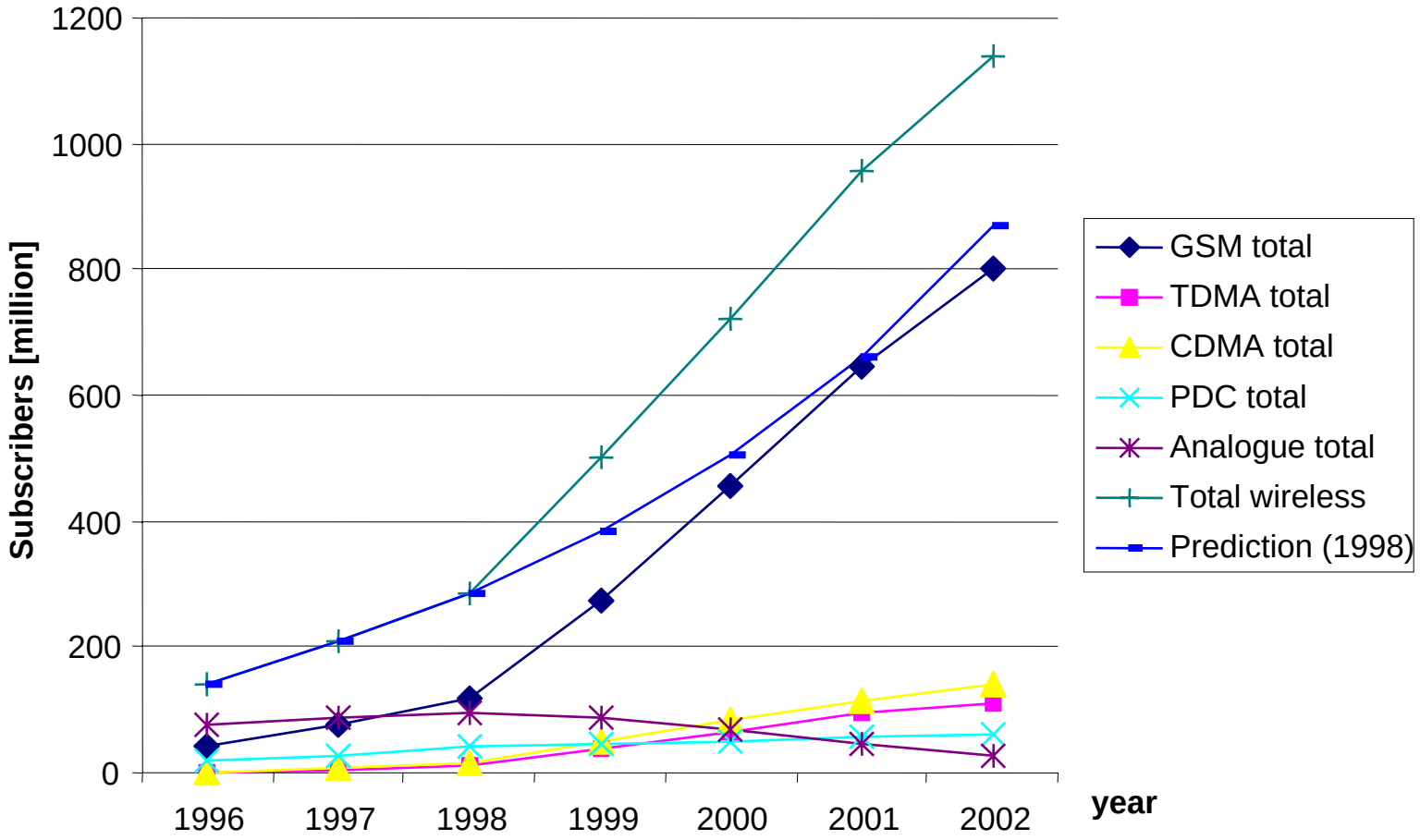
Introduction to Wireless Networks

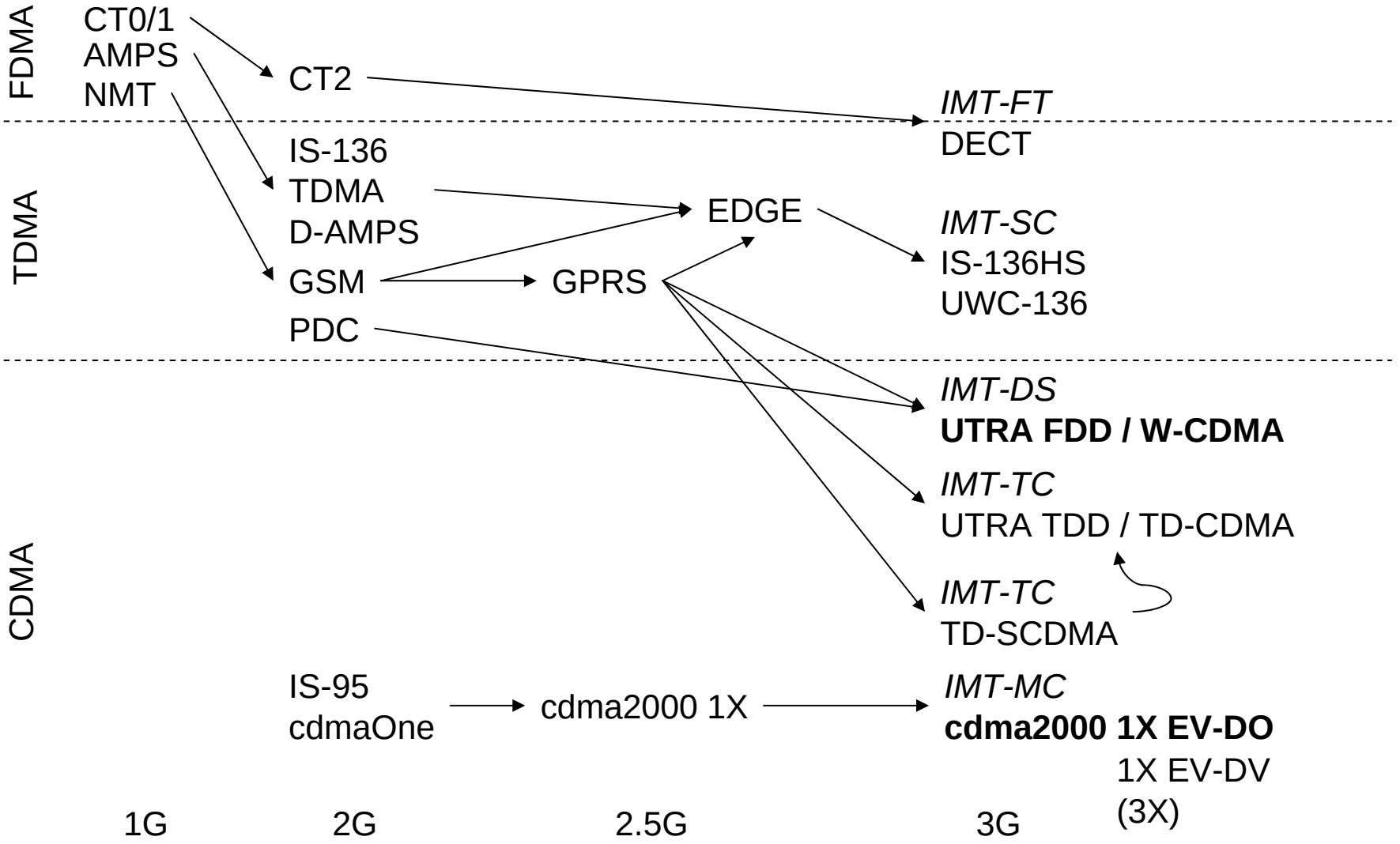
Chapter 4: Introduction to GSM

Prof. Yuh-Shyan Chen
Department of CSIE
National Taipei University

Mobile phone subscribers worldwide



Development of mobile telecommunication systems



GSM: Overview

GSM

- formerly: Groupe Spéciale Mobile (founded 1982)
- now: Global System for Mobile Communication
- Pan-European standard (ETSI, European Telecommunications Standardisation Institute)
- simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations (Germany: D1 and D2)
  ➔ seamless roaming within Europe possible
- today many providers all over the world use GSM (more than 184 countries in Asia, Africa, Europe, Australia, America)
- more than 747 million subscribers
- more than 70% of all digital mobile phones use GSM
- over 10 billion SMS per month in Germany, > 360 billion/year worldwide

Performance characteristics of GSM (wrt. analog sys.)

Communication

- mobile, wireless communication; support for voice and data services

Total mobility

- international access, chip-card enables use of access points of different providers

Worldwide connectivity

- one number, the network handles localization

High capacity

- better frequency efficiency, smaller cells, more customers per cell

High transmission quality

- high audio quality and reliability for wireless, uninterrupted phone calls at higher speeds (e.g., from cars, trains)

Security functions

- access control, authentication via chip-card and PIN

Disadvantages of GSM

There is no perfect system!!

- no end-to-end encryption of user data
- no full ISDN bandwidth of 64 kbit/s to the user, no transparent B-channel

- reduced concentration while driving
- electromagnetic radiation

- abuse of private data possible
- roaming profiles accessible

- high complexity of the system
- several incompatibilities within the GSM standards

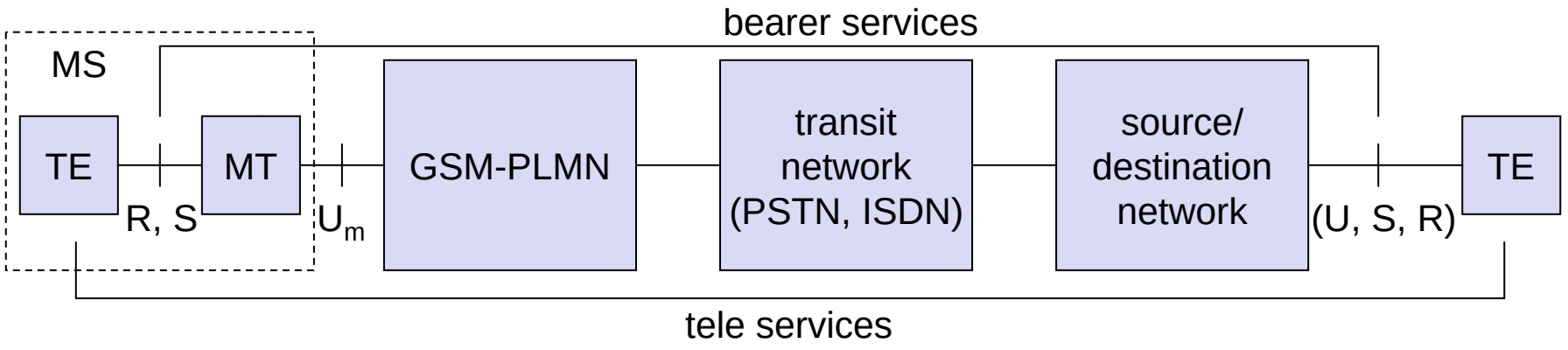
GSM: Mobile Services

GSM offers

- several types of connections
  - voice connections, data connections, short message service
- multi-service options (combination of basic services)

Three service domains

- Bearer Services
- Telematic Services
- Supplementary Services



Bearer Services

- Telecommunication services to transfer data between access points
- Specification of services up to the terminal interface (OSI layers 1-3)
- Different data rates for voice and data (original standard)
  - data service (circuit switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 1200 bit/s
  - data service (packet switched)
    - synchronous: 2.4, 4.8 or 9.6 kbit/s
    - asynchronous: 300 - 9600 bit/s

Today: data rates of approx. 50 kbit/s possible – will be covered later!

