EEC173B/ECS152C, Winter 2006

Cellular Wireless Network

- Architecture and Protocols
- Applying concepts learned in first two weeks:
  - *Frequency planning, channel allocation & hand-offs*

* Acknowledgment: Selected slides from Prof. Schiller

Wireless Wide-Area Networks (WWANs)

- Early mobile system achieves large coverage area by using a single, high powered transmitted with an antenna mounted on a tall tower
  - E.g., Bell mobile system in New York City (1970s) could support 12 simultaneous calls over a thousand square miles
- Cellular concept was a major breakthrough to solve the problem of spectral congestion and user capacity
  - Replace single, high power transmitted (large cell) with many low power transmitters (small cells)
  - Each base station (BS) gets a portion of the total number of channels
  - Neighboring BSs are assigned different groups of channels so that interference is minimized

1st Generation Cellular System: AMPS

- Advanced Mobile Phone System (AMPS)
  - Divides 800 MHz spectrum into several channels, each 30 KHz wide => 832 full-duplex channels
  - Cellular structure uses cluster size of seven (*N*=7), r=10-20 Km
  - Use concept of trunking (as in phone networks)
  - Grade-of-service (GoS) measures network accessibility, i.e., probability of call being block or experiencing a queuing delay greater than a threshold value
    - AMPS is designed for GoS=2%

3

Problems with 1G Systems

- No use of encryption
- Inferior call quality
  - Analog traffic is degraded by interference. In contrast to digital traffic, no coding or error correction is applied
- Spectrum inefficiency
  - Dedicated channel allocated per user
  - Unlike digital signals that allow compression, cannot reduce amount of capacity needed to send data

➡ 2G systems

- 2G systems are Digital: convert speech into digital code (a series of pulses)

4

2nd Generation: 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

5

GSM: Performance Characteristics

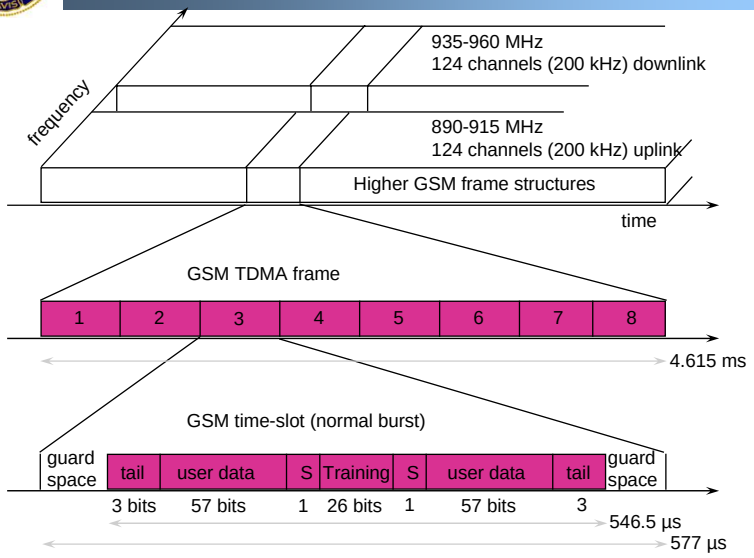
- Support for voice and data services
- Total mobility
  - International access, chip-card enables use of access points of different providers
  - Worldwide connectivity
    - One number, the network handles localization
- High capacity
  - Better frequency efficiency, smaller cells, more customers per 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

6

GSM - TDMA/FDMA (1)

- GSM uses FDM to separate the channels
  - Each call is allotted a duplex channels separated by 45MHz, each channel has 200KHz bandwidth
  - Downlink (BS->MT) channels: 935-960MHz
  - Uplink (MT-> BS) channels: 890-915 MHz

GSM - TDMA/FDMA (2)



