

# Mobile Computing

## Lecture 11

### Digital Mobile Phone Systems 4

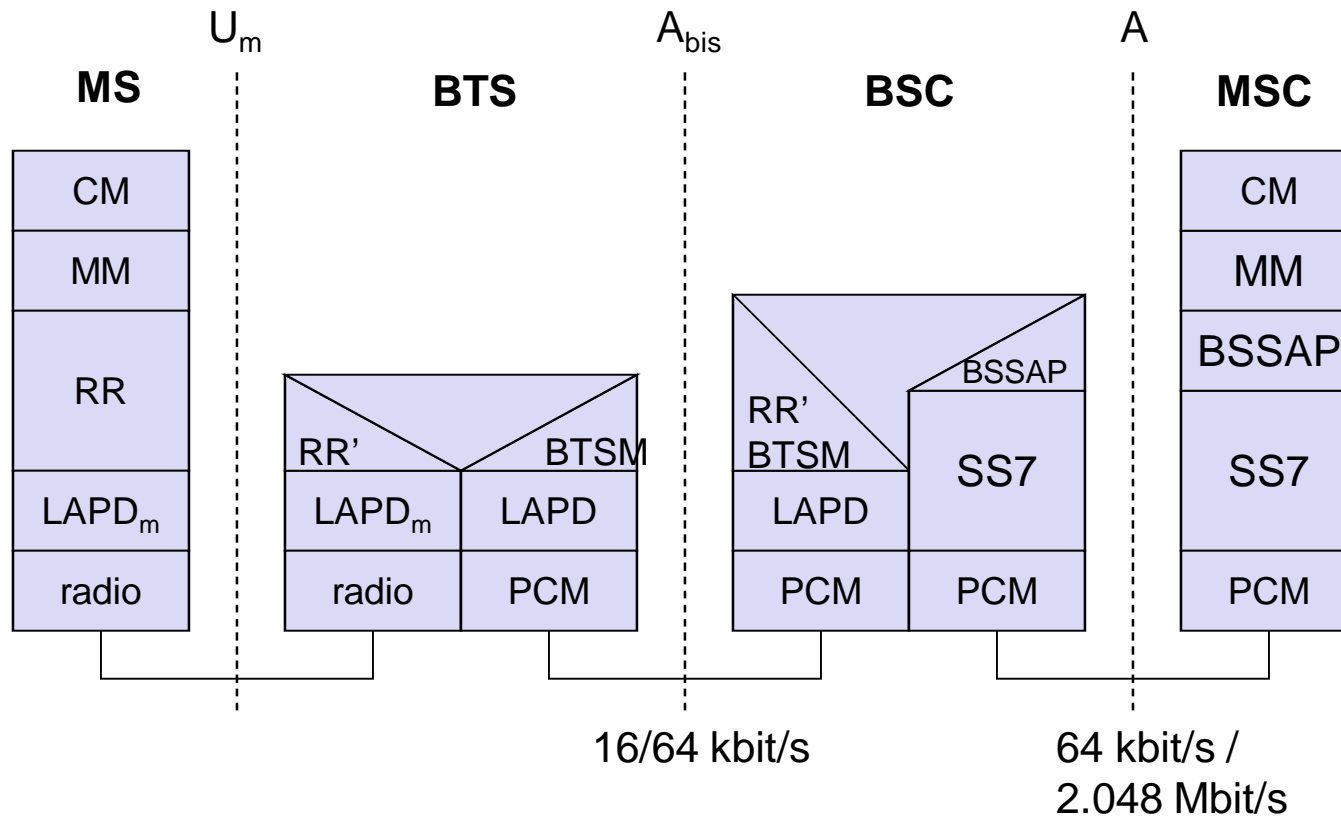


# Contents



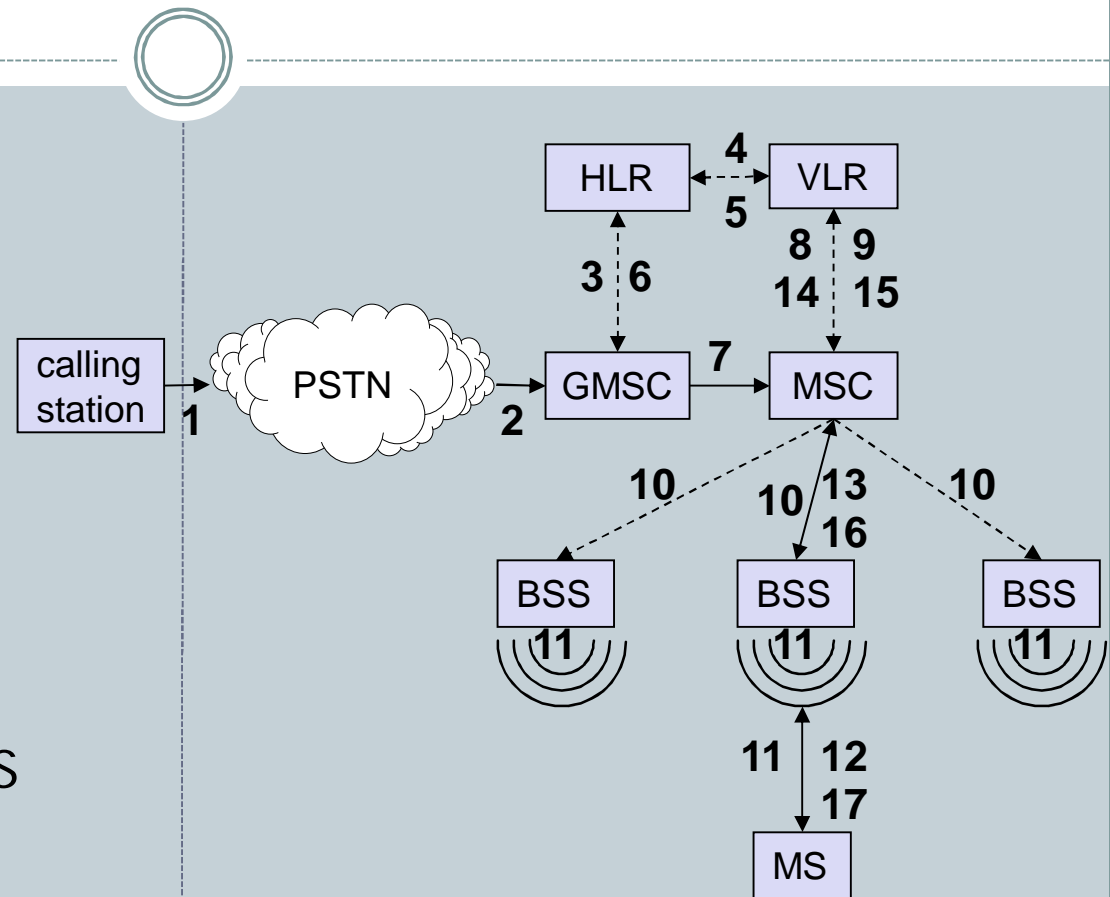
- GSM protocol layers for signaling
- Mobile Terminated Call
- Mobile Originated Call
- MTC/MOC
- 4 types of handover
- Security in GSM
- GPRS

