

18-452/18-750
Wireless Networks and Applications
Lecture 16:
Cellular: 1G, 2G, and 3G

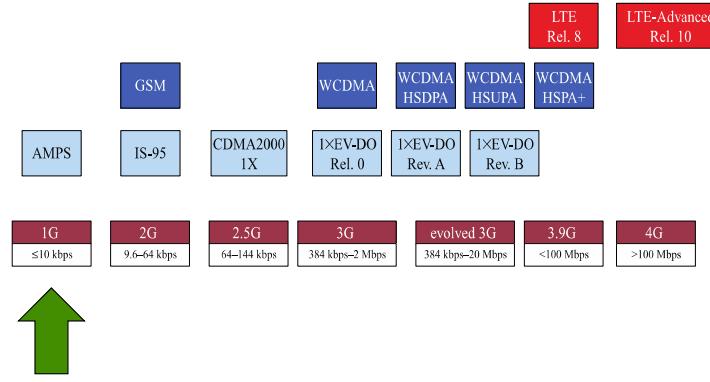
Peter Steenkiste

Spring Semester 2018
<http://www.cs.cmu.edu/~prs/wirelessS18>

Peter A. Steenkiste, CMU

1

Evolution of Cellular Wireless Systems



Peter A. Steenkiste, CMU

3

Outline

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

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

Peter A. Steenkiste, CMU

2

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
- Conversations carried in analog using frequency modulation
 - » Effectively extends analog telephone over wireless
- Cell size = 2–20Km, frequency reuse is exploited

Peter A. Steenkiste, CMU

4

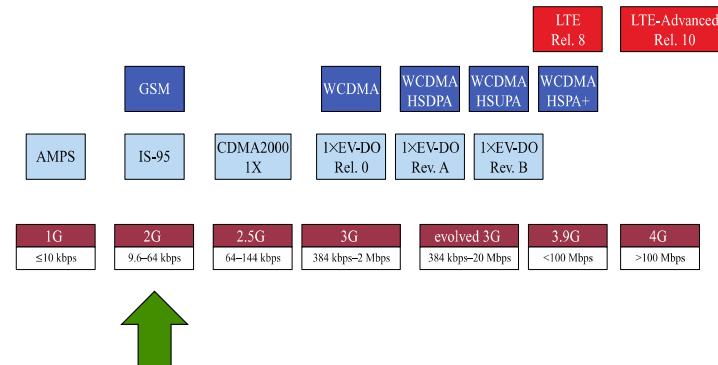
AMPS Operation

- 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/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

Peter A. Steenkiste, CMU

5

Evolution of Cellular Wireless Systems



6

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 or CDMA
- 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

Peter A. Steenkiste, CMU

7

Motivation for Switch from Analog to Digital

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

Peter A. Steenkiste, CMU

8

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
 - » For 2G only – 2-3 Billion if you include all versions

Peter A. Steenkiste, CMU

9

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 μ sec**
- **Bandwidth: up to 200 KHz, ~25 kHz/channel**

Peter A. Steenkiste, CMU

10

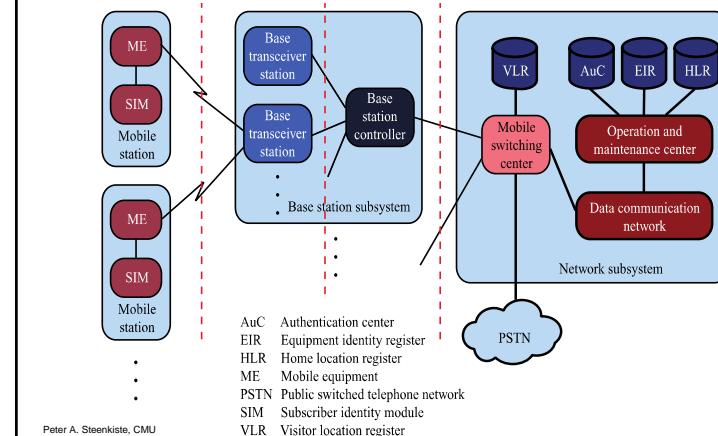
GSM Features

- 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, such as a telephone or PCS
 - » 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

Peter A. Steenkiste, CMU

11

Global GSM System



12

GSM SIM

- Users have a **Subscriber Identity Module (SIM)** – a smart card
- The user identity is associated with a mobile 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

Peter A. Steenkiste, CMU

13

Base Station Subsystem (BSS)

