Course Overview

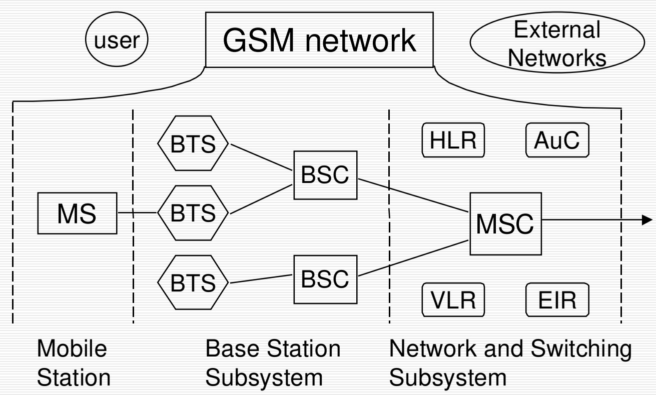
- Introduction and History
- Regulatory Issues
- Fundamentals of Cellular Systems
- 1st Generation: AMPS and CDPD
- 2nd Generation: GSM
- 3rd Generation: IMT-2000
- Mobile IP
- TCP over Wireless Link

GSM History

- 1978 - Europe allocated 2 x 25 MHz spectrum in 900 MHz range for mobile communications
- 1982 - Groupe Special Mobile formed under CEPT (French acronym for European Conference of Posts and Telecommunications)
- 1987 - GSM Memorandum of Understanding (MoU) signed by first members, which includes agreements between operators for roaming, numbering and routing aspects, tariffs and accounting.
- 1988 - GSM transferred to newly formed ETSI (European Telecommunication Standards Institute)

(thanks to John Scourias for providing many of the GSM transparencies)

GSM Network Architecture



GSM: Mobile Station

- subscriber identity module
  - ISO compliant removable smart card, with limited storage and computational functionality
  - necessary for operation of mobile station, and involved in location management, authentication, and ciphering
  - one or more directory numbers per SIM, one or more SIMs per subscriber
  - SIM realizes model of "personal mobility" (e.g., the subscriber is the focus of attention and it is he/she who is mobile)
- mobile equipment
  - only emergency calls allowed without SIM
  - calls routed to SIM, not mobile equipment

GSM: Base Station Subsystem

- Base Transceiver Station (BTS)
  - contains one or more transceivers (TRX), one for each allocated frequency
  - handles radio signal processing and transmission over the radio interface
  - high density of deployed BTSs, so requirements include compactness, reliability, and low cost
- Base Station Controller (BSC)
  - contains processing power and some switching necessary for management of several BTSs
  - manages channel setup, frequency hopping and handover

GSM: Network and Switching Subsystem

- Visitor Location Register (VLR)
  - contains subset of HLR information associated with subscribers currently roaming in controlled geographical area
  - associated with one or more MSCs to avoid constant querying of HLR
  - in practice associated with exactly one MSC
- Authentication Center (AuC)
  - protected part of HLR containing secret subscriber key K_i
  - manages authentication and ciphering in cooperation with SIM
- Equipment Identity Register (EIR)
  - stores lists of International Mobile Equipment Identities (IMEI) of valid mobile stations

GSM Services

- speech
  - most important and widely used service
  - uses discontinuous transmission and voice activity detection
    - transmit at about 40% of time, when user actually speaks
    - complete silence at receiver unnerving - comfort noise
- data
  - different services available, depending on end-to-end transmission type, transmission mode, terminal capability
  - supports data rates of 300 bps up to 9600 bps
- facsimile
- short message service
  - alphanumeric messages of up to 160 characters
  - messages saved on SIM

GSM: Radio Transmission Aspects

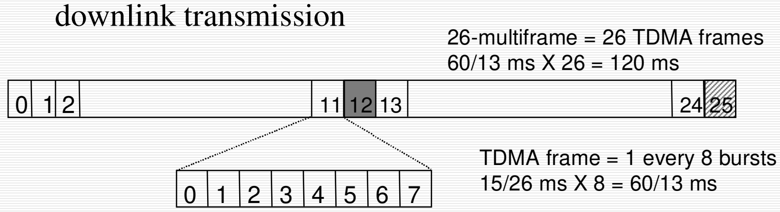
- spectrum allocation
  - in 1978 Europe allocated 2x25 MHz in the 900 MHz range for mobile communications
    - 890 - 915 MHz for the uplink (mobile station to base station)
    - 935 - 960 MHz for the downlink (base station to mobile station)
  - top 10 MHz in each band reserved for a pan-European mobile system, since band was also used by national analog systems
- multiple access:
  - GSM divides allocated bandwidth into carriers spaced 200 kHz apart, starting 200 kHz from the edge - maximum of 124 carriers in GSM900, 374 carriers in DCS1800 (2x75 MHz allocation)
  - TDMA divides time on each carrier frequency into burst periods lasting 15/26 (0.577) ms

