Telecommunication Systems (GSM)

Mobile Communications (Ch. 4)

John Schiller, Addison-Wesley

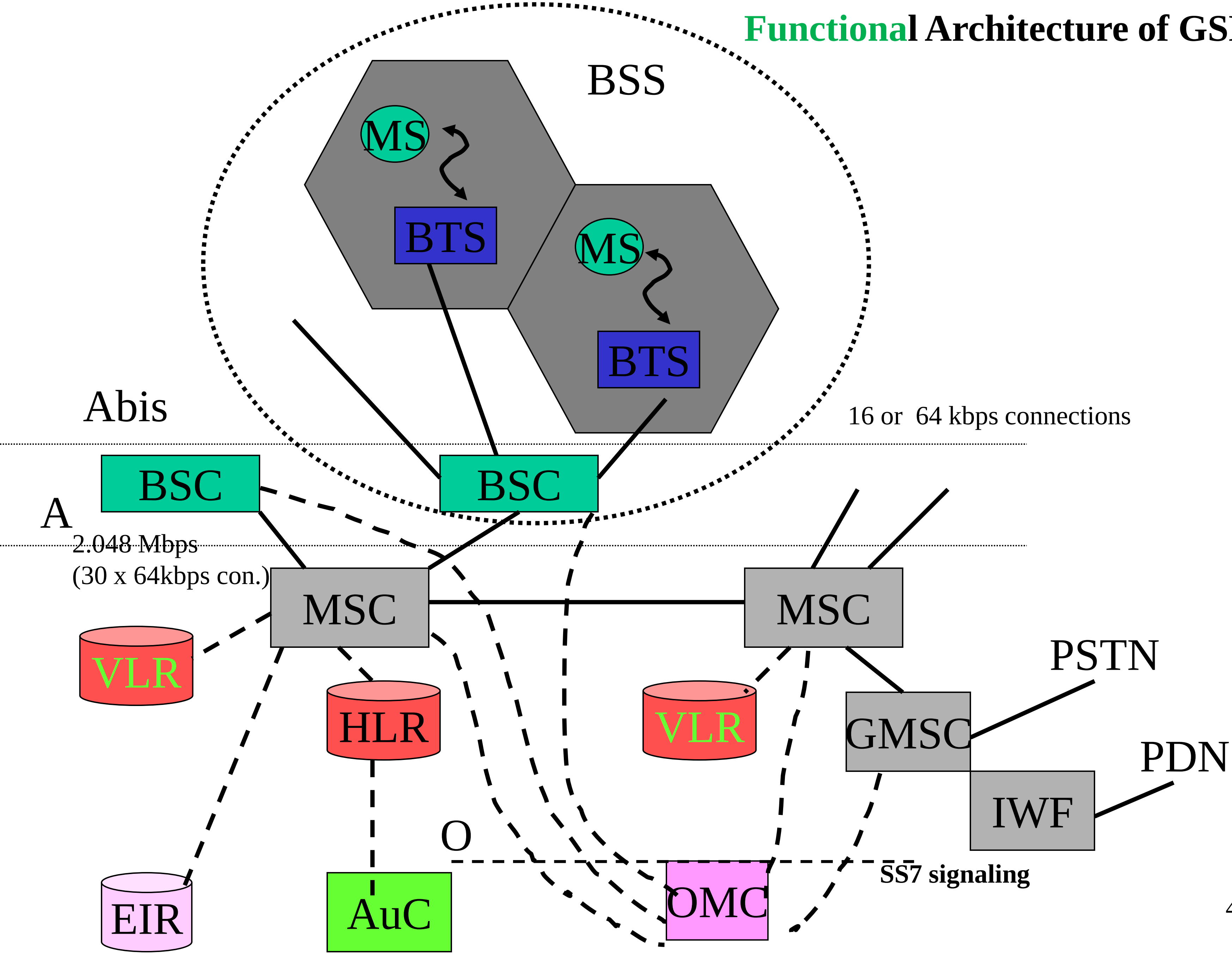
Wireless Communication Systems

- Infrastructure-based communication
  - Wide Area Networks (**GSM**, LTE)
  - Metropolitan Area Networks (WiMAX)
  - Wireless LANs (WiFi)
- Infrastructure-less communication
  - Ad hoc, sensor, vehicular networks
- Hybrid networks
  - Combination of the above two

GSM (Global System for Mobile comm.)

- Primary goal: phone + roaming in Europe
- Different GSM systems
  - GSM 900
    890-915 MHz uplink, 935-960 MHz downlink
  - GSM 1800 (DCS: Digital Cellular System)
    1710-1785 MHz uplink, 1805-1880 MHz downlink
  - GSM 1900 (Personal Comm Service) ← US, Canada
    1850-1910 MHz uplink, 1930-1990 MHz downlink
- Learn two architectures
  - **Functional** and **Protocol**

Functional Architecture of GSM



Interfaces

- A-interface (BSC ←→ MSC)
  - circuit switched, 2.048 Mbits/s
  - carrying up to 30 64 Kbits/s connections
- O-interface (OMC ←→ Others)
  - SS7 signaling, management data
- Abis-interface (BSC ←→ BTS)
  - 16 or 64 Kbits/s connections

Subsystems

- BSS: GSM net ➔ several BSS, 1 BSC/BSS
- BTS: radio equipment. Forms a radio cell.
- BSC
    - Reserves frequencies (**frequency/ch. assignment**)
    - Handles **handovers**
    - Performs **paging of MS**
    - **Multiplexes** radio channels onto fixed net connections.

Subsystems

- MS: User equipment and software for comm.
  - SIM (Subscriber Identity Module): IMSI, LAI..
  - GSM 900: transmit power up to 2 w
  - GSM 1800: transmit power 1 w
  - Two parts: TE for comm with network + Services

Subsystems

- MSC
  - Manages several BSCs
  - (Gateway)MSC ➔ other fixed network
  - Interworking Function (IWF) ➔ data nets
  - Connection setup, release and handover
  - Supplementary services (forwarding, conf.)

Subsystems

- HLR (Home Location Register)
  - Most important database with all user relevant info.
  - Static Info.:
    - MSISDN number and IMSI number
    - Subscribed services (call forwarding, roaming, GPRS)
  - Dynamic Info.:
    - Current location area (LA) of the MS
    - Current MSC and VLR
    - Accounting information
  - Specialized databases to meet real-time reqs.
  - Handle millions of users.

Subsystems

- VLR (Visitor Location Register)
  - One VLR is associated with one MSC (1:1 mapping)
  - Info about <u>all users</u> in the LA associated to the MSC
  - Info per user (copied from HLR): IMSI, MSISDN, HLR address
  - Need: To avoid frequent communication with HLR
  - Large, real-time database

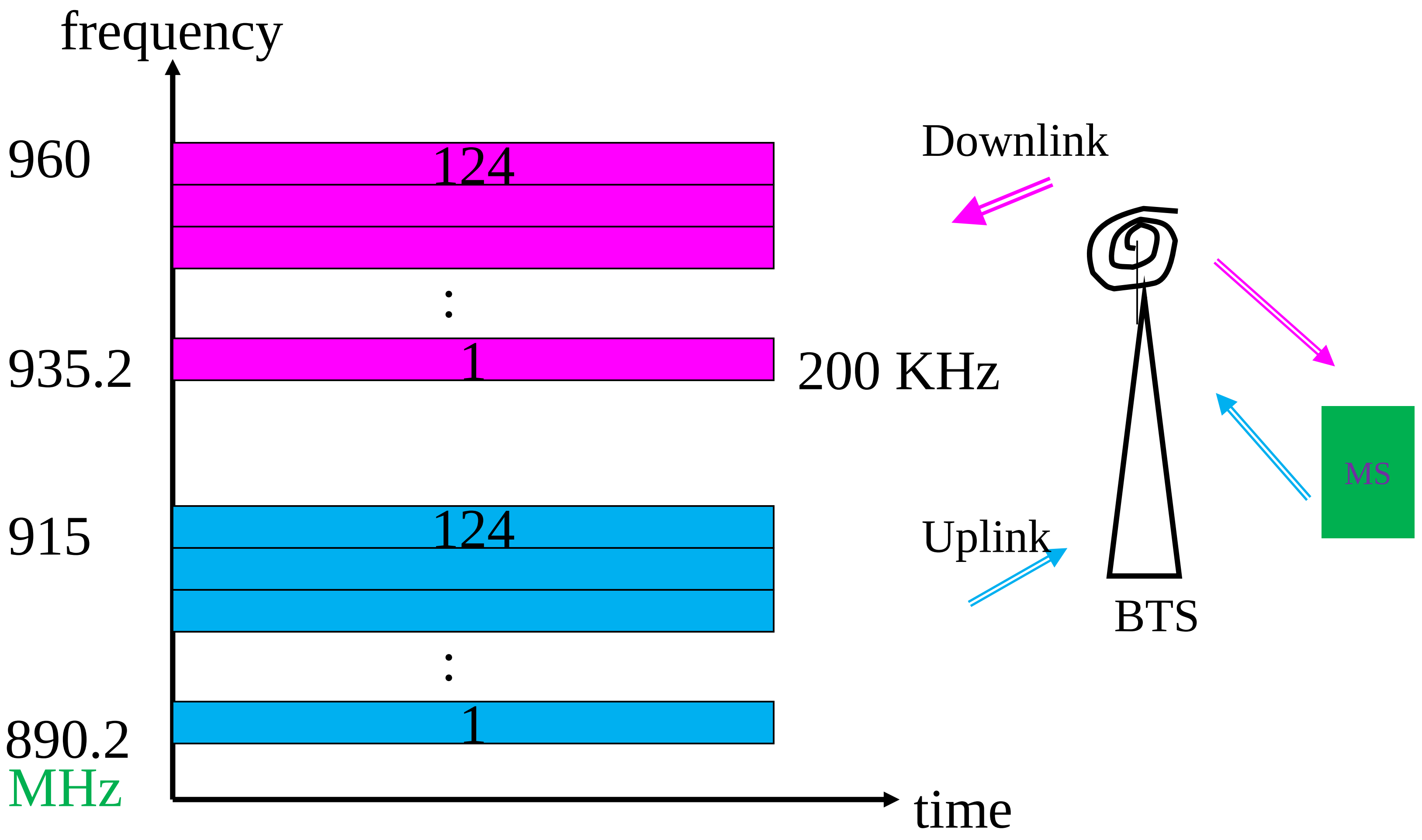
Subsystems

- Operation and Maintenance Centre (OMC)
  - Monitor: traffic, status of all network entities
  - Accounting and billing
- Authentication Center (AuC)
  - Contains algorithms for authentication and keys for encryption
  - Can be a part of the HLR.
- Equipment Identity Register (EIR)
  - Blacklist of stolen/locked MS

Radio Interface

- FDD is used to separate downlink & uplink.
- Media access combines TDMA and FDMA.
- GSM 900: 124 carriers, each 200 KHz wide, FDMA
  - 90 carriers to support customers
  - 32 reserved
  - 2 not used (1 and 124)

