CS8601 -MOBILE COMPUTING

UNIT 2

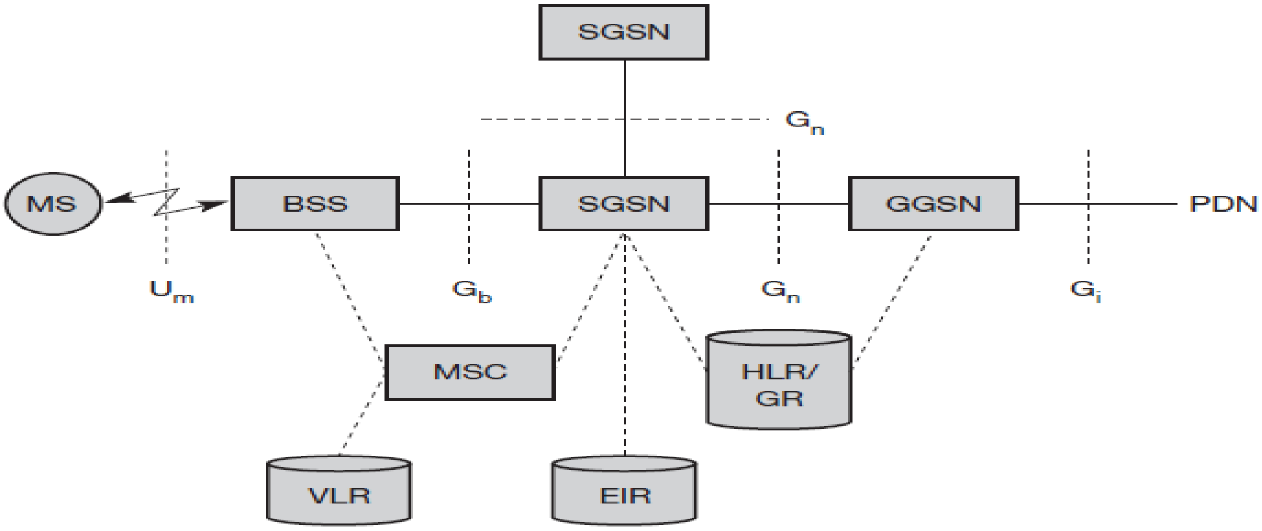
MOBILE TELECOMMUNICATION SYSTEM

2.4.GPRS:

The next step toward more flexible and powerful data transmission avoids the problems

of HSCSD by being fully packet-oriented. The **general packet radio service (GPRS)** provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission ofsmall volumes (e.g., typical web requests) or infrequent transmissions of small or medium volumes (e.g., typical web responses) according to the requirement specification. For the new GPRS radio channels, the GSM system can allocate between one and eight time slots within a TDMA frame. Time slots are not allocated in a fixed, pre-determined manner but on demand. Alltime slots can be shared by the active users; up- and downlink are allocated separately. Allocation of the slots is based on current load and operator preferences. The GPRS concept is independent of channel characteristics and of the type of channel (traditional GSM traffic or control channel), and does not limit the maximum data rate (only the GSM transport system limits the rate). All GPRS services can be used in parallel to conventional services. GPRS includes several **security services** such as authentication, access control, user identity confidentiality, and user information confidentiality.

