Course Overview

- Introduction
- Data in Wireless Cellular Systems
- Data in Wireless Local Area Networks
- Internet Protocols
- TCP over Wireless Link
- Ad-Hoc Networks, Sensor Networks
- Services and Service Discovery
- System Support for Mobile Applications

Regulatory Issues

- Wireless Spectrum scarce, shared among many different users with distinct needs
- Need either license to operate in specific frequency band or use unlicensed frequency band
- Unlicensed bands: no limit on number of users, but rules governing "behavior"
- Licenses used to be given away basically for free, but this became controversial, plus governments saw this as easy source of revenue…..
- Need for international standardization: meetings every 2 years (WARC), many international standards bodies and regulatory offices involved

Unlicensed Bands

- Industrial, Scientific, and Medical (ISM):
  - 915 MHz band (902 - 928 MHz, 26 MHz bandwidth)
    - only available in North America
    - highly crowded, expected to become even more crowded
    - many existing users are non-spread-spectrum applications
  - 2.4 GHz band (2.4 - 2.4835 GHz, 83.5 MHz bandwidth)
    - available worldwide
    - lightly loaded, but interference from microwave ovens
  - 5.8 GHz band (5.725 - 5.85 GHz, 125 MHz bandwidth)
    - only available in North America
    - lightly loaded, radar interference

Licensing 3G Bands

Source: *http://www.umts-forum.org/brochures/3G_licensing_09_October.pdf*

- VERY different country rules:
  - **US**: finalise spectrum options by Q3 2001, prior to licensing 3G systems by Q4 2002. consultation process completed 30 March 2001 with reports from FCC and NTIA.
  - **Canada** auctioned PCS spectrum in January 2001 that can be used for 3G services, with 52 licences attracting bids totalling $1.48 billion.
  - Spectrum policy in USA and Canada is today not service specific. This means that any licensee can deploy 3G systems in their existing spectrum, if equipment exists for that particular spectrum.
  - **France:** 4 National licenses, beauty contest plus fixed cost. First two licences awarded to Itineris (France Telecom) and SFR (Cegetel). Conditions have yet to be set for the award of two further licences. First licences awarded 31.05.01. Date of second call for tender not yet confirmed
  - **Germany:** 6 National licences awarded, five 2x10 + 5 MHz, one 2x10 MHz. 1st stage auction completed (17.8.00), raising DM98.8 billion. Second stage closed 18.8.00, awarding an additional 1x5Mhz unpaired to all except one.

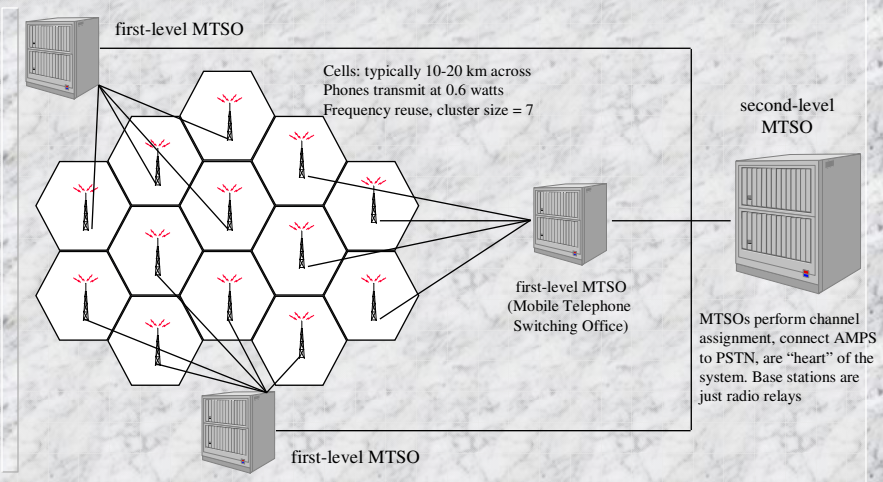
Course Overview

- Introduction
- Data in Wireless Cellular Systems: AMPS and CDPD
- Data in Wireless Local Area Networks
- Internet Protocols
- TCP over Wireless Link
- Ad-Hoc Networks, Sensor Networks
- Services and Service Discovery
- System Support for Mobile Applications