Disadvantages of GSM

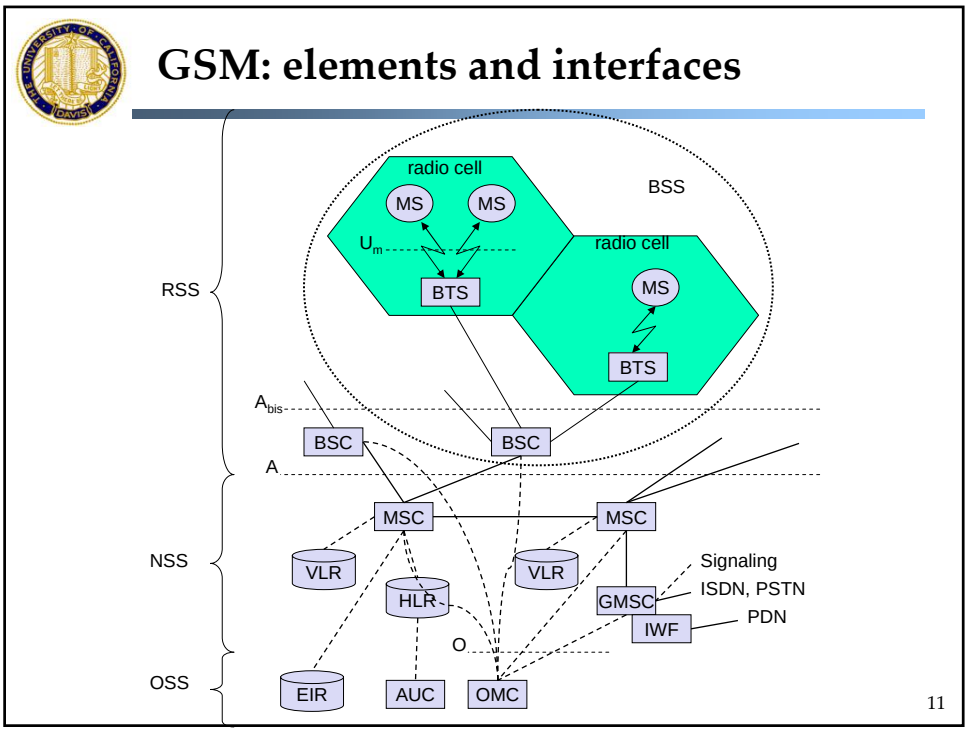
- There is no perfect system!!
- No end-to-end encryption of user data
- No full ISDN bandwidth of 64 kbit/s to the user, no transparent B-channel
- Security and Privacy issues
  - Abuse of private data possible
  - Roaming profiles accessible
- High complexity of the system
- Several incompatibilities within the GSM standards
- Safety issues
  - Reduced concentration while driving
  - Electromagnetic radiation

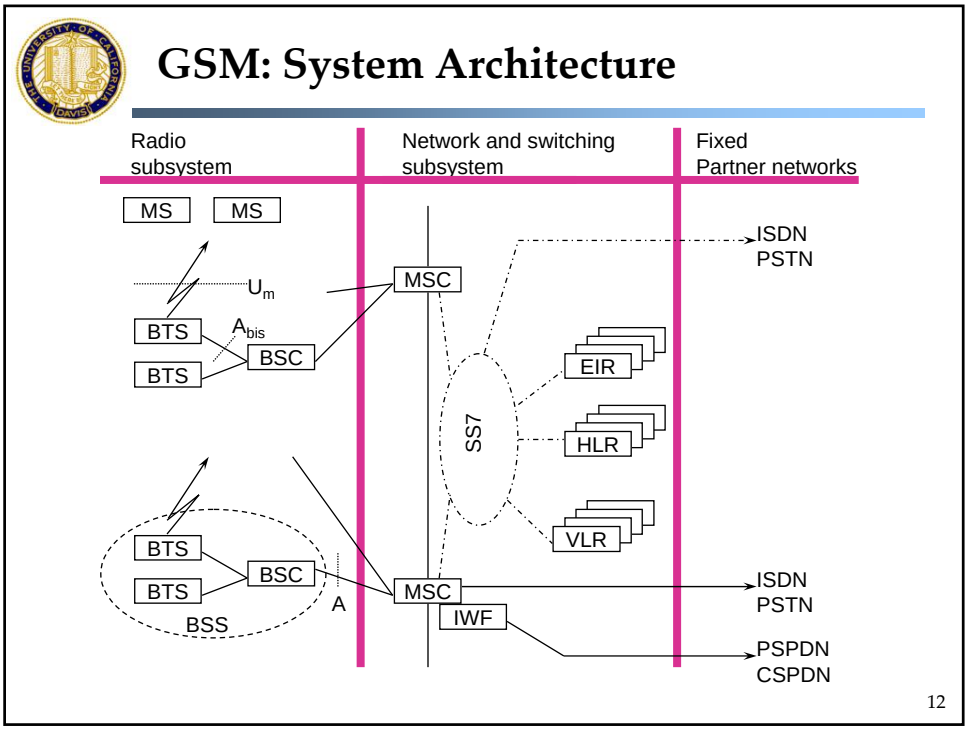
9

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)
    - Home location register (HLR) vs. Visitor location register (VLR)
- Subsystems
  - RSS (radio subsystem): covers all radio aspects
  - NSS (network and switching subsystem): call forwarding, handover, switching
  - OSS (operation subsystem): management of the network

