Rhizomatica

GSM Protocol Introduction

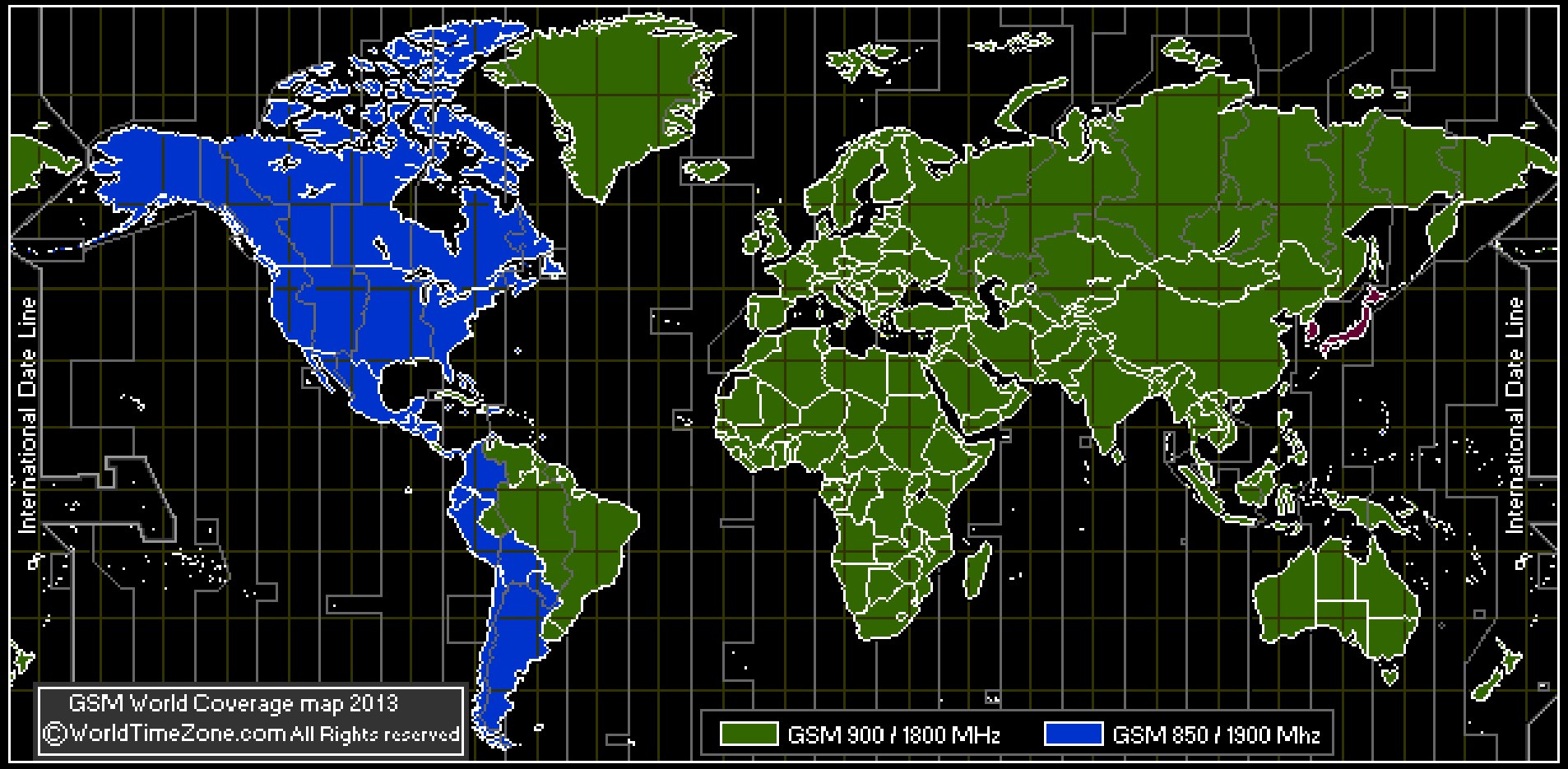
GSM Introduction

- GSM (Global System for Mobile Communication) is a mobile network architecture comprised of different protocols and used worldwide for mobile voice and data communication.
- It relies on MS (Mobile Stations) and a network backbone comprised of different components (BTS, BSC, MSC, HLR, VLR, etc. etc.).
- It's now a worldwide standard, used in more than 80% of the countries worldwide.

GSM Introduction

- GSM can operate on multiple frequencies, depending on the country.
- Most of the world use the original 900/1800Mhz specification.
- Some countries in the American Continent use 850/1900Mhz, or a combination of the four different frequencies.