AMPS: History

- FCC allocated spectrum space in the 800 MHz spectrum and issued licenses for test systems in Chicago and Washington, D.C.
- first commercial systems available 1983, available in all major cities in US in a few years
- AMPS result of extensive research by Bell Labs in 1960s and 1970s
- 800 MHz band was compromise
  - lower frequencies occupied by FM and TV systems
  - higher frequencies were deemed too unreliable (information loss due to weather conditions, multipath fading, etc.) with existing technology

AMPS Architecture



AMPS Spectrum and Allocation

- A band set up for independent carriers
- B band set up for traditional wireline carriers, such as the Regional Bell Operating Companies (RBOC)
- idea was to ensure competition in all markets, while restrict potential proliferation of companies that would complicate spectrum allocation/management
- today, many independent carriers bought by RBOCs, so it is not uncommon to have one company operating in Band A in one market and Band B in another market
- channels always come in pairs, spaced 45 MHz apart

AMPS Identification Numbers

- three identification numbers are used:
  - mobile station's serial number (SN)
    - 32-bit binary number
    - uniquely identifies a cellular unit
    - established by manufacturer at the factory
      - 8-bit manufacturer code, assigned by FCC to manufacturer
      - 6 bit reserved (currently all 0)
      - 18 bits serial number, assigned by manufacturer
    - should not be easily alterable, burned into ROM
  - system identification number (SID)
    - 15-bit binary number, uniquely identifies cellular system
    - FCC assigns SID
    - mobile station in the cell must transmit the SID
  - mobile identification number (MIN)
    - digital representation of mobile's 10-digit telephone number

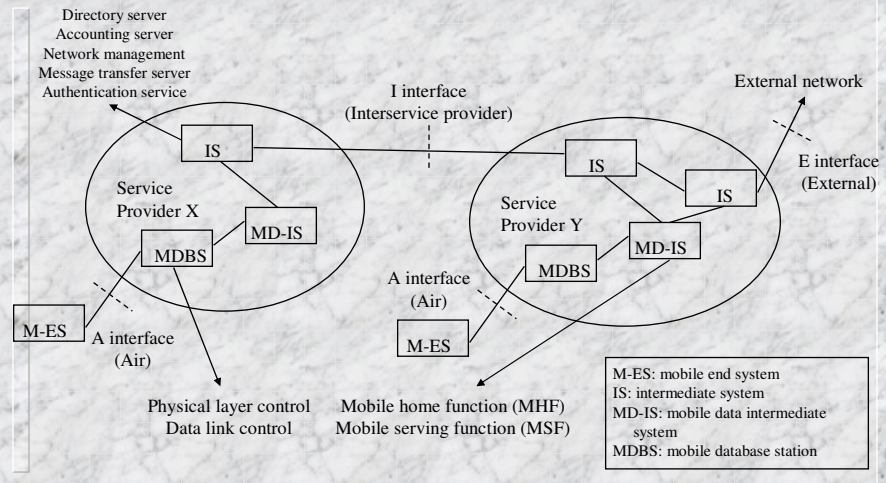
AMPS: Call Initiation

- user enters number and presses SEND
- phone sends number to be called and own identity on access channel (random access channel), retry in case of collision
- MTSO looks for idle channel (if caller is customer of MTSO's company or one of its partners) and sends back channel number on the control channel
- mobile phone switches to the selected voice channel and waits until the called party picks up the phone

AMPS: Call Reception

- idle phones continuously listen to the paging channel to detect messages directed at them
- when someone initiates call to mobile, message is sent to home MTSO to find out where mobile currently is
- a packet is then sent to base station in current cell, which pages the mobile on the paging channel
- if mobile replies, base assigns channel number and sends it to mobile
- mobile switches to this channel and starts making ringing sound

CDPD: Architecture



CDPD: Architecture

- M-ES: user device, mobile, identified by at least one globally unique Network Entity Identifier (NEI)
- IS: basically a router, might provide additional services
- MD-IS: only entity that has knowledge of mobility, runs MNLP (Mobile Network Location Protocol):
  - each M-ES belongs to a fixed home area, MHF keeps track of this information
  - MSF handles packet transfer services for visiting M-ES
  - requires that M-ES register with serving MD-IS when roaming
- MDBS: supports air interface to M-ES
  - resides at the AMPS cell
  - uses AMPS transmit and receive equipment

