This lecture is being recorded

18-452/18-750
Wireless Networks and Applications

Lecture 14:
Cellular: 1G and 2G

Peter Steenkiste

Spring Semester 2022

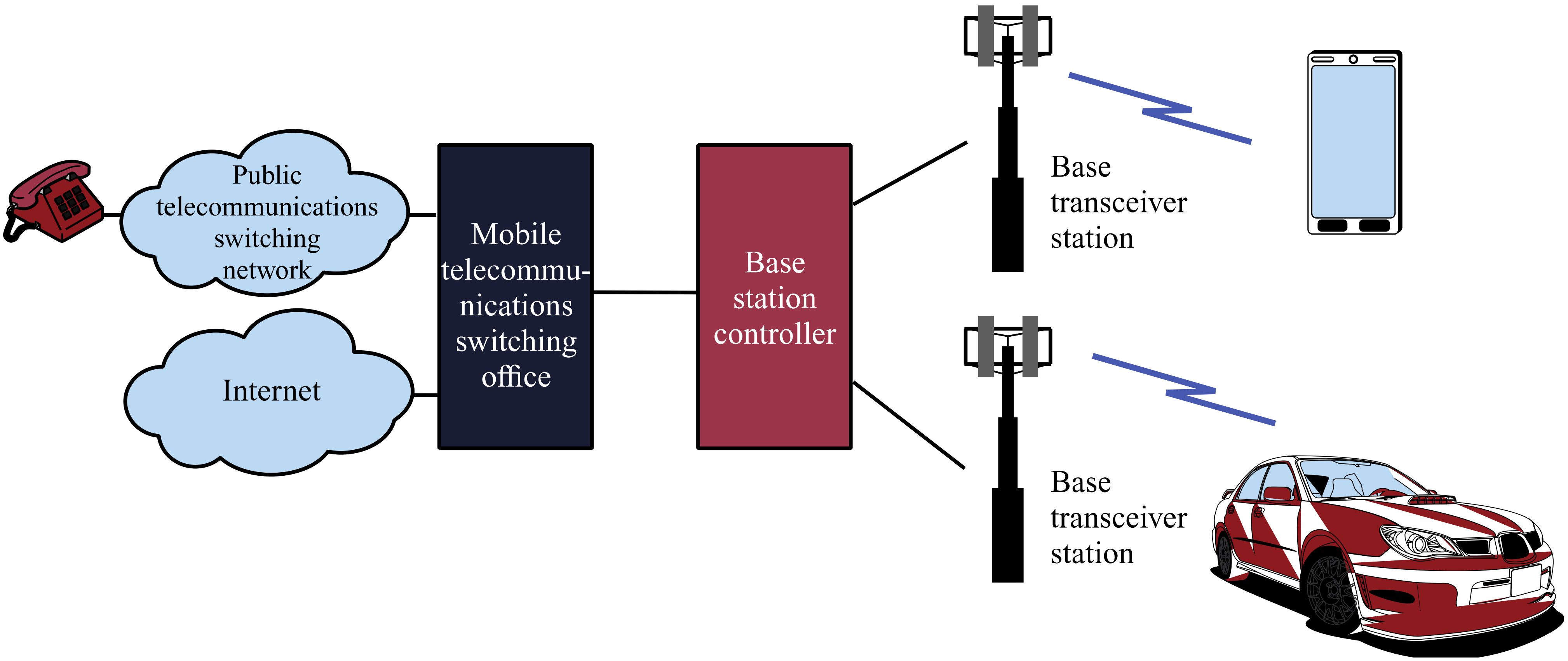
http://www.cs.cmu.edu/~prs/wirelessS22

Overview

- Cellular principles – “classic” view
  - A bit of history
  - Cellular design
  - How does a mobile phone call take place?
  - Handoff
  - Frequency Allocation, Traffic Engineering
- Early cellular generations: 1G, 2G, 3G
- Today’s cellular: 4G – LTE
- Emerging: 5G widely advertised

Some slides based on material from
“Wireless Communication Networks and Systems”
© 2016 Pearson Higher Education, Inc.