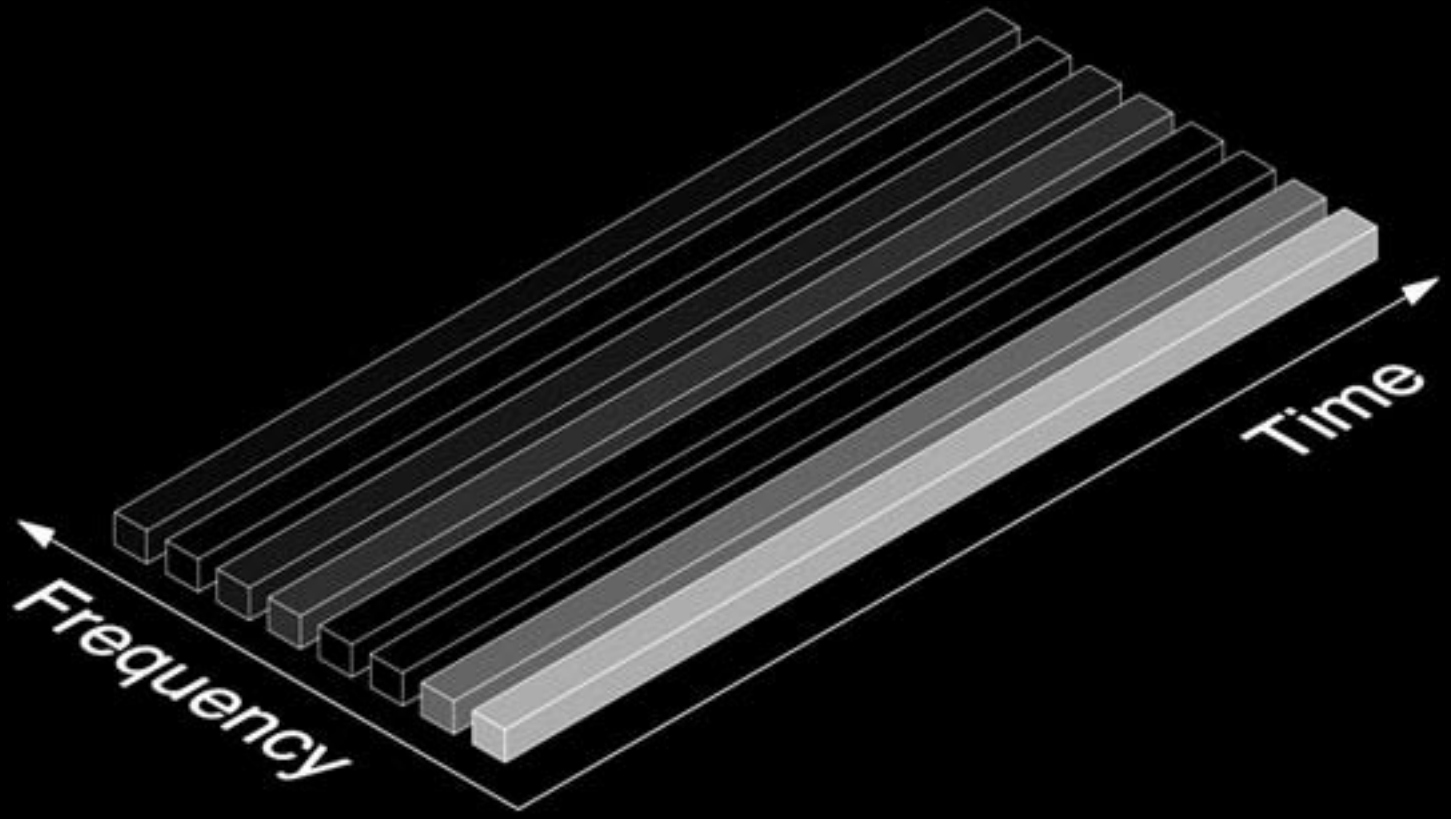
GSM World Map



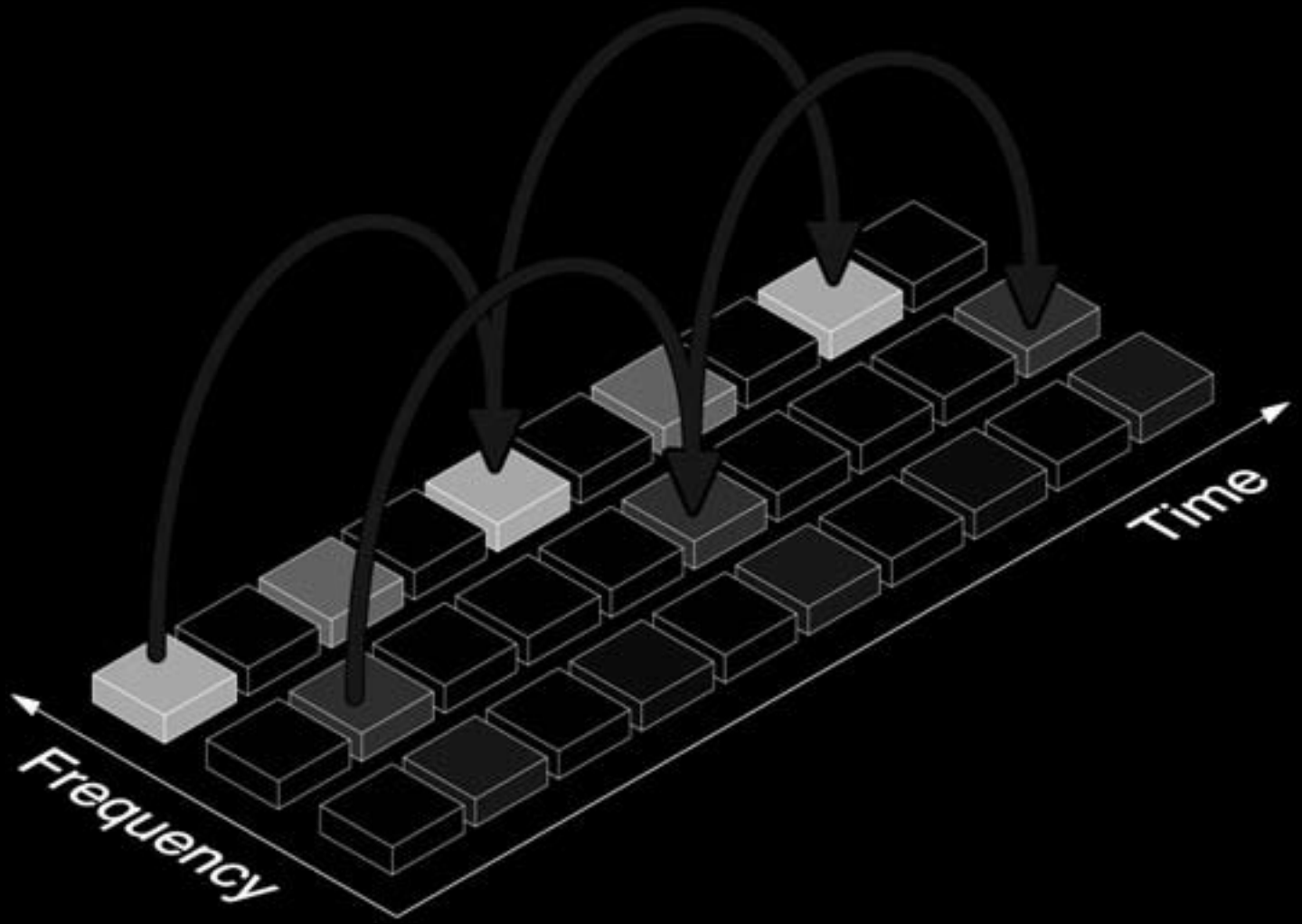
Radio Interface (Um)