FDMA in GSM 900

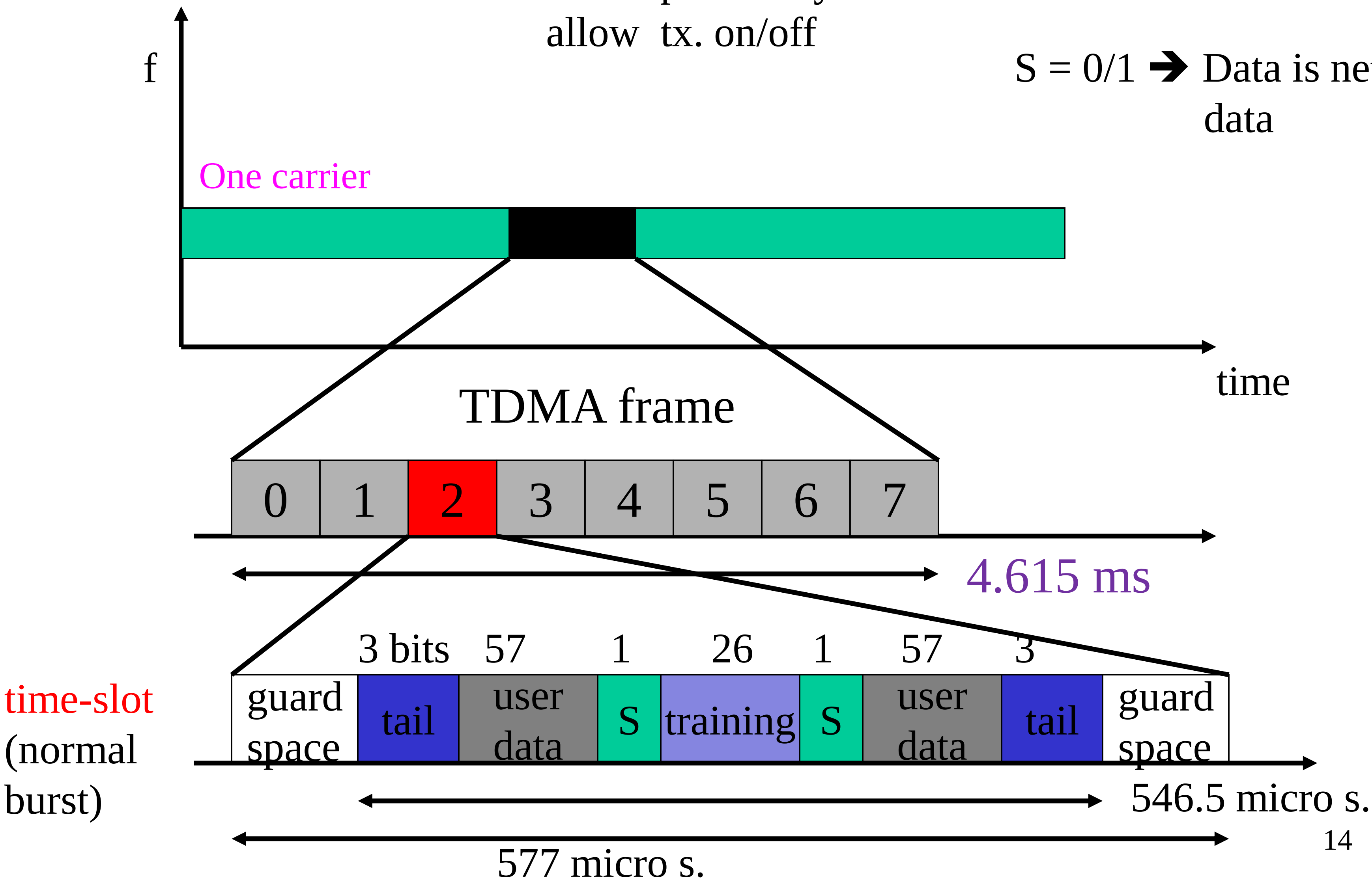


TDMA in GSM 900

Guard space: avoid overlap of bursts due to path delay + allow tx. on/off

Tail + training for better receiver performance

S = 0/1 ➔ Data is net/user data



Simple MS

- TDMA frame on the uplink is **shifted by three slots** from frame on the downlink.

- If BTS sends data at t_0 in slot #1 on the downlink, the MS accesses slot #1 on the uplink at time t_0 + 3*577 micro sec.

  ➔ MS does not need a full-duplex Tx

Logical channel and frame hierarchy

- **Physical channel**: a slot repeated every 4.615 ms. (114 bits in 4.615 ms ➔Rate = 24.7 Kbps)
- Reality: Out of every 26 consecutive slots of a phy. ch.
  - 12 data slots + 1 signaling slot + 12 data slots + 1 unused
  - Rate of a physical channel = (24/26)*24.7 = 22.8 Kbps
- **Logical channel**: A physical channel may be split into several (logical) channels:
  - Logical channel C1: every 4th slot
  - Logical channel C2: every other slot
  - C1 and C2 could use the same physical channel with the pattern C1C2xC2C1C2xC2C1

Logical channels …

- Two basic groups of logical channels
  - Traffic channels (TCH)
  - Control channels (CCH)

- TCH
  - Carries user data (voice, fax)
  - Full-rate TCH/F: 22.8 kbits/sec
  - Half-rate TCH/H: 11.4 kbits/sec ← capacity x 2
  - Other (data)rates: TCH/F4.8, TCH/F9.6, TCH/F14.4

  (They differ in their voice coding schemes.)

Logical channels (CCH)

- CCH: access control, ch alloc., mobility
  - Broadcast CCH (BCCH):
    - Slot #0 of C_0 (On the down link)
    - BTS ➔ MS: Used by BTS to send info to all MS
      - » Cell ID, options available (f. hop), freq available
- Common CCH (CCCH): for conn. Setup
  - RACH: MS ➔ BTS. MS wants to make a call. Accessed by all MS in a cell. (random access, coll.)
    - Slot #0 of C_0 (On the up link)
  - AGCH: BTS ➔ MS. BTS tells MS to use a TCH or an SDCCH.
  - Paging CH: BTS ➔ MS for paging an MS

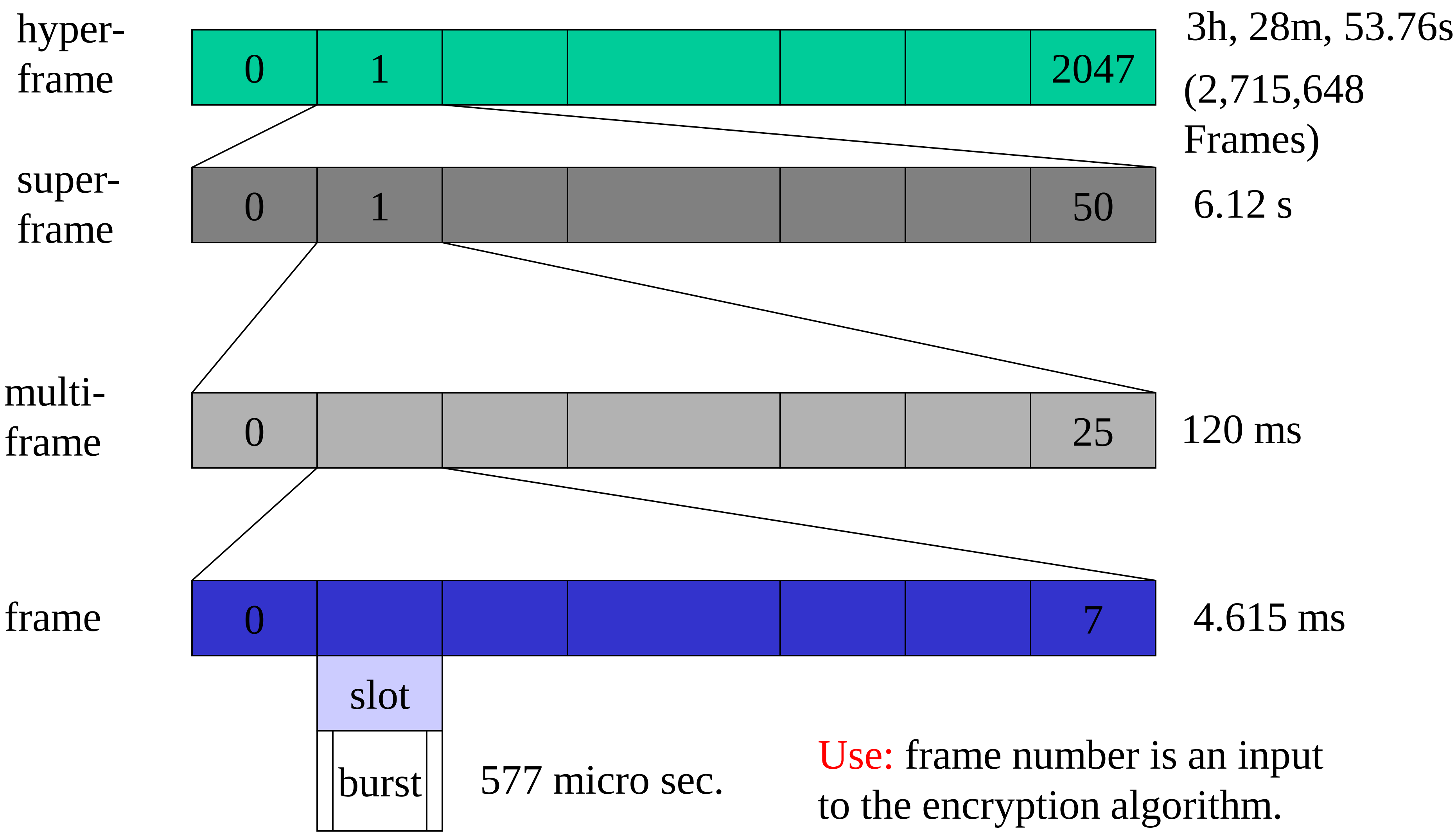
Logical channels

- Dedicated control channel (DCCH): bidirectional
  - Stand-alone DCCH (SDCCH) is used while an MS has not established a TCH with a BTS. Time slot #1 of C_0
    - **SDCCH** (782 bits/sec): authentication, registration, etc. needed for setting up a TCH.
  - Slow associated dedicated control ch (**SACCH**): Associated with each TCH. For <u>small amount</u> of system info: ch quality, signal power level. Time slot #1 of C_0
  - Fast associated dedicated control ch (**FACCH**): Uses time slots from the TCH. Handover info.

Typical use of TCH and SACCH

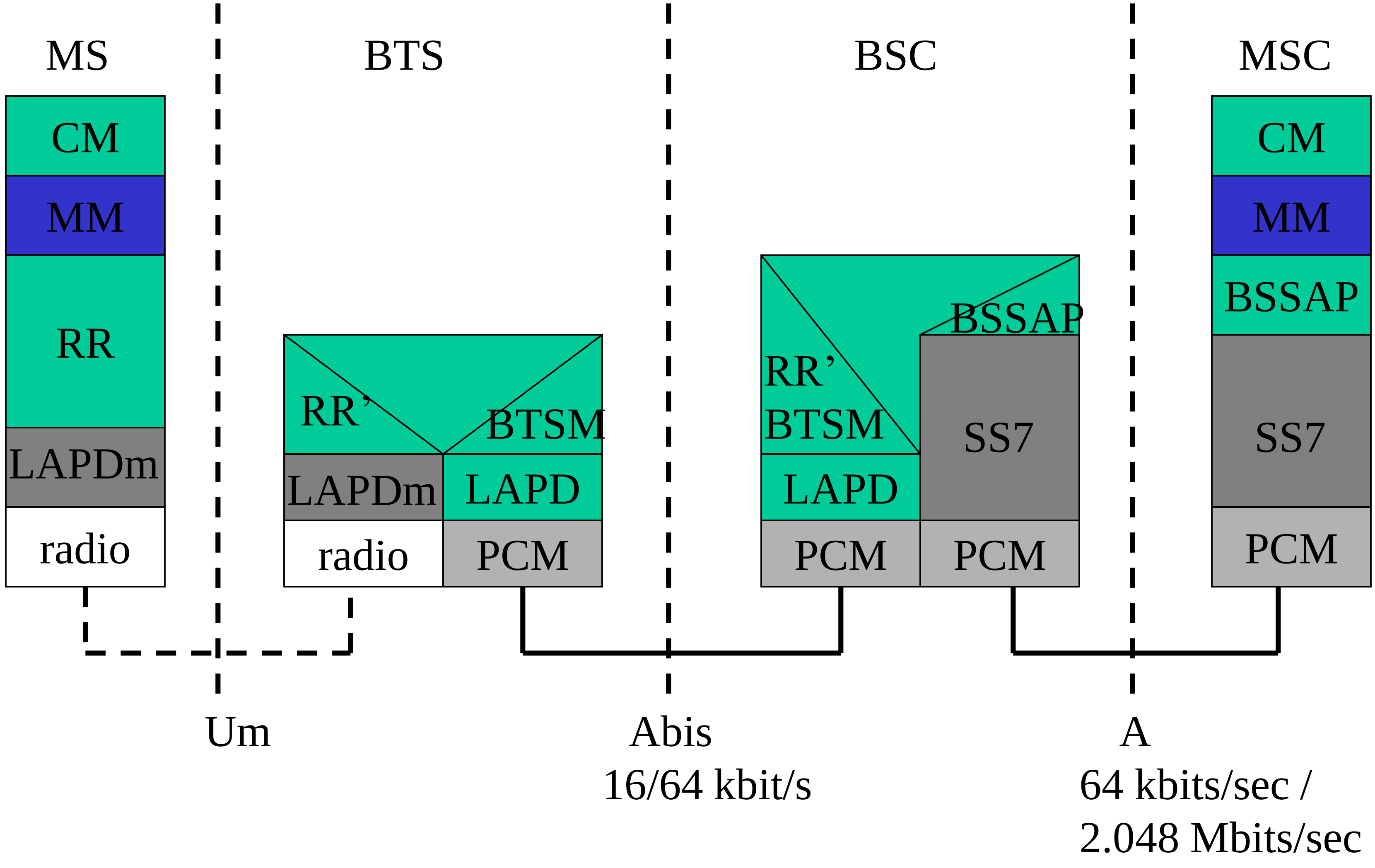
- TTTTTTTTTTTT**S**TTTTTTTTTTTT**x**
- T = user traffic in TCH/F, S = signalling
- x = unused slot
- Normal burst carries 114 bits of user data and is repeated every 4.615 ms (24.7 kbit/sec data rate)
- TCH uses 24/26 slots→rate = 22.8 kbit/s
- SACCH: 950 bit/sec

Structuring of time using frames



Use: frame number is an input to the encryption algorithm.