Overview of Cellular System

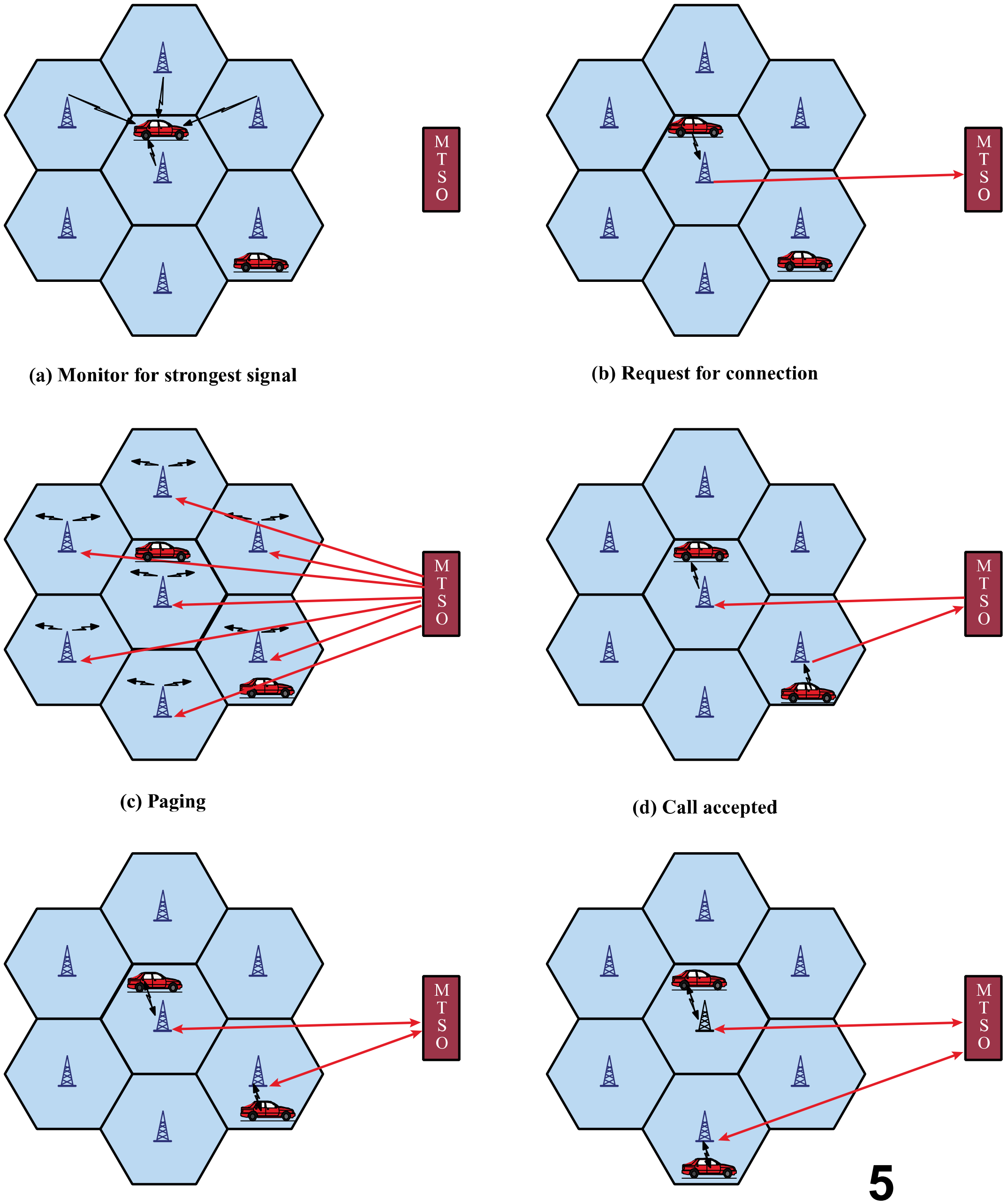

Public telecommunications switching network
Internet
Mobile telecommu-nications switching office
Base station controller
Base transceiver station
Base transceiver station

Elements of a cellular system

- Base Station (BS): includes antenna, a controller, and a number of transceivers for communicating on the channels assigned to that cell
- Controller handles the call process between the mobile unit and the rest of the network
- MTSO: Mobile Telecommunications Switching Office, serving multiple BSs. Connects calls between mobiles and to the PSTN. Assigns the voice channel, performs handoffs, billing
  - » The management and control infrastructure
  - » The name is different in each generation

MTSO Sets up Call between Mobile Users

- Mobile unit initialization
- Mobile-originated call
- Paging
- Call accepted
- Ongoing call
- Handoff



(a) Monitor for strongest signal

(b) Request for connection

(c) Paging

(d) Call accepted

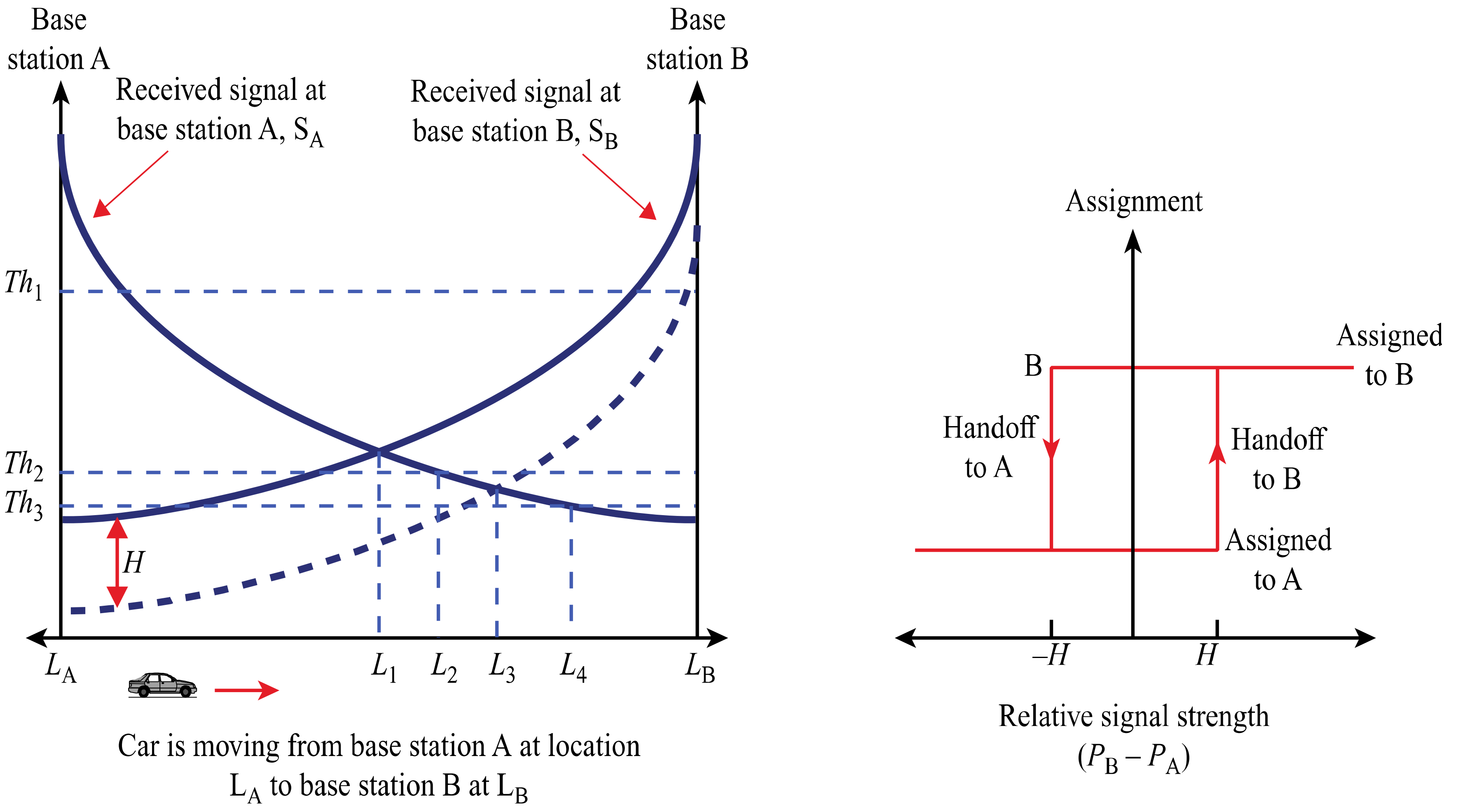
(e) Ongoing call

(f) Handoff

Handoff Strategies Used to Determine Instant of Handoff

- **Metrics related to handoff:**
  - » **Call blocking probability: probability of a new call being blocked**
  - » **Call dropping probability: probability that a call is terminated due to a handoff**
- **Possible strategies for scheduling handoffs:**
  - » **Relative signal strength – L_1**
  - » **Relative signal strength with threshold Th_2 – L_2**
  - » **Relative signal strength with hysteresis H – L_3**
  - » **Relative signal strength with hysteresis and threshold Th_1 or Th_2 – L_3; Th_3 – L_4**
  - » **Prediction techniques**
- **Details are different across the generations**