- A combination of TDMA and FDMA.
- FDMA = Frequency Division Multiple Access.
- TDMA = Time Division Multiple Access.
- Each frequency is 200Khz wide (ARFCN).
- Uplink and Downlink are 45Mhz apart.
- Each ARFCN is divided in 8 time-slots.

FDMA



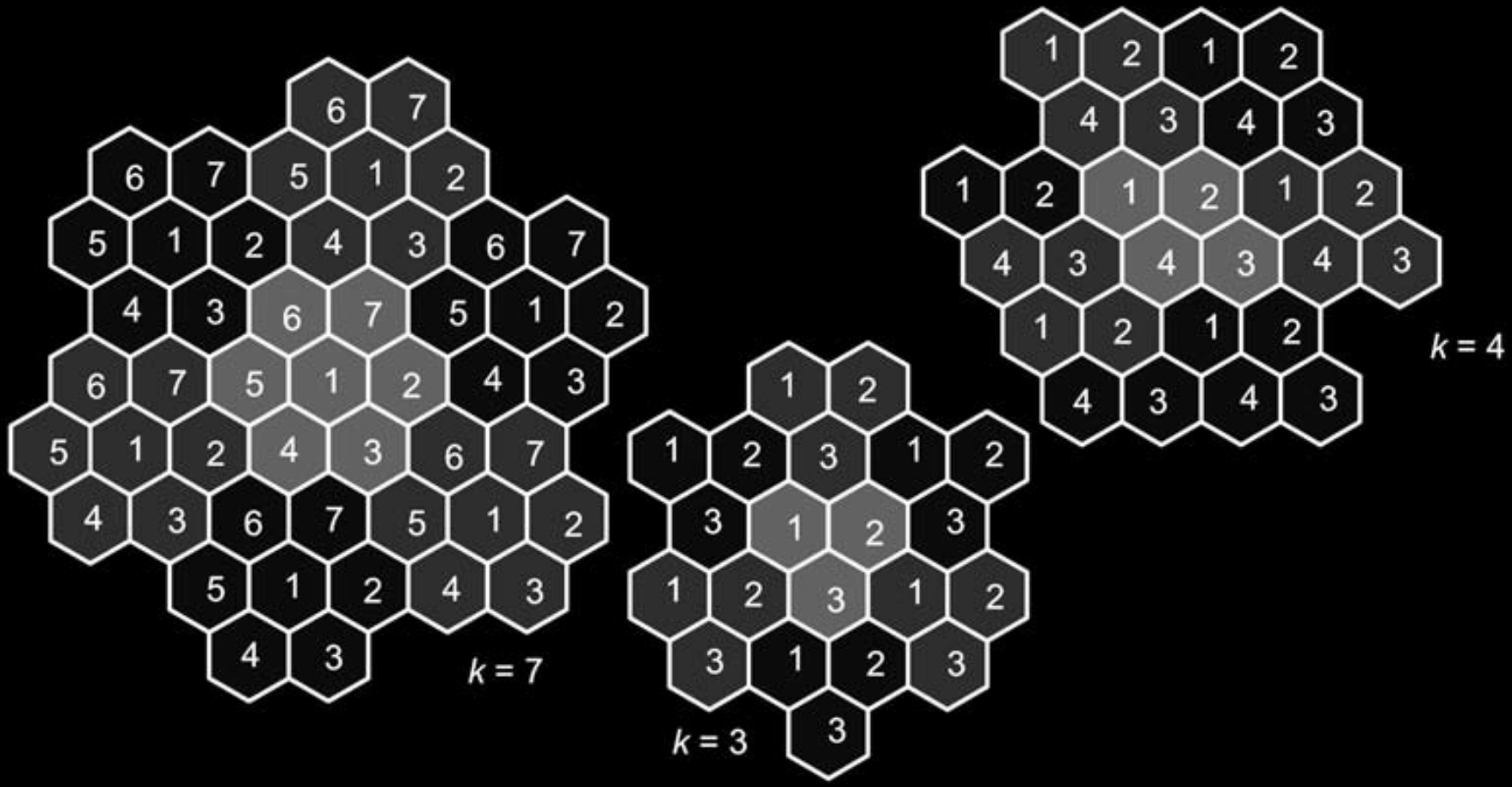
TDMA



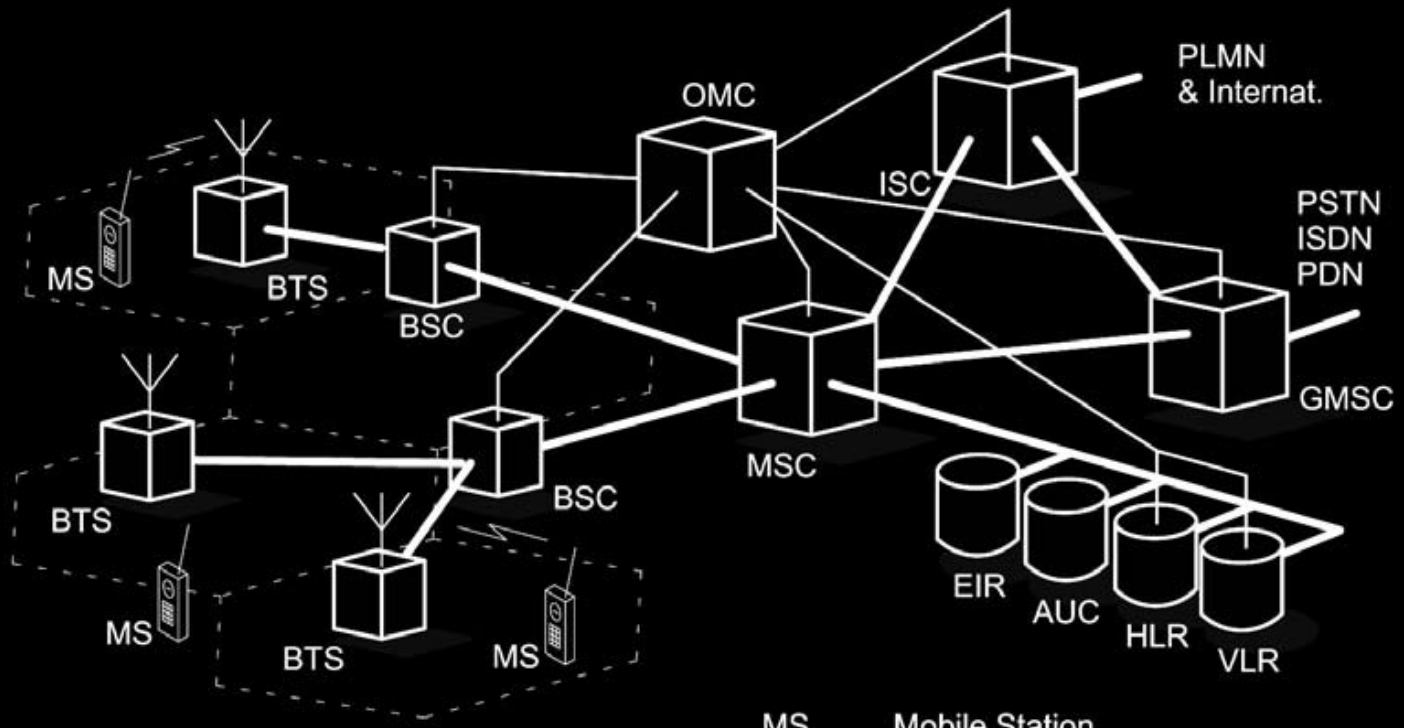
Cellular principle

- There are only so many frequencies available in one network, so we need to re-use them in different places.
- The network has to be divided in cells, normally represented with a hexagonal shape.
- The same frequency can be re-used only when two cells are far apart enough to not interfere with each others.

Cellular principle



System architecture



BTS	Base Transceiver Station
BSC	Base Station Controller
MSC	Mobile Switching Center
GMSC	Gateway MSC
ISC	International Switching Center

MS	Mobile Station
HLR	Home Location Register
VLR	Visited Location Register
EIR	Equipment Identity Register
AUC	Authentication Center
OMC	Operation and Maintenance Center

System architecture

- MS (Mobile Station)
- BTS (Base Transceiver Station)
- BSC (Base Station Controller)
- MSC (Mobile Switching Center)

- GMSC (Gateway MSC)
- ISC (International Switching Center)
- HLR (Home Location Registry)
- VLR (Visitor Location Registry)
- AUC (Authentication Center)
- EIR (Equipment Identity Register)
- OMC (Operation and Maintenance Center)