Protocol Stacks in GSM Network



Protocols

- Radio
  - Creation of bursts, multiplexing, sync with BTS, detection of idle channel, measurement of quality of downlink, encryption/decryption
  - Channel coding/error detection using FEC
    - (Alternative is retransmission. Expensive. Good for upper layers.)
  - GSM tries to correct errors, but does not deliver erroneous data.

Protocols

- LAPDm (Link Access Protocol D-channel)
    - Light weight LAPD (no sync, no checksum)
    - Flow control: Receiver controls transmissions.
    - Segmentation + reassembly
- RR (radio resource management)
    - Setup, maintenance, release of radio channels
- BTSM (BTS Management)

Protocols

- MM (Mobility Management)
  - Registration, authentication, **location updating**, temporary mobile subscriber identity (TMSI)
  - TMSI replaces IMSI to *hide the real identity* of MS
  - TMSI is valid only in current location area of a VLR

Protocols

- CM (Call Management)
  - Call Control (CC)
    - Point-to-point connection between terminals
  - Short Message Service (SMS)
    - Uses SDCCH + SACCH

Localization and calling

- Feature of GSM
  - Automatic, worldwide localization of users
  - Performs periodic location update. Location is the area in all the cells under one MSC.
- Roaming
  - Changing VLRs with uninterrupted availability
    - » Within the network of one provider
    - » Between two providers in one country
    - » Between different providers in different countries

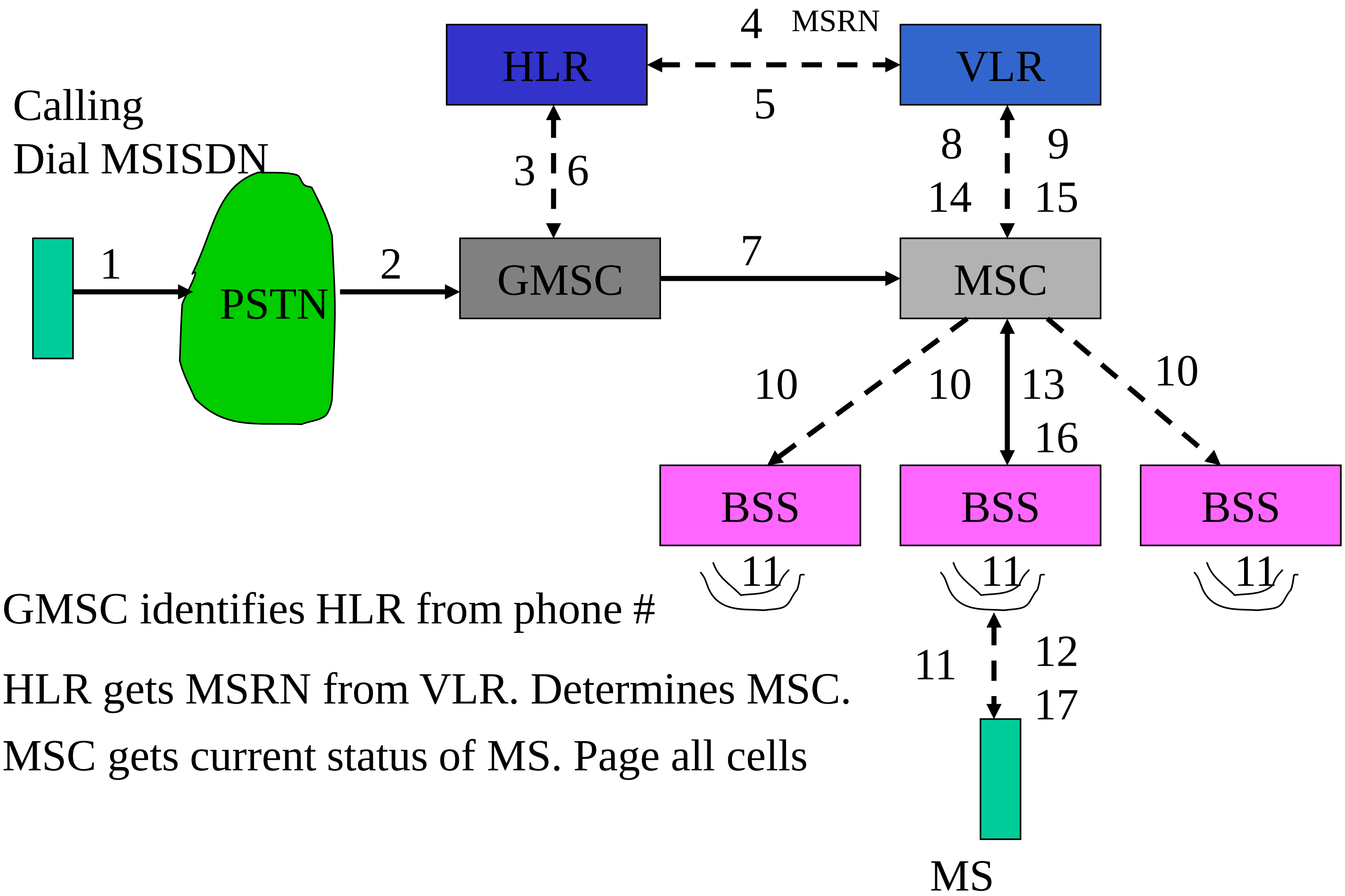
Localization and calling

- To locate/address an MS, several #s needed
  - International Mobile Equipment Identity (IMEI)
    - » Uniquely identifies an MS (device)
  - MS International ISDN number (MSISDN) ← Misden
    - » Mobile Station International Subscriber Directory Number
      (Telephone number to the SIM card)
    - » Country code + national destn code + subscriber num
    - » You dial this number
  - International Mobile Subscriber Identity (IMSI): 64 bits
    - » Mobile country code + mobile net code + MSIN (Mob. Sub. Identification Number: assigned by network op.)
    - » Uniquely identifies a user
  - Note: An MS can only be operated if a SIM with a

Localization and calling

- To locate/address an MS, several #s needed
  - Mobile Station Roaming Number (MSRN)
    - » (MSRN) is a temporarily telephone number assigned to a mobile station which roams into another numbering area.
    - » Same structure as MSISDN
    - » Hides the ID and location of a subscriber
    - » Helps HLR to find a subscriber for an incoming call
  - Temporary Mobile Subscriber Identity (TMSI)
    - » Hides IMSI. Assigned by VLR. Not known to HLR.

Mobile *Terminated* Call

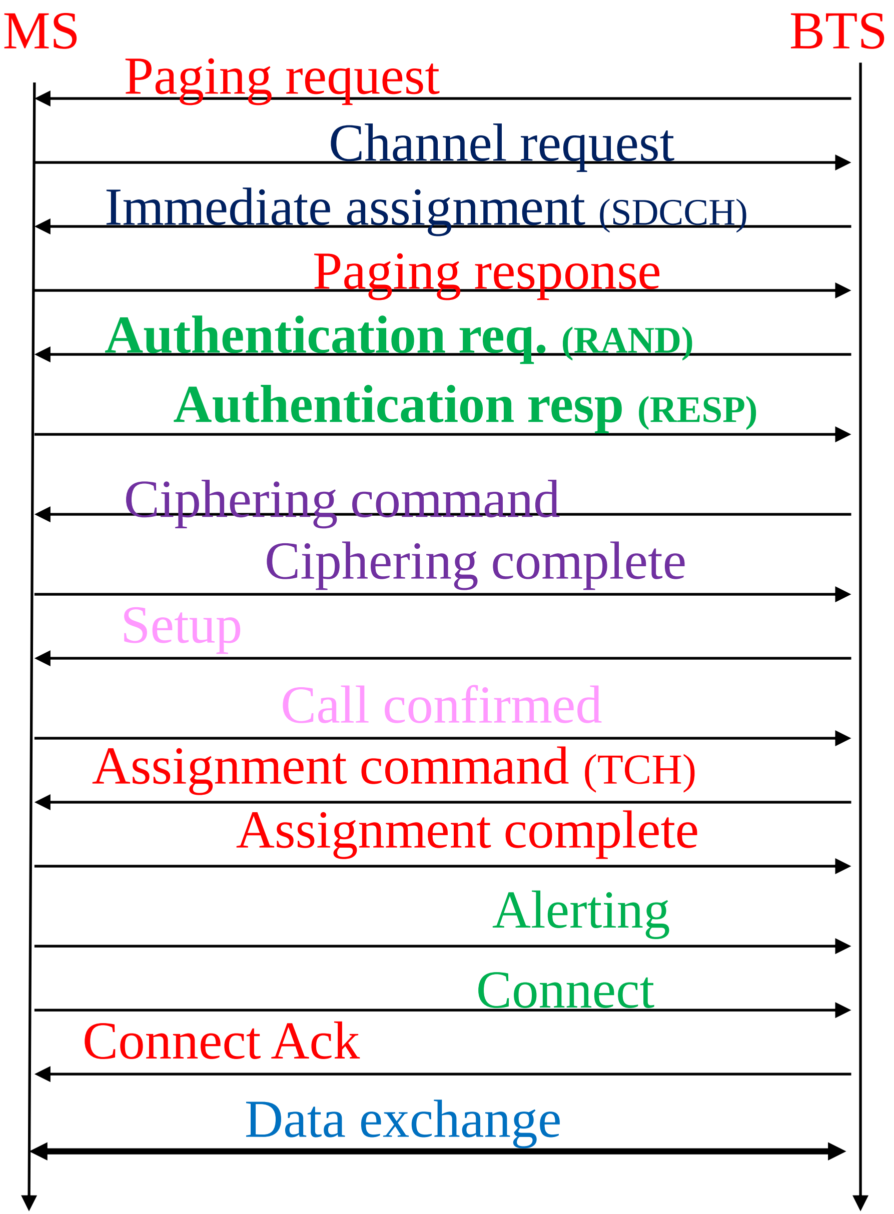


* GMSC identifies HLR from phone #

* HLR gets MSRN from VLR. Determines MSC.