Example of Handoff



Car is moving from base station A at location L_A to base station B at L_B

(a) Handoff decision as a function of handoff scheme

(b) Hysteresis mechanism

https://media.pearsoncmg.com/ph/esm/ecs_stallingsbeard_wcns_1/animations/13_7_handoff_between_two_cells/index.html

Mobile Radio Propagation Effects

- Signal strength
  - » Must be strong enough to maintain signal quality at the receiver
  - » Must not be so strong as to create too much co-channel interference with channels in another cell using the same frequency band
  - » Fading may distort the signal and cause errors
- Mobile transmission power minimized to avoid co-channel interference, alleviate health concerns and save battery power

Open and Closed Loop Power Control

- Open loop power control: BS sends pilot
  - » Used by mobile to acquire timing and phase reference, and to assess channel attenuation
  - » Mobile adjust power accordingly
    - – Assume up and down channels are similar
  - » Can adjust quickly but not very accurate
- Closed loop power control: power is adjust based on explicit feedback from receiver
  - » Reverse signal power level, received signal-to-noise ratio, or received bit error rate
  - » Mobile to BS: BS base station sends power adjustment command to mobile based on observed signal
  - » BS to mobile: BS adjust power based on information provided by mobile

Fixed Channel Assignment (FCA)

- Each cell is allocated a predetermined set of voice channels.
- Any call attempt within the cell can only be served by the unused channels in that cell
- If all the channels in that cell are being used the call is blocked → user does not get service
- A variation of FCA: the cell whose channels are all being used is allowed to borrow channels from the next cell. MTSO supervises this operation.

Dynamic Channel Assignment (DCA)

- Channels are not permanently assigned to cells. Instead, for each request the BS requests a channel from the MTSO.
- MTSO allocates a channel using an algorithm that takes many factors into account
  - » The likelihood of future blocking within the cell, the frequency of use of the candidate channel, the reuse distance of the channel, and other cost functions.
  - » MTSO only allocates a channel if it is not being used in the restricted distance for co-channel interference
- DCA can use channels more effectively but incurs measurement, communication, and computer overhead

Overview

- Cellular principles – “classic” view
- Early cellular generations: 1G, 2G, 3G
  - 1G: AMPS
  - 2G: GSM
  - 2.5G: EDGE, CDMA
  - 3G: WCDMA
- Today’s cellular: 4G – LTE
- Emerging: 5G widely advertised

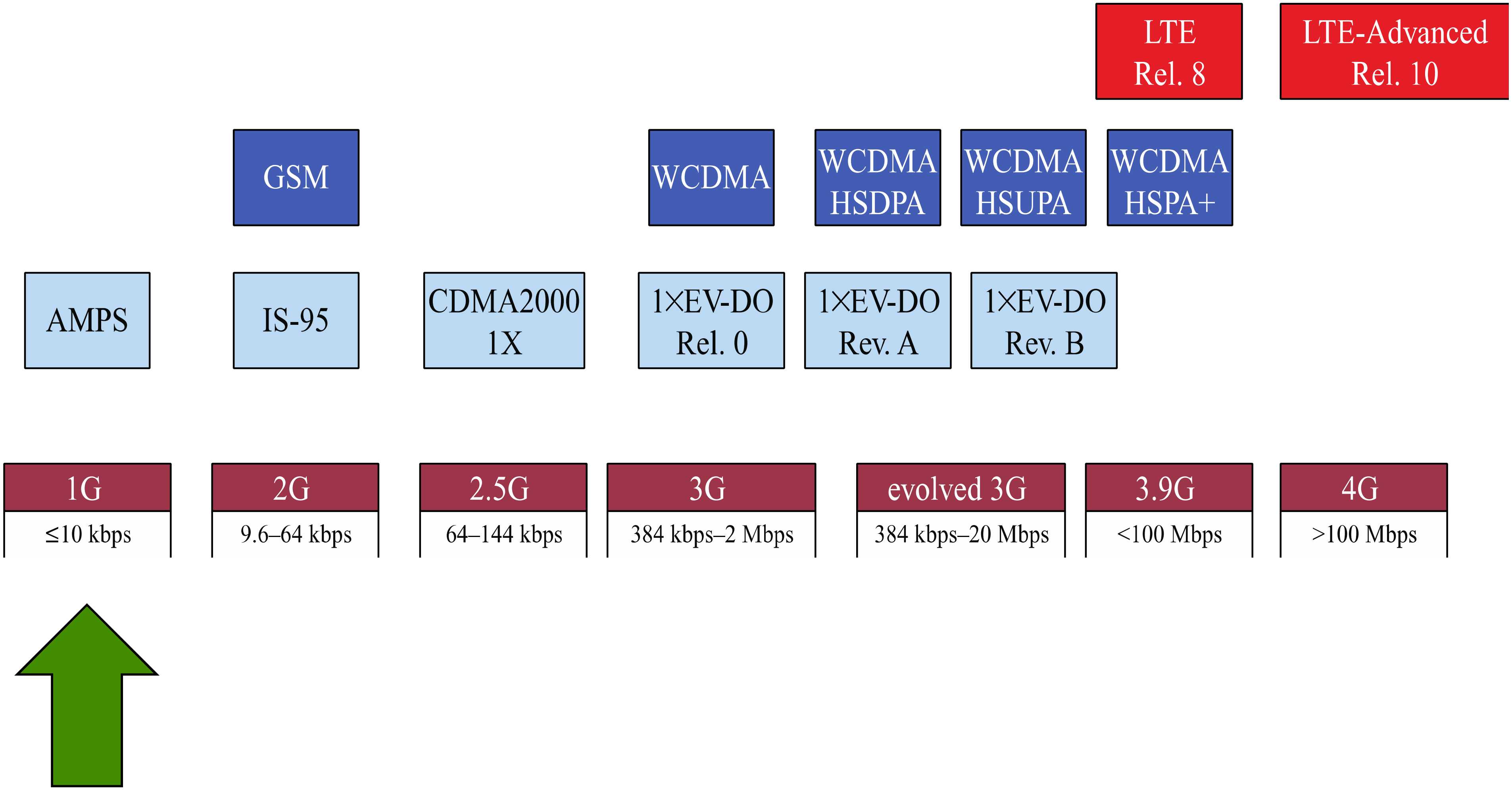
Some slides based on material from
“Wireless Communication Networks and Systems”