Mobile Station

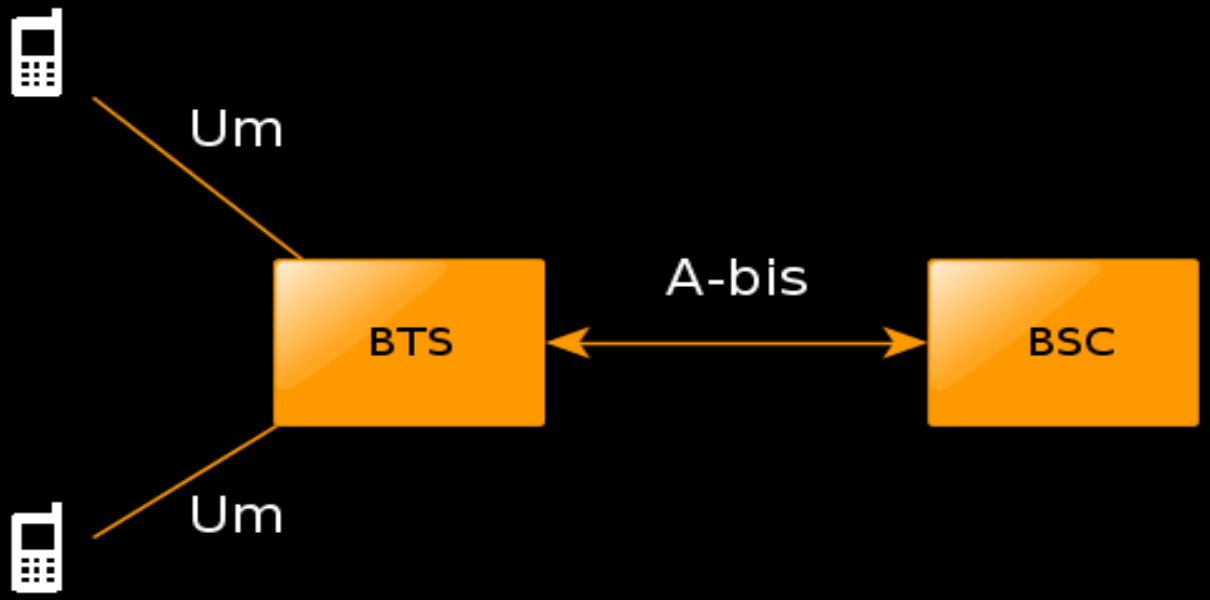
- Also known as “Mobile Phone” :-)
- Identified by the IMEI (International mobile station equipment identity).
- Includes a SIM Card (Subscriber Identity Module).
- The SIM is identified by the IMSI (International mobile subscriber identity).
- The “real” phone number is called MSISDN (Mobile Subscriber ISDN Number).

Mobile Station

- IMEI = equipment.
- IMSI = subscriber.
- The MSISDN is not in the SIM card.
- MSISDN is associated with the IMSI (in the HLR).
- Talks with the BTS using the Um protocol.

Base Transceiver Station

- 1 frequency channel = 1 Transceiver (Transmit/Receive).
- Talks the Um interface (radio) to MS.
- Talks the A-Bis interface to the BSC.



Base Station Controller

- Handles multiple BTSs.
- Manages the channel assignment.
- Checks signal quality, handles handover.
- Power management of the MS.

Mobile Switching Center

- Routes voice and SMS.
- Authenticates the MS.
- Keeps track of the MS location.
- Handles inter-BSC handover.
- Assigns the TMSI
  (Temporary Mobile Subscriber Identifier).

Other Databases

- HLR - users information.
- VLR - information about user location.
- AUC - security-related data (authentication keys, encryption keys).
- EIR - IMEI of all the phones, can also be used to block broken/stolen MS.

Radio channels (1/2)

- TCH: Traffic channels
  - TCH/F: Full Rate channel
  - TCH/H: Half Rate channel
- BCH: Broadcast channels
  - BCCH: Broadcast Control channel
  - FCCH: Frequency Correction channel
  - SCH: Synchronization channel