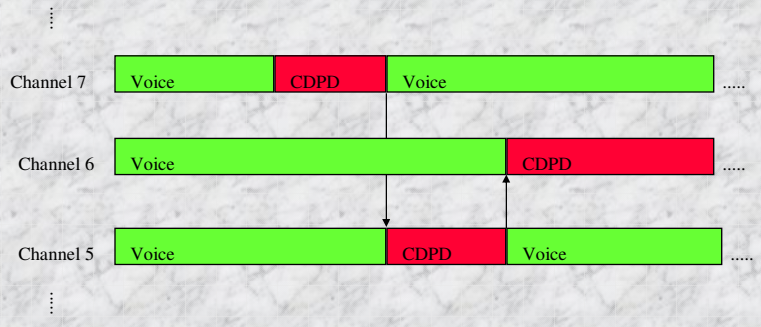
CDPD: Protocol Stack

- follows OSI stack
- CDPD basically specifies physical layer and data link layer protocols only
- nominal channel rate: 19.2 kbps, maximum throughput after coding & framing, ignoring contention, is 11.8 kbps on downlink (to mobile), 13.3 kbps on uplink
- standard specifies support for CLNP (ConnectionLess Network Protocol) and IP (Internet Protocol) at layer 3
- higher layers can be TCP or TP4
- CDPD also specifies a wide variety of upper-layer protocols (directory management, electronic messaging, etc.), based on OSI and Internet services

CDPD: MAC Protocol

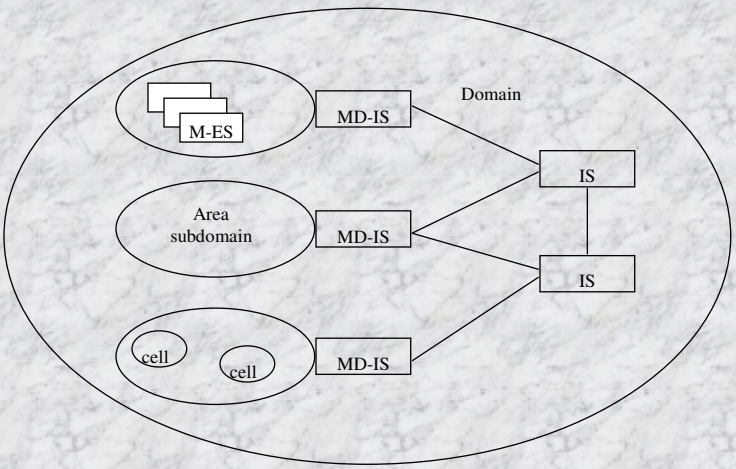
- downlink/forward channel: no contention, only one sender: the MDBS. All frames are broadcasted, each M-ES picks out the ones destined for it or for everyone
- uplink/reverse channel: contention is a problem
  - access to channel follows a DSMA/CD protocol:
    - uses time slots of 60 bit times (see structure of forward channel)
    - "digital sense": watch forward channel to determine whether reverse channel is busy or idle (busy/idle flags every 60 bits)
    - if busy, skip a random number of slots and try again. If still busy, wait for longer period (statistically twice as long) and retry
    - if idle, start transmitting
    - "collision detection": decode flag in forward channel indicates with delay whether there was a collision
    - keep sending until collision is detected or until maximum number of slots is set or until MDBS tells M-ES to shut down

CDPD: Sharing AMPS Channels



Two scenarios:
- AMPS channel currently not in use (not assigned to a voice connection)
- AMPS channel currently assigned to a voice connection, but no talk activity (50%-60% of time)

CDPD: Mobility Management



CDPD: Mobility Management Identifiers

- NEI (Network Entity Identifier): identifies mobile
- LCI (Local Cell Identifier): unique cell identifier for all cells controlled by the same MDBS
- CSI (Channel Stream Identifier): unique 6-bit identifier for all channel streams in a cell
- LCI and CSI together uniquely identify all channels on any given cell or its adjacent cells
- LSAI (Local Service Area Identifier): 16-bit unique number for all service areas in a CDPD network
- SPNI (Service Provider Network Identifier): 16-bit unique CDPD network identifier