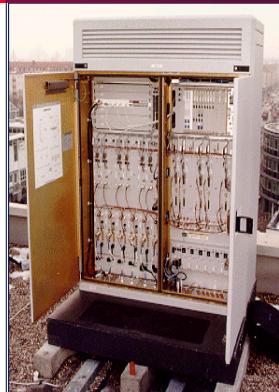
- **BSS** consists of base station controller (BSC) and one or more base transceiver stations (BTS)
- **BSC** reserves radio frequencies, manages handoff of mobile unit from one cell to another within the BSS, and controls paging
- **Each BTS defines a single cell**
 - » Includes radio antenna, radio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

Peter A. Steenkiste, CMU

14

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



Peter A. Steenkiste, CMU

15

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
 - ...

Peter A. Steenkiste, CMU



16

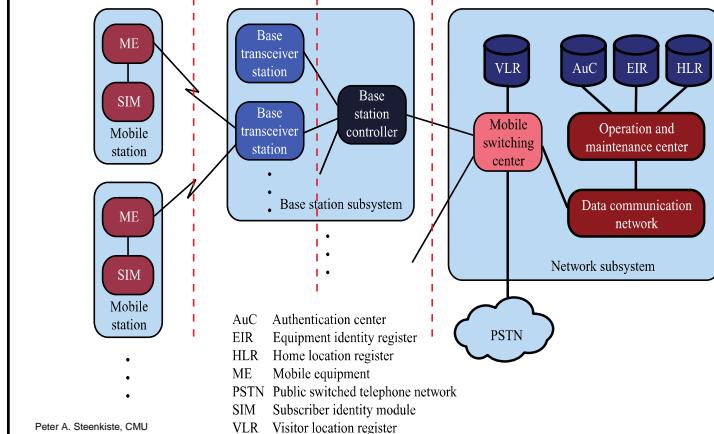
Network Subsystem (NS)

- 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)

Peter A. Steenkiste, CMU

17

Global GSM System



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



Peter A. Steenkiste, CMU

Handover

- Executed by BSC (channels) and by MSC (routing)
- Initiated by base station:
 - » BS monitors the signal coming from the MT
 - » Low signal => HO! 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

Peter A. Steenkiste, CMU

20

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

Peter A. Steenkiste, CMU

21

Home Location Register

- One per “Public Land Mobile Network”
 - » Basically an 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!

Peter A. Steenkiste, CMU

22

Visitor Location Register

- One per MSC
- Stores data on all mobile stations which are currently in the administrative area of the respective MSC
- 1 VLR could be responsible for more than 1 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

Peter A. Steenkiste, CMU

23

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)

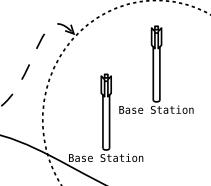
Peter A. Steenkiste, CMU

24

GSM Address Lookup ("registers")

Home Location Register
*Phone_Number (MSISDN)
*(Current) VLR

Visitor Location Register
Subscriber_Id (IMSI)
Roaming Number (MSRN)
Location Area Id (LAI)
Temporary Subscriber Id (TMSI)



- **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!

Peter A. Steenkiste, CMU

25

GSM Multiple Access

- Combination of FDMA and TDMA
- 890-915 MHz for uplink
- 935-960 MHz for downlink
- Each of those 25 MHz bands is sub divided into 124 single carrier channel of 200 KHz
 - » Each with a data rate of 270.833 kbps
- In each uplink/downlink band there is a 200 KHz guard band
- Each 200 KHz channel carries 8 TDMA channels

Peter A. Steenkiste, CMU

26

Additional GSM Features

- **GSM uses GMSK modulation**
 - » Gaussian Minimum Shift Keying
 - » Optimized version of Frequency Shift Keying (FM)
- **Slow frequency hopping: successive TDMA frames are sent over a different frequency**
 - » Switches every 4.615 msec
 - » Spreads out effect of multipath fading
 - » Also helps with co-channel interference
- **Delay equalization**
 - » Mobile stations sharing a frame can be at different distances from the base station
 - » Tail bits and guard bits provide margin to avoid overlap

Peter A. Steenkiste, CMU

27

Generalized Packet Radio Service (GPRS)