Tele Services I

- Telecommunication services that enable voice communication via mobile phones
- All these basic services have to obey cellular functions, security measurements etc.
- Offered services
  - mobile telephony
    primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz
  - Emergency number
    common number throughout Europe (112); mandatory for all service providers; free of charge; connection with the highest priority (preemption of other connections possible)
  - Multinumbering
    several ISDN phone numbers per user possible

Tele Services II

Additional services

- Non-Voice-Teleservices
  - group 3 fax
  - voice mailbox (implemented in the fixed network supporting the mobile terminals)
  - electronic mail (MHS, Message Handling System, implemented in the fixed network)
  - ...

  - Short Message Service (SMS)
    alphanumeric data transmission to/from the mobile terminal using the signaling channel, thus allowing simultaneous use of basic services and SMS

Supplementary services

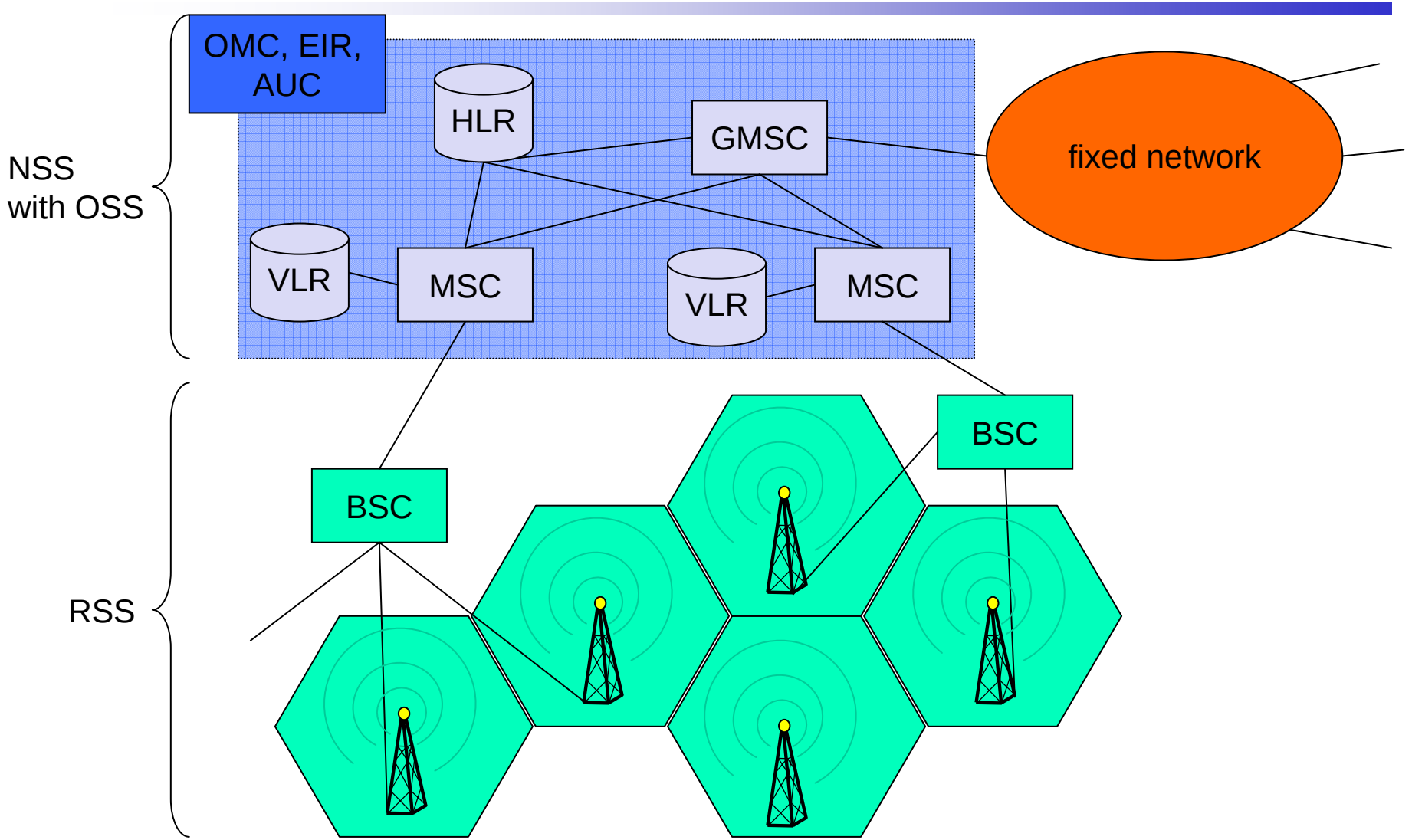
- Services in addition to the basic services, cannot be offered stand-alone
- Similar to ISDN services besides lower bandwidth due to the radio link
- May differ between different service providers, countries and protocol versions
- Important services
  - identification: forwarding of caller number
  - suppression of number forwarding
  - automatic call-back
  - conferencing with up to 7 participants
  - locking of the mobile terminal (incoming or outgoing calls)
  - ...

Architecture of the GSM system

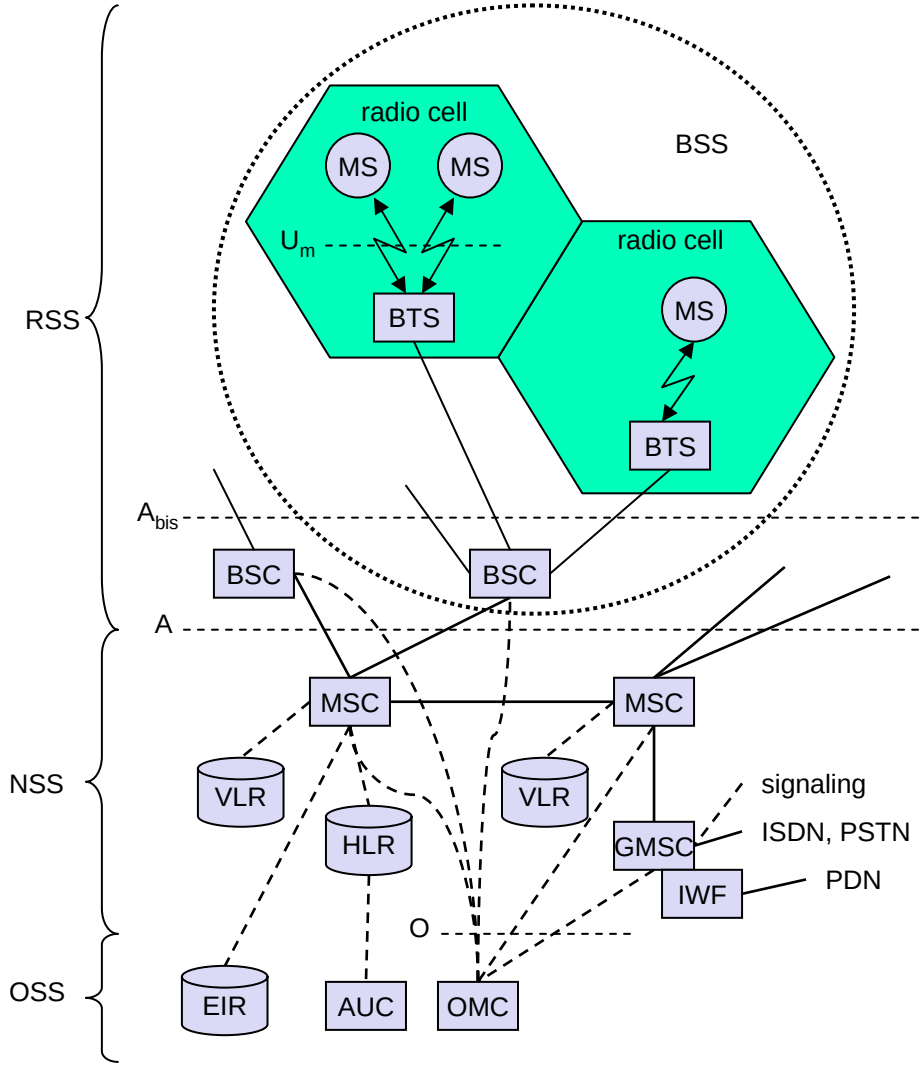
GSM is a PLMN (Public Land Mobile Network)

- several providers setup mobile networks following the GSM standard within each country
- components
  - MS (mobile station)
  - BS (base station)
  - MSC (mobile switching center)
  - LR (location register)
- subsystems
  - RSS (radio subsystem): covers all radio aspects
  - NSS (network and switching subsystem): call forwarding, handover, switching
  - OSS (operation subsystem): management of the network