Outline

- 1G: AMPS
- 2G: GSM
- 2.5G: EDGE, CDMA
- 3G: WCDMA

Some slides based on material from
"Wireless Communication Networks and Systems"

Evolution of Cellular Wireless Systems



LTE Rel. 8

LTE-Advanced Rel. 10

GSM

WCDMA

WCDMA HSDPA

WCDMA HSUPA

WCDMA HSPA+

AMPS

IS-95

CDMA2000 1X

1×EV-DO Rel. 0

1×EV-DO Rev. A

1×EV-DO Rev. B

1G	2G	2.5G	3G	evolved 3G	3.9G	4G
≤10 kbps	9.6–64 kbps	64–144 kbps	384 kbps–2 Mbps	384 kbps–20 Mbps	<100 Mbps	>100 Mbps

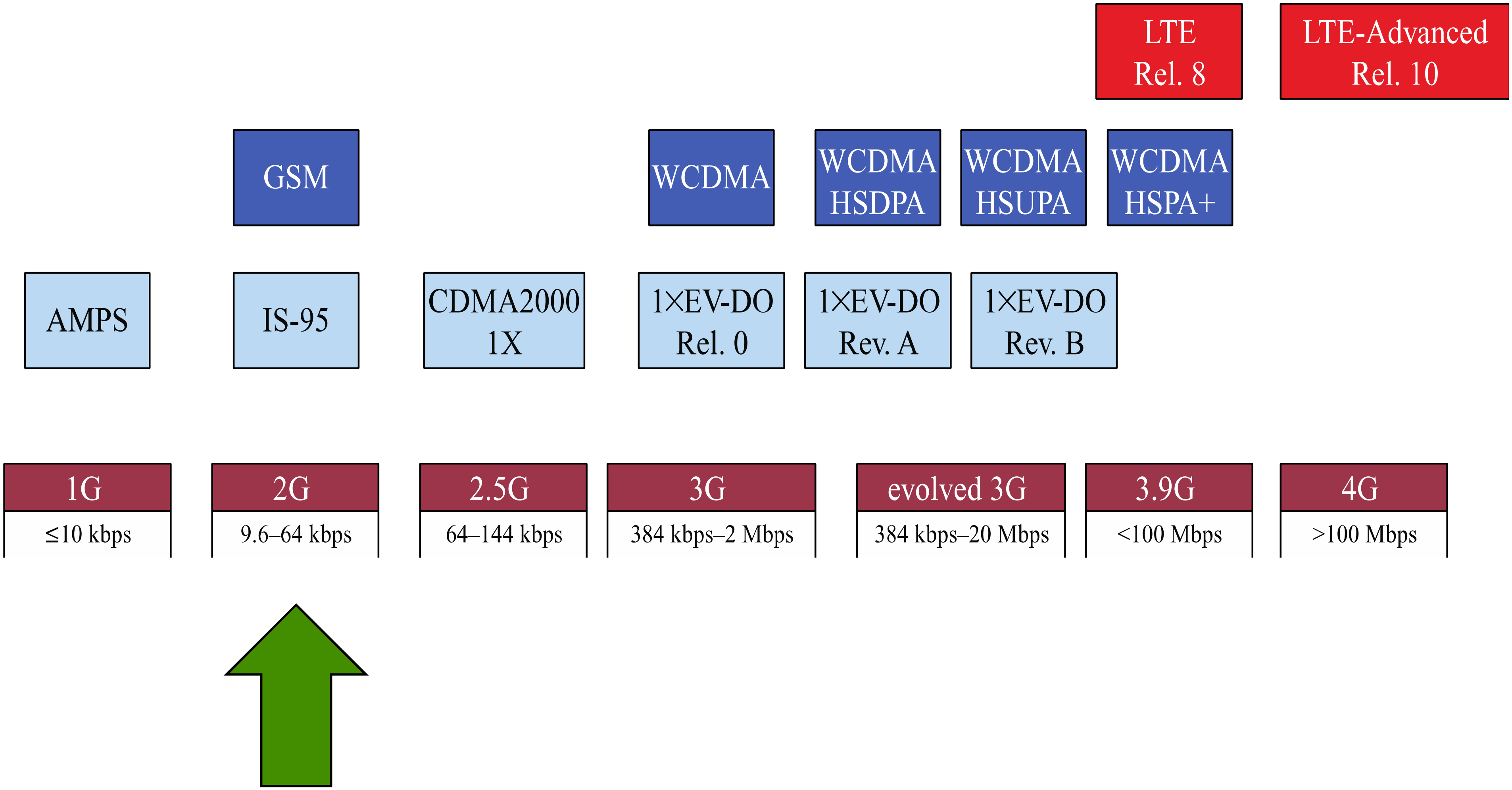
Advanced Mobile Phone Service (AMPS)

- In North America, two 25-MHz bands were allocated (DL: 869-894 MHz, UP: 824-849 MHz)
  - » Deployed since early 80's by two providers
- Channels are spaced by 30 KHz, allowing for 416 channels (21 control, 395 for voice calls)
  - » Control channels are full duplex data channels at 10 Kbps
  - » Includes preamble, word sync, and Digital Color Code identifying the base station
  - » Can send urgent control in data channels
- Voice calls carried in analog using frequency modulation
  - » Effectively extends analog telephone over wireless
- Cell size = 2-20Km, frequency reuse is exploited

AMPS Operation

- When unit wakes up, it sends telephone and serial number to the Mobile Telephone Switching Office (MTSO) over control channel
  - » Both stored in read-only memory
  - » Used for billing purposes and to detect stolen phones
- Steps in placing a call:
  1. User dials in a number – sent to the MTSO
  2. MTSO verifies validity of service request
  3. MTSO notifies user of channels to use for up and down link
  4. MTSO sends ring signal to the called party
  5. MTSO completes circuit when party picks up
  6. When either party hangs up, MTSO releases circuit and wireless channels, and completes billing
  - » Same as a ``regular'' phone call!