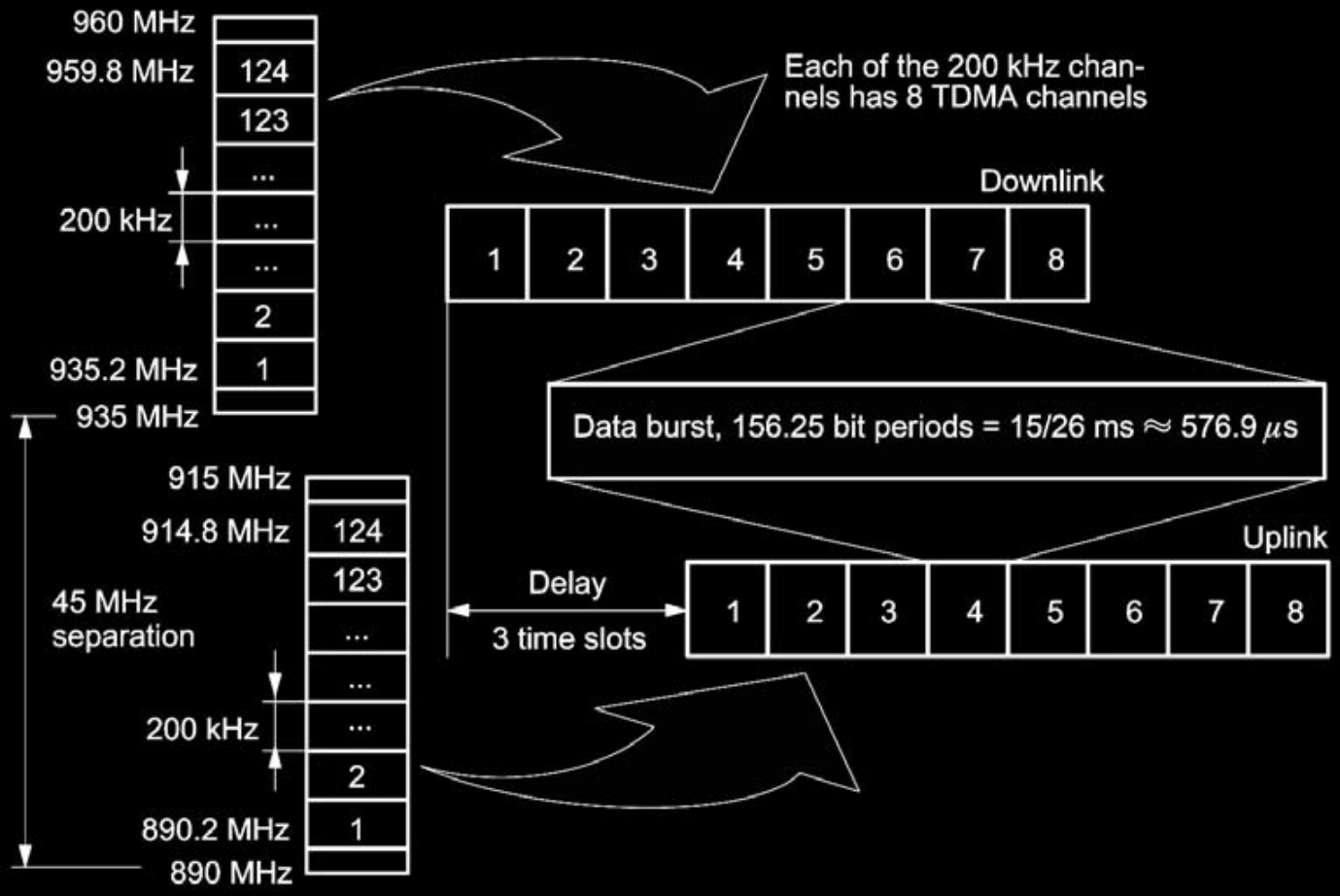
Radio channels (2/2)

- CCCH: Common Control channels
  - RACH: Random Access channel
  - AGCH: Access Grant channel
  - PCH: Paging channel
- DCH: Dedicated Control channels
  - SDCCH: Stand-Alone Dedicated Control channel
  - SACCH: Slow Associated Control channel
  - FACCH: Fast Associated Control channel

Channel combinations

	B1	B2	B3	B4	B5	B6	B7	B8	B9
TCH/F									
TCH/H									
TCH/H									
BCCH									
FCCH									
SCH									
CCCH									
SDCCH									
SACCH									
FACCH									

Duplexing


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
Each of the 200 kHz chan-
nels has 8 TDMA channels
Downlink
1 2 3 4 5 6 7 8
Data burst, 156.25 bit periods = 15/26 ms ≈ 576.9 μs
Uplink
Delay
3 time slots
1 2 3 4 5 6 7 8

MS Initialization

- Frequency Synchronization
  - Find a GSM signal
  - Check if the frequency is a beacon frequency
- Time Synchronization
  - Detect the start of a time-slot
  - FCCH (frequency) + SCH (training sequence)
- Network and cell information acquisition
  - Acquire the LAI (MCC, MNC, LAC), Cell ID (CID), BCCH allocation list, channel locations