- **Packet-oriented data transport service**
 - » Bursty, non-periodic traffic typical for Internet access
- **Uses a new architecture for data traffic**
 - » Allows users to open a persistent data connection
 - » Sending data traffic over a voice connection would add too much setup and teardown overhead
- **Uses the same frame structure as voice**
 - » 21.4 kbps from a 22.8 kbps gross data rate
 - » Can combine up to 8 GSM connections
 - Overall throughputs up to 171.2 kbps
 - » Enhanced Data Rates for GSM Evolution (EDGE) further increased rates using a more aggressive PHY

Peter A. Steenkiste, CMU

28

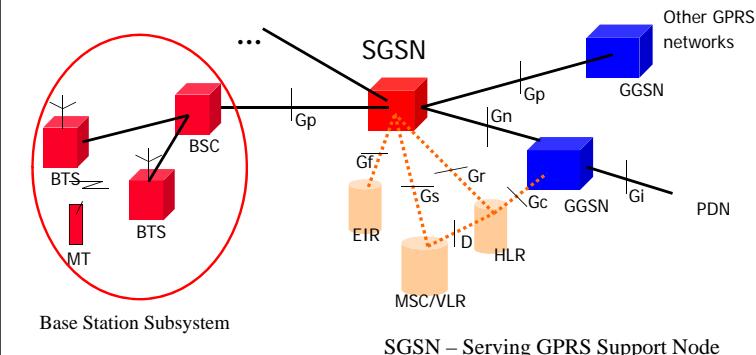
GPRS Architecture

- Network Subsystem includes several new entities:
 - Serving GPRS Support Node (SGSN): data transfer between Base Station and Network Subsystem
 - Gateway GPRS Support Node: connects to other GPRS networks and the packet data network (Internet)
 - New interfaces between the various entities
- Transmission plane
 - Data packets are transmitted by a tunnel mechanisms
- Control plane
 - Protocol for tunnel management: create, remove, ...
 - GPRS Tunnel Protocol
- Radio interface
 - Changes the logical channels and how they are managed

Peter A. Steenkiste, CMU

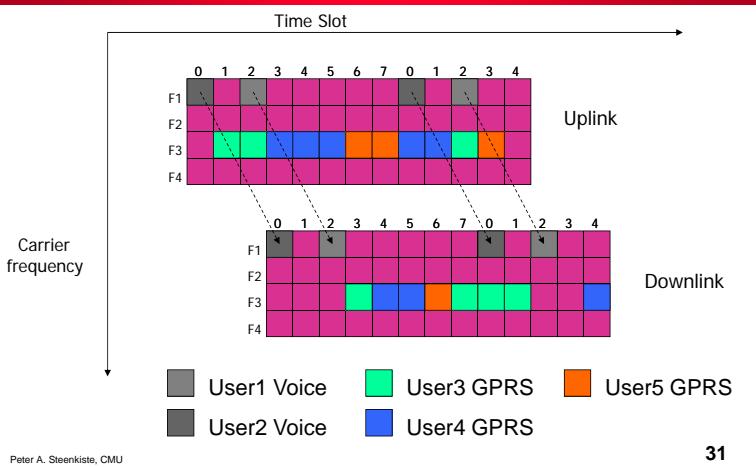
29

GPRS Architecture



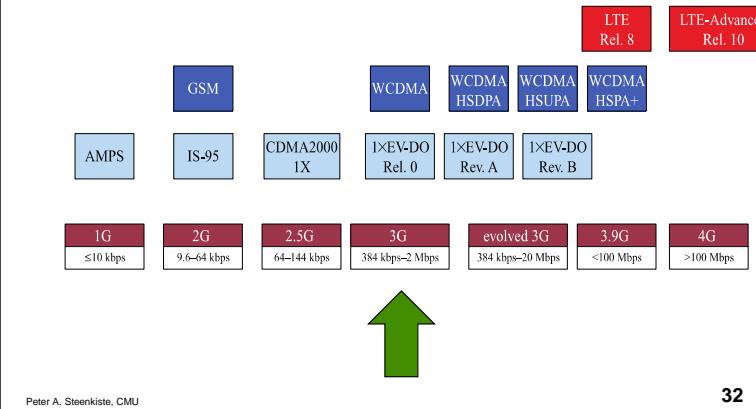
30

GPRS Radio Interface



31

Evolution of Cellular Wireless Systems



32

Who is Who

- International Telecommunications Union (ITU) - agency of the United Nations responsible for:
 - » Assisting in the development and coordination of worldwide standards
 - » Coordinate shared use of the global spectrum
 - » Defined the International Mobile Telecommunications 2000 (IMT-2000) project for 3G telecommunications
- Third Generation Partnership Project (3GPP)
 - » A group of telecommunications associations that represent large markets worldwide
 - » Defined a group of 3G standards as part of the IMT-2000 framework in 1999
 - » Originally defined GSM, EDGE, and GPRS
 - » Later defined follow-on releases and also LTE (4G)