# GSM protocol layers for signaling



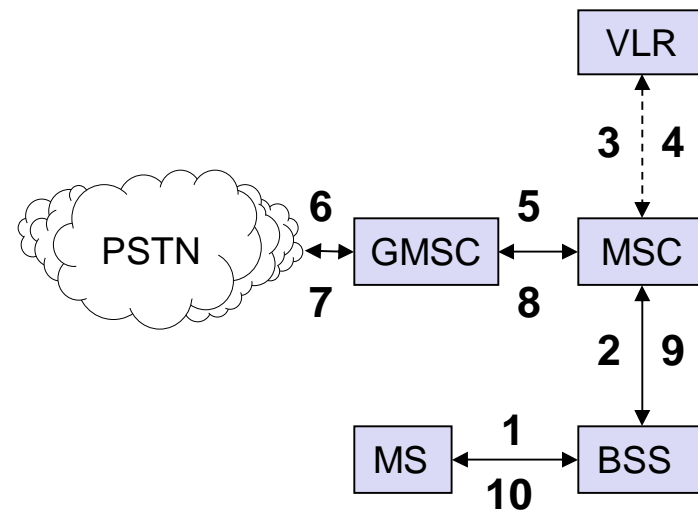
# Mobile Terminated Call

- 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

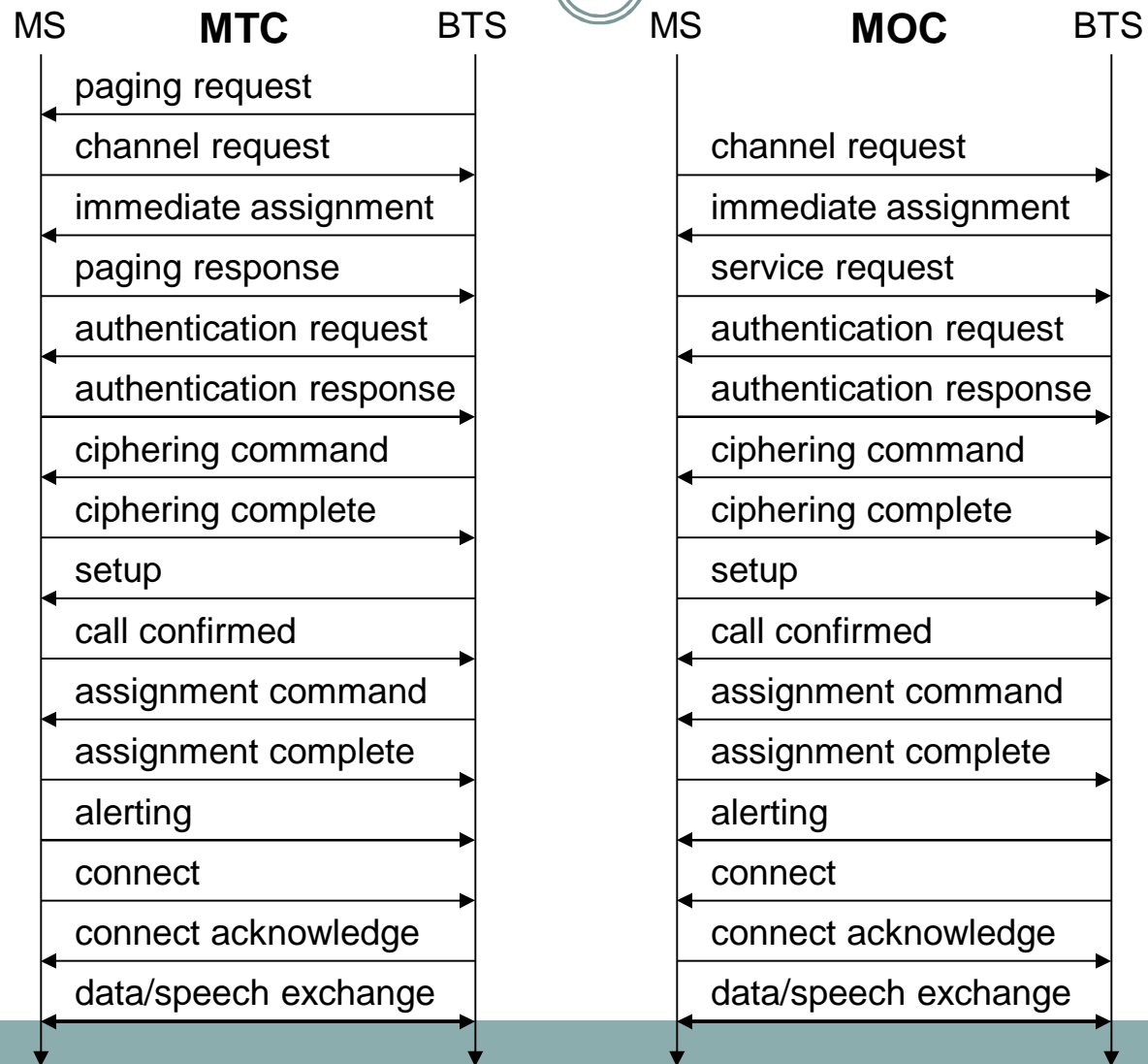