* MSC gets current status of MS. Page all cells

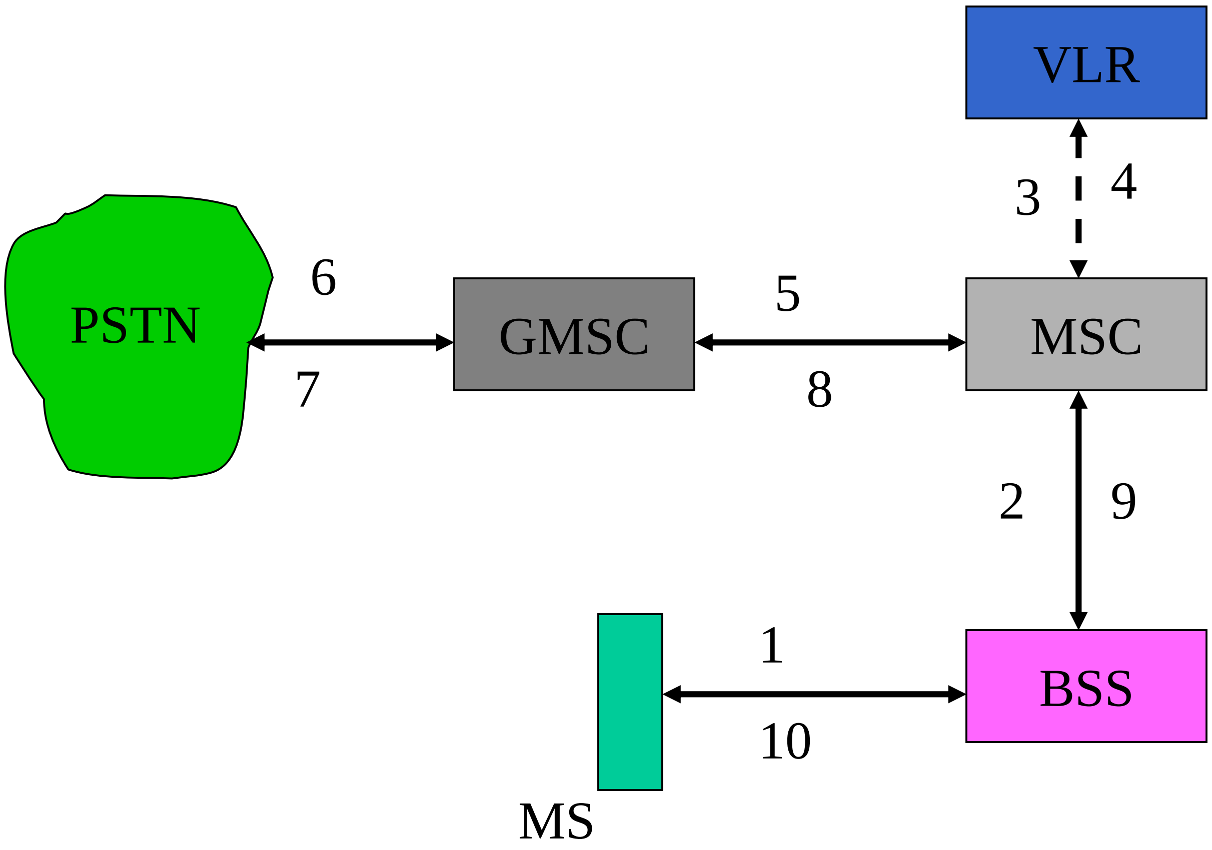
Message flow for MTC



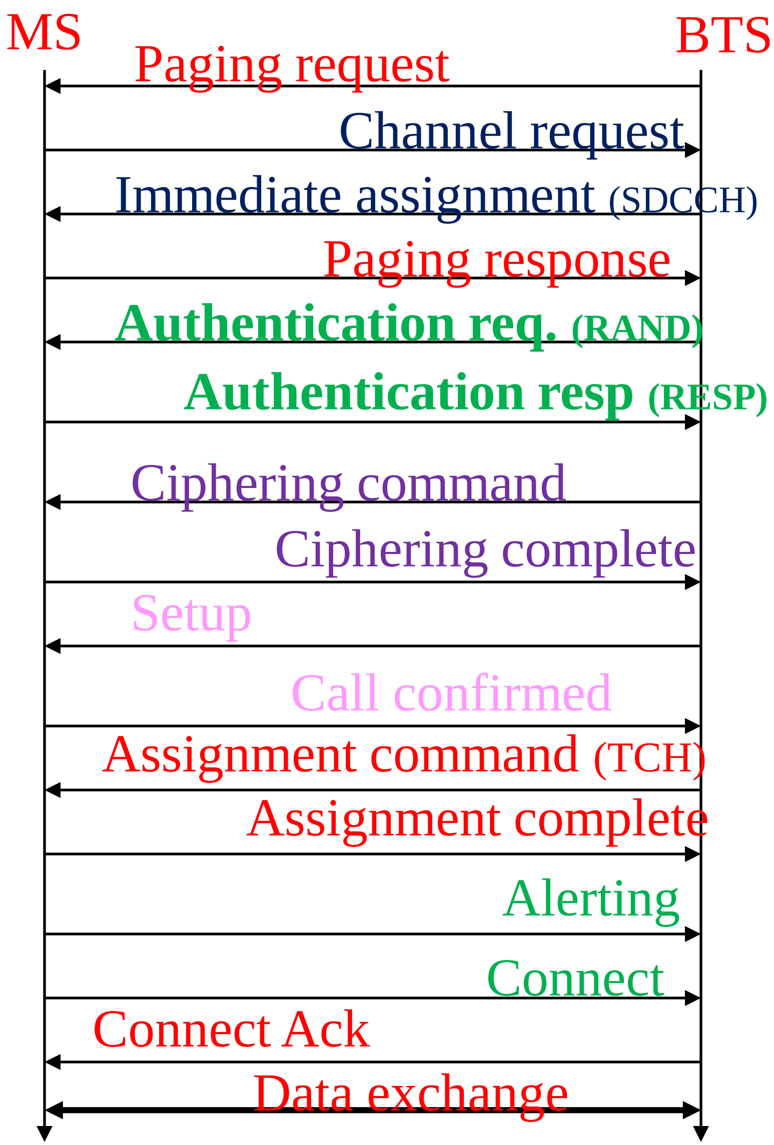
Localization and calling

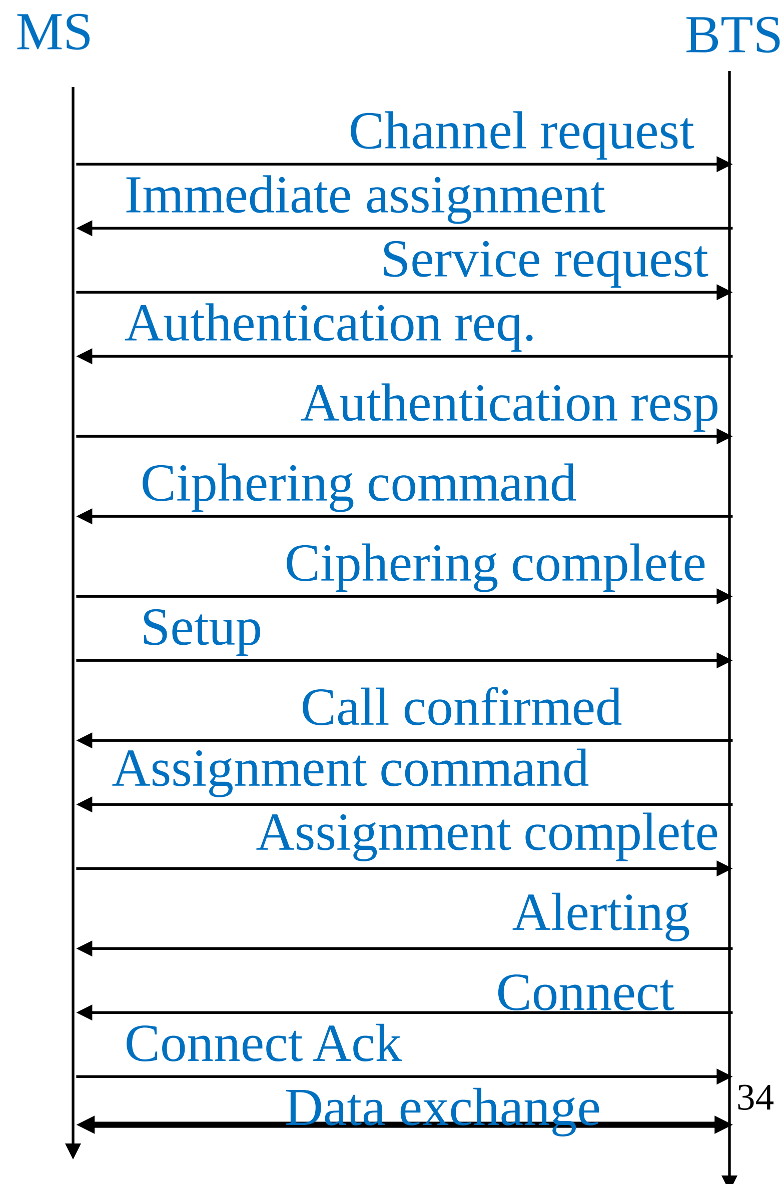
- HLR
  - Checks whether the number exists and whether the user has subscribed to the service.
  - Asks for an MSRN from the VLR.
- MSC
  - Gets the current status of MS from VLR (8/9).
  - If the MS is available, start paging.
  - :
  - Ask VLR to perform security check (14).

