Course Overview

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

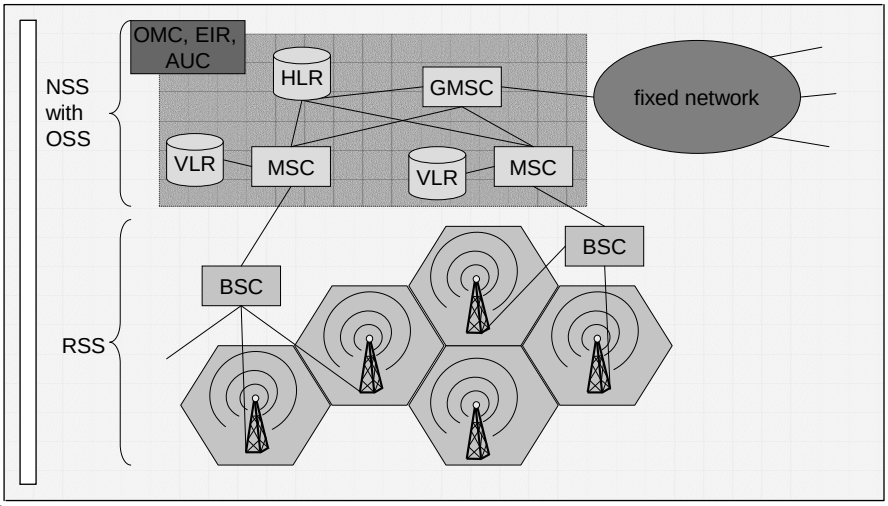
GSM History

- 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)