Evolution of Cellular Wireless Systems



LTE Rel. 8

LTE-Advanced Rel. 10

GSM

WCDMA

WCDMA HSDPA

WCDMA HSUPA

WCDMA HSPA+

AMPS

IS-95

CDMA2000 1X

1×EV-DO Rel. 0

1×EV-DO Rev. A

1×EV-DO Rev. B

1G	2G	2.5G	3G	evolved 3G	3.9G	4G
≤10 kbps	9.6–64 kbps	64–144 kbps	384 kbps–2 Mbps	384 kbps–20 Mbps	<100 Mbps	>100 Mbps

Differences Between First and Second Generation Systems

- Digital traffic channels – first-generation systems are almost purely analog; second-generation systems are digital
  - » Using FDMA/TDMA, CDMA, OFDM, …
- Encryption: second generation systems use encryption to prevent eavesdropping
- Error detection and correction: digital encoding allows for error detection and correction, giving clear voice reception
- Channel access – channels can be dynamically shared by a number of users
  - » I.e., multiplexing in time and frequency

Motivation for Switch from Analog to Digital

- Higher quality
- Compression
- Encryption
- Error Detection and Correction
- Multiplexing channels by different users
  - » I.e. TDMA

Global System for Mobile (GSM) - Background

- GSM is a set of ETSI standards specifying the infrastructure for a digital cellular service
  - » European Telecommunications Standards Institute
  - » Developed to provide a common second-generation technology for Europe
- The standard was used in approx. 109 countries around the world including Europe, Japan and Australia
- Order 44 million subscribers
- Process: define a set of requirements, and then develop technologies to meet them

Design Requirements for GSM-like 2G Systems

- Degree of multiplexing: at least 8
  - » Not worth adding TDMA complexity otherwise
- Maximum cell radius: ~35km
  - » Needed for rural areas
- Frequency: around 900 MHz
- Maximum speed: 250 km/hr – high-speed train
- Maximum coding delay: 20 msec
  - » Do not want to add too much to network delay (voice!)
- Maximum delay spread: ~10 μsec
  - » Multi-path property: ~3.3 km
- Bandwidth: up to 200 KHz, ~25 kHz/channel

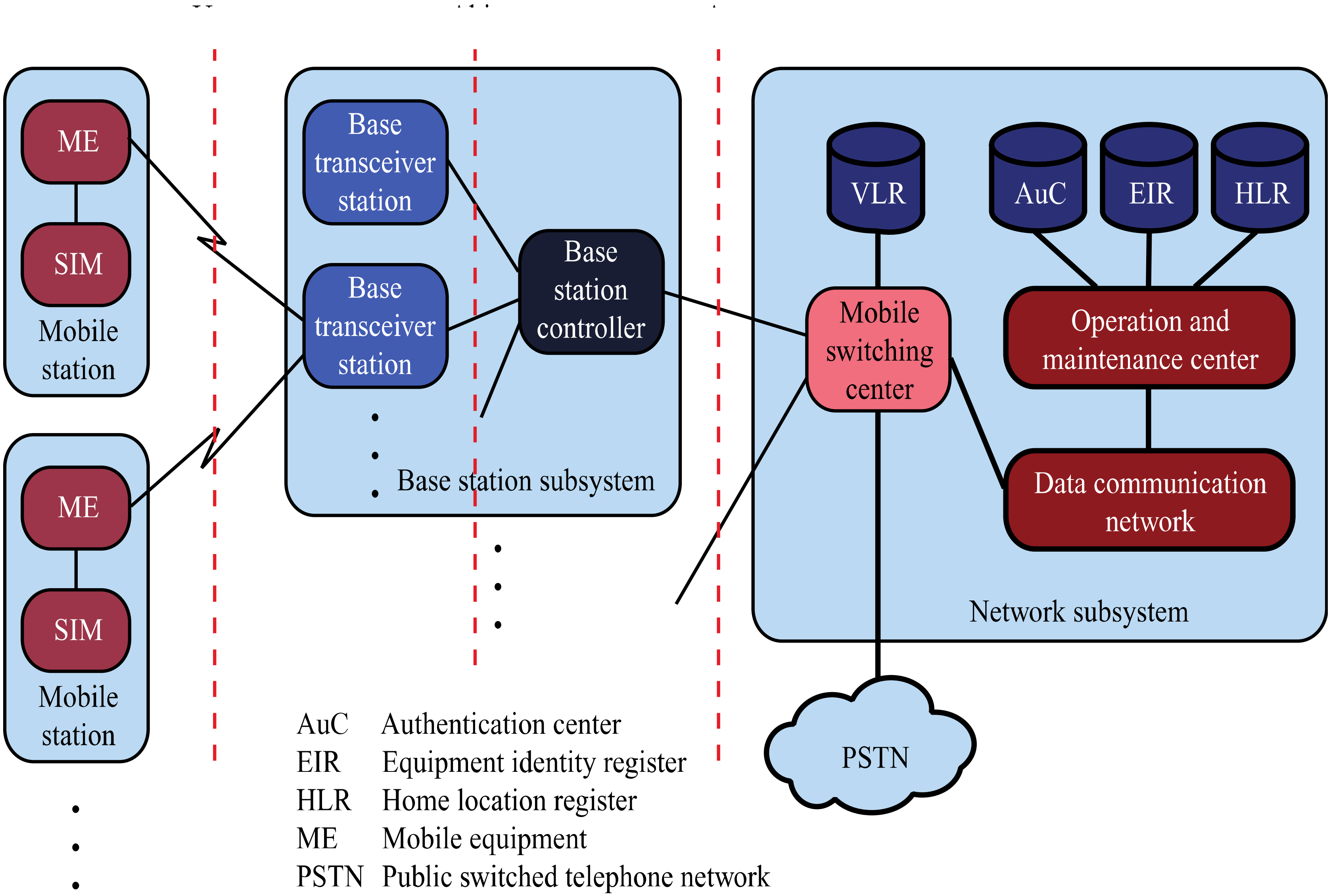
GSM Features

- Hybrid FDMA/TDMA approach
- Mobile station communicates across the air interface with base station in the same cell as mobile unit
- Mobile equipment (ME) – physical terminal, e.g., a telephone or “personal communication system”
  - » ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)
- GSM subscriber units are generic until a SIM is inserted
  - » SIMs roam since they are based on single standard
  - » Not necessarily the case for subscriber devices – may use different versions of the protocol

GSM SIM

- Users have a Subscriber Identity Module (SIM) – a smart card
- The user identity is associated with a mobile device through the SIM card
- The SIM is portable and transferable
- All cryptographic algorithms (for authentication and data encryption) can be realized in the SIM
- May also store short messages, charging info, ..
- SIM implications:
  - » Equipment mobility and user mobility are not the same
  - » International roaming independent of the equipment and network technology