Peter A. Steenkiste, CMU

33

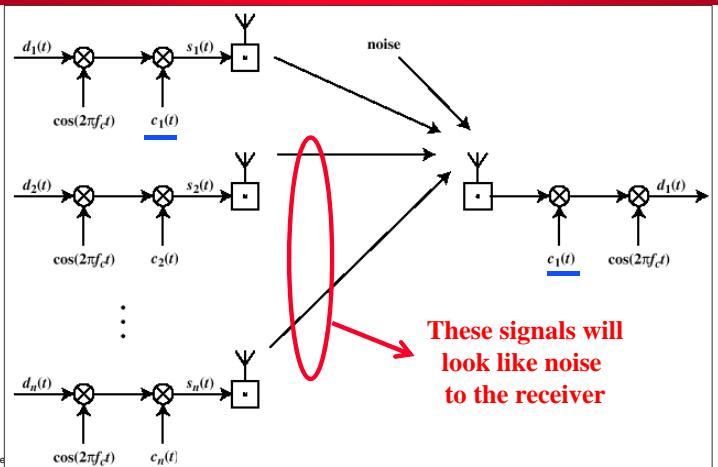
UMTS and WCDMA

- Part of a group of 3G standards defined as part of the IMT-2000 framework by 3GPP
- Universal Mobile Telecommunications System (UMTS)
 - » Successor of GSM
- W-CDMA is the air interface for UMTS
 - » Wide-band CDMA
 - » Originally 144 kbps to 2 Mbps, depending on mobility
- Basically same architecture as GSM
 - » Many GSM functions were carried over WCDMA
 - » But they changed all the names!

Peter A. Steenkiste, CMU

34

Reminder: CDMA - Direct Sequence Spread Spectrum



Later Releases Improved Performance

- High Speed Downlink Packet Access (HSDPA): 1.8 to 14.4 Mbps downlink
 - » Adaptive modulation and coding, hybrid ARQ, and fast scheduling
- High Speed Uplink Packet Access (HSUPA): Uplink rates up to 5.76 Mbps
- High Speed Packet Access Plus (HSPA+): Maximum data rates increased from 21 Mbps up to 336 Mbps
 - » 64 QAM, 2x2 and 4x4 MIMO, and dual or multi-carrier combinations
- Eventually led to the definition of LTE

Peter A. Steenkiste, CMU

36

Advantages of CDMA for Cellular systems

- Frequency diversity – frequency-dependent transmission impairments have less effect on signal
- Multipath resistance – chipping codes used for CDMA exhibit low cross correlation and low autocorrelation
- Privacy – privacy is inherent since spread spectrum is obtained by use of noise-like signals
- Graceful degradation – system only gradually degrades as more users access the system

Peter A. Steenkiste, CMU

37

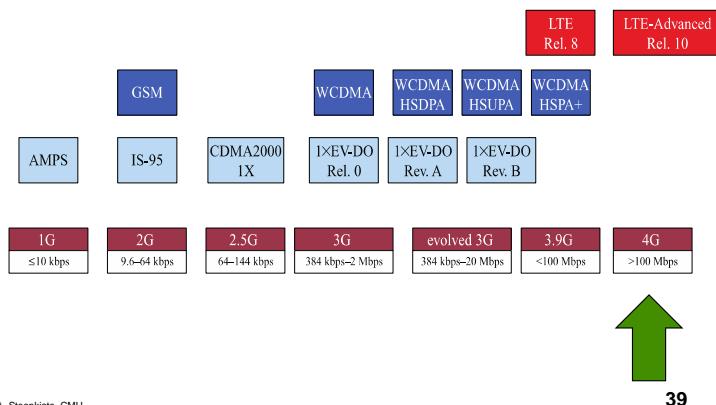
Mobile Wireless CDMA Soft Hand-off

- Soft Handoff – mobile station temporarily connected to more than one base station simultaneously
- Requires that the mobile acquire a new cell before it relinquishes the old
- More complex than hard handoff used in FDMA and TDMA schemes

Peter A. Steenkiste, CMU

38

Evolution of Cellular Wireless Systems



Peter A. Steenkiste, CMU

39