CDPD: Mobility Management

- cell transfer decision: compare relevant parameters on previous RF channel and current RF channel (after channel hop):
  - no change in LCI, CSI, cell group color or area color: channel hop occurred within current cell
  - area color is the same, but LCI and CSI are different: intra-area cell transfer is performed
  - different area colors: inter-area cell transfer procedure is performed

CDPD: Intra-Area Cell Transfer

- intra-area cell transfer: controlled by same MD-IS
- M-ES initiates transfer if channel becomes bad (extended loss of channel synchronization and/or unacceptable error rate)
- to assist M-ES in locating CDPD channel, MDBS periodically broadcasts RF channel number in use or as candidates for use in adjacent cell
- after M-ES synchronized with new RF channel, sends link-layer receive ready to serving MD-IS
- MD-IS acknowledges frame and updates its information for M-ES (physical media association)

CDPD: Inter-Area Cell Transfer

- starts out identical to intra-area cell transfer
- once M-ES synchronized with new channel, mobile sends “end system hello” (ESH) to new serving MD-IS
- ESH informs MD-IS of presence of M-ES, register its address (NEI)
- new serving MD-IS sends message to home MD-IS to tell it where data for M-ES should be redirected
- home MD-IS acknowledges if registration is successful
- new serving MD-IS confirms successful registration to M-ES
- home MD-IS “flushes” previous serving MD-IS, telling it that messages are no longer forwarded for this M-ES

Course Overview

- Introduction
- Data in Wireless Cellular Systems: GSM and GPRS
- Data in Wireless Local Area Networks
- Internet Protocols
- TCP over Wireless Link
- Ad-Hoc Networks, Sensor Networks
- Services and Service Discovery
- System Support for Mobile Applications

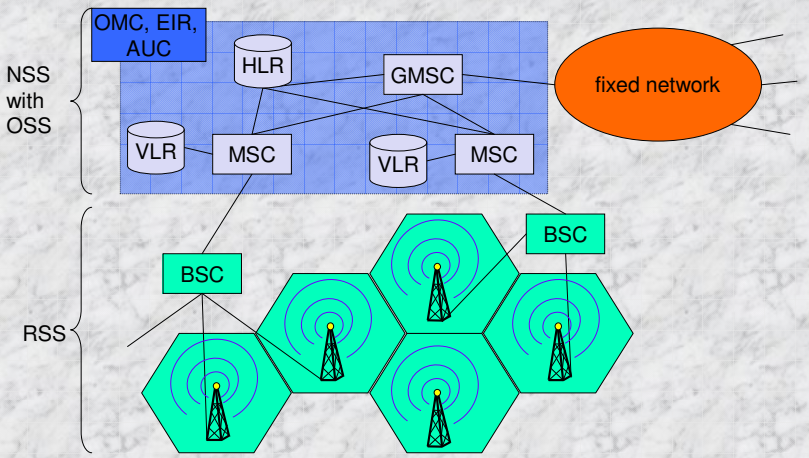
GSM History

- 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)

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)
  - subsystems
    - RSS (radio subsystem): covers all radio aspects
    - NSS (network and switching subsystem): call forwarding, handover, switching
    - OSS (operation subsystem): management of the network

GSM: Overview

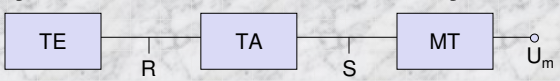


Radio Subsystem

- The Radio Subsystem (RSS) comprises the cellular mobile network up to the switching centers
- Components
  - Base Station Subsystem (BSS):
    - Base Transceiver Station (BTS): radio components including sender, receiver, antenna - if directed antennas are used one BTS can cover several cells
    - Base Station Controller (BSC): switching between BTSs, controlling BTSs, managing of network resources, mapping of radio channels (U_m) onto terrestrial channels (A interface)
    - BSS = BSC + sum(BTS) + interconnection
  - Mobile Stations (MS)