Mobile *Originated* Call



Message flow for MTC and MOC

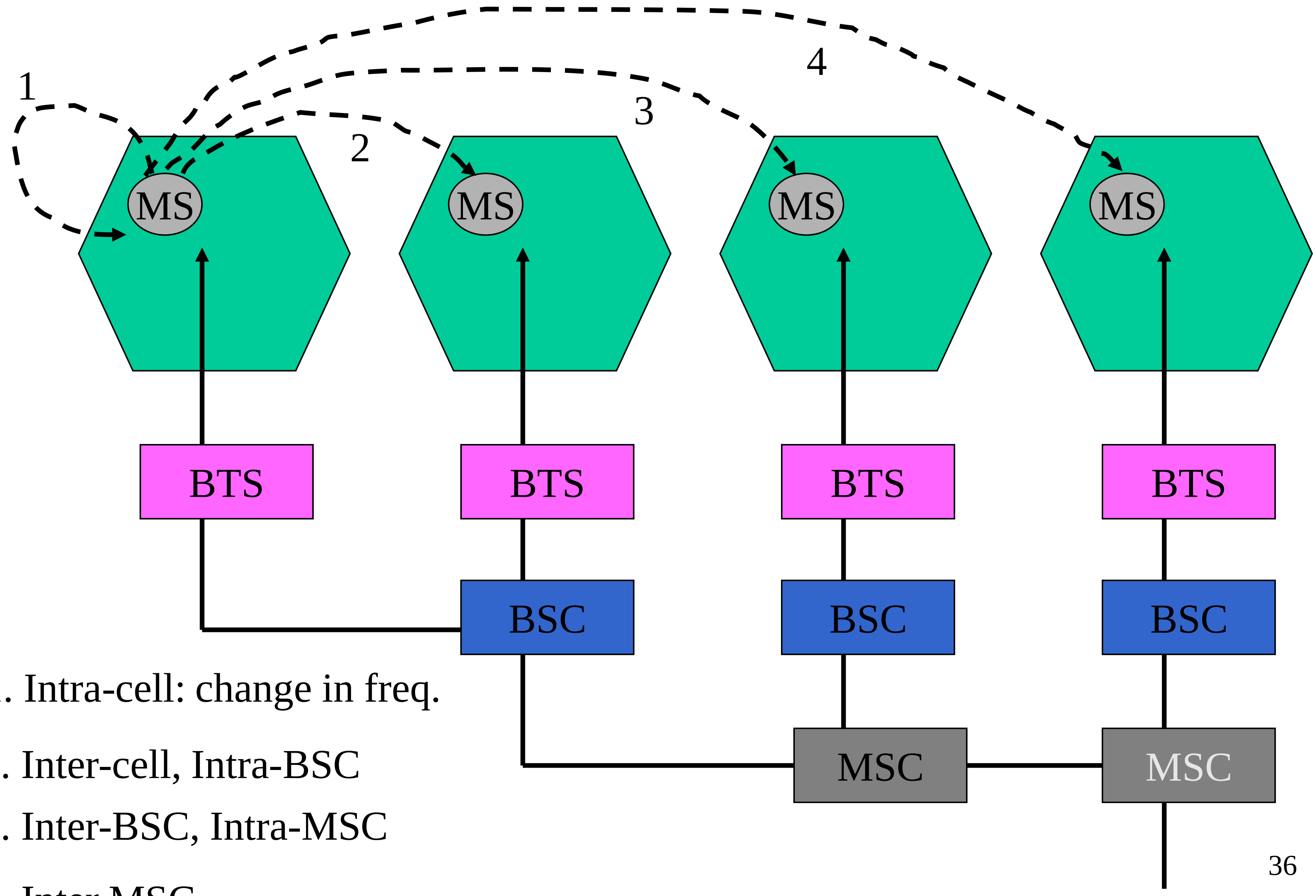




Handover

- Diminished quality of radio link
- Load balancing

Types of handover in GSM



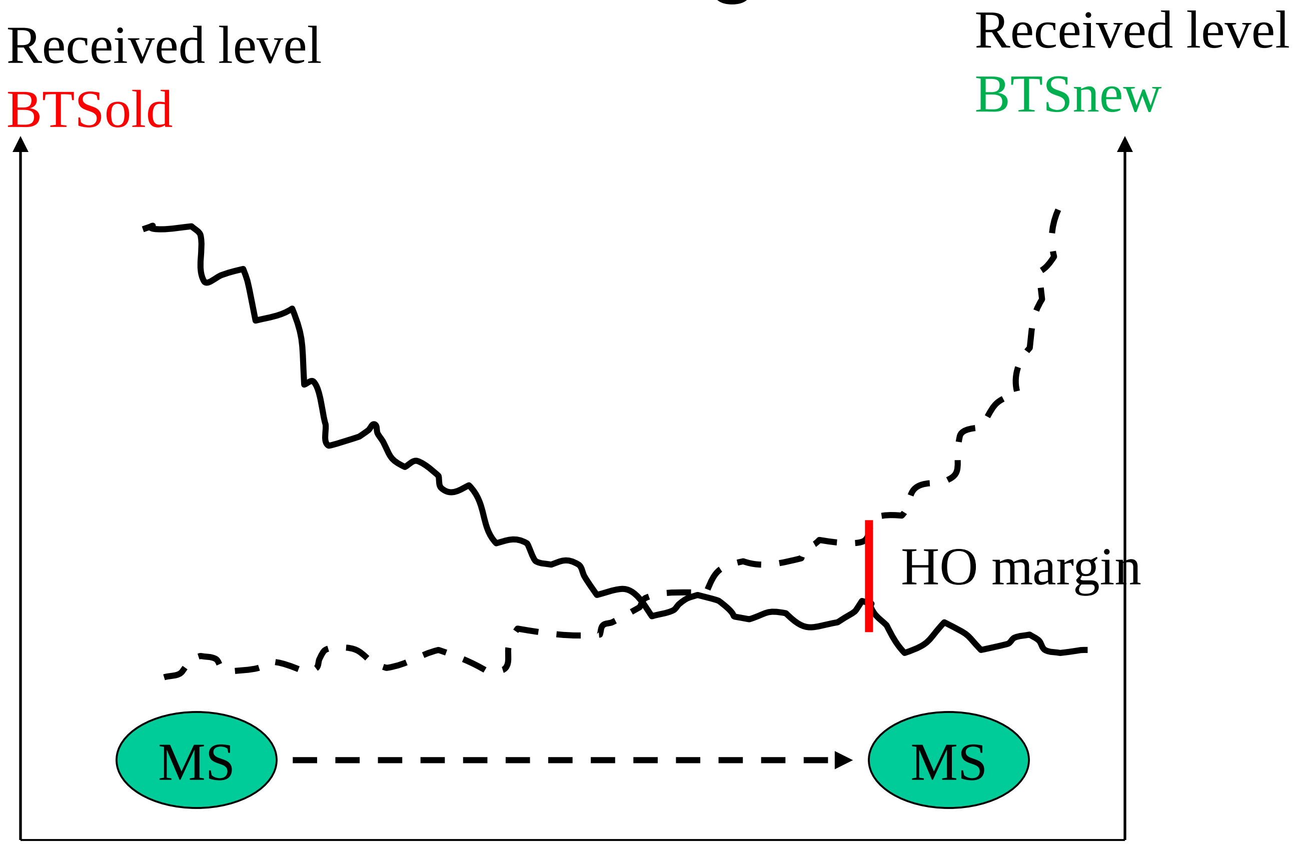
1. Intra-cell: change in freq.

2. Inter-cell, Intra-BSC

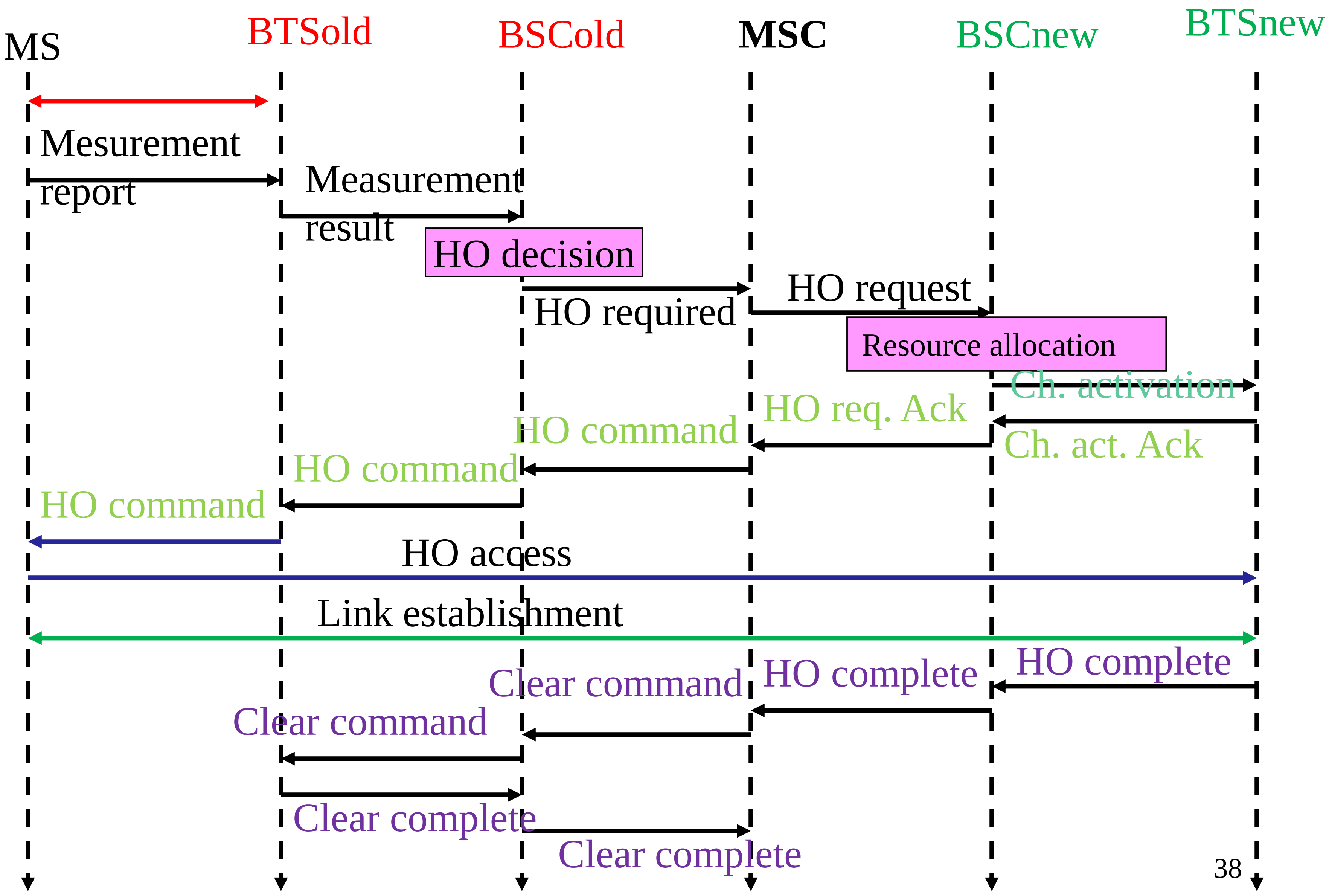
3. Inter-BSC, Intra-MSC

4. Inter MSC

Handover decision based on received signal



Intra-MSC handover



Security in GSM

Security services offered by GSM

- Access control and authentication
  - Authentication of a valid user for the SIM: The user needs a secret PIN to access the SIM
  - The next step is subscriber authentication (Fig. 4.10 in book. See message flow for MTC and MOC. Shown before.) This is based on a Challenge/Response explained on the following slide (Fig. 4.14)
- Confidentiality
  - All user data is encrypted. Shown in Fig. 4.15, on a following slide.
- Anonymity
  - All data is encrypted before transmission.
  - User identifiers are not used over air. Rather, a TMSI is transmitted. A VLR generates a new TMSI after a location update.
  - TMSI is sent to MS after authentication and encryption processes have taken place.

Fig. 4.14: Subscriber authentication

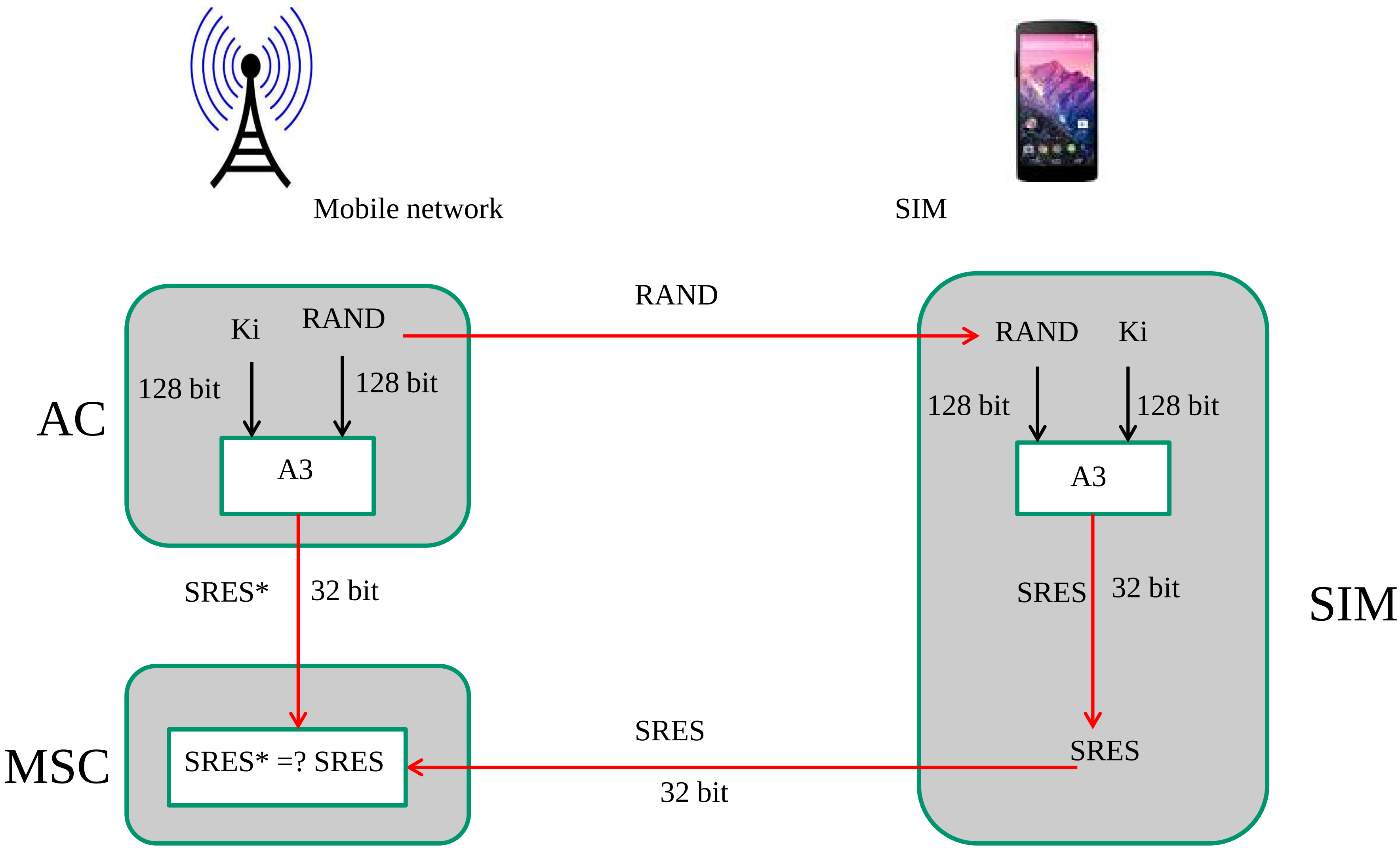
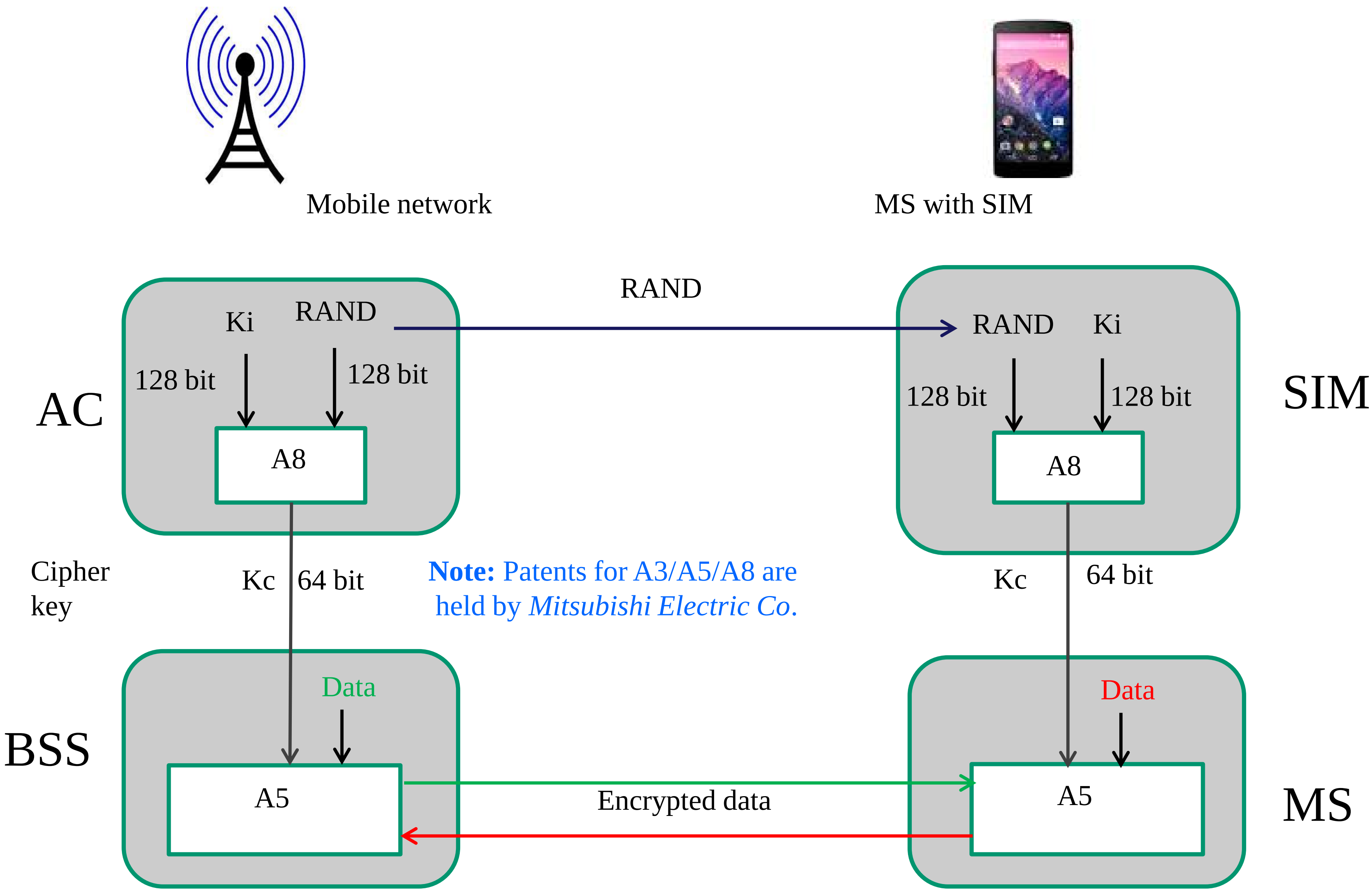