GSM: Dedicated Channels

- traffic channels (TCH) carry user speech and data, as well as some signaling
- a TCH is always allocated with a corresponding Slow Associated Control Channel (SACCH) used for reporting handover measurements
- TCH slots may be ‘stolen’ from a traffic channel for Fast Associated Control Channel (FACCH) signaling, used for call establishment, handover execution, and authentication
- full rate TCH/SACCH occupies one time slot every 8 burst periods (TDMA frame), allowing 8 traffic channels per carrier frequency

GSM: Full Rate TCH/SACCH

- Time slot Number (TN) equals burst number modulus 8, and identifies a particular channel
- cycles every 26 TDMA frames (120 ms, defined so as to be ISDN compatible)
- uplink transmission delayed by 3 burst periods from downlink transmission

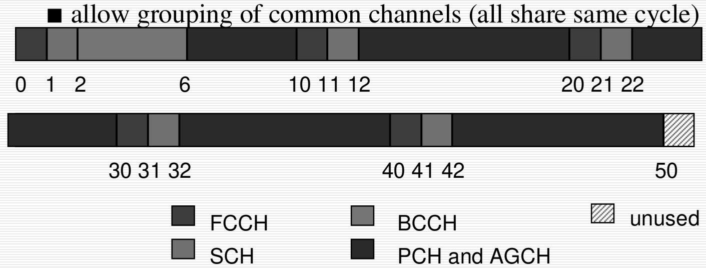


GSM: Other Dedicated Channels

- eighth rate TCH/SACCH or Stand-alone Dedicated Control Channel (SDCCH)
  - either group 8 (called SDCCH/8 in specs), or group 4 plus other common channels (called SDCCH/4), to form equivalent of full-rate TCH
  - used only for signaling, no user data mode specified (but could well be imagined, for example telemetry)
  - complex definition, with 8 traffic slots and 4 SACCH slots every 102 burst periods
- half rate TCH/SACCH
  - not included in Phase I recommendations, although partly specified by 1990
  - occupies, on average, one time slot every 16 burst periods

GSM: Common Channels

- common channels are accessible by all mobiles, both in idle and dedicated mode
- all common channels have cycle of 51 TDMA frames:
  - allows access by dedicated mobile stations (during one unused time slot in full-rate TCH) every once in a while
  - allow grouping of common channels (all share same cycle)



GSM: Common Channels

- Frequency Correction Control Channel (FCCH) and Synchronization Channel (SCH) - downlink
  - mobile stations listen to the FCCH and SCH to acquire time synchronization with base station
  - FCCH transmits a unique radio burst (F burst with 142 bits set to 0)
  - SCH immediately follows FCCH, and its burst (S burst with 64 bit training sequence) gives cell's burst numbering - all frequencies in cell follow same numbering
  - exactly one set of FCCH and SCH channels per cell, by definition on TN 0, on a non-hopping frequency called the *beacon frequency*

GSM: Common Channels

- Broadcast Control Channel (BCCH) - downlink
  - carries general information including parameters to control cell selection, control channel configuration, random access parameters, and beacon frequencies of neighboring cells
- Paging Channel (PCH) and Access Grant Channel (AGCH) - downlink
  - time separation between PCH and AGCH depends on cell parameters
  - discontinuous reception increases battery life by dividing PCH into paging sub-channels
    - mobiles belong to sub-channels in pre-determined way
  - smaller PCH/AGCH possible, of 1/3 capacity
  - PCH/AGCH may be extended in up to three extra TNs along with BCCH and RACH on the uplink