Mobile Station

- Terminal for the use of GSM services
- A mobile station (MS) comprises several functional groups
  - MT (Mobile Terminal):
    - offers common functions used by all services the MS offers
    - corresponds to the network termination (NT) of an ISDN access
    - end-point of the radio interface (U_m)
  - TA (Terminal Adapter):
    - terminal adaptation, hides radio specific characteristics
  - TE (Terminal Equipment):
    - peripheral device of the MS, offers services to a user
    - does not contain GSM specific functions
  - SIM (Subscriber Identity Module):
    - personalization of the mobile terminal, stores user parameters



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

Network and Switching Subsystem

- NSS is the main component of the public mobile network GSM
  - switching, mobility management, interconnection to other networks, system control
- Components
  - Mobile Services Switching Center (MSC)
    controls all connections via a separated network to/from a mobile terminal within the domain of the MSC - several BSC can belong to a MSC
  - Databases (important: scalability, high capacity, low delay)
    - Home Location Register (HLR)
      central master database containing user data, permanent and semi-permanent data of all subscribers assigned to the HLR (one provider can have several HLRs)
    - Visitor Location Register (VLR)
      local database for a subset of user data, including data about all user currently in the domain of the VLR

Mobile Services Switching Center

- The MSC (mobile switching center) plays a central role in GSM
  - switching functions
  - additional functions for mobility support
  - management of network resources
  - interworking functions via Gateway MSC (GMSC)
  - 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

Operation Subsystem

- The OSS (Operation Subsystem) enables centralized operation, management, and maintenance of all GSM subsystems
- Components
  - Authentication Center (AUC)
    - generates user specific authentication parameters on request of a VLR
    - authentication parameters used for authentication of mobile terminals and encryption of user data on the air interface within the GSM system
  - Equipment Identity Register (EIR)
    - registers GSM mobile stations and user rights
    - stolen or malfunctioning mobile stations can be locked and sometimes even localized
  - Operation and Maintenance Center (OMC)
    - different control capabilities for the radio subsystem and the network subsystem

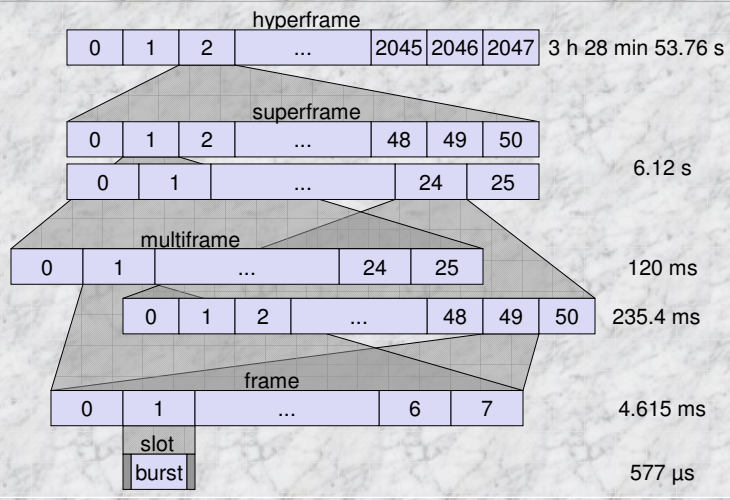
GSM Services

- 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 Hierarchy of Frames



GSM Logic Channels

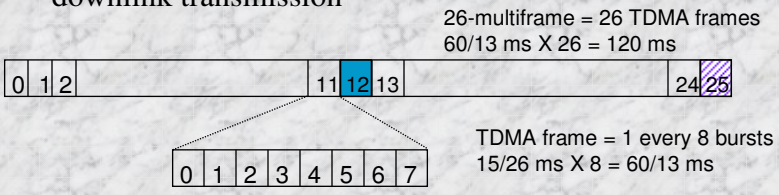
- Traffic channels (2-way)
  - Full-rate (TCH/F)
  - Half-rate (TCH/H)
- Signaling Channels
  - Broadcast Channels (base to mobile)
    - Frequency Correction Channel (FCCH)
    - Synchronization Channel (SCH)
    - Broadcast Control Channel (BCCH)
  - Common Control Channels
    - Paging Channel (PCH) - base to mobile
    - Access Grant Channel (AGCH) - base to mobile
    - Random Access Channel (RACH) - mobile to base
  - Dedicated Control Channels (2-way)
    - Stand-alone Dedicated Control Channel (SDCCH)
    - Slow Associated Control Channel (SACCH)
    - Fast Associated Control Channel (FACCH)