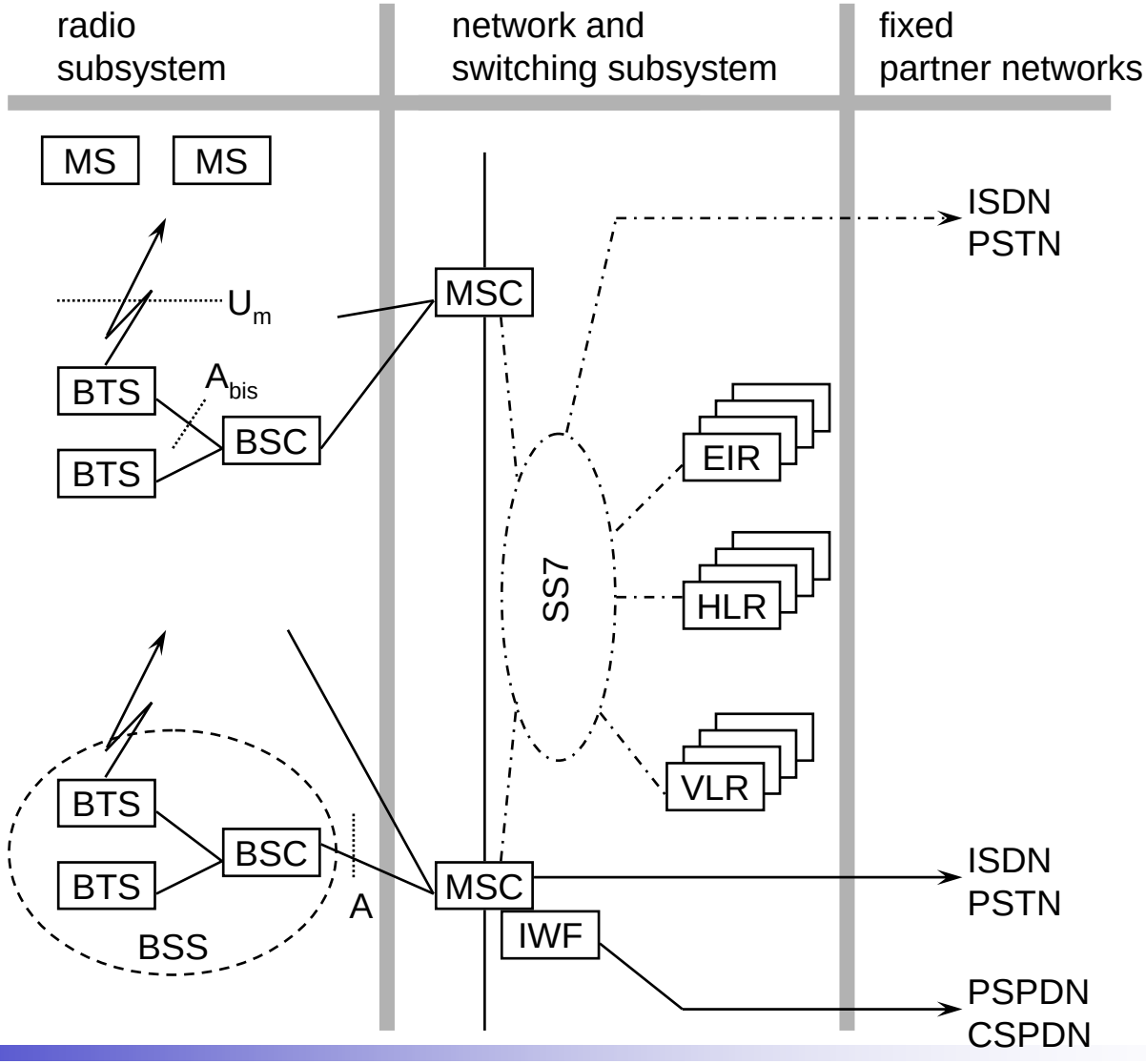
GSM: overview



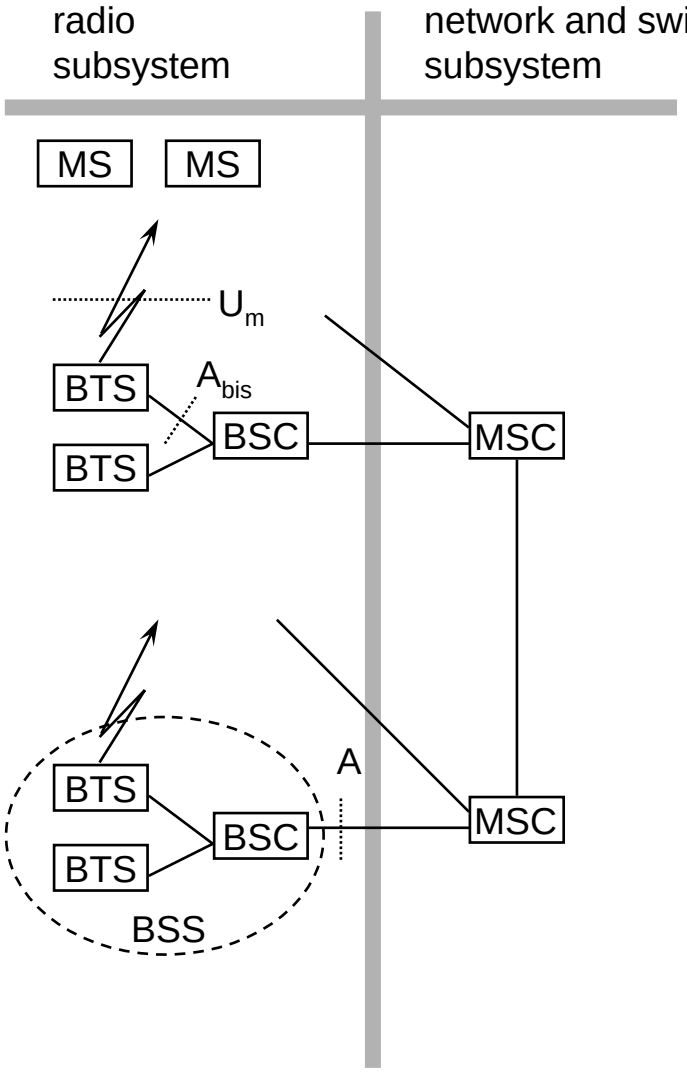
GSM: elements and interfaces



GSM: system architecture



System architecture: radio subsystem



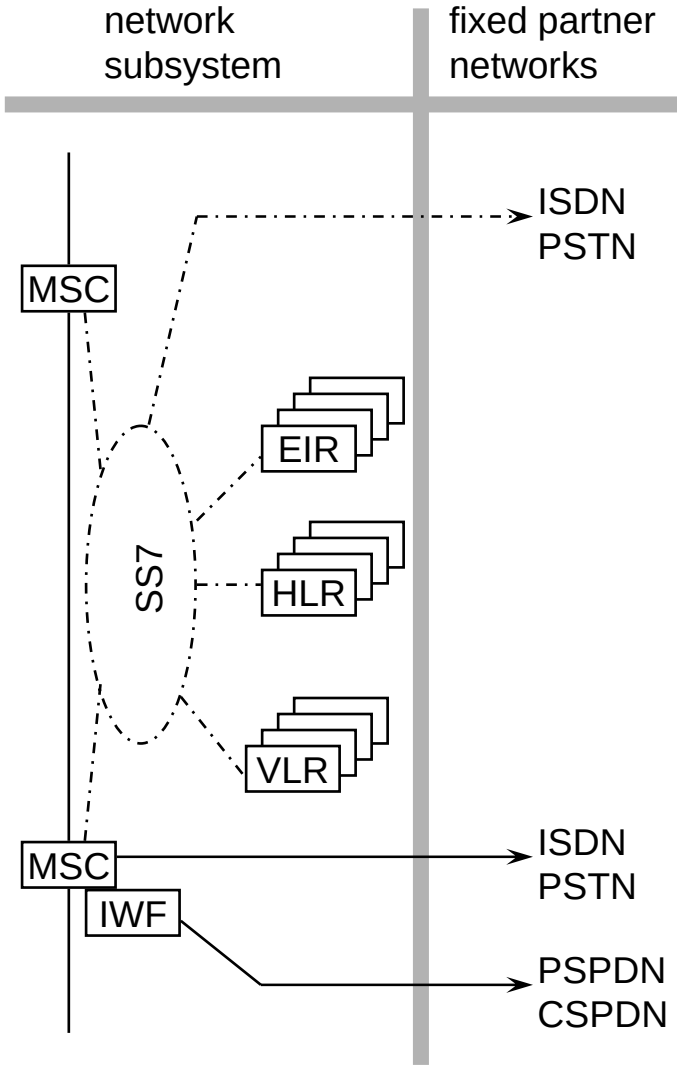
Components

- *MS* (Mobile Station)
- *BSS* (Base Station Subsystem): consisting of
  - *BTS* (Base Transceiver Station): sender and receiver
  - *BSC* (Base Station Controller): controlling several transceivers

Interfaces

- U_m : radio interface
- A_{bis} : standardized, open interface with 16 kbit/s user channels
- *A*: standardized, open interface with 64 kbit/s user channels

System architecture: network and switching subsystem



Components

- *MSC* (Mobile Services Switching Center):
- *IWF* (Interworking Functions)

- *ISDN* (Integrated Services Digital Network)
- *PSTN* (Public Switched Telephone Network)
- *PSPDN* (Packet Switched Public Data Net.)
- *CSPDN* (Circuit Switched Public Data Net.)

