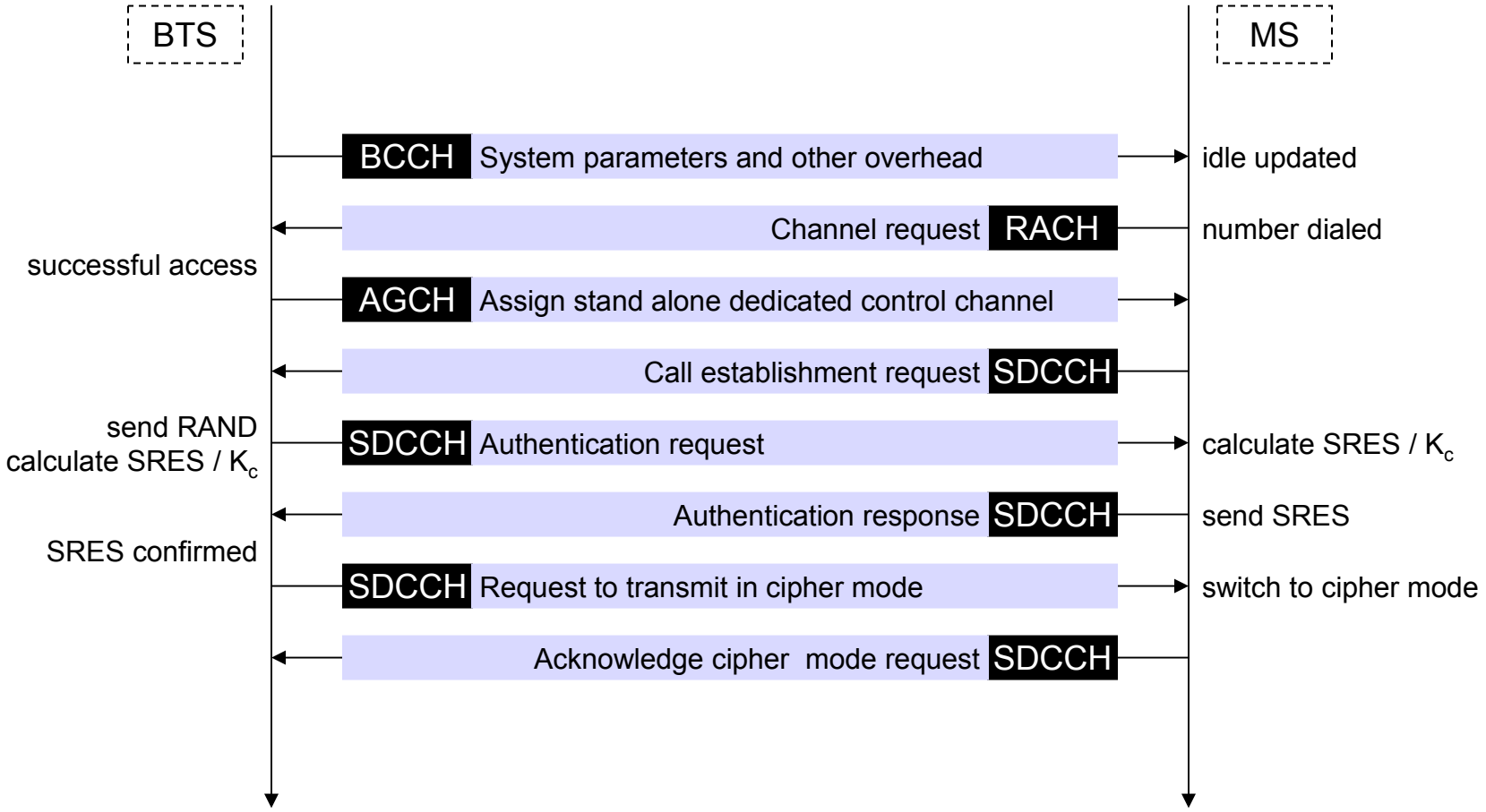
Mobile Originated Call

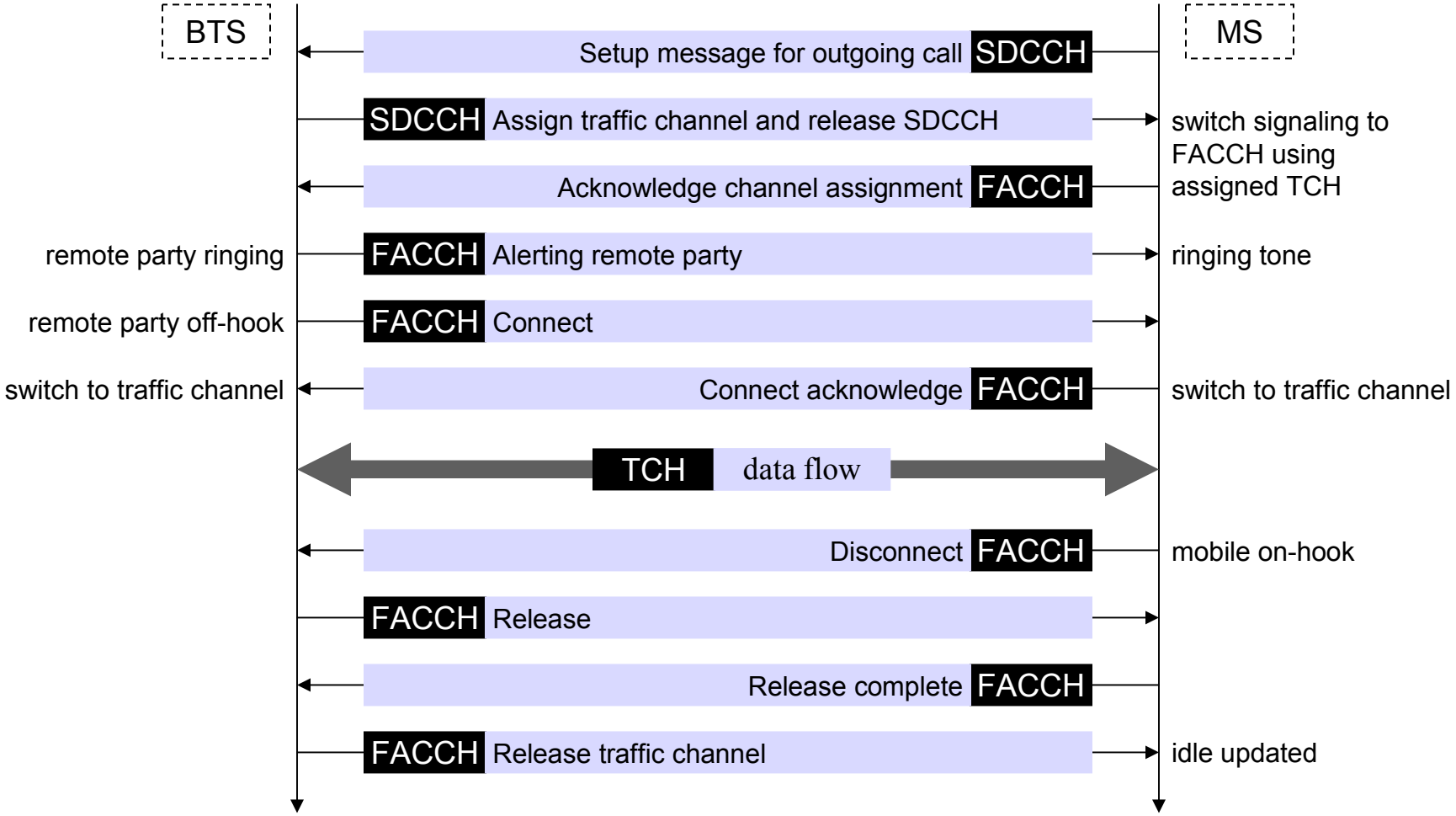
- 1, 2: connection and authentication request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



Mobile Originated Call

Channel activity at radio interface



Mobile Originated Call

Channel activity at radio interface