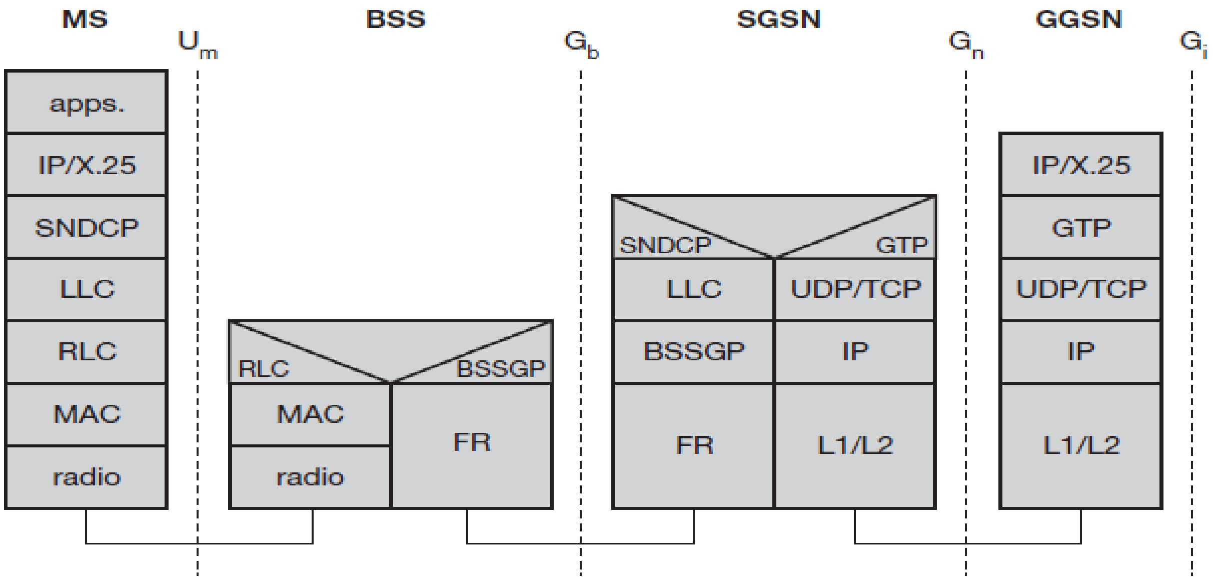
The GPRS architecture introduces two new network elements, which are called GPRS support nodes (GSN) and are in fact routers. All GSNs are integrated into the standard GSM architecture, and many new interfaces have been defined. The gateway GPRS support node (GGSN) is the interworking unit between the GPRS network and external packet data networks (PDN). This node contains routing information for GPRS users, performs address conversion, and tunnels data to a user via encapsulation. The GGSN is connected to external networks (e.g., IP or X.25) via the Gi interface and transfers packets to the SGSN via an IPbased GPRS backbone network (Gn interface). The other new element is the **serving GPRS support node (SGSN)** which supports the MS via the Gb interface. The SGSN, for example, requests user addresses from the **GPRS register (GR)**, keeps track of the individual MSs' location, is responsible for collecting billing information (e.g., counting bytes), HLR, stores all GPRS-relevant data.



GPRS Architecture Reference Model

As shown above, packet data is transmitted from a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS. The MSC, which is responsible for data transport in the traditional circuit-switched GSM, is only used for signaling in the GPRS scenario. Before sending any data over the GPRS network, an MS must attach to it, following the procedures of the mobility management. The attachment procedure includes assigning a temporal identifier, called a temporary logical link identity (TLLI), and a ciphering key sequence number (CKSN) for data encryption. For each MS, a GPRS context is set up and stored in the MS and in the corresponding SGSN. Besides attaching and detaching, mobility management also comprises functions for authentication, location management, and ciphering.

The following figure shows the protocol architecture of the transmission plane for GPRS. All data within the GPRS backbone, i.e., between the GSNs, is transferred using the GPRS tunnelling protocol (GTP). GTP can use two different transport protocols, either the reliable TCP (needed for reliable transfer of X.25 packets) or the non-reliable UDP (used for IP packets). The network protocol for the GPRS backbone is IP (using any lower layers). To adapt to the different characteristics of the underlying networks, the subnetwork dependent convergence protocol (SNDCP) is used between an SGSN and the MS. On top of SNDCP and GTP, user packet data is tunneled from the MS to the GGSN and vice versa. To achieve a high reliability of packet transfer between SGSN and MS, a special LLC is used, which comprises ARQ and FEC mechanisms for PTP (and later PTM) services.



GPRS Transmission Plane Protocol Reference Model

A base station subsystem GPRS protocol (BSSGP) is used to convey routing and QoS-related information between the BSS and SGSN. BSSGP does not perform error correction and works on top of a frame relay (FR) network. Finally, radio link dependent protocols are needed to transfer data over the Um interface. The radio link protocol (RLC) provides a reliable link, while the MAC controls access with signalling procedures for the radio channel and the mapping of LLC frames onto the GSM physical channels. The radio interface at Um needed for GPRS does not require fundamental changes compared to standard GSM.