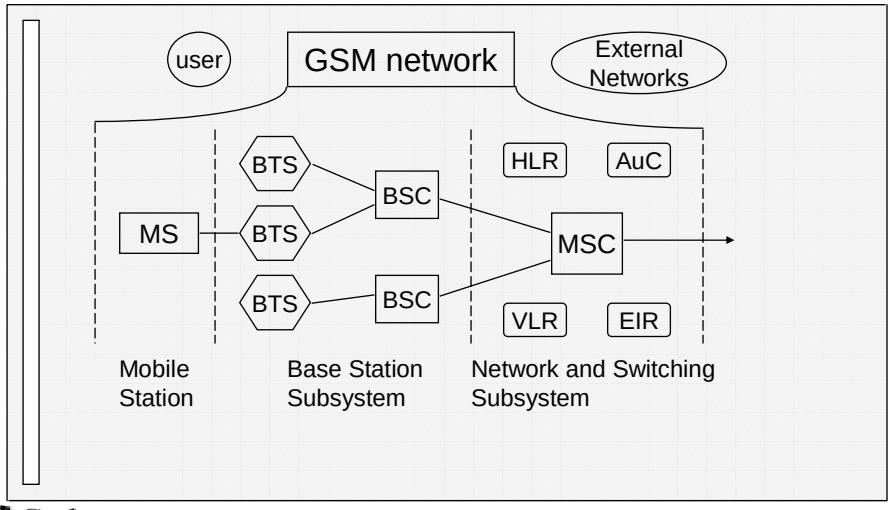
Architecture of the GSM system

- 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



GSM Network Architecture

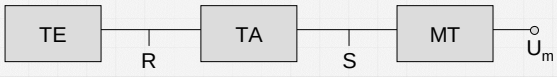


Radio Subsystem

- 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

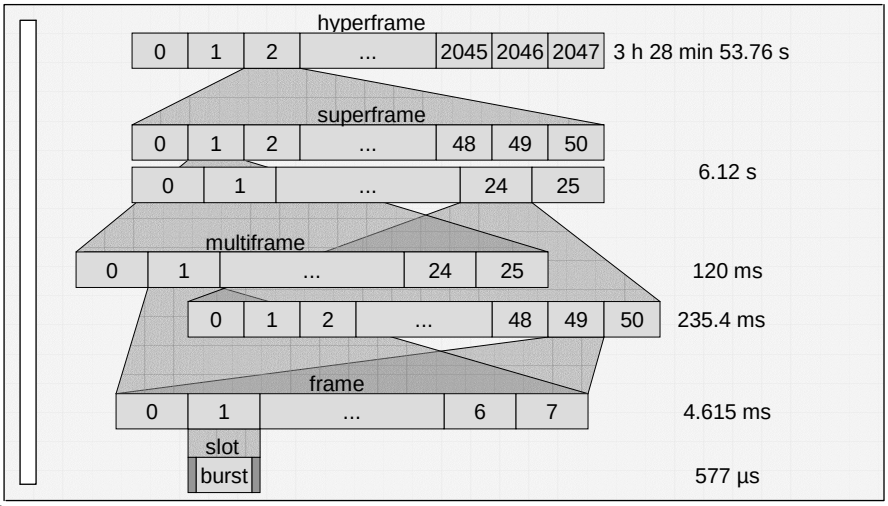
GSM Services

- 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

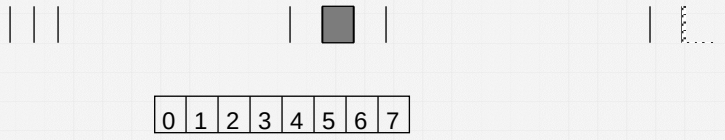
- Traffic channels (2-way)
  - Full-rate (TCH/F)
  - Half-rate (TCH/H)
- Signaling Channels
  - Broadcast Channels (base to mobile)
    - Frequency Correction Channel (FCCH)
    - Synchronization Channel (SCH)
    - Broadcast Control Channel (BCCH)
  - Common Control Channels
    - Paging Channel (PCH) - 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’ 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: 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
  - one message (spread over 4 bursts every 51 frame cycle
- 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 Common Channels

- Random Access Channel
  - initiate calls, send short messages, respond to paging messages, initiate location updates
  - shared among all mobiles, use slotted Aloha
  - messages are short (87 bits) to fit into one burst
  - use random 5-bit sequence to distinguish messages
  - mobile transmits, wait for acknowledgement (including 5 bits and info about SDCCH for further signaling)
  - if two stations choose same sequence, transmit in same interval, and one signal is stronger than the other: base will acknowledge receipt, both handsets will tune to same traffic channel (use call mgmt procedures)

GSM: Frequency Hopping

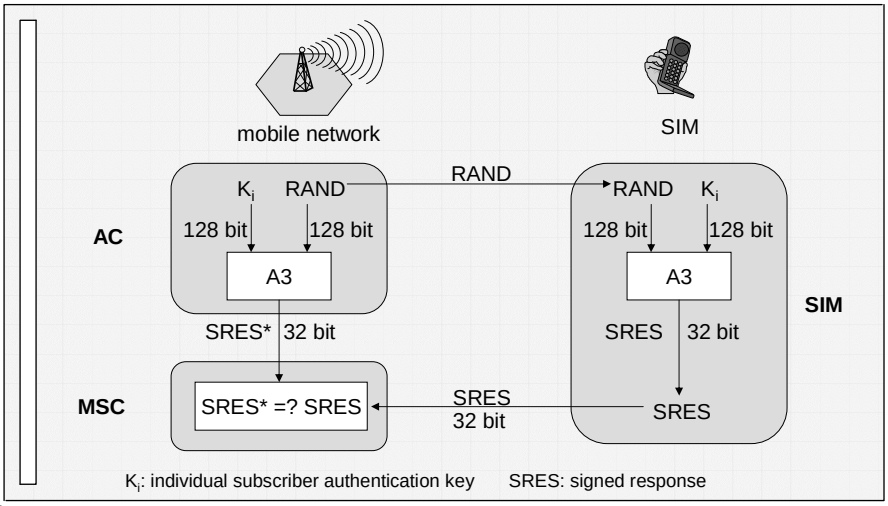
- GSM potentially uses slow frequency hopping, changing the transmission frequency before every burst
- frequency diversity improves reception since different frequencies are affected differently during propagation
- interferer diversity improves reception by distributing relative interference of particular frequency among many calls
- if operator chooses to employ frequency hopping, sequences within cells and between neighboring cells must be coordinated
- 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