Databases

- *HLR* (Home Location *R*egister)
- *VLR* (Visitor Location *R*egister)
- *EIR* (Equipment Identity Register)

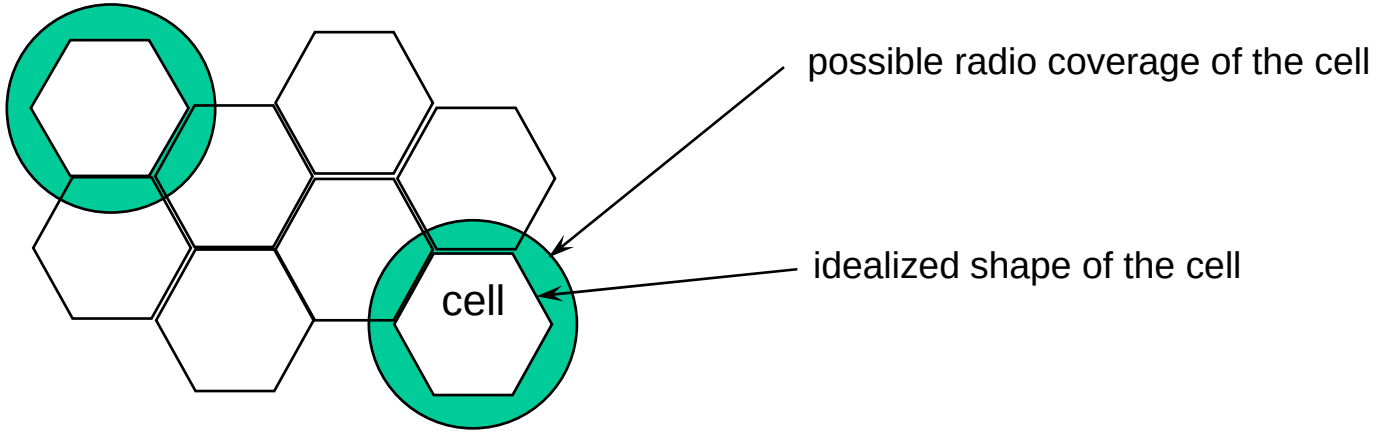
Radio subsystem

The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers

- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
    - BSS = BSC + sum(BTS) + interconnection
  - Mobile Stations (MS)

GSM: cellular network

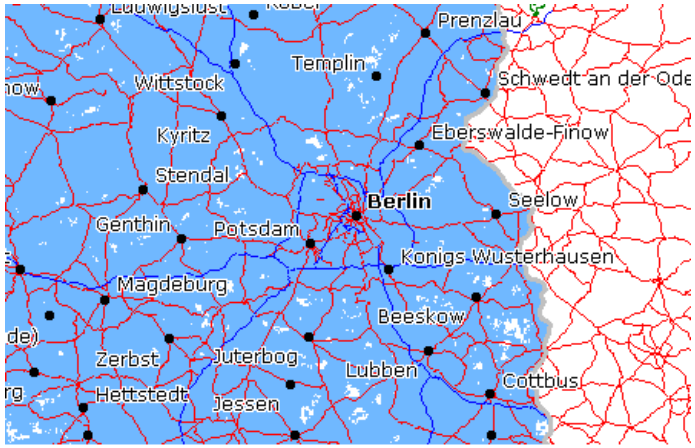
segmentation of the area into cells



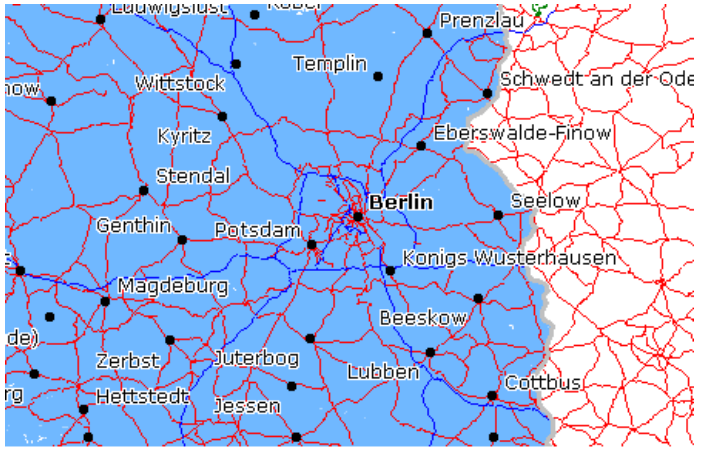
- use of several carrier frequencies
- not the same frequency in adjoining cells
- cell sizes vary from some 100 m up to 35 km depending on user density, geography, transceiver power etc.
- hexagonal shape of cells is idealized (cells overlap, shapes depend on geography)
- if a mobile user changes cells
  ➧ handover of the connection to the neighbor cell

Example coverage of GSM networks (www.gsmworld.com)

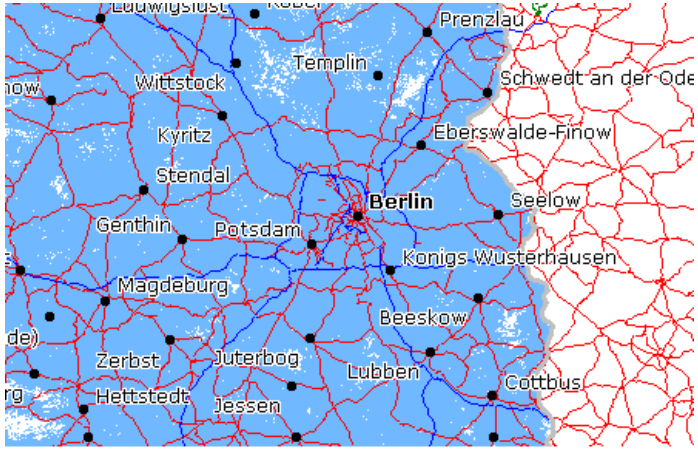
T-Mobile (GSM-900/1800) Berlin



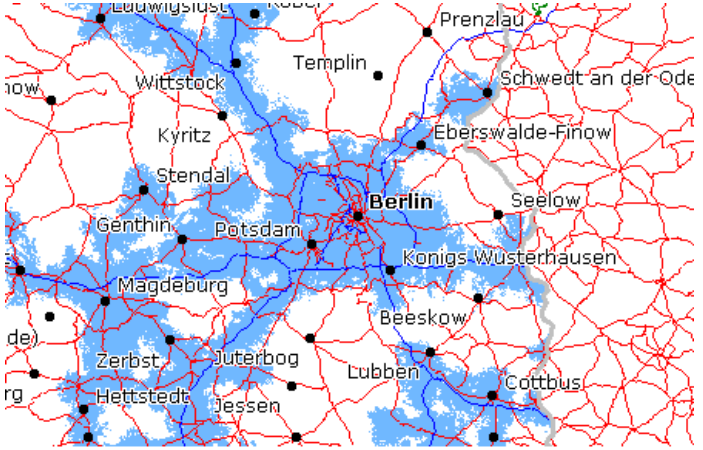
Vodafone (GSM-900/1800)



e-plus (GSM-1800)



O_2 (GSM-1800)



Base Transceiver Station and Base Station Controller

Tasks of a BSS are distributed over BSC and BTS

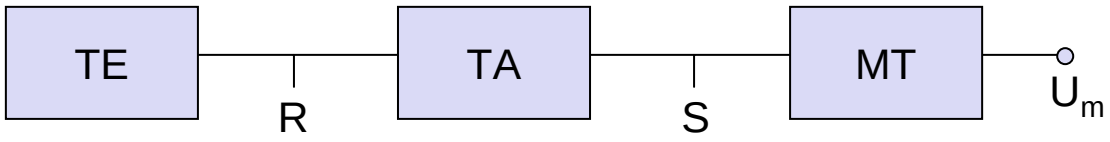
- BTS comprises radio specific functions
- BSC is the switching center for radio channels

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 station

Terminal for the use of GSM services

- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - corresponds to the network termination (NT) of an ISDN access
    - end-point of the radio interface (U_m)
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters



Network and switching subsystem

NSS is the main component of the public mobile network GSM

- switching, mobility management, interconnection to other networks, system control

- Components
  - Mobile Services Switching Center (MSC)
    controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)
      central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)
      local database for a subset of user data, including data about all user currently in the domain of the VLR

Mobile Services Switching Center

The MSC (mobile switching center) plays a central role in GSM

- switching functions
- additional functions for mobility support
- management of network resources
- interworking functions via Gateway MSC (GMSC)
- integration of several databases

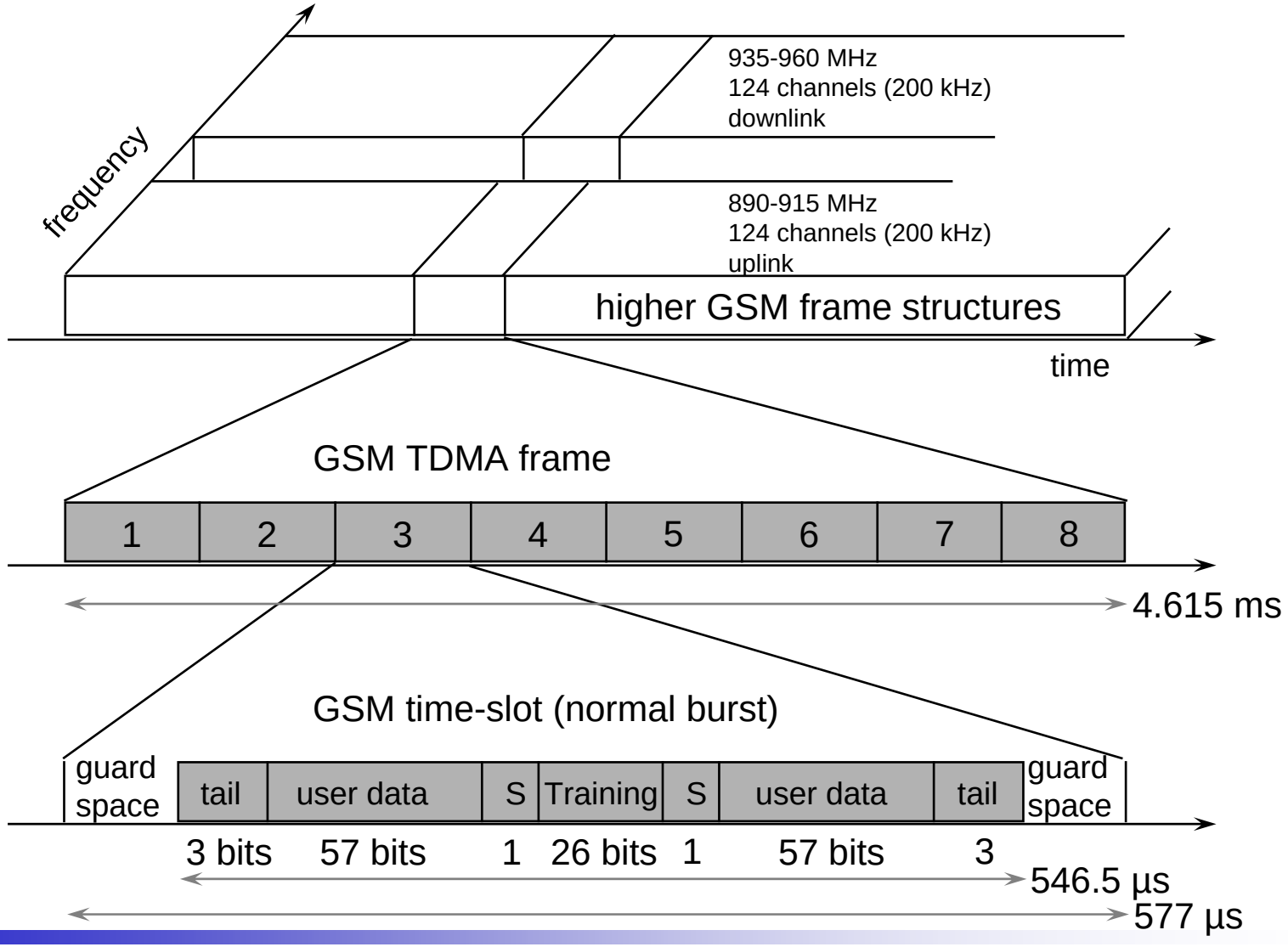
- Functions of a MSC
  - specific functions for paging and call forwarding
  - termination of SS7 (signaling system no. 7)
  - mobility specific signaling
  - location registration and forwarding of location information
  - provision of new services (fax, data calls)
  - support of short message service (SMS)
  - generation and forwarding of accounting and billing information