CS8601 -MOBILECOMPUTING

UNIT 2

MOBILE TELECOMMUNICATIONSYSTEM

2.2. GSM [Global System for Mobile Communication]

GSM is the most successful digital mobile telecommunication system in the world today. It is used by over 800 million people in more than 190 countries. GSM permits the integration of different voice and data services and the interworking with existing networks. Services make a network interesting for customers. GSM has defined three different categories of services:

Bearer Services, Tele and Supplementary Services

Bearer services:

GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services. Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission.
Transparent bearer services only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur. Transmission quality can be improved with the use of forward error correction (FEC), which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors. Transparent bearer services do not try to recover lost data in case of, for example, shadowing or interruptions due to handover. Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services, adding a radio link protocol (RLP). This protocol comprises mechanisms of high-level data link control (HDLC), and special selective-reject mechanisms to trigger retransmission of erroneous data. Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN, and packet switched public data networks (PSPDN) like X.25, which is available worldwide. Data transmission can be full- duplex, synchronous with data rates of 1.2, 2.4, 4.8, and 9.6 kbit/s or full-duplex, asynchronous from 300 to 9,600 bit/s.

Tele services:

GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN (e.g., fax). The primary goal of GSM was the provision of high-quality digital voice transmission. Special codecs (coder/decoder) are used for voice transmission, while other codecs are used for the transmission of analog data for communication with traditional computer modems used in, e.g., fax machines. Another service offered by GSM is the emergency number (eg 911, 999). This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center. A useful service for very simple message transfer is the short message service (SMS), which offers transmission of messages of up to 160 characters. Sending and receiving of SMS is possible during data or voice transmission. It can be used for "serious" applications such as displaying road conditions, e-mail headers or stock quotes, but it can also transfer logos, ring tones, horoscopes and love letters.

The successor of SMS, the enhanced message service (EMS), offers a larger message size, formatted text, and the transmission of animated pictures, small images and ring tones in a standardized way. But with MMS, EMS was hardly used. MMS offers the transmission of larger pictures (GIF, JPG, WBMP), short video clips etc. and comes with mobile phones that integrate small cameras. Another non-voice tele service is group 3 fax, which is available worldwide

Supplementary services:

In addition to tele and bearer services, GSM providers can offer supplementary services. these services offer various enhancements for the standard telephony service, and may vary from provider to provider. Typical services are user identification, call redirection, or forwarding of ongoing calls, barring of incoming/outgoing calls, Advice of Charge (AoC) etc. Standard ISDN features such as closed user groups and multiparty communication may be available.

GSM Architecture

A GSM system consists of three subsystems, the radio sub system (RSS), the network and switching subsystem (NSS), and the operation subsystem (OSS).

Network Switching Subsystem[NSS]:

The NSS is responsible for performing call processing and subscriber related functions. The switching system includes the following functional units:

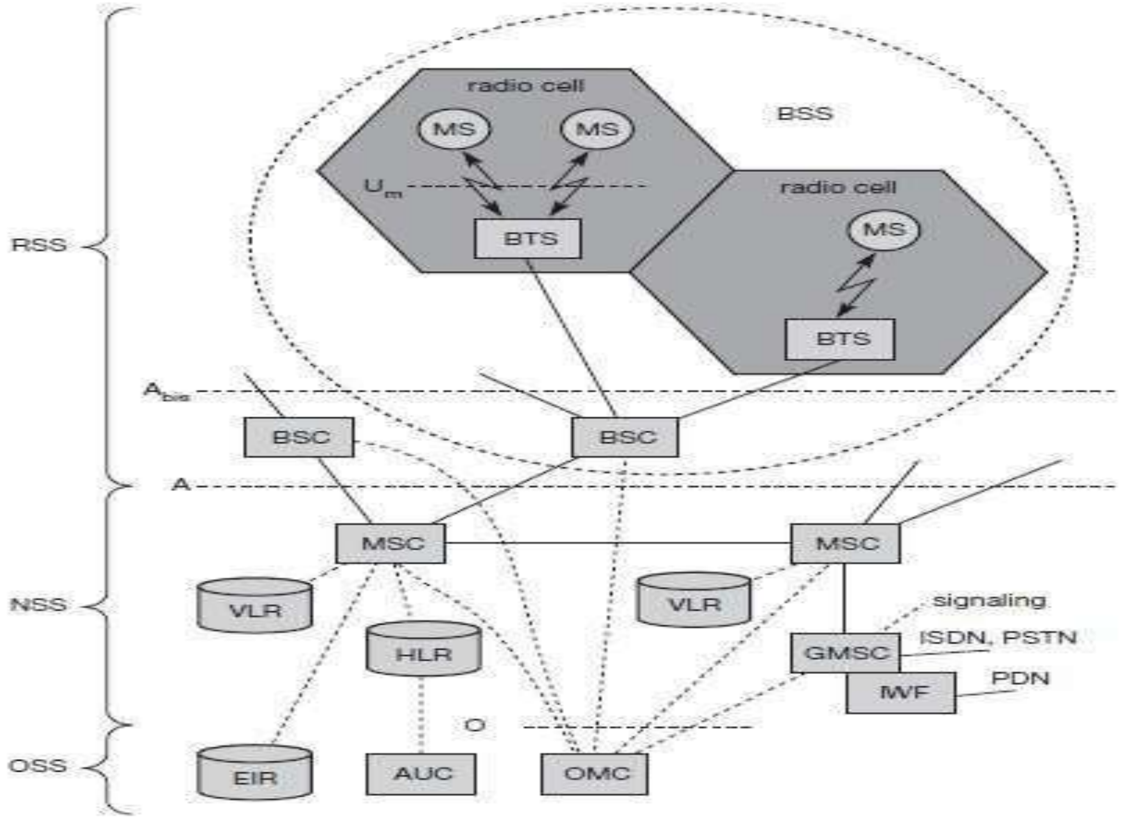
Home location register (HLR): It is a database used for storage and management of subscriptions. HLR stores permanent data about subscribers, including a subscribers service profile, location information and activity status. When an individual buys a subscription from the PCS provider, maintains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers.