Security in GSM

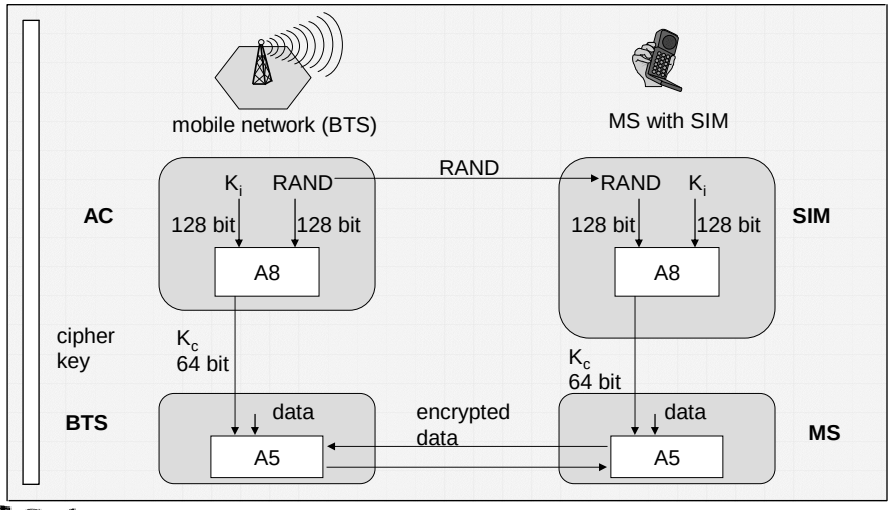
- Security services
  - access control/authentication
    - user ⌫ SIM (Subscriber Identity Module): secret PIN (personal identification number)
    - SIM ⌫ network: challenge response method
  - confidentiality
    - voice and signaling encrypted on the wireless link (after successful authentication)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



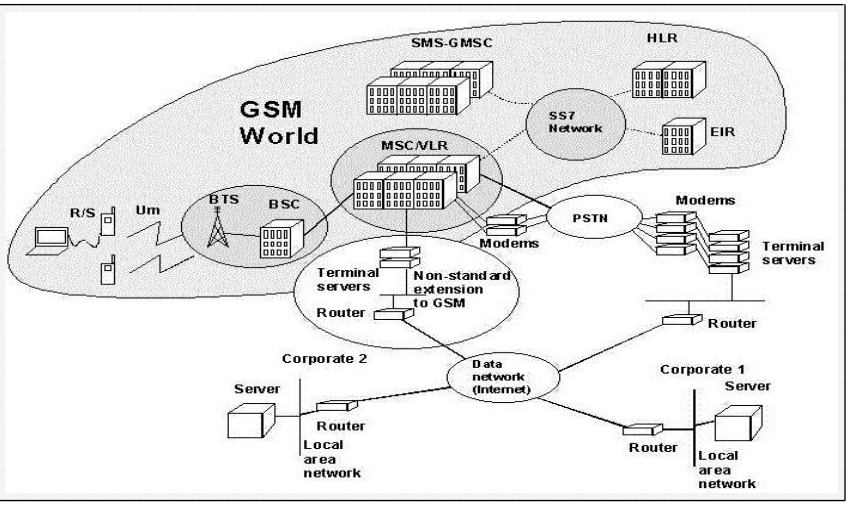
GSM: Security

- 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

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

GSM Voice and Data Architecture



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

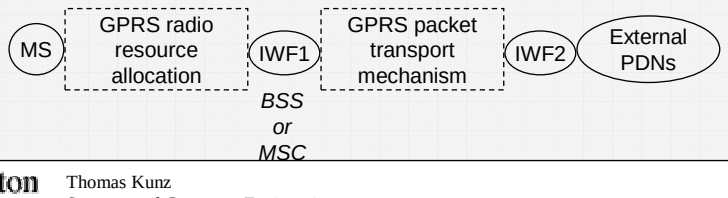
- Circuit-switched operation
  - uplink and downlink channels allocated for a user for entire call period
    - busy user uses only one direction of link (typically), so 50% of resources are wasted
  - user pays for the connection time, not for the amount of data
    - bad connections - more retransmissions - 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)
- ⇒ Packet switched service is needed for GSM
- ⇒ GPRS standardization was started

GPRS Alternatives

- GPRS functional architecture
  - GSM transmission must deal with two semi-independent aspects so is divided into two functional entities
    - GPRS radio resource allocation deals with efficient usage of radio interface channels
    - GPRS packet transport mechanism deals with efficient packet routing through GSM infrastructure to the interworking function (IWF2) with the external Packet Data Network (PDN)
    - two functions are connected by another interworking function (IWF1)



GPRS Alternatives

- radio resource allocation
  - proposal one
    - normal traffic channel used with modified access and setup mechanism
    - Radio Link Protocol (RLP) used for retransmission
    - standard authentication and ciphering applied
  - proposal two
    - special GPRS Packet Channel (GPCH) allocated in every cell
    - reservation procedure reserves channel for duration of transaction
    - number of allocated GPCHs should be dynamically allocated depending on traffic (one user per GPCH)
    - RLP can be used
    - ciphering and authentication require some modification due to shared channel (shared over time, no multiplexing)