Operation subsystem

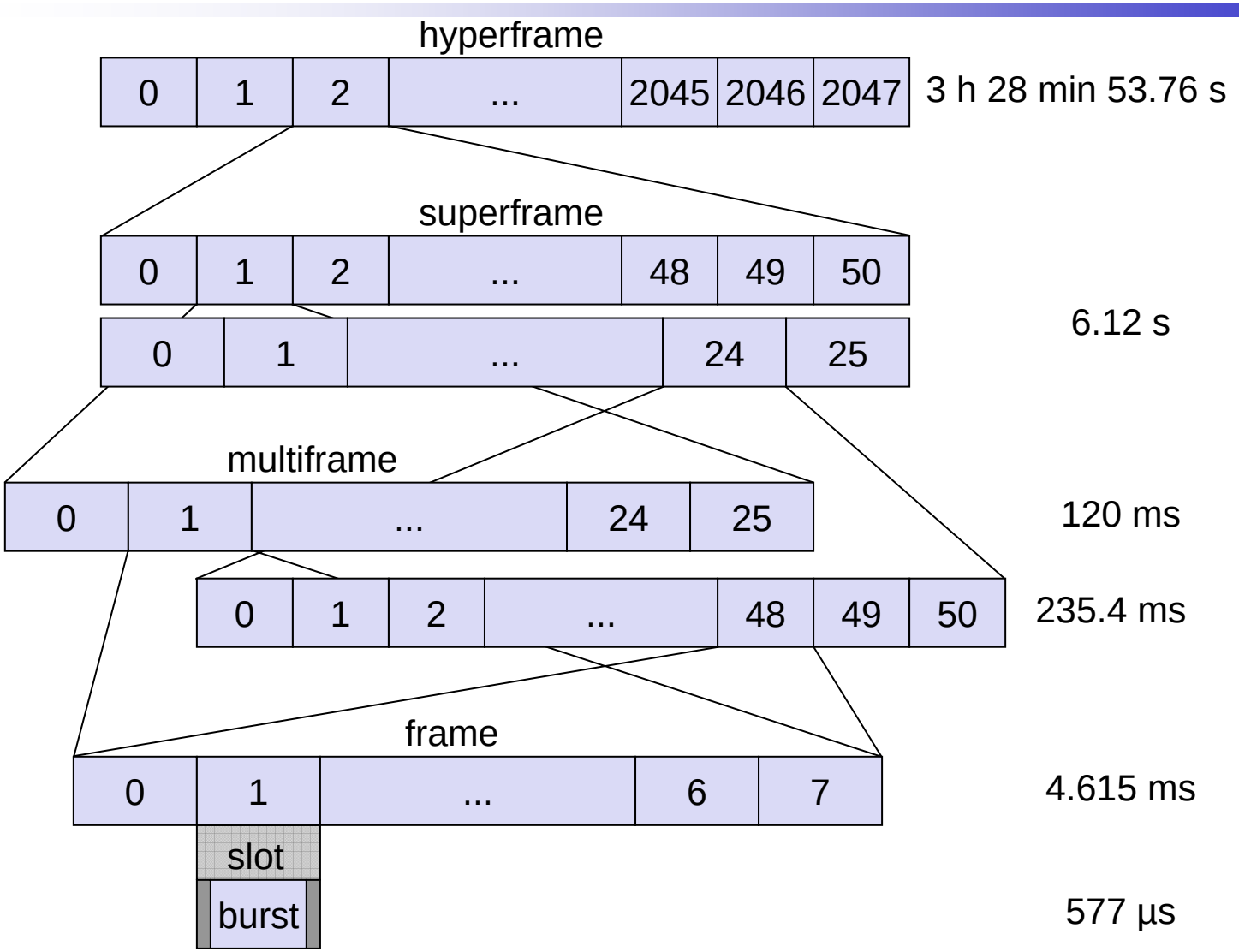
The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems

- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

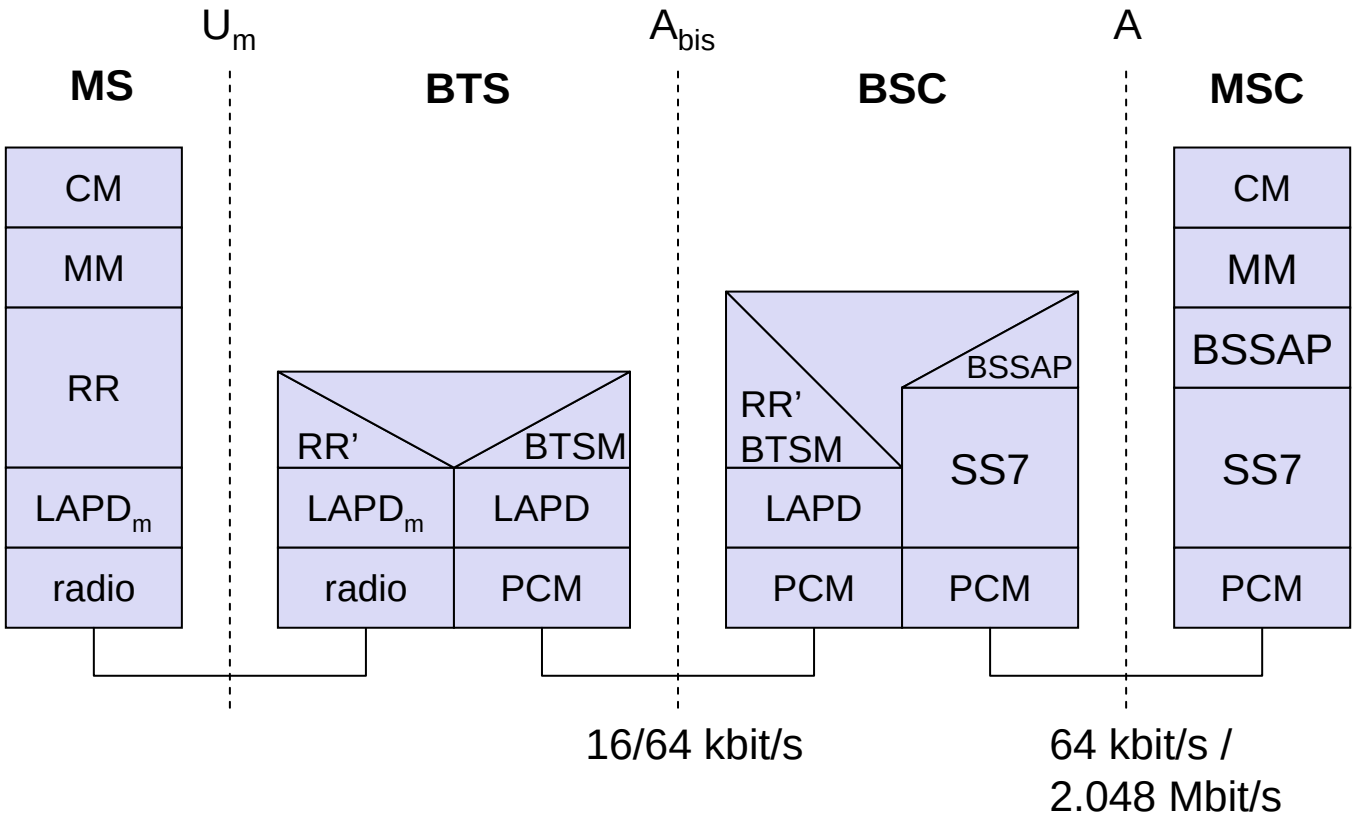
GSM - TDMA/FDMA



GSM hierarchy of frames

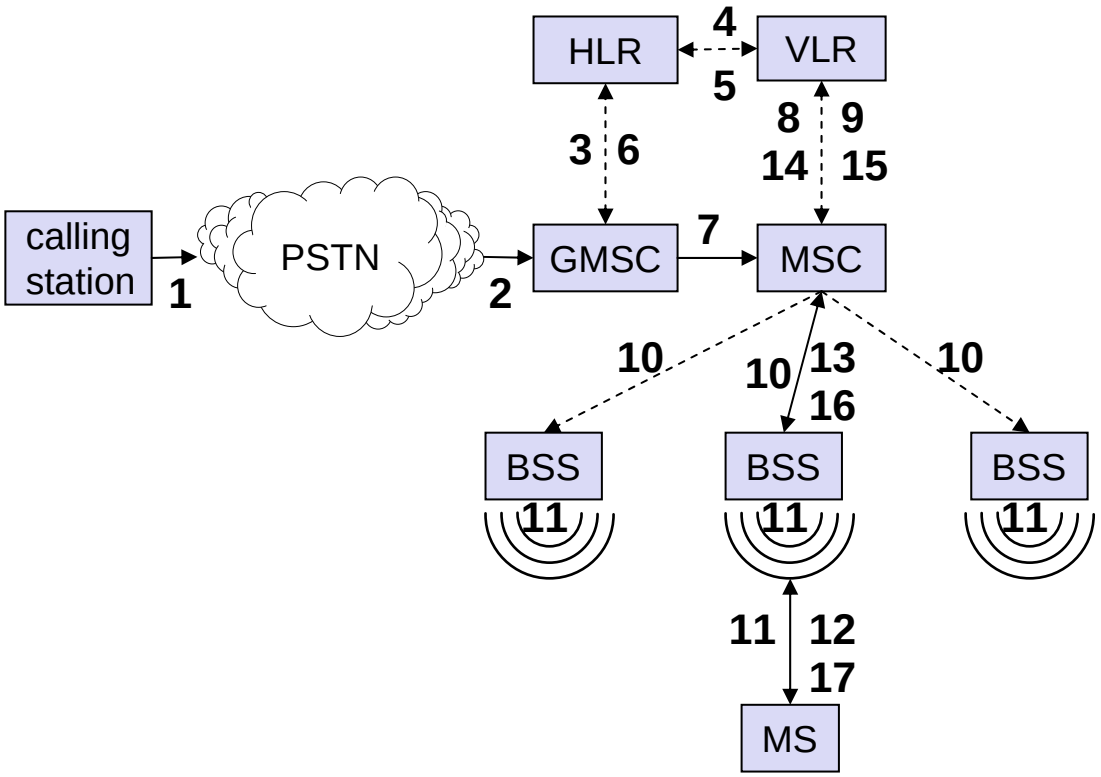


GSM protocol layers for signaling



Mobile Terminated Call

1: calling a GSM subscriber
2: forwarding call to GMSC
3: signal call setup to HLR
4, 5: request MSRN from VLR
6: forward responsible MSC to GMSC
7: forward call to current MSC
8, 9: get current status of MS
10, 11: paging of MS
12, 13: MS answers
14, 15: security checks
16, 17: set up connection