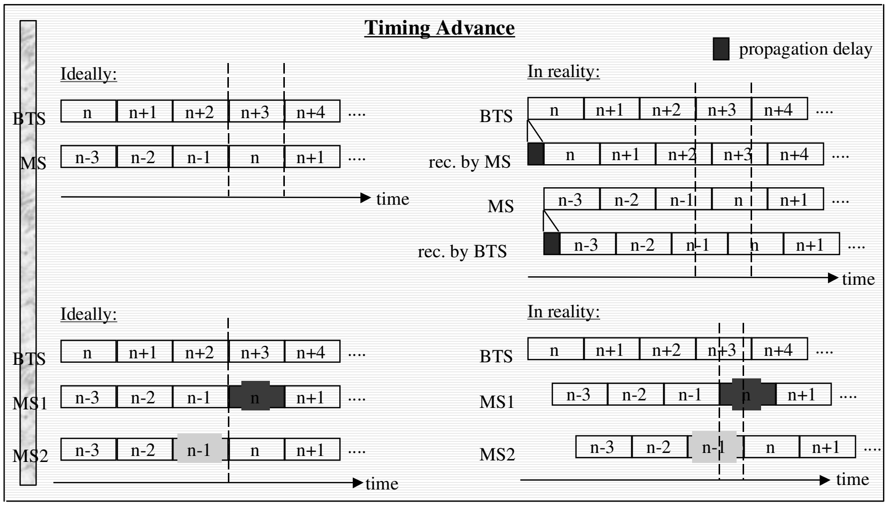
GSM: Frequency Hopping

- GSM uses slow frequency hopping, changing the transmission frequency before every burst
- frequency diversity improves reception since different frequencies are affected differently during propagation
- interferer diversity improves reception by distributing relative interference of particular frequency among many calls
- hopping sequences are sets of (time slot number, frequency) pairs, where frequency is one of up to 64 different frequencies
  - Mobile Allocation Index Offset (MAIO) is a value between (1, number of allocated frequencies in cell)
  - Hopping Sequence Number (HSN) is a value between (0, 63)
  - MAIO and HSN combination determine a pseudo-random hopping sequence

GSM: Radio Resource Management

- Radio Resource (RR) layer includes the functions required to manage the radio interface
- concept of RR session
  - started when mobile station leaves idle mode, and terminated when idle mode is re-entered
  - contains signaling and data path between mobile station and MSC, which may be modified by handovers
  - characteristics such as transmission mode and cipher mode may be altered
  - more than one communication is possible during an RR session
- handles access (including paging), transmission management, **timing advance,** handover**, power control**

GSM: Radio Resource Management



GSM: Radio Resource Management

- power control
  - mobile station and BTS transmission power can be independently modified
  - improves spectral efficiency by reducing system interference levels and increases mobile station battery life
  - each mobile station's transmission power can be changed in steps of 2 dB over the range specified by the power class of mobile station
  - either BSC or BTS manages power control in both directions
  - access messages and initial messages are sent at fixed power level specified in BCCH

GSM: Mobility Management

- PLMN and cell selection
  - PLMN: Public Land Mobile Network
  - in idle mode, mobile station *camps* on one cell, on which it listens for paging messages
  - cell and PLMN selection has administrative and technical aspects
  - subscriptions are made with a home PLMN operator, who may have roaming agreements with other operators
  - PLMN selection occurs upon request from user or when user moves out of coverage area of serving PLMN

GSM: Mobility Management

- cell selection of best cell within serving PLMN always done automatically by mobile station
  - selection of best cell determined by C1 criterion
  - C1 = *average receive level - p1 - max((p2 - maximum MS power level), 0)*
    - p1 is value between -110 dBm and -48 dBm broadcast on BCCH
    - p2 is value between 13 dBm and 43 dBm indicating maximum transmit power on RACH - also on BCCH
  - only cells with positive C1 (which are not barred) within the selected PLMN are considered, and cell with highest value of C1 is selected
  - C1 effectively determines cell boundaries
    - hysteresis value may be used to delay cell selection requiring location update