GPRS Alternatives

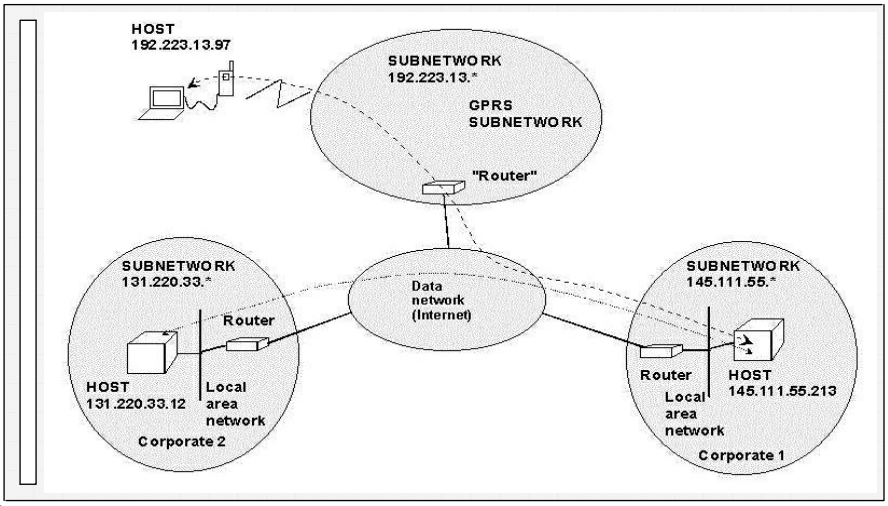
  - proposal three
    - GPCHs allocated per cell
    - packets from multiple users are multiplexed on channel
    - RLP and security mechanisms need to be modified
    - requires dynamic allocation of GPCH depending on traffic
- packet transport mechanism
  - proposal one
    - use existing signaling network along with SMS (Short Message Services)
    - Gateway MSC contains IWF2 which queries HLR for routing information
    - message size constrained to SMS limit: max. frame length of 272 octets on A interface (between MSC and BSC), overhead of higher protocol layers leaves 140 octets, enough for 160 7-bit ASCII characters
    - transfer delay must be improved

GPRS Alternatives

- proposal two
  - use external Packet Data Network
  - IWF1 incorporates IWF2 function - concentrates packets and performs protocol conversions
    - IWF1 located in BSS (Base Station Sub-system) requires many access units to external network
    - IWF1 located in MSC requires functions to route packets to proper BSC
  - router able to access HLR (and VLR if IWF1 is located in BSS) required in external PDN
- proposal three
  - use dedicated GPRS packet network from IWF1 to IWF2
  - protocol routers interface with HLR (and VLR if IWF1 is located in BSS)
  - packet routing information could be cached at routers to avoid HLR check for individual packets

GPRS: Outside View

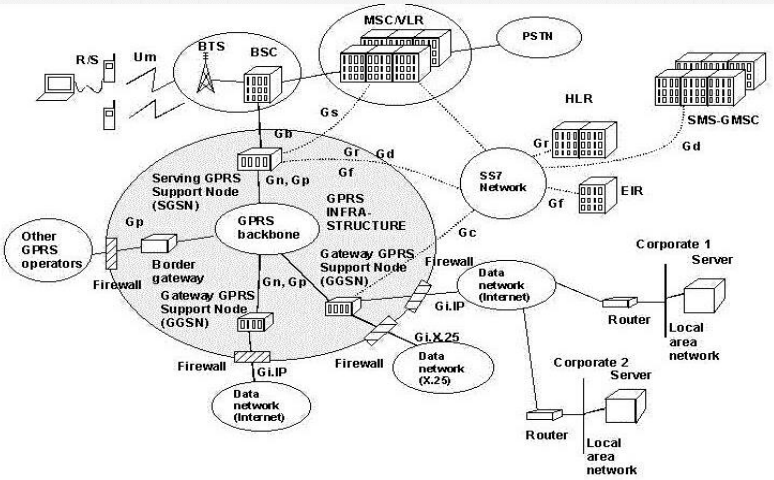
(see also `http://www.cs.hut.fi/~hhk/GPRS/gprs_index.html`)