# Mobile Originated Call

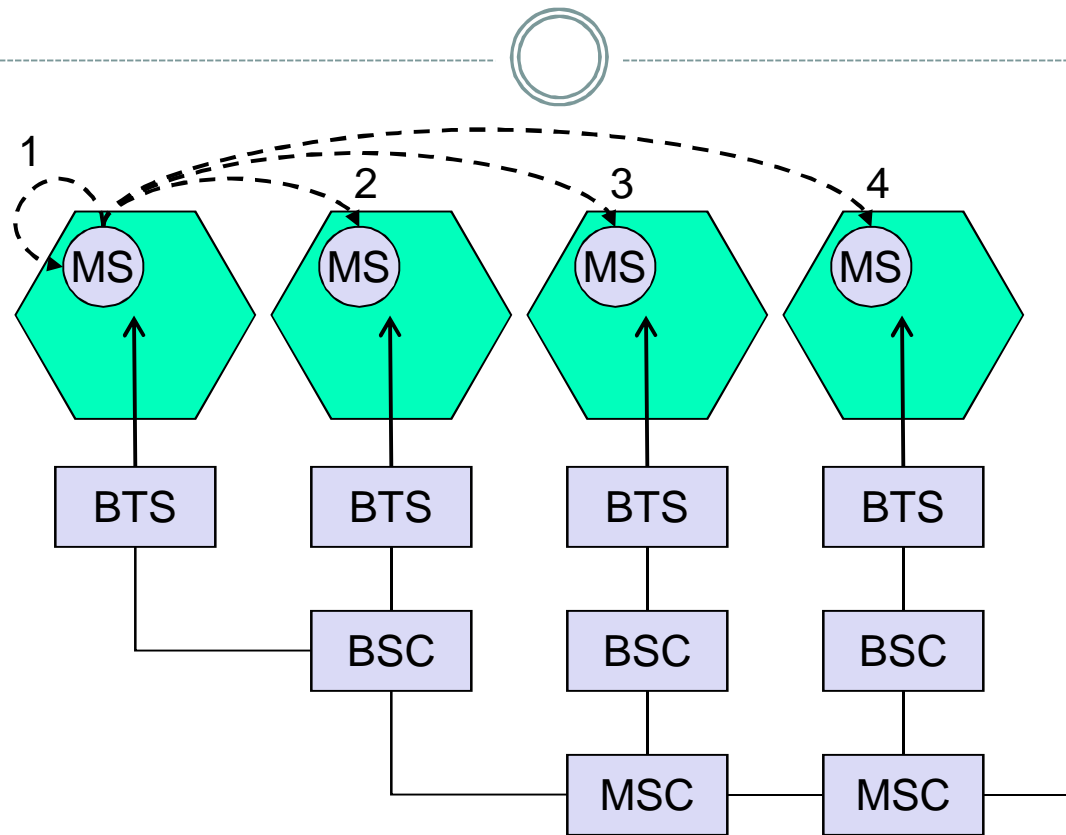
- 1, 2: connection request
- 3, 4: security check
- 5-8: check resources (free circuit)
- 9-10: set up call