Global GSM System



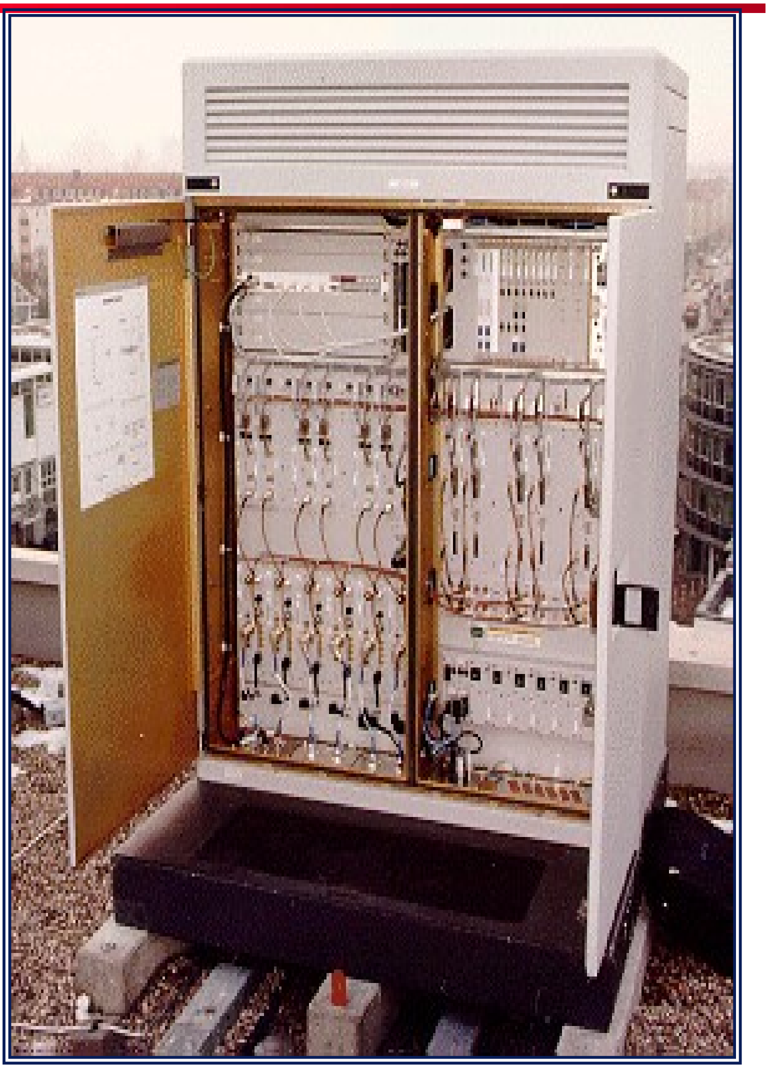
AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
ME	Mobile equipment
PSTN	Public switched telephone network
SIM	Subscriber identity module
VLR	Visitor location register

Base Station Subsystem (BSS)

- BSS consists of base station controller (BSC) and one or more base transceiver stations (BTS)
- BSC reserves radio frequencies, manages handoff of mobile unit from one cell to another within the BSS, and controls paging
- Each BTS defines a single cell
  - » Includes radio antenna, radio transceiver and a link to a base station controller (BSC)

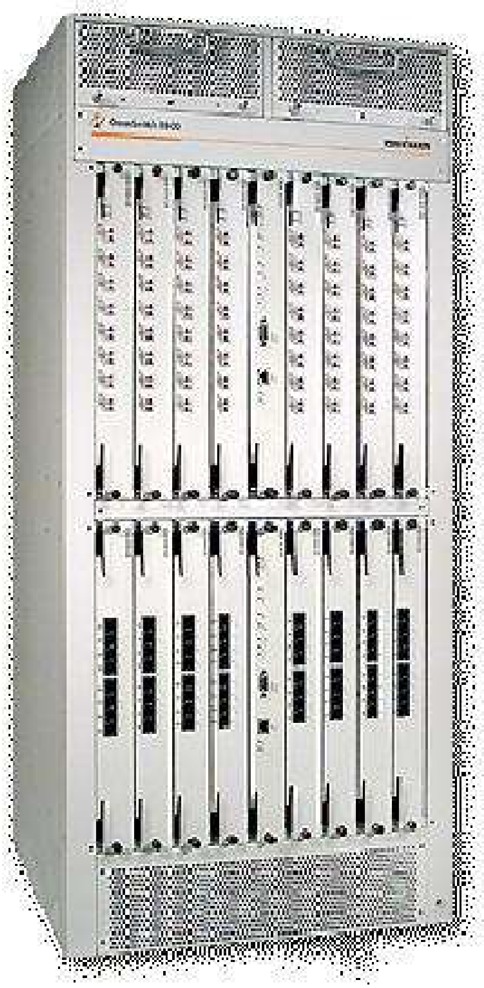
Base Transceiver Station

- Radio transmission/reception management (modulation/demodulation, equalisation, interleaving ...)
- Physical layer management (TDMA transmission, SFH, coding, ciphering ...)
- Link layer management
- Received signal quality and power measurement