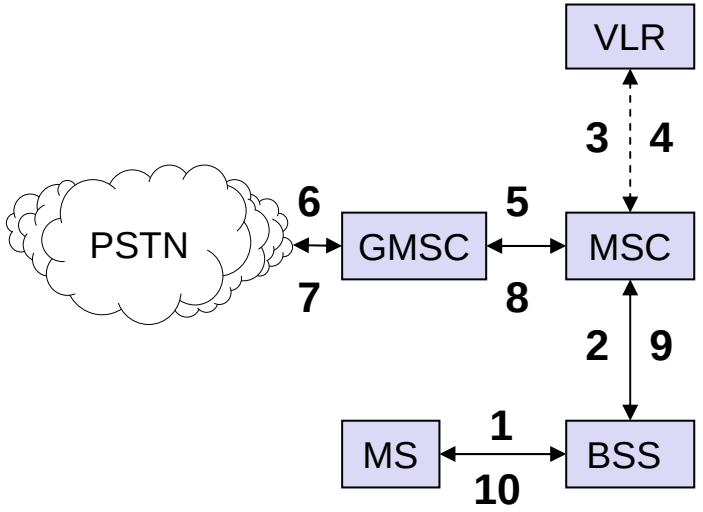
Mobile Originated Call

1, 2: connection request

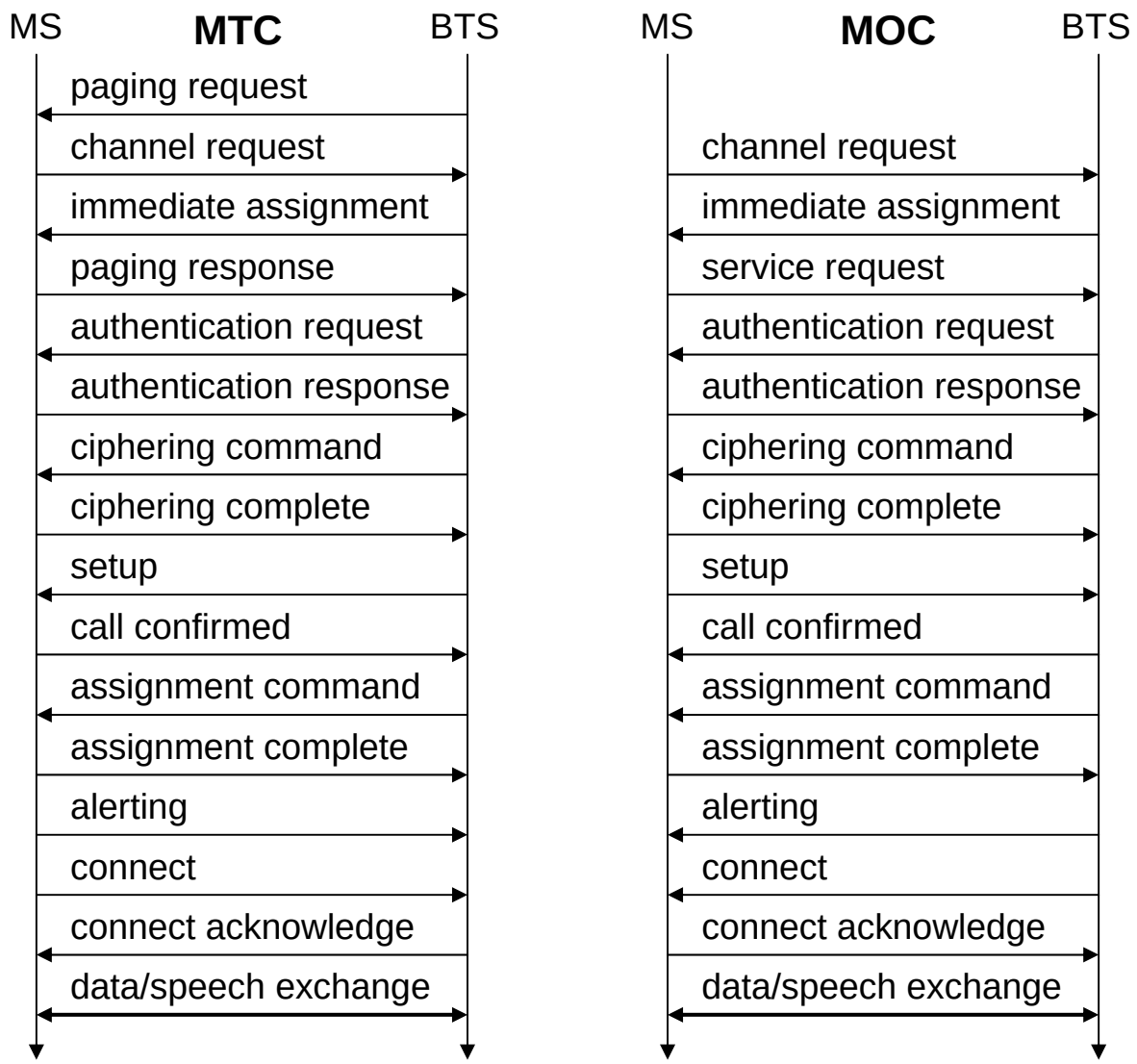
3, 4: security check

5-8: check resources (free circuit)