Visitor location register (VLR): The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI,MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information. Some VLRs in existence, are capable of managing up to one million customers.

Authentication center (AUC): A unit called the AUC provides authentication and encryption parameters that verify the users identity and ensure the confidentiality of each call.

Equipment identity register (EIR): It is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized or defective mobile stations.

Mobile switching center (MSC): The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems.



Radio Subsystem [RSS]:

The radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS). The figure shows the connection between the RSS and the NSS via the A interface (solid lines) and the connection to the OSS via the O interface (dashed lines).

Base station subsystem (BSS): A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.

Base station controllers (BSC): The BSC provides all the control functions and physical links between the MSC and BTS. It is a high capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in BTS. A number of BSC's are served by and MSC.

Base transceiver station (BTS): The BTS handles the radio interface to the mobile station. A BTS can form a radio cell or, using sectorized antennas, several and is connected to MS via the Um interface, and to the BSC via the Abis interface. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.)The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTS's are controlled by an BSC.

Operation and Support system[OSS]:

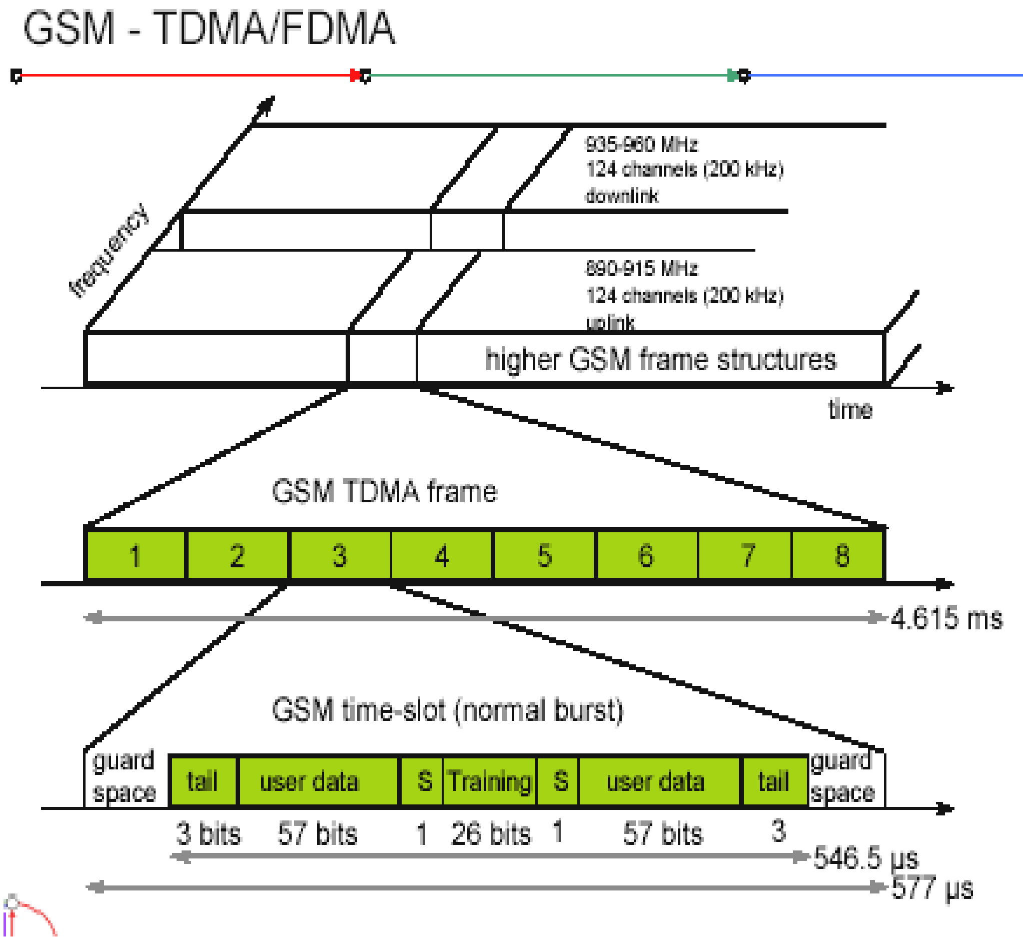
The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. Implementation of OMC is called operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. OSS provides a network overview and allows engineers to monitor, diagnose and troubleshoot every aspect of the GSM network.