Network selection

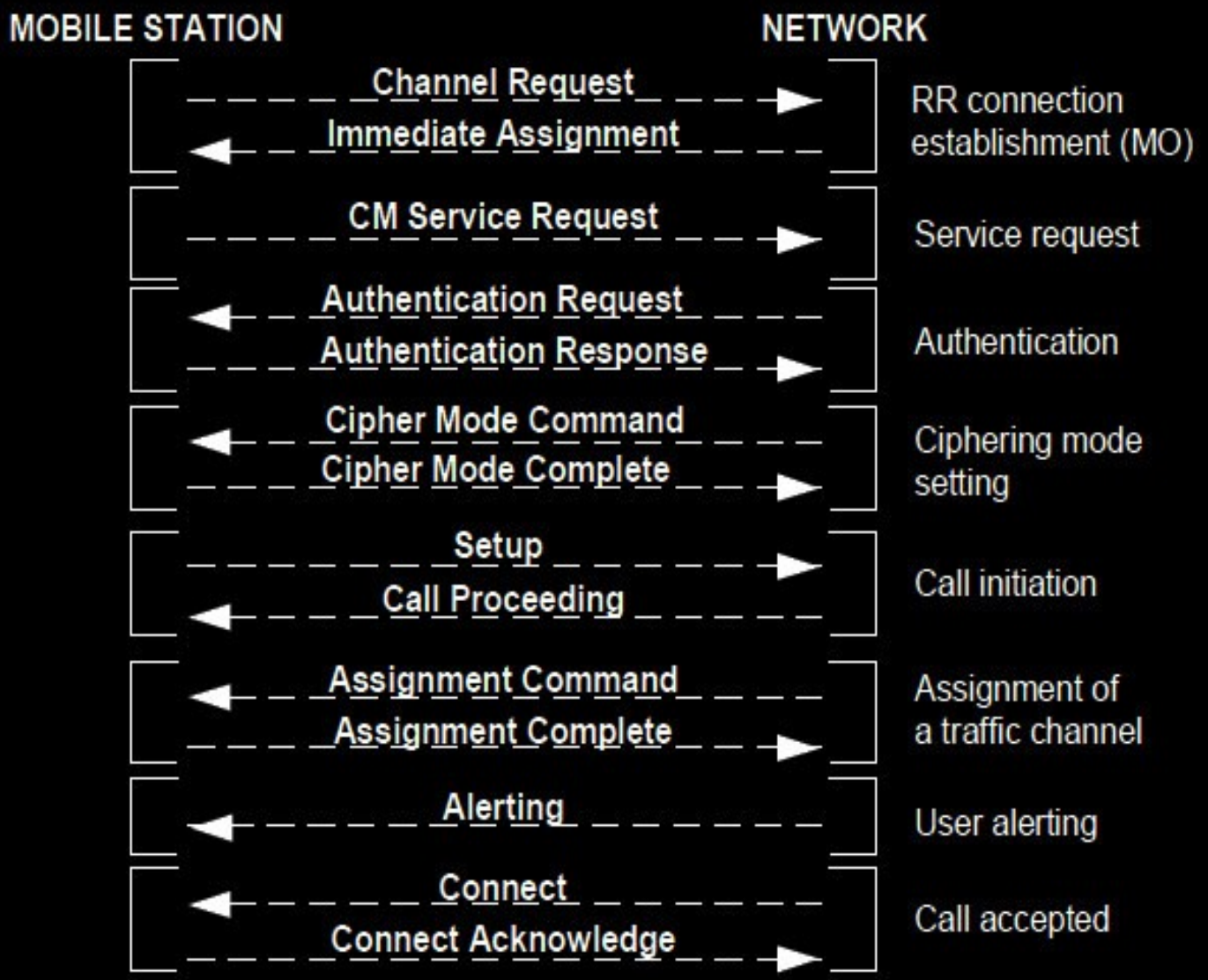
- Try to find the home network.
- Connect to networks in the preferred list.
- Connect to any other network, except ones in the blacklist.

- Home network, preferred list and blacklist are stored in the SIM card.

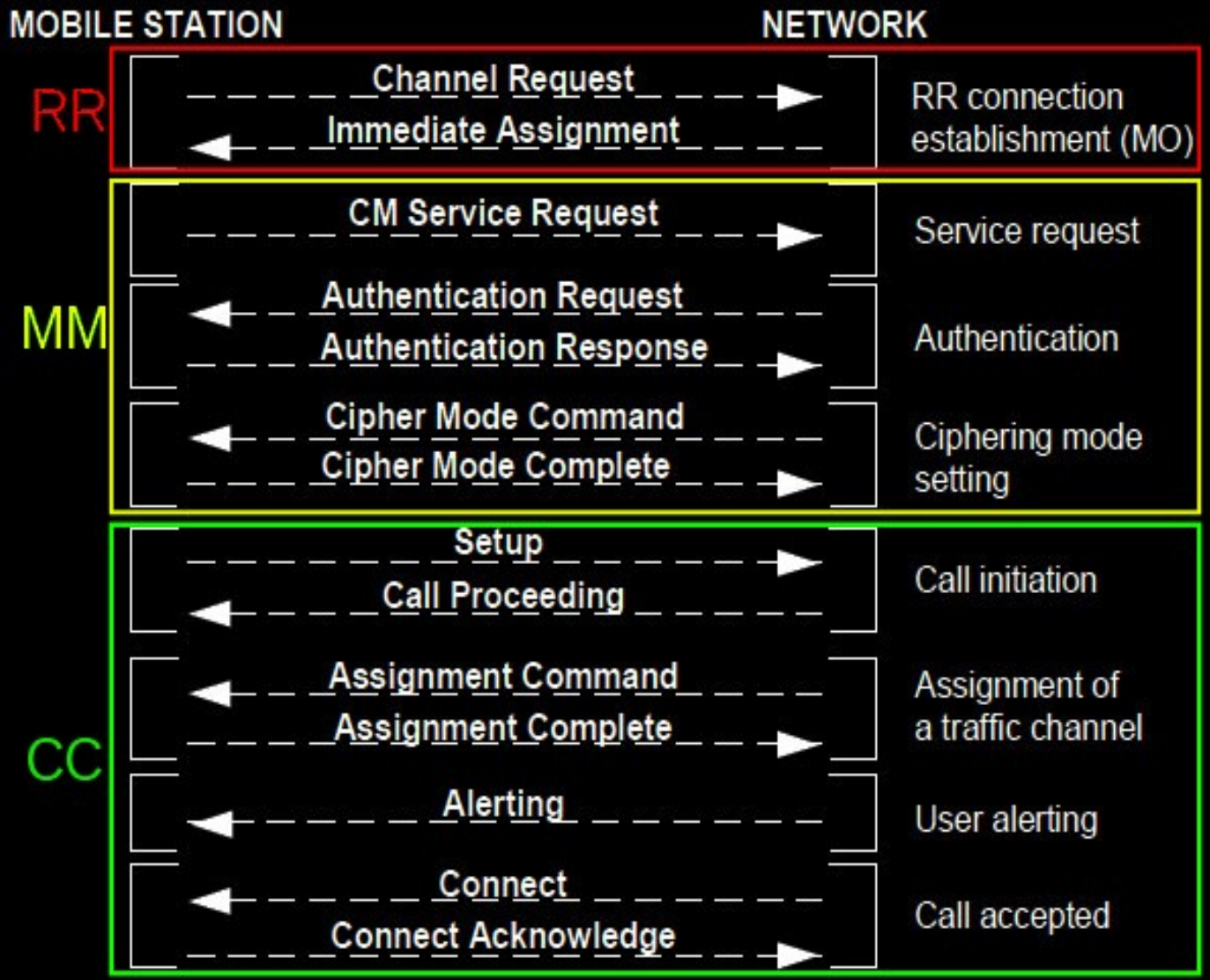
Phone call (1/3)