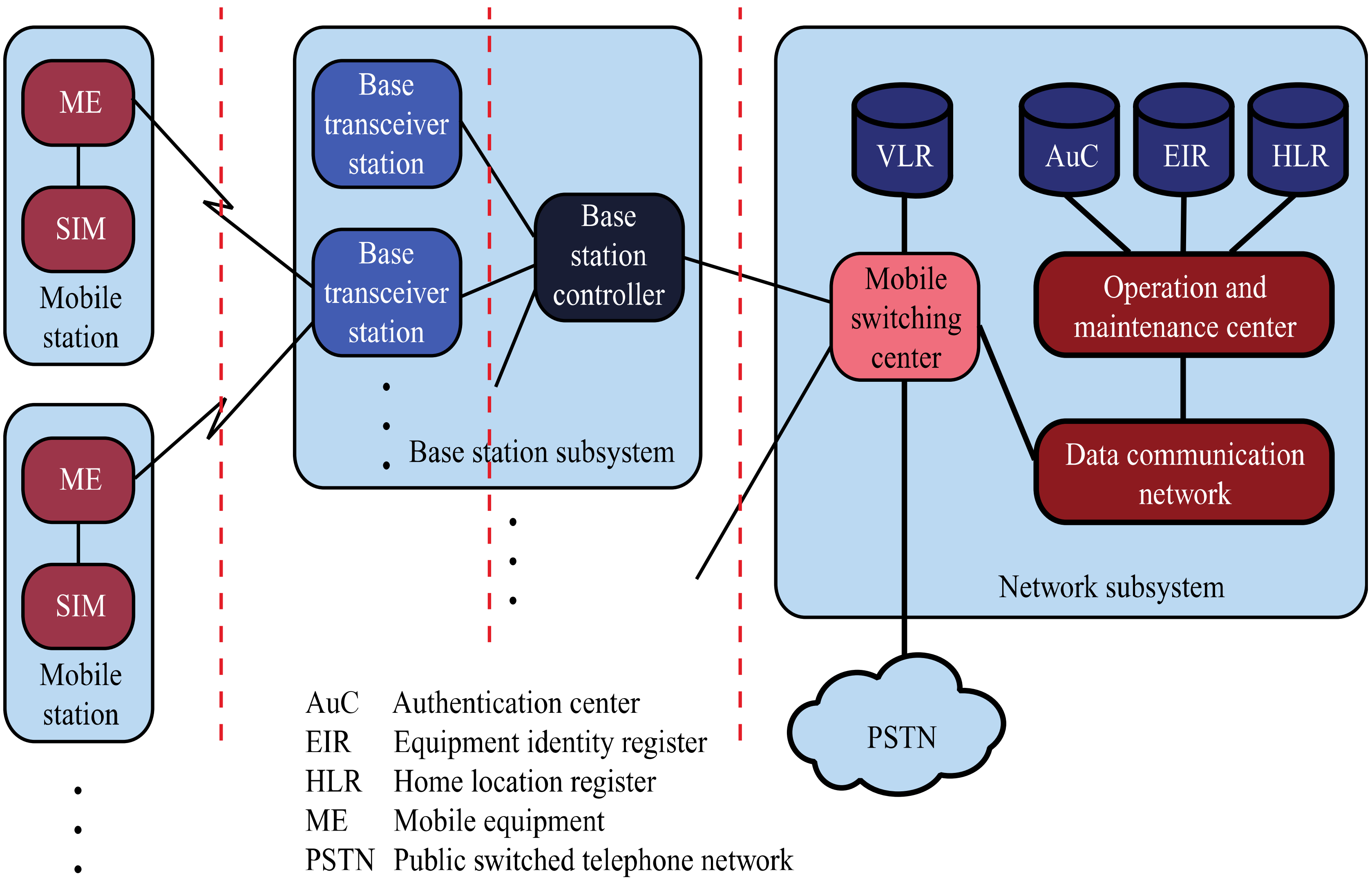


Base Station Controller

- Interface between MSC and BTSs
  - Forwarding of traffic
  - Coordination of and with BTSs
- Radio resource management for the Base Station Subsystem
  - Channel allocation
  - BTS measures processing
  - BTS and MS power control
  - Handover
  - ...



Global GSM System



AuC	Authentication center
EIR	Equipment identity register
HLR	Home location register
ME	Mobile equipment
PSTN	Public switched telephone network
SIM	Subscriber identity module
VLR	Visitor location register

Network Subsystem (NS)

- NS provides link between cellular network and public switched telecommunications networks (PSTN)
  - » Controls handoffs between cells in different Base Station Subsystems
  - » Authenticates users and validates accounts
  - » Enables worldwide roaming of mobile users
- Central element of NS is the Mobile Switching Center (MSC)

Mobile Switching Center

- Management of the communication between mobiles and the fixed network
  - The Gateway Mobile Switching Controller forms the gateway for calls to and from external networks
- MSC is also responsible for mobility management
  - Handover between Base Station Subsystems
  - Roaming across networks

Handover

- Executed by BSC (channels) and by MSC (routing)
- Initiated by base station:
  - BS monitors the signal coming from the MT
  - Low signal => Need to do handover
- Mobile-terminal aided:
  - BS transmit beacon
  - MT, hearing better beacon, request join
    - Sends the identity of the old BS to the new BS
  - BS accepts the MT, calls are then forwarded
- Inter-system system handover is managed MSC
  - With extra connections to the HLR/VLR

Mobile Switching Center (MSC) Databases

- Home location register (HLR) database – stores information about each subscriber that belongs to this MSC
- Visitor location register (VLR) database – maintains information about subscribers currently physically in the region
- Authentication center database (AuC) – used for authentication activities, holds encryption keys
- Equipment identity register database (EIR) – keeps track of the type of equipment that exists at the mobile station

Home Location Register

- One per Network Subsystem
  - » Basically a local operator
- Contains entries for every subscriber and every mobile ISDN number that is homed in the respective network
- Permanent subscriber data and relevant temporary information
- Current location of the mobile station
- All administrative activities of the subscriber happen here!

Visitor Location Register

- Typically one per MSC, but 1 VLR could be responsible for more than 1 MSC
- Stores data on all mobile stations which are currently in the administrative area of the respective MSC
- A roaming MS may be registered in a VLR of its home network or the foreign network depending on its location
- MS registers upon entering a LA. The MSC passes the identity of the MS and LAI to VLR
  - » See next slide