The mobile station (MS) consists of the mobile equipment (the terminal) and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to subscribed services irrespective of a specific terminal.

By inserting the SIM card into another GSM terminal, the user is able to receive calls at that terminal, make calls identified by the International Mobile Equipement Identity (IMEI)). The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other information. The IMEI and the IMSI are independent, thereby allowing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

Each of the 248 channels is additionally separated in time via a GSM TDMA frame, i.e., each 200 kHz carrier is subdivided into frames that are repeated continuously. The duration of a frame is 4.615 ms. A frame is again subdivided into 8 GSM time slots, where each slot represents a physical TDM channel and lasts for 577 µs. Each TDM channel occupies the 200 kHz carrier for 577 µs every 4.615 ms. Data is transmitted in small portions, called bursts. The following figure shows a so called normal burst as used for data transmission inside a time slot. As shown, the burst is only 546.5 µs long and contains 148 bits. The remaining 30.5 µs are used as guard space to avoid overlapping with other bursts due to different path delays and to give the transmitter time to turn on and off. The first and last three bits of a normal burst (tail) are all set to 0 and can be used to enhance the receiver performance. The training sequence in the middle of a slot is used to adapt the parameters of the receiver to the current path propagation characteristics and to select the path propagation. A flag S indicates whether the data field contains user or network control data.

Apart from the normal burst, ETSI (1993a) defines four more bursts for data transmission: a frequency correction burst allows the MS to correct the local oscillator to avoid interference with neighbouring channels, a synchronization burst with an extended training sequence synchronizes the MS with the BTS in time, an access burst is used for the initial connection setup between MS and BTS, and finally a dummy burst is used if no data is available for a slot.



GSM TDMA Frame, Slots and Bursts

Logical channels and frame hierarchy:

Two types of channels, namely physical channels and logical channels are present.

Physical channel: channel defined by specifying both, a carrier frequency and a TDMA timeslot number.

Logic channel: logical channels are multiplexed into the physical channels. Each logic channel performs a specific task. Consequently the data of a logical channel is transmitted in the corresponding timeslots of the physical channel. During this process, logical channels can occupy a part of the physical channel or even the entire channel.

Each of the frequency carriers is divided into frames of 8 timeslots of approximately 577s (15/26 s) duration with 156.25 bits per timeslot. The duration of a TDMA frame is 4.615ms (577s x 8 = 4.615 ms). The bits per timeslot and frame duration yield a gross bit rate of about 271kbps per TDMA frame.