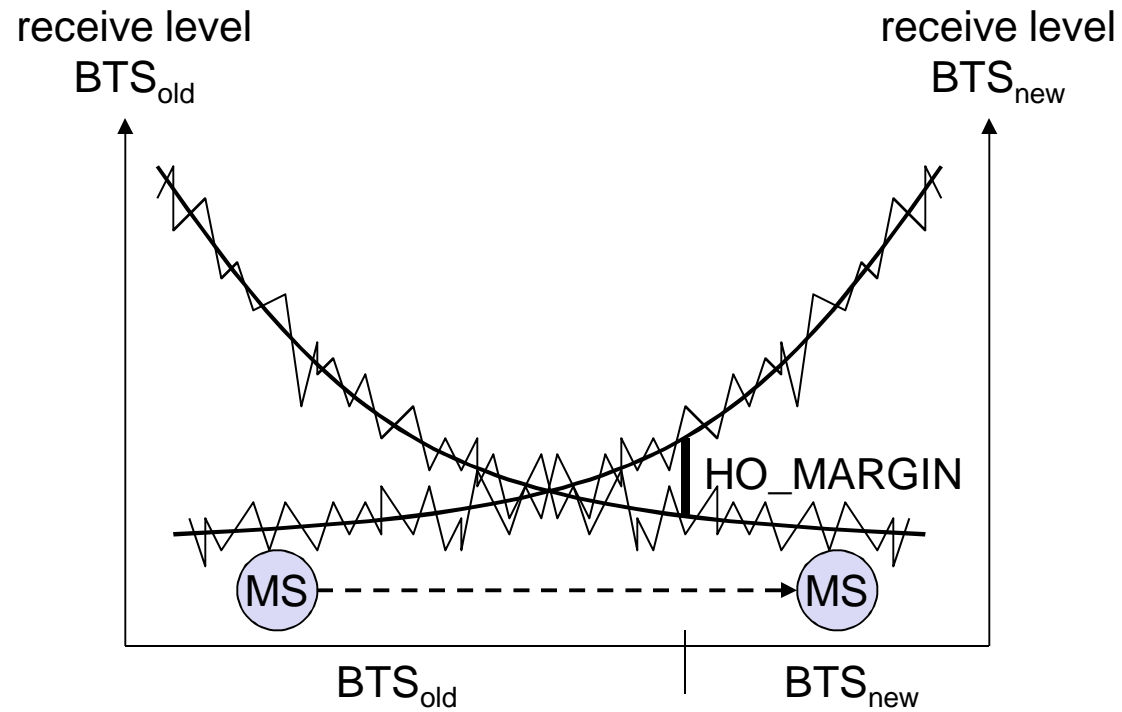
# MTC/MOC



# 4 types of handover

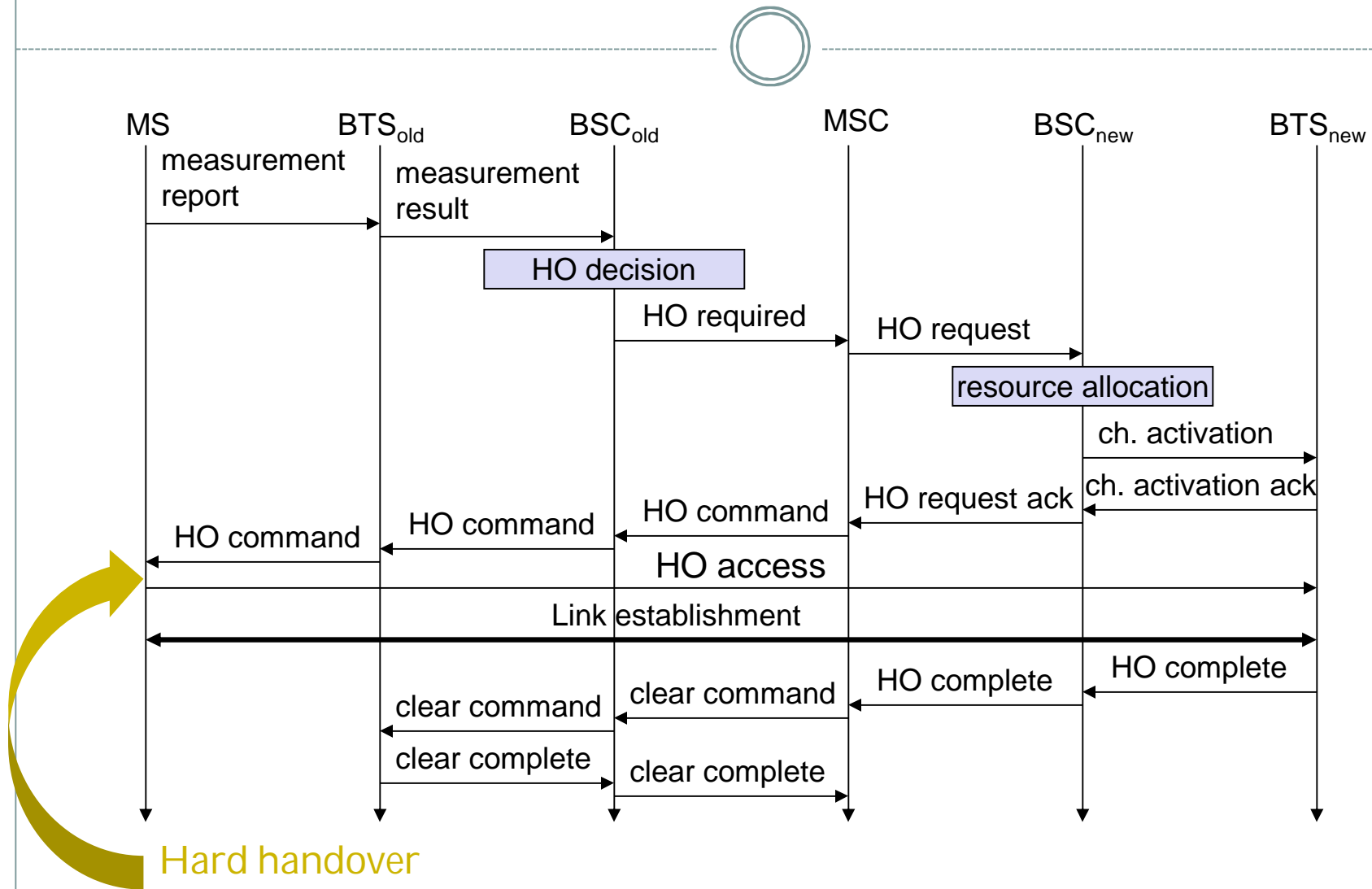


# Handover decision





# Handover procedure



# Security in GSM

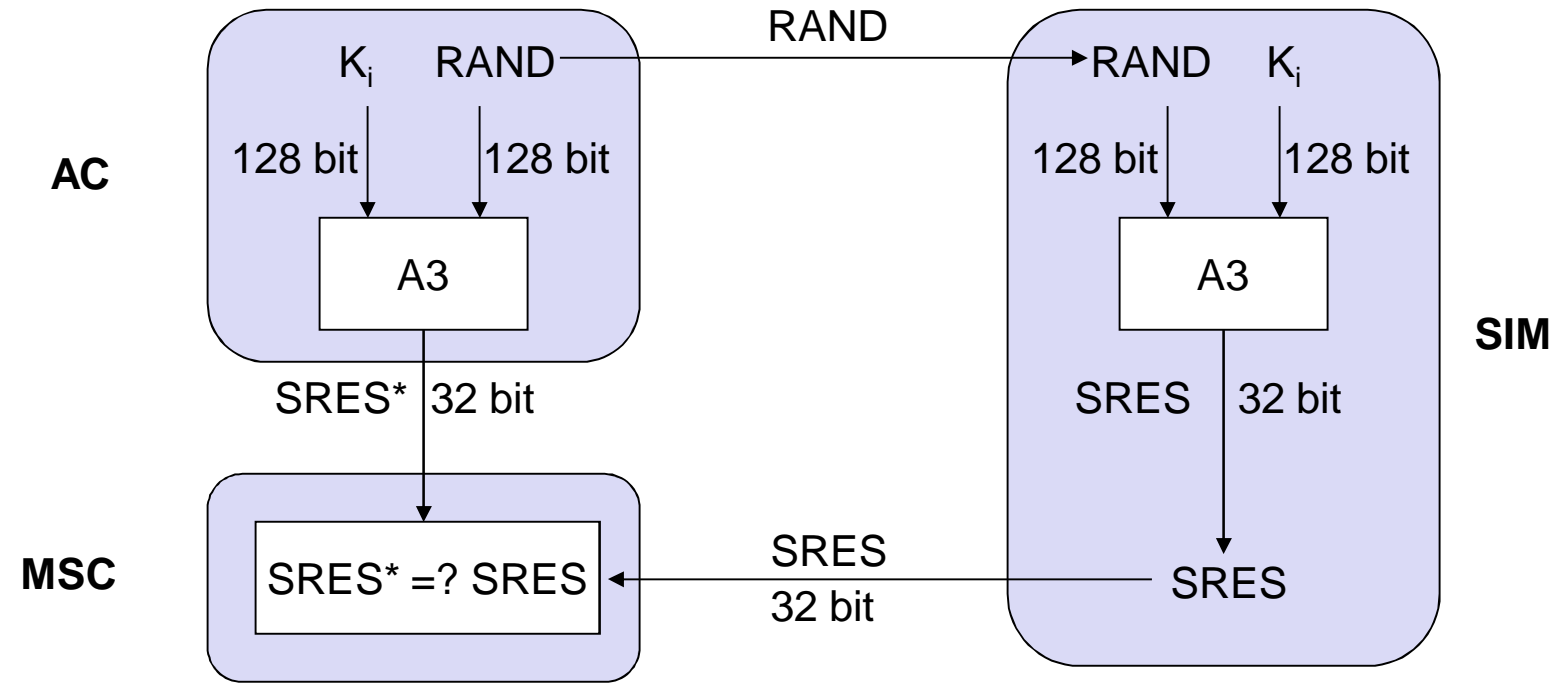
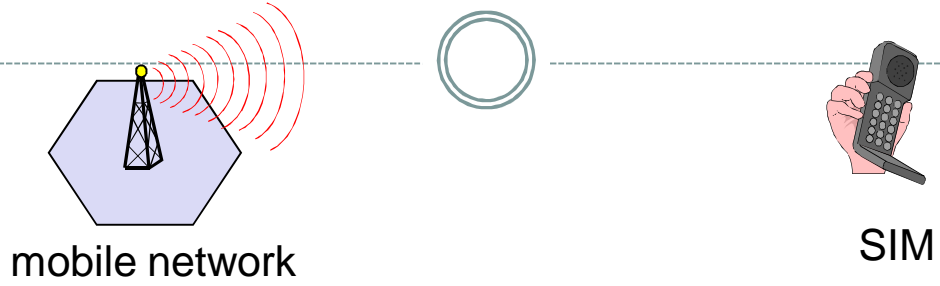


- Security services
  - access control/authentication
    - ✦ user  $\Leftrightarrow$  SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - ✦ SIM  $\Leftrightarrow$  network: challenge response method
  - confidentiality
    - ✦ voice and signaling encrypted on the wireless link (after successful authentication)
  - anonymity
    - ✦ temporary identity TMSI (Temporary Mobile Subscriber Identity)
    - ✦ newly assigned at each new location update (LUP)
    - ✦ encrypted transmission
- 3 algorithms specified in GSM
  - A3 for authentication ("secret", open interface)
  - A5 for encryption (standardized)
  - A8 for key generation ("secret", open interface)

"secret":