- MS does a channel request, BTS reply
- MS does a service request, SDCCH gets allocated
- From the SDCCH, MS require a TCH channel
- MSC authenticate the MS, set the cypher mode
- TCH channel gets allocated
- MSC connects the call at both ends

Phone call 2/3



Phone call 3/3

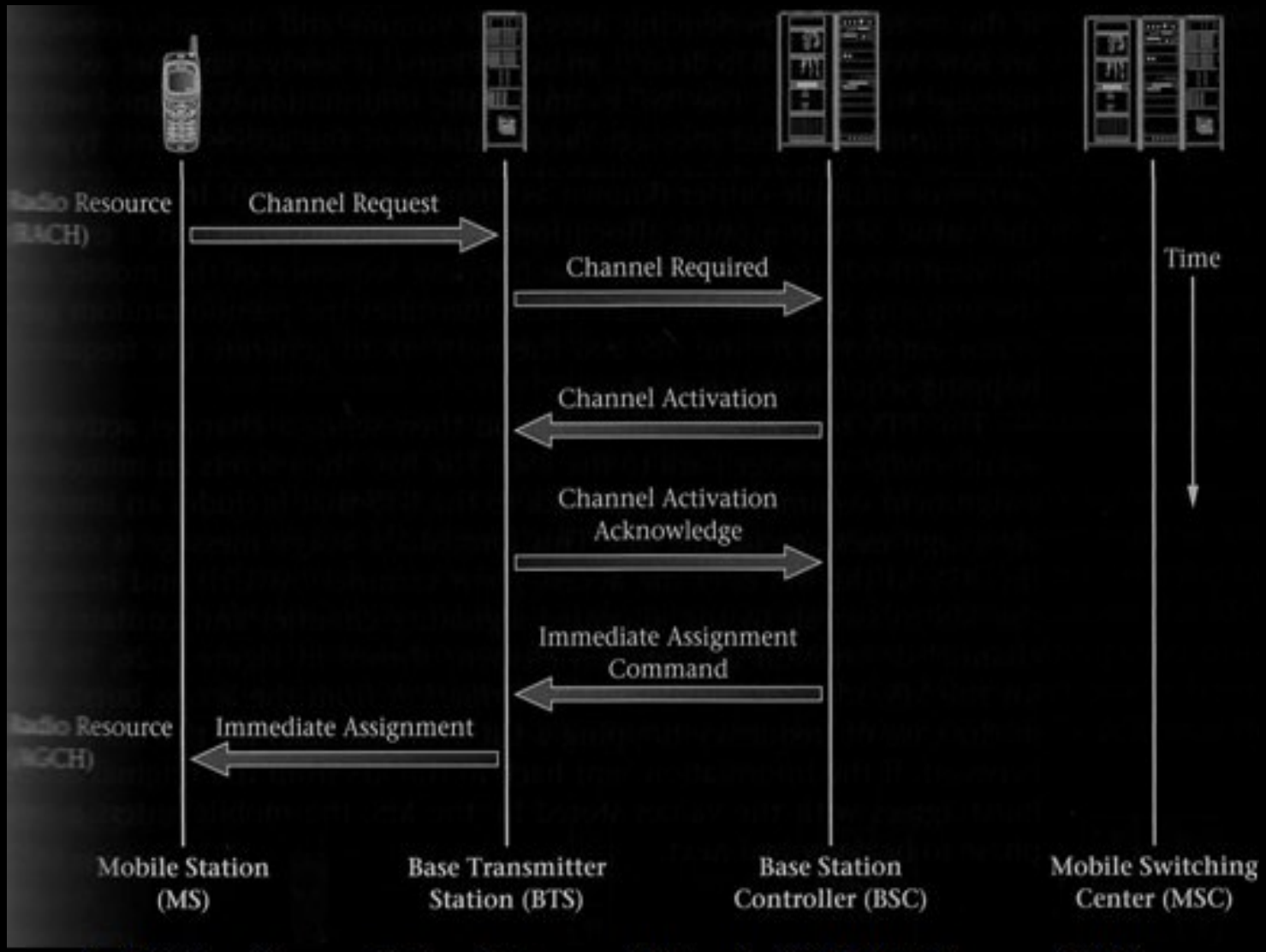


Channel request (1/2)

- MS sends the request on the RACH.
- BSC allocates the SDCCH.
- BSC sends the Immediate Assignment on the AGCH

RACH = Random Access Channel
SDCCH = Stand-alone Dedicated Control Channel
AGCH = Access Grant Channel

Channel request (2/2)



Ref: Wireless Communications Systems and Networks, By Mullett, Thomson Publisher