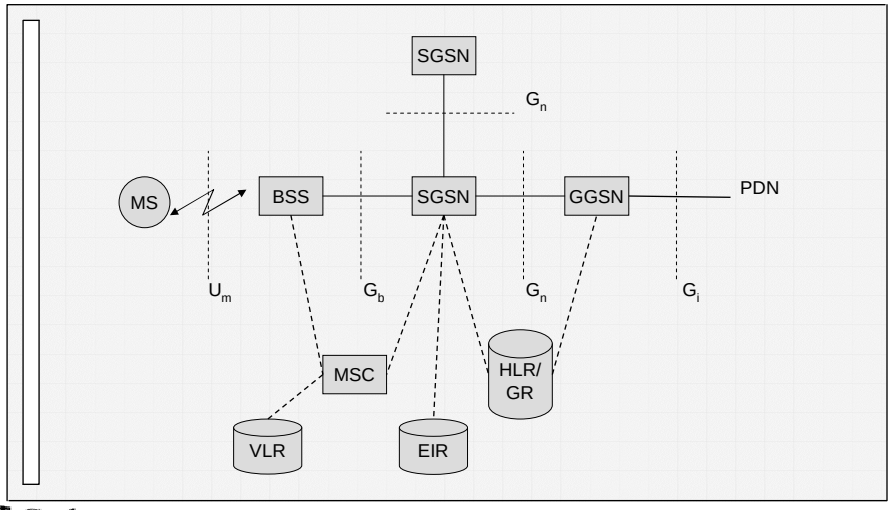
GPRS Architecture: Services

- Packet-based access to data networks
  - Internet (IPv4, IPv6)
  - X.25
  - Private/public networks
- Fast carrier of SMSs
- User QoS categorization
  - priorities, mean/peak throughput, delay definition, transmission reliability
- Security (operator, user, identity, data)
- Mobility management