10


GSM: elements and interfaces
radio cell
MS
MS
BSS
U_m
radio cell
BTS
MS
BTS
RSS
A_{bis}
BSC
BSC
A
MSC
MSC
NSS
VLR
VLR
HLR
GMSC
Signaling
ISDN, PSTN
IWF
PDN
O
OSS
EIR
AUC
OMC
11

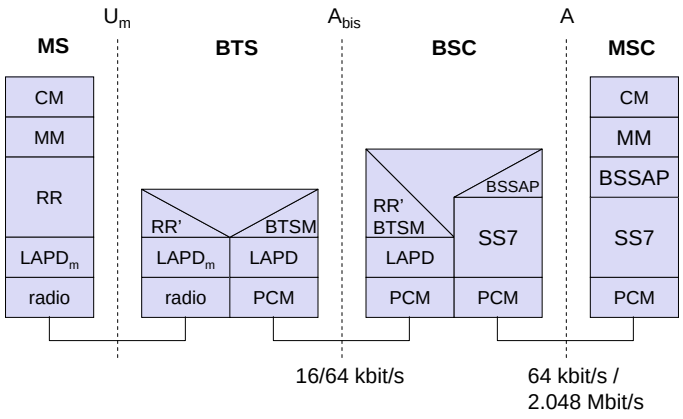

GSM: System Architecture
Radio subsystem
Network and switching subsystem
Fixed Partner networks
MS
MS
ISDN
PSTN
U_m
MSC
BTS
A_{bis}
BSC
BTS
EIR
SS7
HLR
VLR
BTS
BSC
BTS
A
MSC
ISDN
PSTN
BSS
IWF
PSPDN
CSPDN
12

Mobile Services Switching Center (MSC)

- The MSC plays a central role in GSM
  - Switching functions
  - Additional functions for mobility support
  - Management of network resources
  - 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

13

GSM Protocol Layers for Signaling



14

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

15

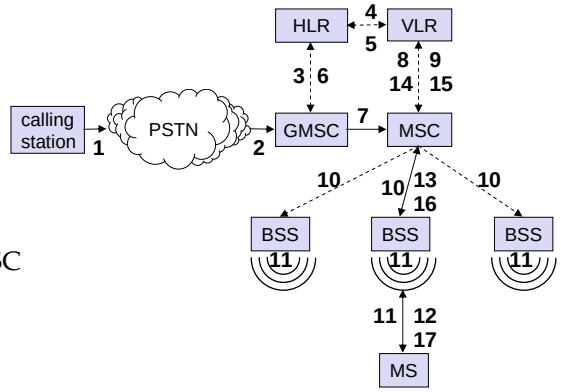
GSM Control Channels

- Broadcast control channel (BCCH)
  - Downlink channel that contains BS's identity and channel status
  - MT monitor BCCH to detect if they have moved into a new cell
- Dedicated Control Channel (DCCH)
  - Every call has its own allotted DCCH for call-setup, location updates, and call management info exchange
  - BS uses info in DCCH to track MT's footprint
- Common Control Channel (CCCH)
  - Downlink Paging Channel: used to page MT to alert it for an incoming call
  - Random Access Channel: support slotted ALOHA-based request from MT to BS for call-initiation
  - Access Grant Channel: BS informs MT of the allotted duplex channel for a call

16

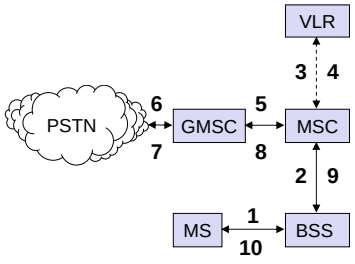
Call to Mobile Terminal

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



Subscriber Identity Module (SIM)

- An important feature of GSM
- SIM: Smart card pluggable into GSM phone
  - Store subscriber's ID@, network/countries subscriber is entitled to service, other user-specific info
- SIM provides personal mobility
  - SIM card can be inserted to another handset

19