Fig. 4.15: Data encryption

A5: a key generation algorithm; A8: a symmetric-key encryption algorithm



Dynamic Channel (carrier) Assignment in Cellular Systems

Sources: Section 2.8 (Schiller) and

A. Baiocchi, F. D. Priscoli, F. Grilli and F. Sestini, **The geometric dynamic channel allocation as a practical strategy in mobile networks**, IEEE TVT, Vol 44, No 1, Feb. 1995, pp. 14-23

Topics

- Cellular systems
- Carrier Assignment Problem
  - Static
  - Dynamic
- DCA Algorithm

Cellular Systems

- A geographic area is divided into smaller, circular areas called **cells**.
- A **base station** (transceiver) is installed at the cell's center. Cell = radio coverage area.
- Cell radius
  - 10s of meters in buildings
  - 100s of meters in cities
  - 10s of KM in countryside

Cellular Systems

- Advantages of smaller cells
  - Higher capacity (frequency **reuse)** 🡸 users
  - Less transmission power for MS (no BS problem)
  - Robust against failures of single components
- Disadvantages of smaller cells
  - Larger infrastructure (antennas, switches, …)
  - Frequent handover
  - Better planning: frequency assignment, etc.

Carrier Assignment Problem

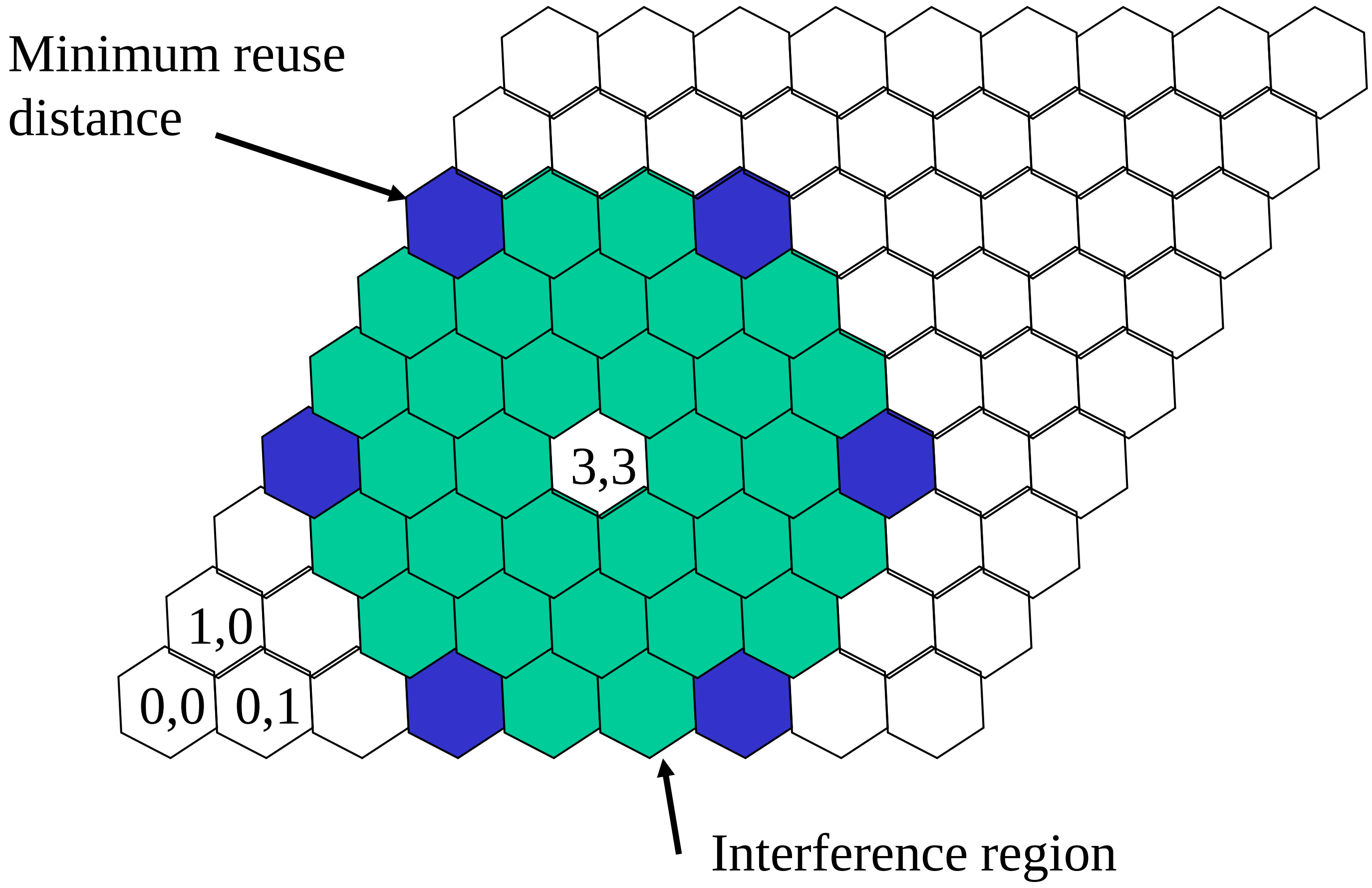
- Facts about GSM 900
  - FDM: 90 frequencies (up/down)
  - TDM: 8 slots/frequency

  ➔ Max number of active users = 90*8
- Low capacity ➔ need for reusing carriers
  - Space division multiplexing: reuse carriers far apart
    - » To reduce interference
    - » To increase capacity (# of users)

Carrier Assignment Problem

- Problem: Given a set of carriers and a cellular system
  - How to assign carriers to cells?
  - Maximum reuse ➔ maximum capacity
  - Lower **failure rate**
    - » **Blocking rate**
    - » **Dropping rate**

Cellular model



Carrier Assignment Algorithms

- **Fixed assignment** of carriers to cells
  - Use these carriers until further notice.
  - Simple to implement. No signaling load.
  - Good (bad) for low (high) traffic.

- **Dynamic assignment** of carriers to cells
  - All carriers are “available” in all cells.
  - Improved performance.
  - High signaling load.

Dynamic Carrier Assignment

- (*m, n*): cell at row *m* and column *n*
- (x, y): center of a cell
- (x,y): center of cell (*m, n*) is computed as
  - (x,y) = (*n, m*) $\begin{bmatrix} \text{Sqrt(3)*R} & 0 \\ \text{Sqrt(3)*R/2} & \text{3*R/2} \end{bmatrix}$ R = cell radius

Dynamic Carrier Assignment

- Reuse condition: Two carriers can be simultaneously used in two cells only if their separation > D_{min}.
- Assume $D_{min} = (3*\sqrt{3})*R$
- Interference neighborhood of a cell c
  - $IN(c) = \{c' | dist(c,c') < D_{min}, c <> c'\}$
  - 30 cells
- If cell c uses a frequency, no cell in IN(c) can reuse it.

Dynamic Carrier Assignment

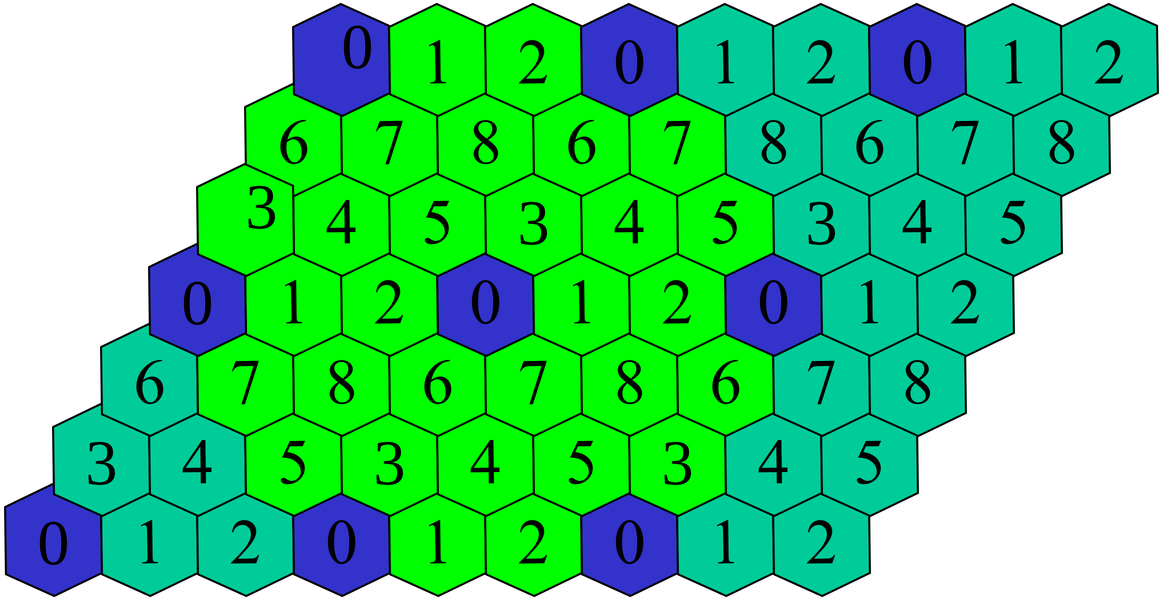
- **Status** of a carrier *r* in a cell *c*
  - **Used**: status(*r*, *c*) = UC
    - if at least one channel of *r* is currently used by some user in *c*.
  - **Interfered**: status(*r*, *c*) = IC
    - if status(*r*, *c’*) = UC for some c’ in IN(c).
  - **Available**: status(*r*, *c*) = AC
    - if status(*r*, *c*) <> UC AND status(*r*, *c*) <> IC.