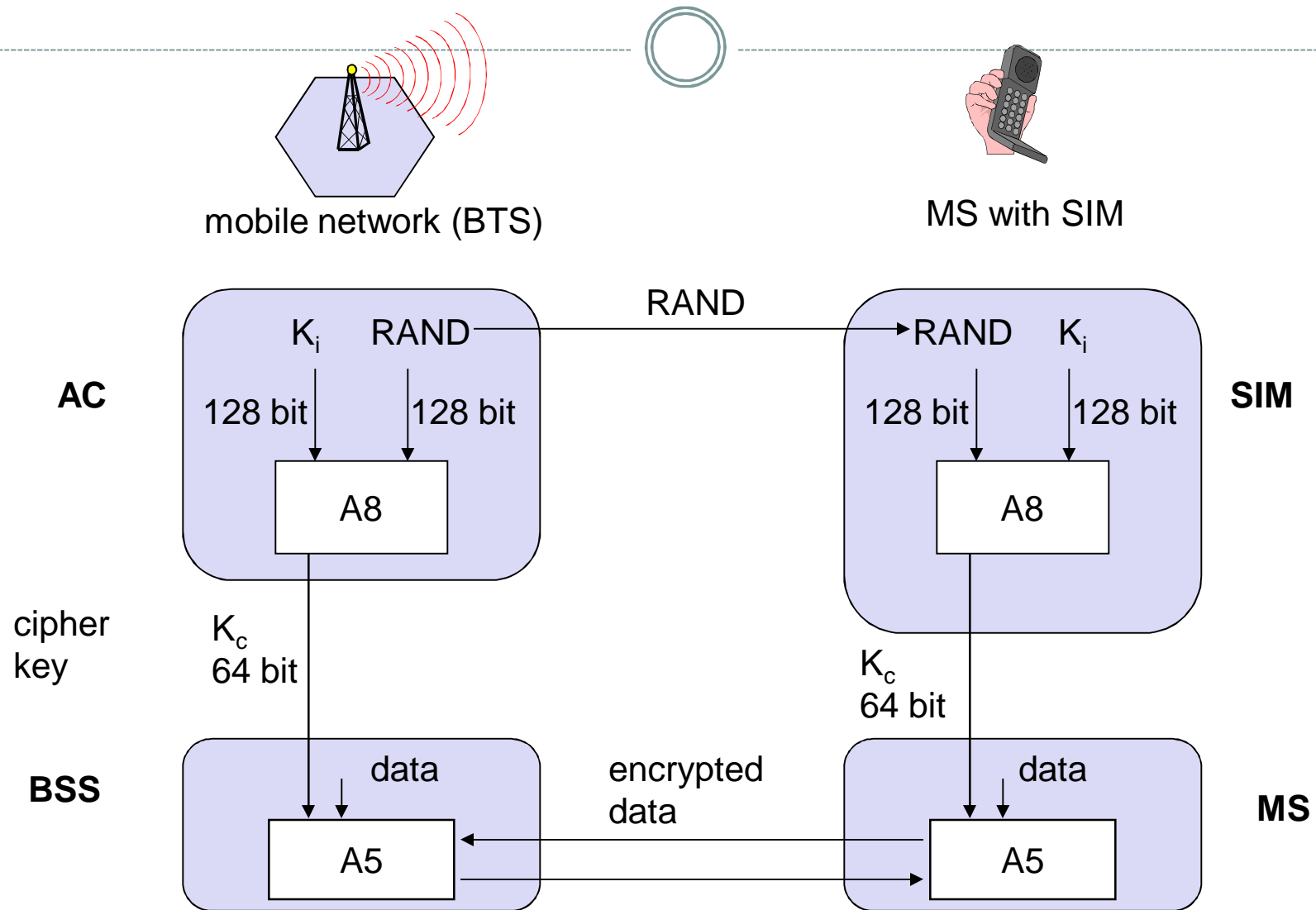
- A3 and A8 available via the Internet
- network providers can (and do) use stronger mechanisms

# GSM - authentication



$K_i$ : individual subscriber authentication key       $SRES$ : signed response

# GSM - key generation and encryption



# Data services in GSM I



- Data transmission standardized with only 9.6 kbit/s
  - advanced coding allows 14.4 kbit/s
  - not enough for Internet and multimedia applications
- HSCSD (High-Speed Circuit Switched Data)
  - mainly software update
  - bundling of several time-slots to get higher AIUR (Air Interface User Rate, e.g., 57.6 kbit/s using 4 slots @ 14.4)
  - advantage: ready to use, constant quality, simple
  - disadvantage: channels blocked for voice transmission

AIUR [kbit/s]	TCH/F4.8	TCH/F9.6	TCH/F14.4
4.8	1		
9.6	2	1	
14.4	3		1
19.2	4	2	
28.8		3	2
38.4		4	
43.2			3
57.6			4

# Data services in GSM II



- GPRS (General Packet Radio Service)
  - packet switching
  - using free slots only if data packets ready to send (e.g., 50 kbit/s using 4 slots temporarily)
  - standardization 1998, introduction 2001
  - advantage: one step towards UMTS, more flexible
  - disadvantage: more investment needed (new hardware)
- GPRS network elements
  - GSN (GPRS Support Nodes): GGSN and SGSN
  - GGSN (Gateway GSN)
    - ✦ interworking unit between GPRS and PDN (Packet Data Network)
  - SGSN (Serving GSN)
    - ✦ supports the MS (location, billing, security)
  - GR (GPRS Register)
    - ✦ user addresses

# GPRS quality of service



Reliability class	Lost SDU probability	Duplicate SDU probability	Out of sequence SDU probability	Corrupt SDU probability
1	$10^{-9}$	$10^{-9}$	$10^{-9}$	$10^{-9}$
2	$10^{-4}$	$10^{-5}$	$10^{-5}$	$10^{-6}$
3	$10^{-2}$	$10^{-5}$	$10^{-5}$	$10^{-2}$

Delay class	SDU size 128 byte		SDU size 1024 byte	
	mean	95 percentile	mean	95 percentile
1	< 0.5 s	< 1.5 s	< 2 s	< 7 s
2	< 5 s	< 25 s	< 15 s	< 75 s
3	< 50 s	< 250 s	< 75 s	< 375 s
4	unspecified			