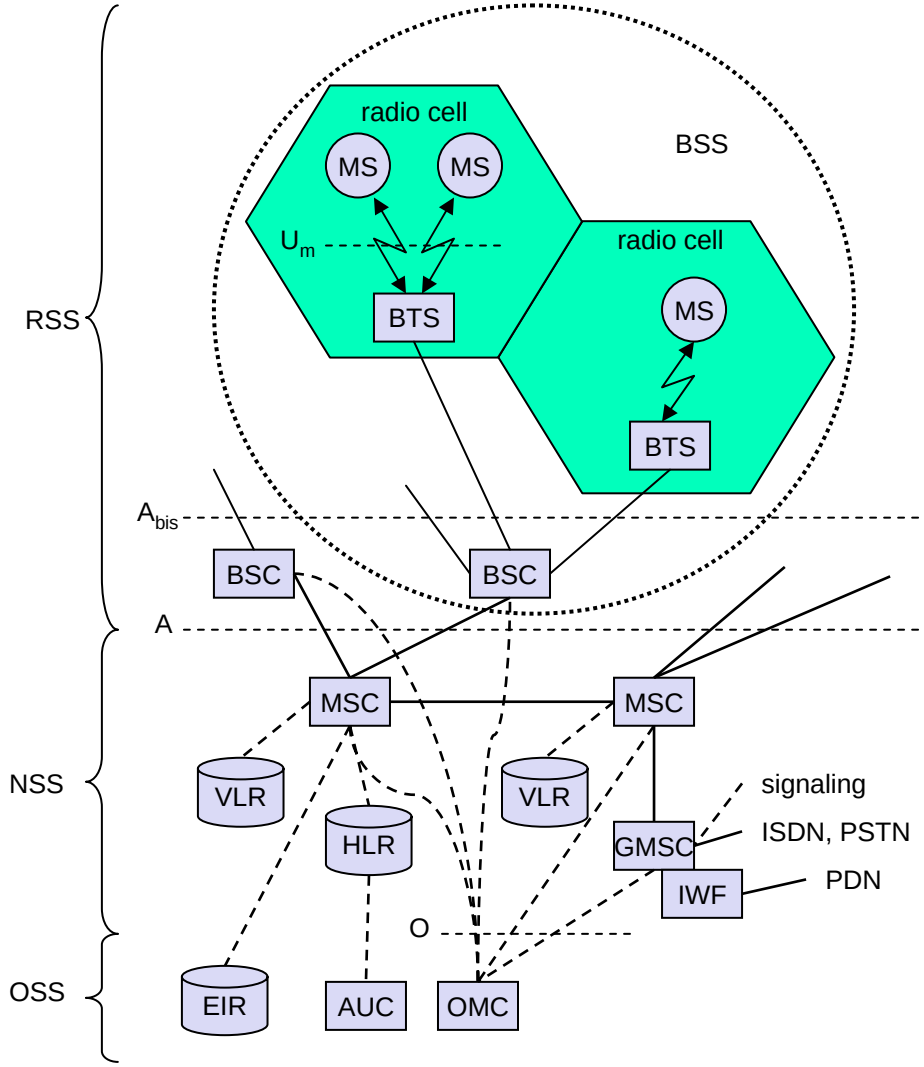
9-10: set up call



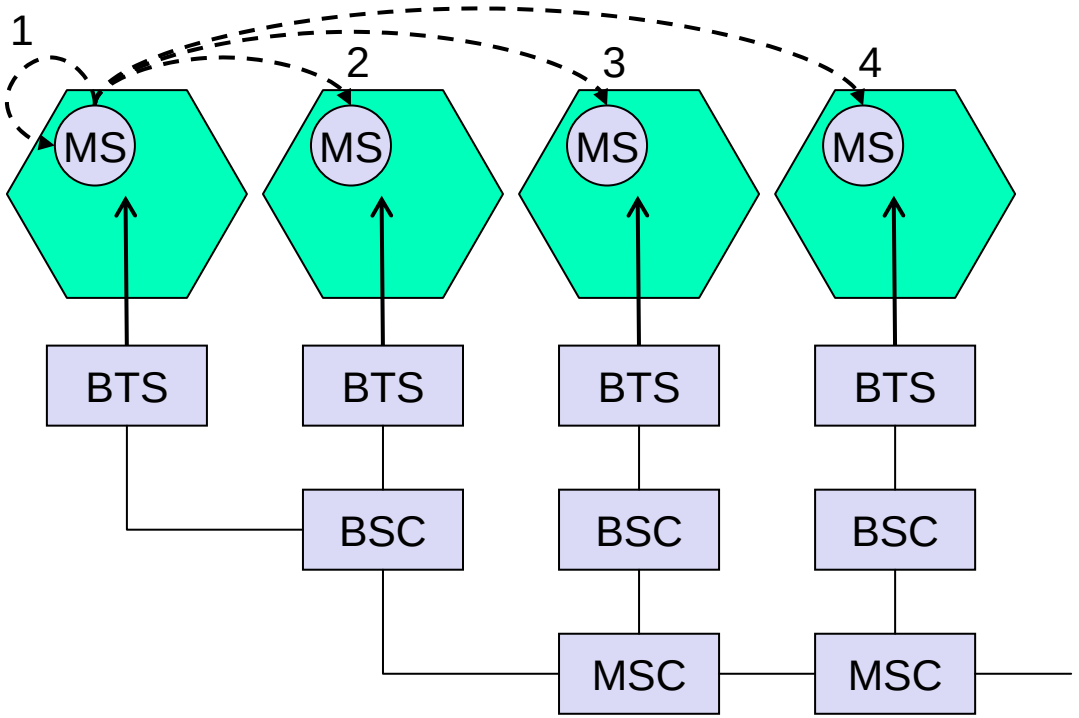
MTC/MOC


MS
MTC
BTS
paging request
channel request
immediate assignment
paging response
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange
MS
MOC
BTS
channel request
immediate assignment
service request
authentication request
authentication response
ciphering command
ciphering complete
setup
call confirmed
assignment command
assignment complete
alerting
connect
connect acknowledge
data/speech exchange