Dynamic Carrier Assignment

- **Geometric strategy**
  - Divide the **cell array** into **k groups** S_0, S_1, …, S_{k-1} such that distance between any pair of cells in the same group is at least D_{min}.
  - The **carrier** set is **split** into **k groups** P_0, P_1, …, $P_{k-1.}$ Carriers in each P_i is considered to be *ordered*.
  - When a cell c in S_i needs a carrier, it **checks the ordered lists** P_i, P_{i+1}, …, P_0, …, P_{i-1} in that order and **acquires** the first **available** carrier encountered.

Dynamic Carrier Assignment

For $D_{min} = (3 * \sqrt{3}) * R$, **k = 9**.



Dynamic Carrier Assignment

- **Performance measures**
  - **Blocking rate (Rb)**: failure to assign a channel to new calls.
  - **Dropping rate (Rd)**: failure to assign a channel to a moved-in call.
  - **Failure rate (Rf)**: Rf = Rb + (1-Rb)*Rd
- **How to obtain Rf**?
    - Analytic
    - Simulation

Dynamic Carrier Assignment

- **Simulation parameters**
  - Cell grid ← how big, wrapped around
  - Total available carriers (90 for GSM)
  - TDM slots (8/frequency) ← invisible in algorithm
  - Traffic: call arrival rate
  - Mobility: handoff rate (pattern??)
  - Mean service time
  - Uniform/nonuniform traffic (hot/normal states)

Techniques for lowering failure rates of DCAs

- Power control
- Adaptive antenna array (also, tri-sector)
- Carrier compaction
- Prioritized release
- Lower QoS (channel sub-rating)
- Call on hold
- Synchronous BTS

GPRS: General Packet Radio Service

Wireless and Mobile Network Architectures

Yi-Bin Lin and I. Chlamtac (Wiley)

+

Schiller

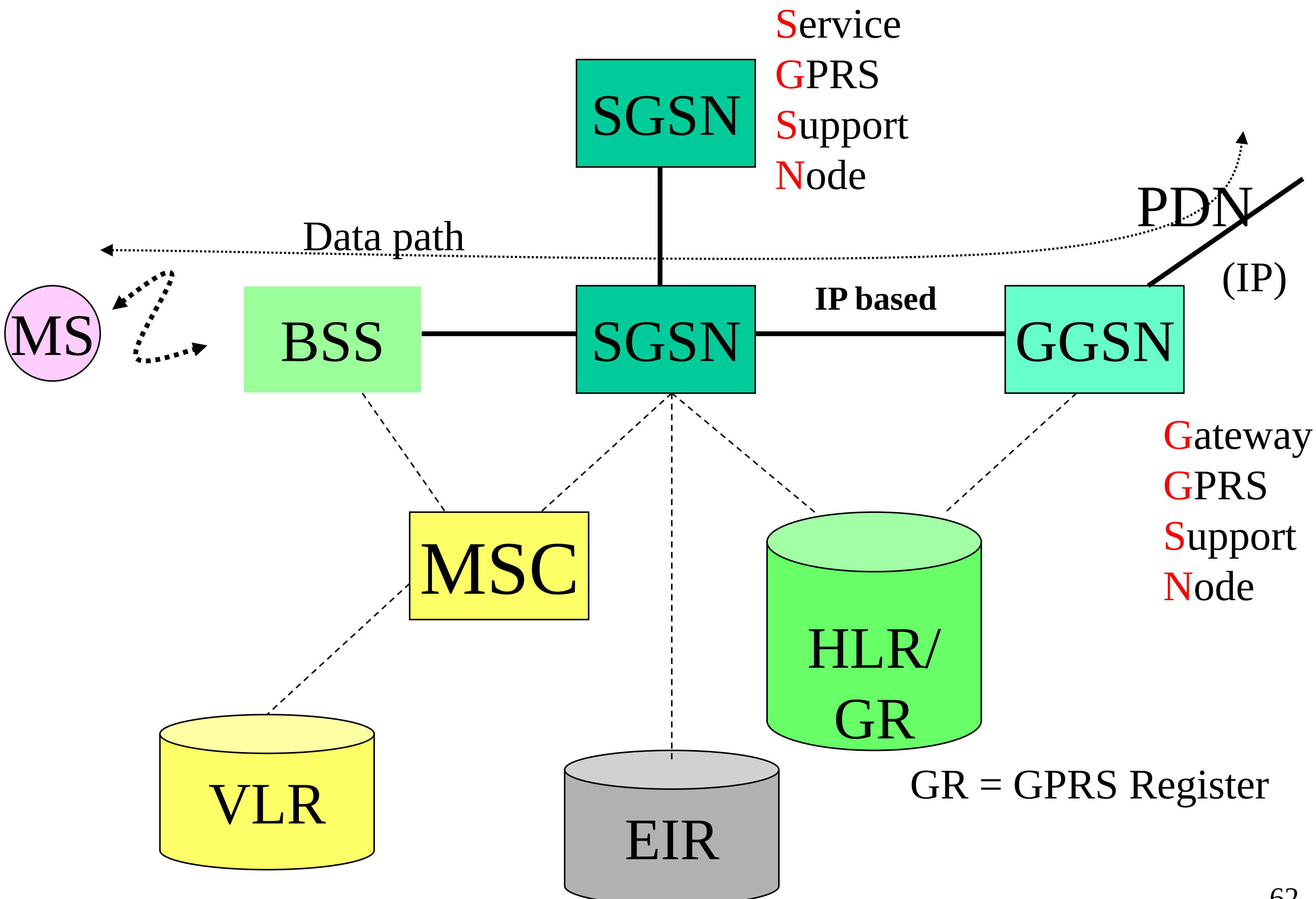
GPRS

- GSM is fully circuit-switched.
  - Not suitable for Internet application
    - Up link: frequent Tx of small volume data
    - Down link: Infrequent Tx of small/medium volume
- Need for packet-oriented service → GPRS
- Success of GPRS:
    - Packet oriented Internet
    - Different services: broadcast, multicast, unicast

Main concepts of GPRS

- For new GPRS channels, GSM system allocates 1-8 slots in a frame
- Time slots are allocated on demand
- Time slots are shared by the active users
- Allocation is based on load + op. preference

GPRS architecture



Gateway GPRS Support Node (GGSN)

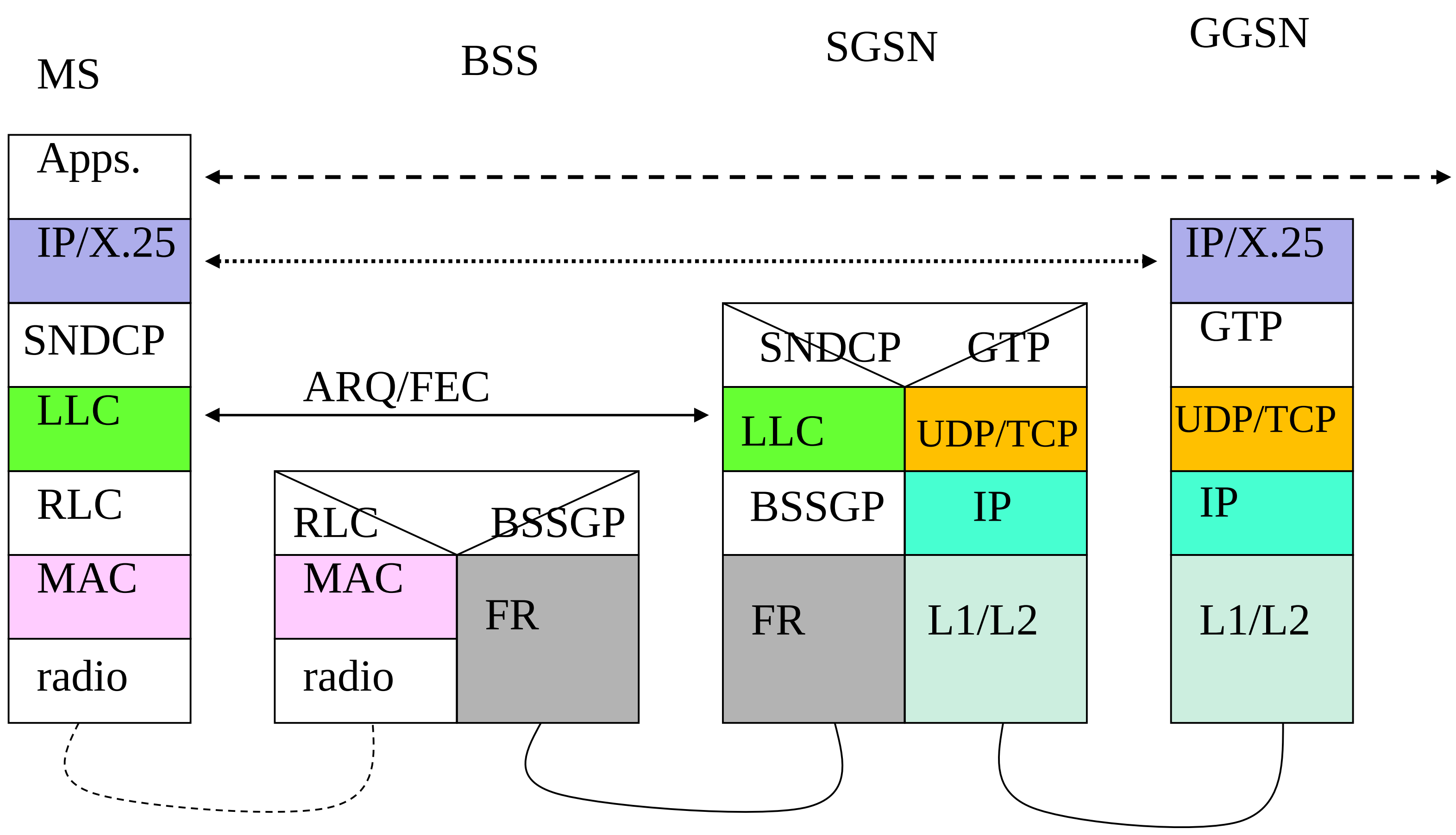
- Link between GPRS and data net (IP)
- Functions
  - routing,
  - tunneling via encapsulation

Serving GPRS Support Node

- Supports MS (through BSS)
- Functions:
    - Requests user addresses from the GR (GPRS Register)
    - Keeps track of individual MSs' location

GPRS protocol stack

All data within GPRS backbone are transmitted using tunneling protocol.



Three GPRS terms

- Mobility Management context
- PDP context
- QoS profile

MM context (MM state)

- MM state
  - IDLE: MS is not attached to the GPRS mm
  - STANDBY: Attached but has not obtained loc. info.
  - READY: Loc info has been identified on cell level

- MM context stored in MS + SGSN
- GPRS attach ➔ (MS ⇔ SGSN logical link)

PDP (packet data protocol) contexts

- Stored in MS, HLR, SGSN, GGSN
- Contain mapping and routing info for packet Tx between MS ←→ GGSN
- After PDP context activation, MS is known to the GGSN
- As many PDP contexts as the number of IP addresses.
- ACTIVE and INACTIVE contexts

QoS profile

- QoS profile maintained in the PDP context
- Indicates radio and network resources required for data transmission.
- QoS attributes
  - Precedence class: three Tx priority levels (congestion ➔ discard)
  - Delay class: four {In 128-octet transfer, expected delays are < 0.5 s, 5 s, 50s, best effort.