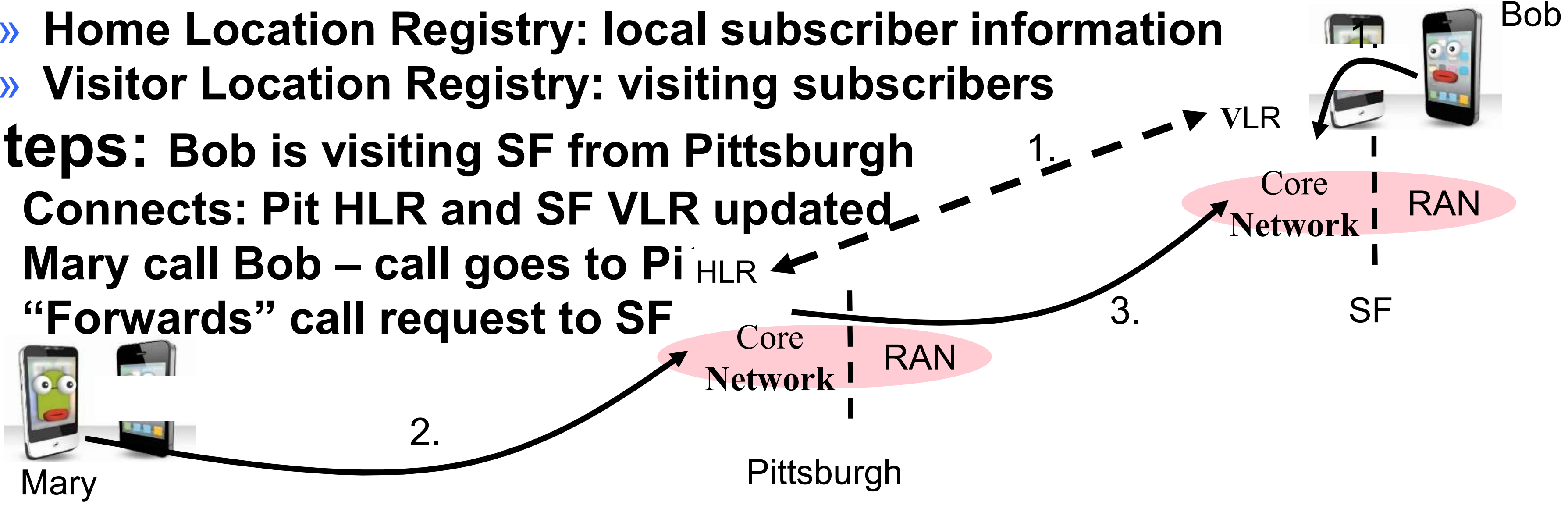
Roaming In Cellular

- Subscribers are associated with a particular network subsystem, e.g, Pittsburgh region
  - » Historically, phone number is associated with this system
- How can you receive a phone call if you are not in your?
  - » Does this sound familiar?
- Roaming falls into two categories
  - » Roaming between systems but in the network of the same provider
  - » Roaming across providers, e.g., when traveling abroad
  - » Roaming mechanisms are similar but business aspects and some details are different

How about Mobility?

- **Subscribers of one network (e.g., Pittsburgh) can get cellular service in other networks (e.g., SF) of same provider**
- **High level solution (2G terminology)**
  - » **Home Location Registry: local subscriber information**
  - » **Visitor Location Registry: visiting subscribers**
- **Steps: Bob is visiting SF from Pittsburgh**

1. **Connects: Pit HLR and SF VLR updated**
2. **Mary call Bob – call goes to Pi**
3. **“Forwards” call request to SF**

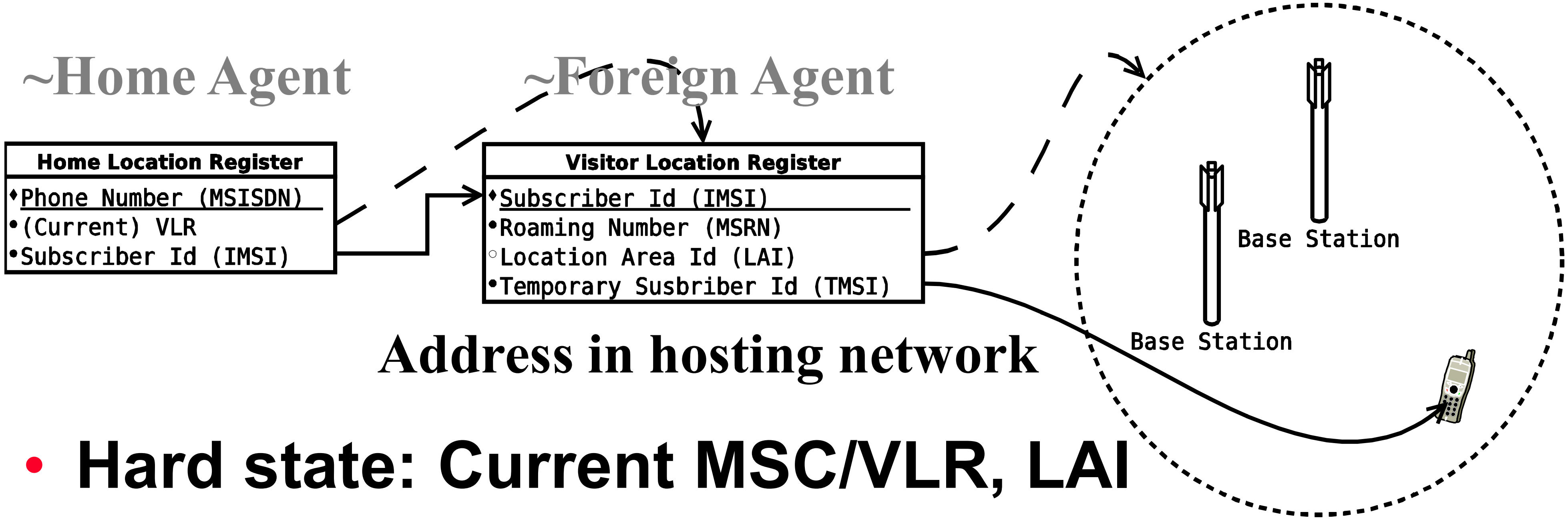


GSM Addressing Hierarchy

- Device
  - » IMEI (International Mobile Equipment Identifier)
- User
  - » IMSI (International Mobile Subscriber Identifier)
  - » MSISDN (Mobile Subscriber IDSN Number)
    - – “Real phone number”
  - » MSRN (Mobile Station Roaming Number)
  - » TMSI (Temporary Mobile Subscriber Identity)
  - » LMSI (Local Mobile Subscriber Identity)
- Other
  - » LAI (Location Area Identity)
  - » CI (Cell Identity)

No need to memorize this list!

GSM Address Lookup (“registers”)



~Home Agent

~Foreign Agent

Home Location Register

- Phone Number (MSISDN)
- (Current) VLR
- Subscriber Id (IMSI)

Visitor Location Register

- Subscriber Id (IMSI)
- Roaming Number (MSRN)
- Location Area Id (LAI)
- Temporary Susbriber Id (TMSI)

Base Station

Base Station

Address in hosting network

- **Hard state: Current MSC/VLR, LAI**
  - » **(Necessary to page phone, updated whenever mobile moves)**
- **Soft-ish state:**
  - » **MSRN, cell ID, TMSI**

Note: Grossly simplified for your safety and sanity!

Roaming Discussion

- Roaming introduces some challenges for the phone, similar to those for Wifi
- When you open your phone, how do you know whether the cellular channels are?
  - » There is a lot of variability across countries
- When you are outside of the coverage area of your provider, how do you know which providers you can use?
- Your phone needs to have this information in its memory (at least enough to get started)
  - » Updated by your provider as part of regular updates