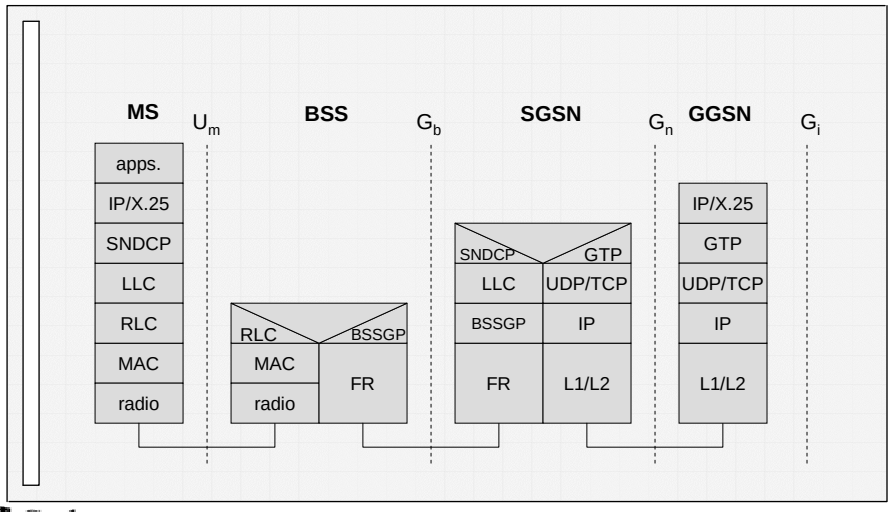
GPRS Architecture Elements



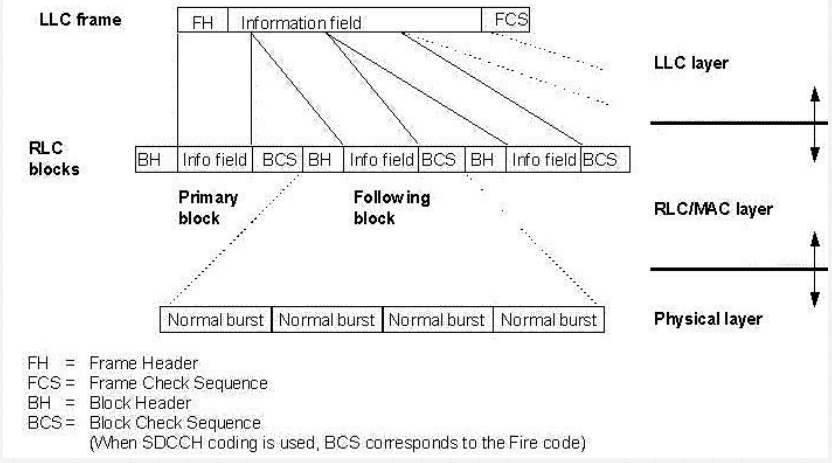
GPRS Architecture and Interfaces



GPRS Protocol Stack



GPRS Radio Link Protocols



GPRS Radio Interface

- Logical channels:
  - packet common control channels (PCCCH), UL+DL
    - packet random access channel (PRACH), UL
    - packet paging channel (PAGCH), DL
    - packet access grant channel (PAGCH), DL
    - packet notification channel (PNCH), DL
  - packet broadcast control channel (PBCCH), DL
  - packet data traffic channel (PDTCH), UL+DL
    - data rates 9.05 to 21.4 kbps, depending on channel coding
  - packet associated control channel (PACCH)
- Physical channels:
  - PCCCH and PBCCH combined into same 51 multiframe
  - PDTCH is mapped to one physical channel
  - dynamic or permanent channel allocation for GPRS possible
  - if no PCCCH possible, MSs park on CCCH

GPRS: New Radio Interfaces

- GPRS can use various radio interfaces:
  - DECT, EDGE, UMTS, IEEE 802.11, IrDA (infrared)
- Radio should:
  - operate using packet mode
  - provide identifier of the downlink packets
  - provide reasonable residual error rates
- Wish list for radio services:
  - fast channel allocation and release
  - battery saving mechanism (sleep mode)
  - adaptive coding (depending on radio quality)
  - just one (efficient) paging channel that can be listened to also when transferring data

GPRS Quality of Service

- QoS described as part of Packet Data Protocol context
- QoS definitions:
  - service precedence (priority)
    - high priority
    - normal priority
    - low priority
  - reliability
  - delay
  - throughput (mean, peak)

GPRS QoS Reliability Classes

Reliability class	Lost SDU probability (a)	Duplicate SDU probability	Out of Sequence SDU probability	Corrupt SDU probability (b)	Example of application characteristics.
1	10^{-9}	10^{-9}	10^{-9}	10^{-9}	Error sensitive, no error correction capability, limited error tolerance capability.
2	10^{-4}	10^{-5}	10^{-5}	10^{-6}	Error sensitive, limited error correction capability, good error tolerance capability.
3	10^{-2}	10^{-5}	10^{-5}	10^{-2}	Not error sensitive, error correction capability and/or very good error tolerance capability.

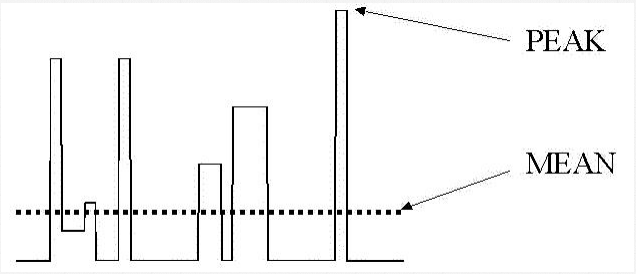
a) To protect against buffer overflow or a protocol malfunction, there is a maximum holding time for each SDU in the GPRS network after which the SDU is discarded. The maximum holding time depends on the protocols used (e.g., TCP/IP).
b) Corrupt SDU probability: the probability that a SDU will be delivered to the user with an undetected error.

GPRS QoS Delay Classes

Delay Class	Packet size			
	128 octets		1024 octets	
	Mean Transfer Delay (sec)	95 percentile Delay (sec)	Mean Transfer Delay (sec)	95 percentile Delay (sec)
1. (Predictive)	0.5	1.5	2	7
2. (Predictive)	5	25	15	75
3. (Predictive)	50	250	75	375
4. (Best Effort)	Unspecified			

GPRS QoS Throughput

- Maximum (peak) bit rate
- Mean bit rate
  - includes, for example, the periods in which no data is transmitted for bursty transmissions



GPRS Evolution

- GPRS is standardized in SMG in ETSI (see also http://www.etsi.fr/SMG/SMG.html)
- Standard was approved March/June 1998
  - changes are still expected
- Some issues delayed for later consideration
  - testing (type approval), charging, ….
- GPRS phase 1: Release 97
  - basic set of GPRS functionality
  - optional features

GPRS Evolution

- GPRS phase 2 or GPRS for UMTS
  - certain issues defined in stage 1 documents not yet included in first release of GPRS standard (mutual authentication, MS initiated QoS renegotiation, support for continuous data flow: voice over GPRS, multicast services)
  - new requirements have been pointed out for UMTS
- GPRS products:
  - official ETSI schedule is 18-24 months after approval of the standard (vary ambitious)
  - Ericsson and Motorola announced deals with operators on GPRS in January 1999
  - Ericsson delivered first GPRS equipment during Summer 1999
  - field trials with 50 or so operators during Fall 1999
  - services launched in Europe in 2001