GSM: Mobility Management

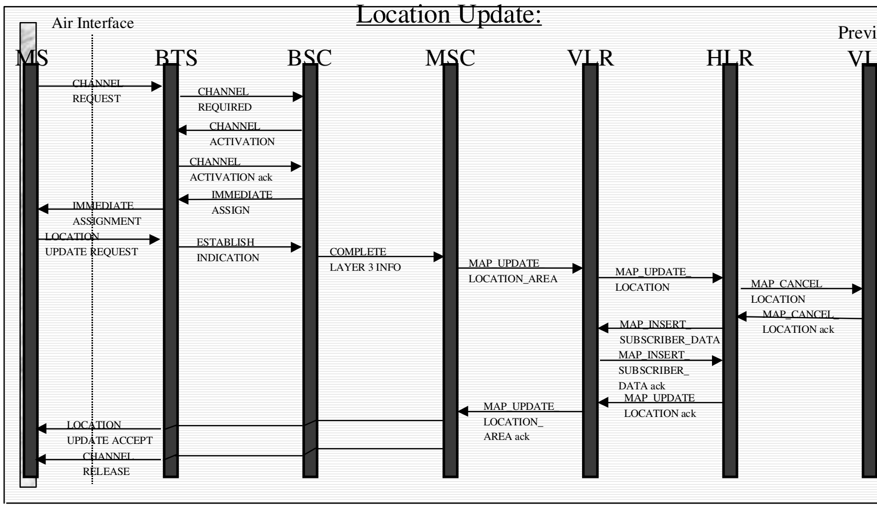
- cell selection at switching on
  - first PLMN tried must be home PLMN
  - mobile searches all frequencies (124 for GSM900, 374 for DCS 1800), or looks up stored beacon frequencies on SIM, for C1 positive and non-barred cells, and selects cell with highest C1
  - if new location area is same as stored value of last location area, IMSI attach is performed, otherwise normal location update is performed
- cell selection during normal service (idle mode)
  - serving cell broadcasts beacon frequencies of neighboring cells in same PLMN
  - if one of neighboring cells has a higher C1 value, and belongs to same location area, mobile starts listening on new cell's paging channel
  - if better cell belongs to new location area, mobile station switches cells and performs location update

GSM: Mobility Management

- cell selection upon change to new PLMN
  - since no beacon frequency list is on the SIM, mobile station scans all frequencies and selects 30 strongest frequencies, stored in *found list*
  - once PLMN is selected, cell from *found list* with best C1 value belonging to selected PLMN is selected and location update is performed

– concept of location area
- compromise between system-wide paging and per-cell location updating
- one or more cells forming smallest location element
- location update required when first entering new location area - all cells within location area paged for incoming calls
- definition of location areas up to operator - only constraint is that they must belong to the same VLR

GSM: Mobility Management



GSM: Mobility Management

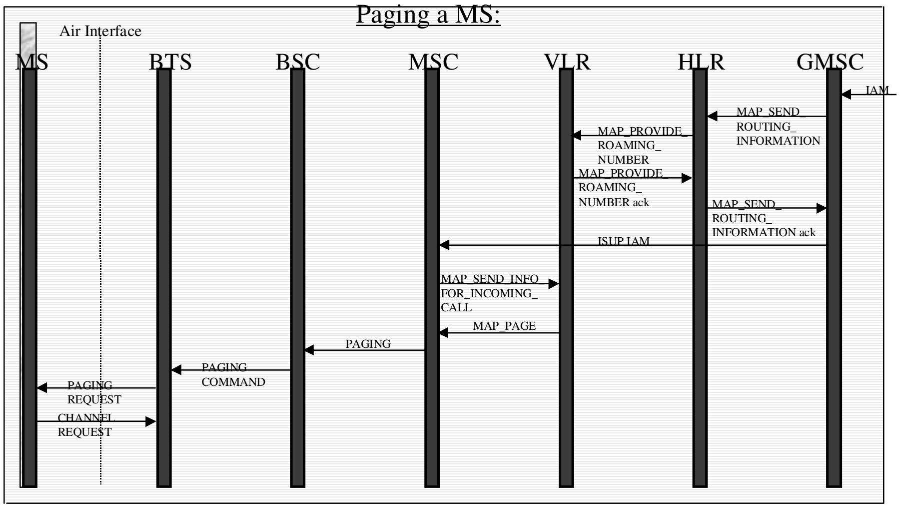
- location updating procedure
  - mobile subscriber is identifiable by the International Mobile Station Identity (IMSI) which consists of a Mobile Country Code, a Mobile Network Code identifying the operator, and a Mobile Subscriber Identity Number, whose first digits may indicate subscriber's HLR
  - mobile station sends a RIL3-MM LOCATION UPDATE REQUEST message to the new MSC containing the IMSI
    - if mobile subscriber is already in the VLR, or if the HLR is not reachable, new MSC replies with accept or reject message