QoS profile (contd)

- Reliability classes (five) define error rate for data loss, out of sequence delivery, and corrupted data.
- Peak throughput classes (nine) specify expected max data rate from 8 Kbps to 2048 Kbps.
- Mean throughput classes (19) specify average data transmission rate.

Mobile Station (MS)

- GPRS MS = MT + TE
- MT ←→ BSS over the air.
- MT ←→ SGSN link
- TE: a computer attached to an MT
- 3 modes of MS operations
  - Class A: circuit + packet switched ← simultaneous
  - Class B: circuit OR packet switched ← one at a time, auto
  - Class C: packet ONLY

MM context info in a GPRS SIM

- IMSI ➔ uniquely identifies an MS. Used as the key to search the databases in VLR, HLR, and GSN.
- P-TMSI (similar to TMSI in GSM)
- Address of routing area where the MS resides.

PDP context in MS

- PDP type (<u>one of</u> X.25, PPP, IP)
- PDP address (e.g. IP address)
- PDP state (ACTIVE/INACTIVE)
- QoS profiles

BSS (Base Station Subsystem)

- BSS = BSC + many BTS
- BSC and BTS are modified to include a new unit: PCU (packet control unit)
- BSC
    - forwards circuit-switched data to MSC and packet-switched data to SGSN (through the PCU)
    - manage GPRS-related radio resources

BSS (some solutions)

- Nortel (Although the company does not exist, the following are possible solutions)
  - GSM (BTS + BSC) + software upgrade
  - PCU functions are implemented in a PCUSN.
  - PCUSN capability: 12 BSCs/cabinet
- Alcatel
  - PCU in a multifunctional server (A935 MFS)
  - Capability: 22 BSS
  - 480 activated GPRS channels/BSC
- Ericsson
  - One PCU/BSC. 512 BTS/PCU. 4K GPRS channels.

GPRS Support Node

- Serving GSN + Gateway GSN
- Functionalities of SGSN and GGSN can be
  - Combined in a physical node (Ericsson)
  - Distributed in separate nodes (Nortel, Cisco, Motorola, Alcatel)
- GSN: multiprocessor system
  - Hardware redundancy
  - Robust software ➔ uninterrupted operation

SGSN

- Role is similar to MSC/VLR in GSM.
  - Inter-SGSN routing area update, statistics collection, charging
  - Establishes an MM context (mobility info)
  - Establishes a PDP context for MS ←→ GGSN comm
  - SGSN maintains MM/PDP context info

GGSN

- Traditional gateway functionality
  - Mapping addresses, routing and tunneling packets
- GGSN maintains an activated PDP context for tunneling packets from MS to SGSN.
  - IMSI, DPD type+address, QoS profile, IP of SGSN, access point name for external data network.
- Support 5-48 K simultaneous data tunnels and 25-48 K simultaneously attached users.

GPRS Interfaces

- Um: MS ←→ BTS
- Gb: BSS ←→ SGSN
- Gn, Gp: Utilize the GPRS Tunneling Protocol (GTP)
- Gs: Databases in MSC/VLR ←→ SGSN
- Gi: GGSN ←→ PDN (IP, PPP)

Um Interface

- GPRS radio tech is based on GSM radio
- GPRS introduces a new logical ch structure.
- Radio channel structure
  - The physical channel dedicated to packet data traffic is called a packet data channel (PDCH).
  - A PDCH can be split into several packet data logical ch.
  - GPRS utilizes packet data traffic channel (PDTCH) for data transfer: 1-many and many-1 mappings.
  - Several packet common control channels (PCCCH) are introduced.

Um (Radio interface)

- PRACH (packet rand. access): MS ➔ BTS
  - Used to initiate uplink transfer for data or signaling.
- Downlink PCCCH
  - Packet paging channel: pages an MS for both circuit and packet switched data.
  - PAGCH (access grant): for resource assignment.
  - Packet notification channel: Used to send a point-to-multipoint multicast (PTM-M) notification to a group of MSs prior to a PTM-M packet ransfer
  - PBCCH (broadcast): System info specific for packet data

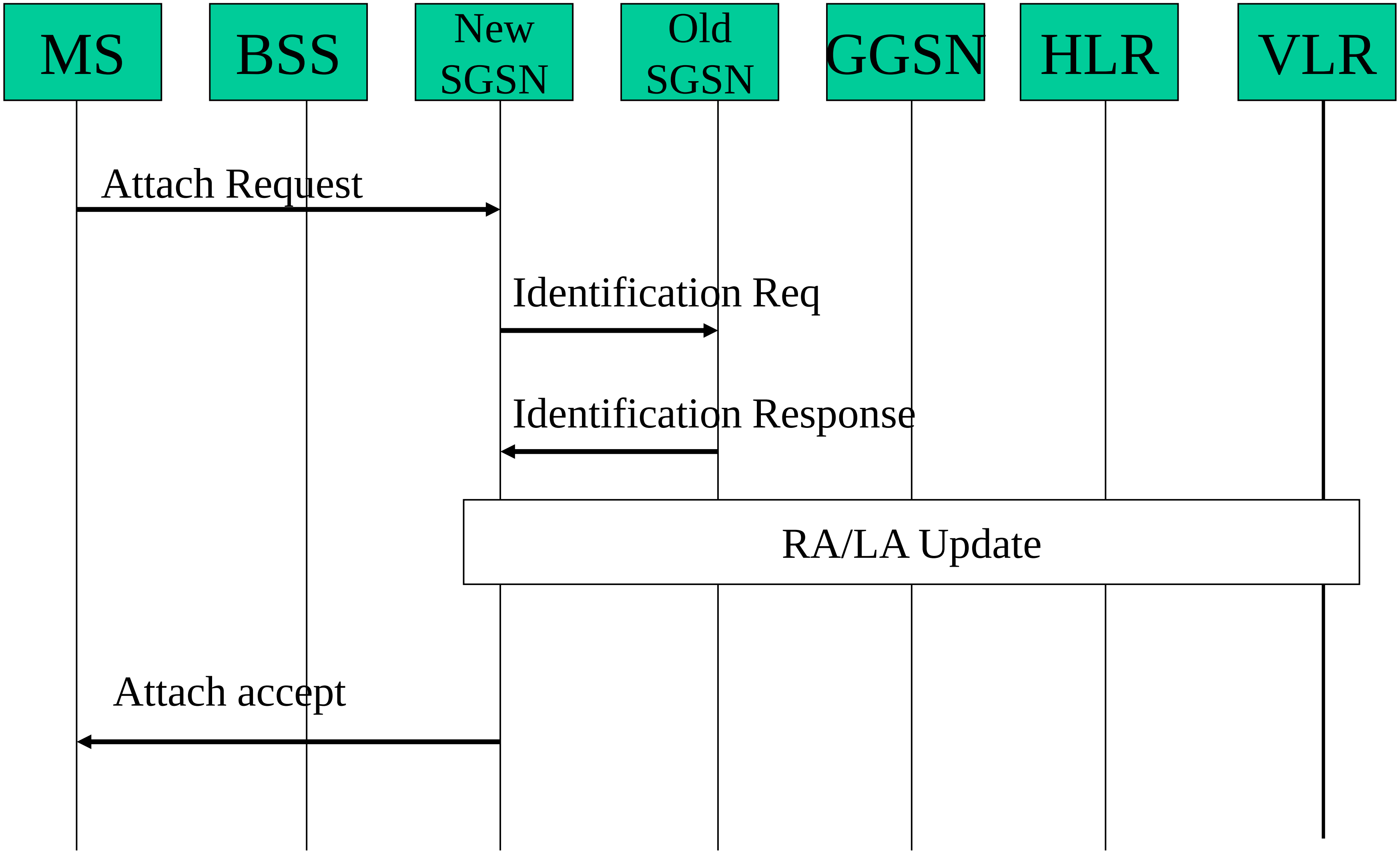
Um (Packet-dedicated control channels)

- PACCH (associated control ch):
  - Conveys signaling info: power control, resource assigment
  - MS involved in packet transfer can be paged for circuit-switched services on PACCH.

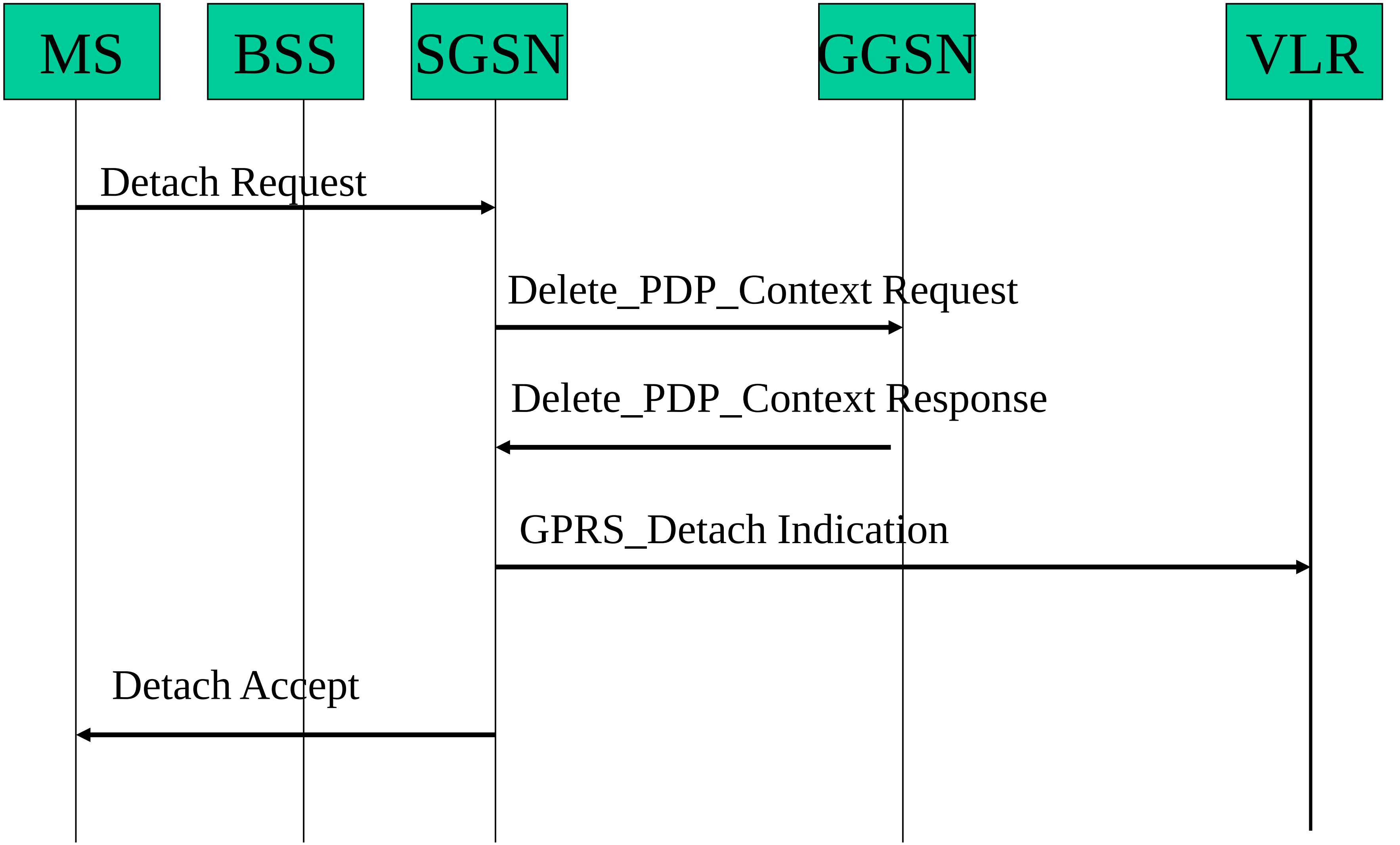
GPRS Procedures

- Attach/Detach procedures:
  - Establishes a logical link between MS ←→ SGSN
- PDP context procedures:
  - allows data transfer between MS and external world
- RA/LA update procedures
  - Tracks location of MS and reestablishes the link between MS ←→ SGSN

Attach procedure



Detach procedure



Cellular model