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’ for 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

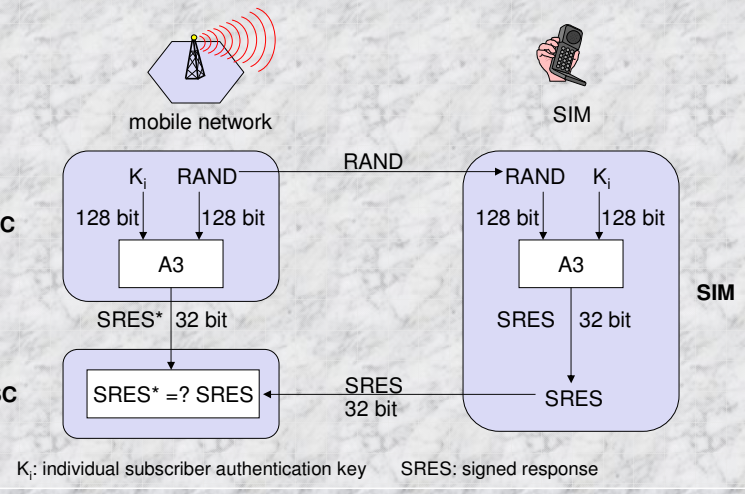


Security in GSM

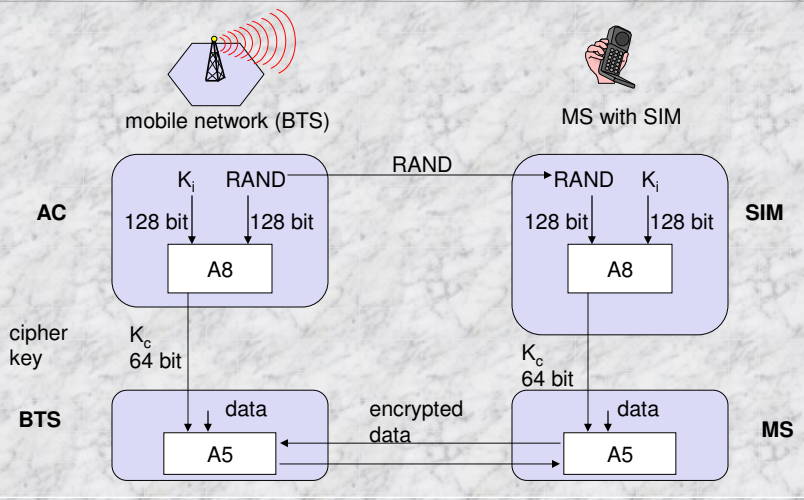
- Security services
  - access control/authentication
    - user ⌫ SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM ⌫ network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)
  - 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 use stronger mechanisms

GSM - Authentication



GSM - Key Generation and Encryption



GSM: Security

- 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

Data Services in GSM

- 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)
  - already standardized
  - bundling of several time-slots to get higher AIUR (Air Interface User Rate)(e.g., 57.6 kbit/s using 4 slots, 14.4 each)
  - 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

GSM Data Properties

- Circuit-switched operation
  - uplink and downlink channels allocated for a user for entire call period
    - busy user uses only one direction of link (typically), so 50% of resources are wasted
  - user pays for the connection time, not for the amount of data
    - bad connections - more retransmissions - make more money for operator
    - pay even if no data is transmitted
  - connection establishment time: 20-25 seconds
    - bad for short-lived transactions
  - capacity: 9.6 kbps (channel coding designed for worst-case radio situation)
  - connections: to any modem service in PSTN

GSM Data Properties: Evaluation

- Circuit-switched data is good for cases when continuous data flow is needed/required
- Billing is based on time, not amount of data
- Limited number of mobiles can be supported per carrier (8 channels)
- Circuit-switched data is not optimal for
  - packet-based protocols such as IP
  - bursty traffic
  - unbalanced traffic (using mainly one channel direction)
- $\Rightarrow$ Packet switched service is needed for GSM
- $\Rightarrow$ GPRS standardization was started

Beyond 2G

- 3G Systems: originally one standard, later “family of compatible standards”
- B3G and 4G: focus on data rates and services, range of wireless access technologies
- → See Introduction