# Examples for GPRS device classes



Class	Receiving slots	Sending slots	Maximum number of slots
1	1	1	2
2	2	1	3
3	2	2	3
5	2	2	4
8	4	1	5
10	4	2	5
12	4	4	5

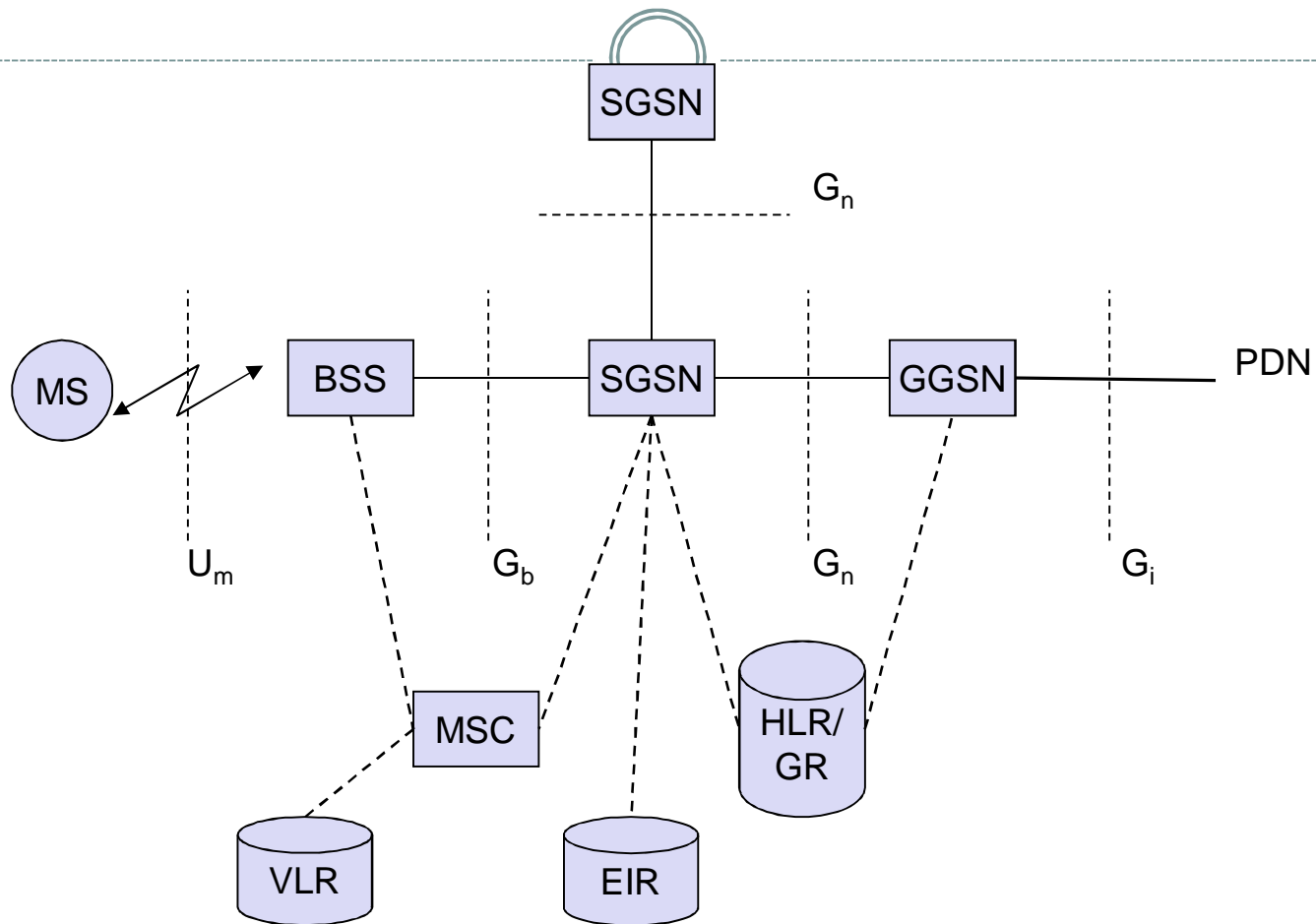


# GPRS user data rates in kbit/s



Coding scheme	1 slot	2 slots	3 slots	4 slots	5 slots	6 slots	7 slots	8 slots
CS-1	9.05	18.1	27.15	36.2	45.25	54.3	63.35	72.4
CS-2	13.4	26.8	40.2	53.6	67	80.4	93.8	107.2
CS-3	15.6	31.2	46.8	62.4	78	93.6	109.2	124.8
CS-4	21.4	42.8	64.2	85.6	107	128.4	149.8	171.2

# GPRS architecture and interfaces



# GPRS protocol architecture