GSM: Mobility Management

- MSC sends MAP UPDATE LOCATION message to subscriber's HLR, containing IMSI and SS7 address of the visited MSC
- if subscription allows registration, HLR is updated, new VLR is sent relevant subscriber data for managing calls, and old VLR is sent cancellation message if subscriber was previously registered
  - otherwise, subscriber is deregistered and cancellation message is sent to old MSC
- periodic location updating is a user option which allows quicker recovery in case of HLR failure

GSM: Mobility Management

Paging a MS:



GSM: Paging a Mobile Subscriber

- paging is actually a function of the radio resource management (though not directly linked with a specific RR session), not directly part of mobility management
  - originating PSTN switch derives Gateway MSC address from the dialed digits (mobile subscriber's MSISDN) and will issue an Initial Address Message (IAM), indicating an incoming call
  - Gateway MSC contacts HLR to eventually obtain a roaming number (MSRN) to route call to destination MSC
  - HLR looks up current location and contacts appropriate VLR, which assigns a MSRN and returns this (via HLR) to Gateway MSC
  - Gateway MSC continues call routing by sending IAM to destination MSC, using the newly assigned MSRN

GSM: Paging a Mobile Subscriber

- MSC contacts VLR, which triggers paging in known location area. MSC will block until subscriber responded to paging.
- VLR sends paging requests (via MSC) to appropriate BSCs, including information such as IMSI, TMSI (if one has been allocated already), a list of cells to be paged, and if applicable and known, the type of channel required for incoming call (e.g., speech or data)
- BSCs issue paging messages to each BTS specified, adding information about *paging group* (section of paging channel, for discontinuous reception by mobile to conserve battery power)
- paging messages are normally repeated an operator-configurable number of times to decrease chance of lost pages
- when mobile successfully receives a paging message, it initiates a channel assignment procedure (similar to location update step), which will complete connection establishment

GSM: Mobility Management

- ciphering
  - provides user privacy by coding the transmission so that only authorized entities can decode message
  - encryption is an operator option - not up to user
  - 64 bit ciphering key K_c obtained by SIM and AuC from K_i and the initial random number RAND input into the operator-dependent A8 algorithm
  - ciphering procedure uses 22 bit frame number (time slot number mod 8) and K_c to produce two 114 bit sequences through the A5 algorithm, which are XORed with the 114 information bits in each traffic direction
  - single A5 algorithm is used, distributed by MoU committee

GSM: Mobility Management

- subscriber identity confidentiality
  - unique IMSI (International Mobile Subscriber Identity) transmitted in the clear during initial access
  - temporary Mobile Subscriber Identity (TMSI) is shorter identity, relevant only within a location area (i.e., in combination with Location Area Identifier (LAI))
  - TMSI first allocated during registration in a particular VLR, and deallocated when subscriber deregisters
  - during location update to another MSC/VLR, TMSI in combination with old LAI can be sent by mobile station, and used to query old MSC/VLR for the IMSI

GSM: Mobility Management

- equipment identity checking
  - Equipment Identity Register (EIR) maintains database related to mobile equipment (hardware) identified by International Mobile Equipment Identity (IMEI)
  - IMEI consists of Type Approval Code (granted when mobile station type passes type approval testing to ensure mobile station behaves properly), Final Assembly Code (indicating manufacturing plant), and the equipment serial number
  - EIR stores three lists of IMEIs
    - *white list* contains ranges of IMEIs of type approved mobile stations, maintained by MoU
    - *black list* contains IMEIs which are stolen or malfunctioning, and are subsequently barred
    - *gray list* contains IMEIs which should be supervised for possible malfunctions

GSM: Future Developments

- phase 2+
  - enhanced full rate speech
    - uses improvements in speech coding to provide wireline quality on current full rate channels
    - possible to use different speech coding algorithms, or use adaptive tradeoff between channel and source coding
  - **GPRS: General Packet Radio Service**
  - high-speed data rates
  - group call allows one group member to talk while others listen, with efficient use of radio channels
  - interworking with satellite communications
  - interworking with developments in fixed networks, in particular Universal Personal Telecommunications (UPT) and Intelligent Networks (IN)
- evolution towards UMTS