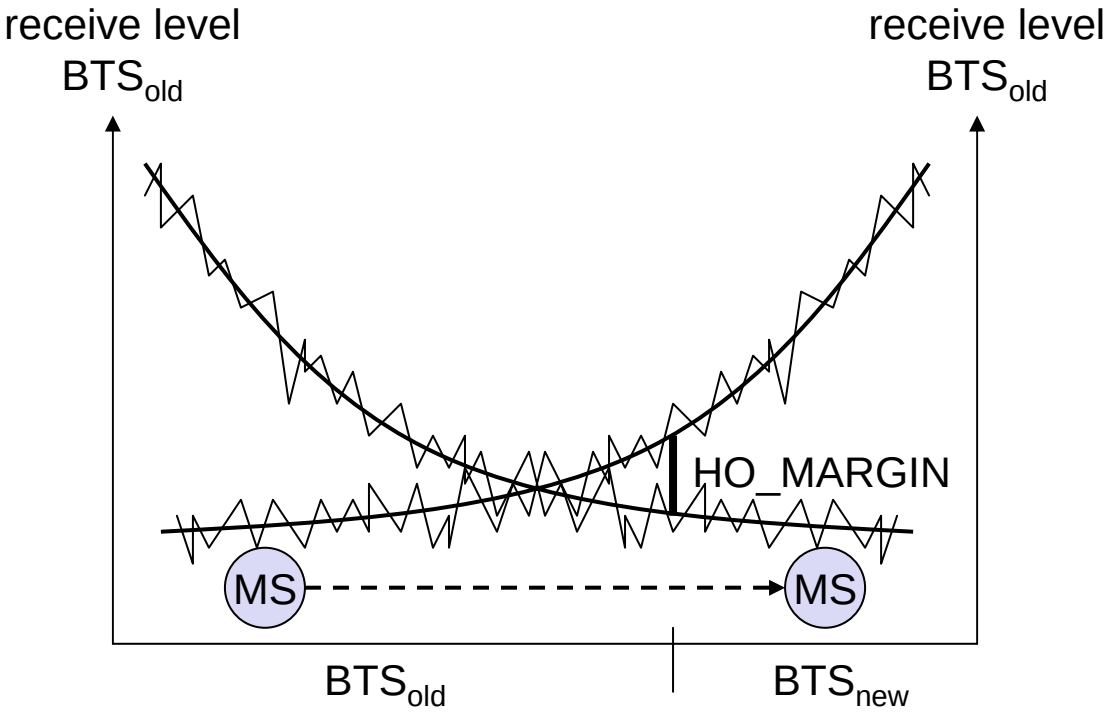
GSM: elements and interfaces



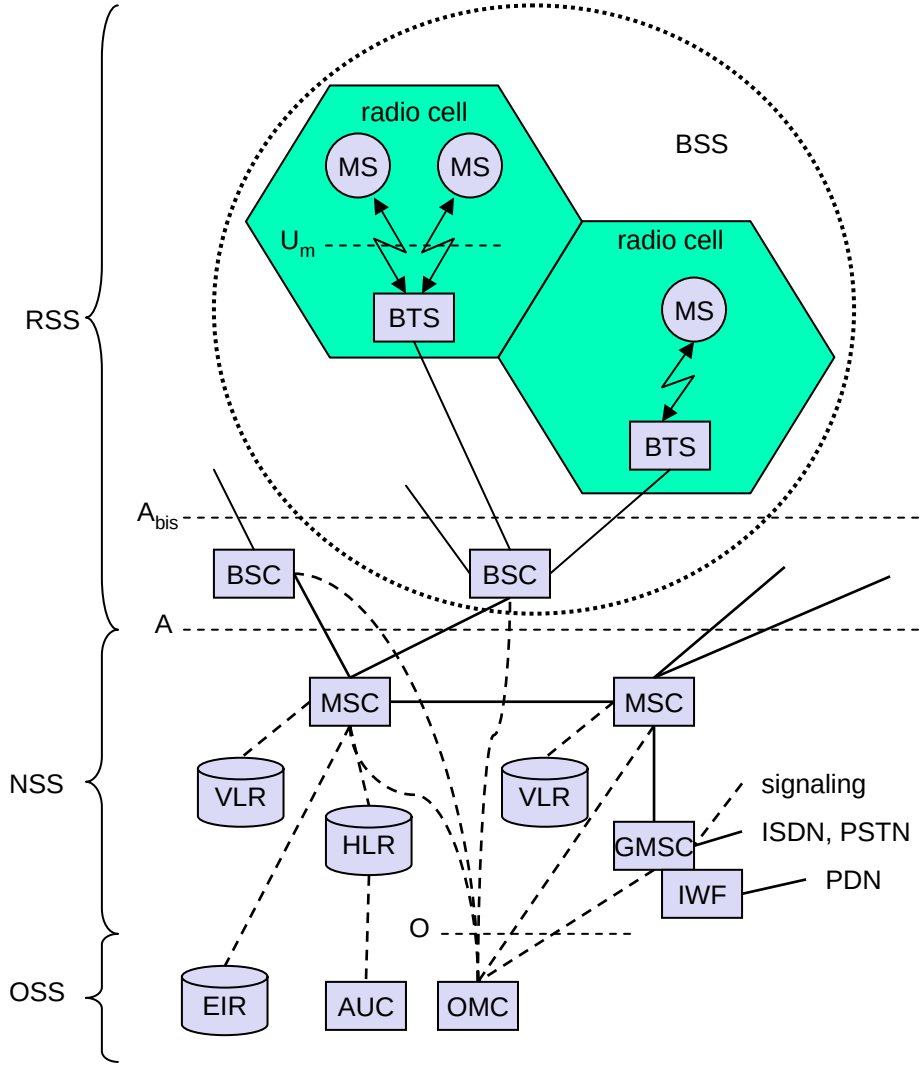
4 types of handover



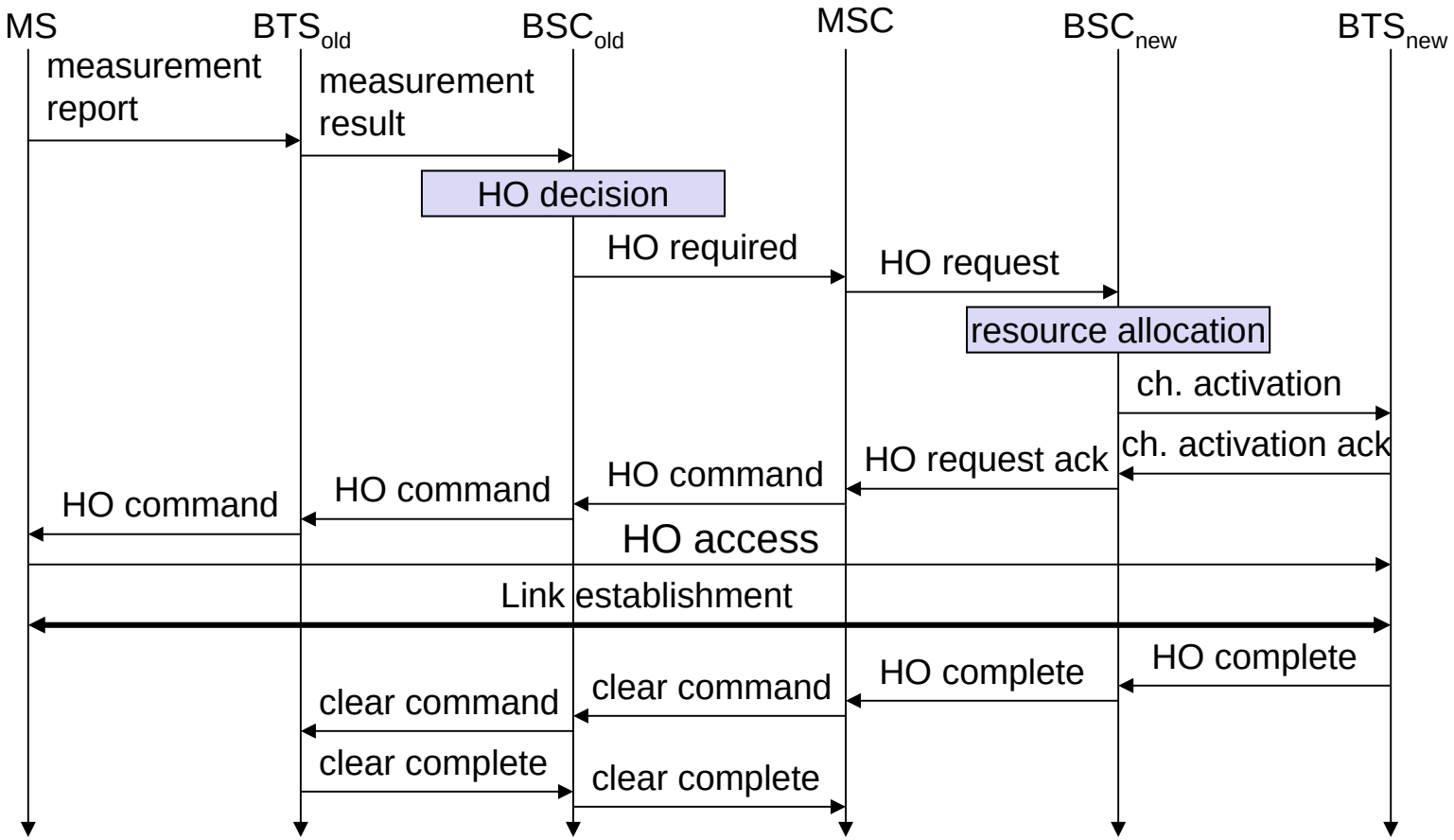
Handover decision



GSM: elements and interfaces



Handover procedure



Security in GSM

Security services

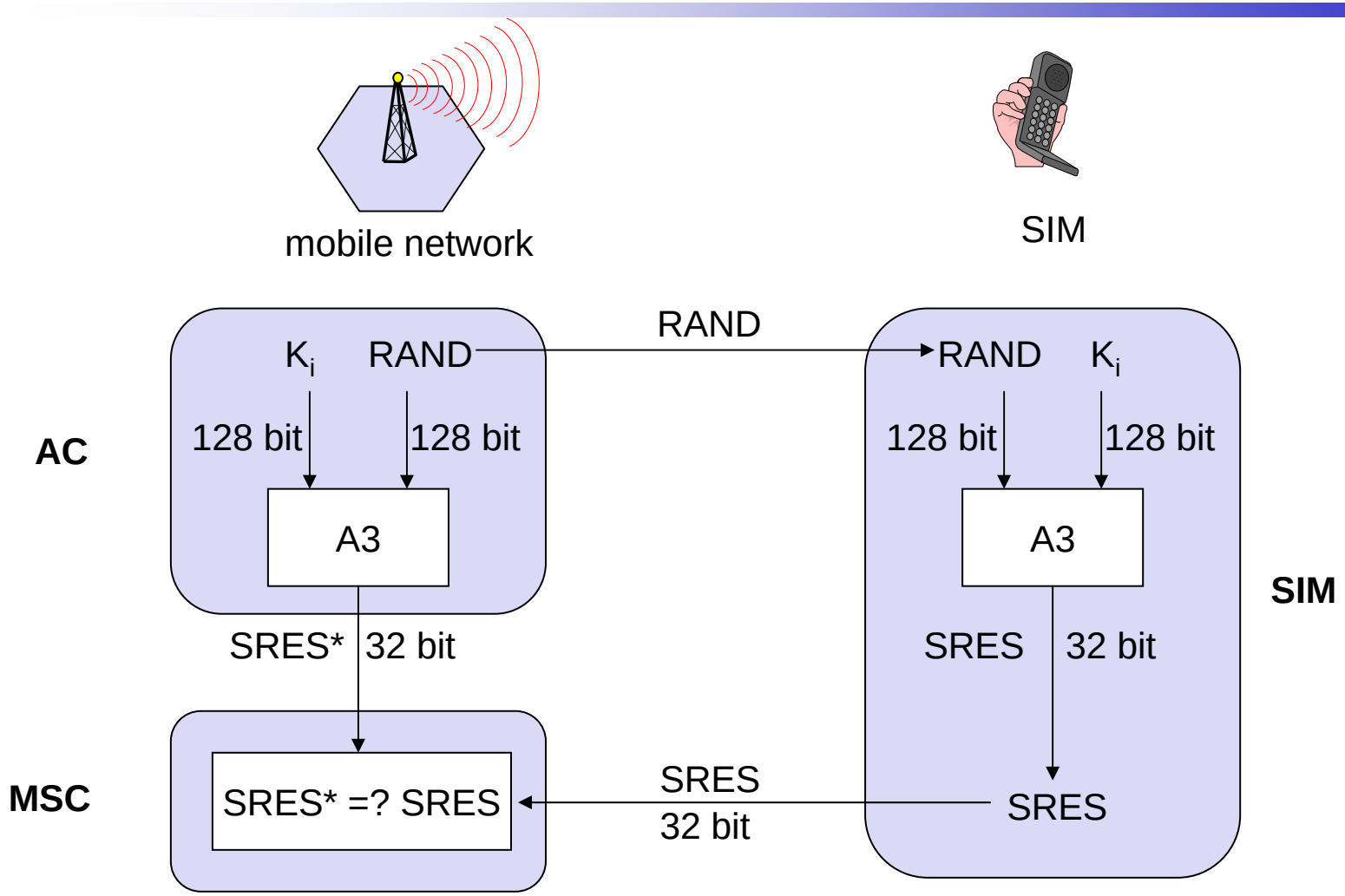
- access control/authentication
  - user ⇔ SIM (Subscriber Identity Module): secret PIN (personal identification number)
  - SIM ⇔ network: challenge response method
- confidentiality
  - voice and signaling encrypted on the wireless link (after successful authentication)
- anonymity
  - temporary identity TMSI (Temporary Mobile Subscriber Identity)
  - newly assigned at each new location update (LUP)
  - encrypted transmission

"secret":
• A3 and A8 available via the Internet
• network providers can use stronger mechanisms

3 algorithms specified in GSM

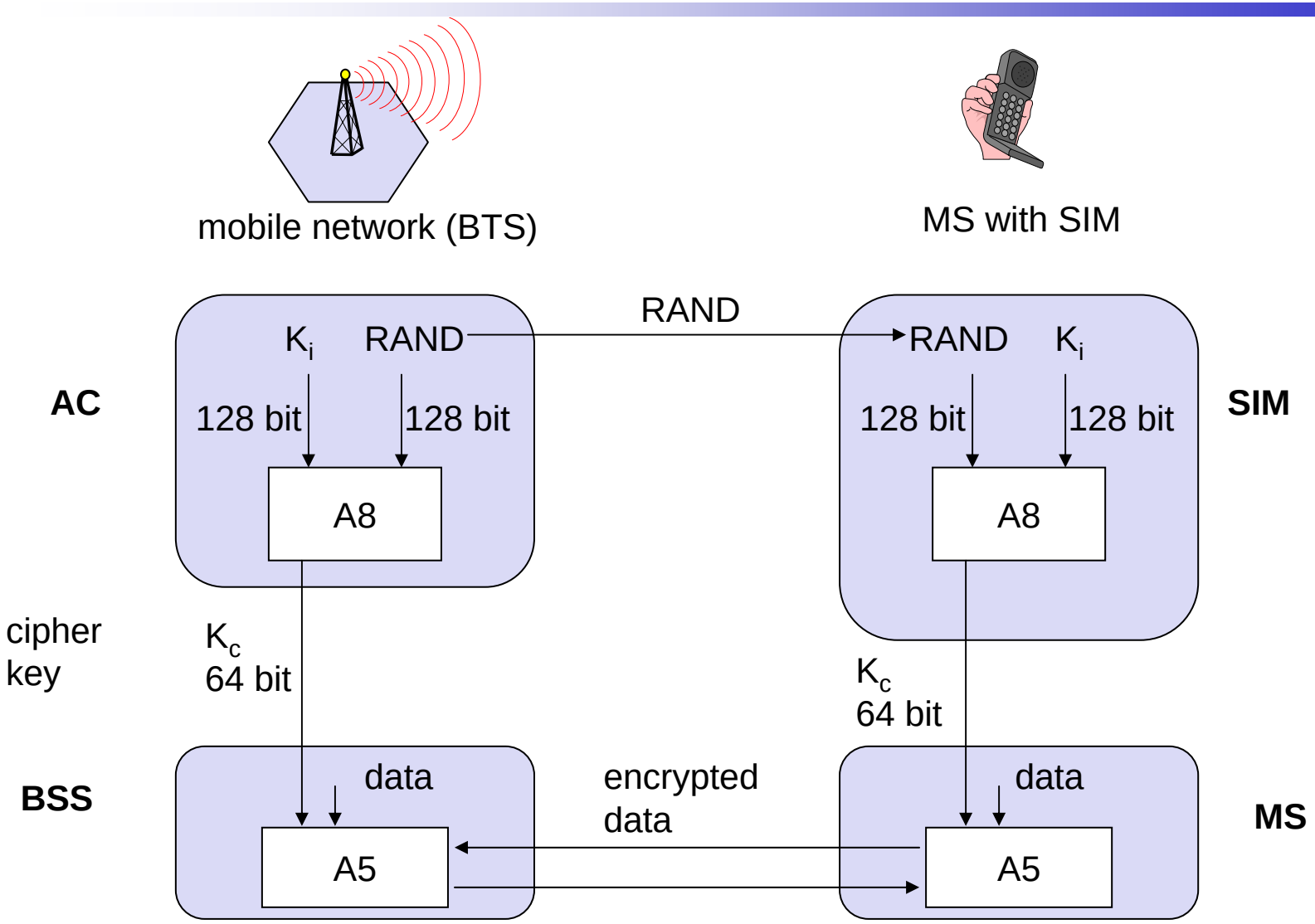
- A3 for authentication ("secret", open interface)
- A5 for encryption (standardized)
- A8 for key generation ("secret", open interface)

GSM - authentication



K_i: individual subscriber authentication key SRES: signed response

GSM - key generation and encryption



Homework #4:

1. What's the architecture of the GSM system (including radio subsystem, network and switching subsystem, and fixed partner networks) ?
2. What's the mobile terminated call in the GSM system ?
3. What's the mobile originated call in the GSM system ?
4. What's handover procedure in the GSM system ?