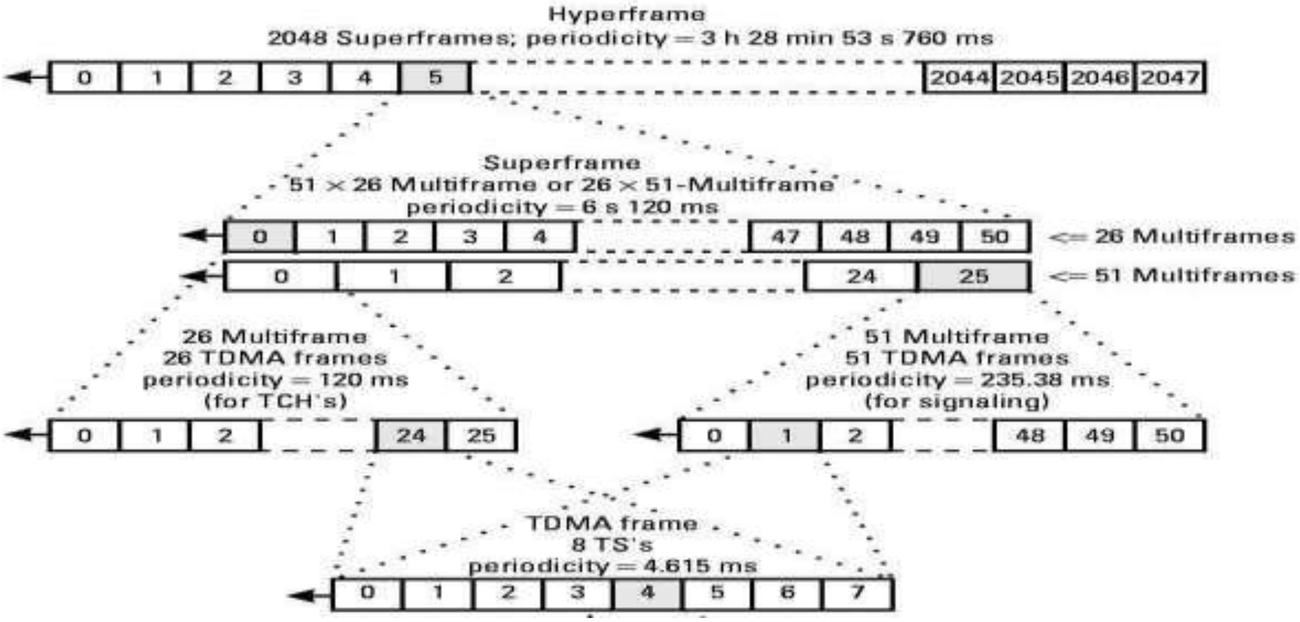
TDMA frames are grouped into two types of multiframes:

26-frame multiframe (4.615ms x 26 = 120 ms) comprising of 26 TDMA frames. This multiframe is used to carry traffic channels and their associated control channels.

51-frame multiframe (4.615ms x 51   235.4 ms) comprising 51 TDMA frames. This multiframe is exclusively used for control channels. The multiframe structure is further multiplexed into a single superframe of duration of 6.12sec. This means a superframe consists of 51 multiframes of 26 frames.

26 multiframes of 51 frames.

The last multiplexing level of the frame hierarchy, consisting of 2048 superframes (2715648 TDMA frames), is a hyperframe. This long time period is needed to support the GSM data encryption mechanisms. The frame hierarchy is shown below:



GSM Frame Hierarchy

There are two different types of logical channel within the GSM system: Traffic channels(TCHs), Control channels (CCHs).

Traffic Channels:

Traffic channels carry user information such as encoded speech or user data. Trafficchannels are defined by using a 26-frame multiframe. Two general forms are defined:
i. Full rate traffic channels (TCH/F), at a gross bit rate of 22.8 kbps (456bits / 20ms)
ii. Half rate traffic channels (TCH/H), at a gross bit rate of 11.4 kbps.
Uplink and downlink are separated by three slots (bursts) in the 26-multiframe structure.

This simplifies the duplexing function in mobile terminals design, as mobiles will not need to transmit and receive at the same time. The 26-frame multiframe structure, shown below multiplexes two types of logical channels, a TCH and a Slow Associated Control Channel (SACCH).

However, if required, a Fast Associated Control CHannel (FACCH) can steal TCH in order to transmit control information at a higher bit rate. This is usually the case during the handover process. In total 24 TCH/F are transmitted and one SACCH.

Control Channels:

Control channels carry system signalling and synchronisation data for control procedures such as location registration, mobile station synchronisation, paging, random access etc. between base station and mobile station. Three categories of control channel are defined: Broadcast, Common and Dedicated. Control channels are multiplexed into the 51-frame multiframe.

Broadcast control channel (BCCH):

A BTS uses this channel to signal information to all MSs within a cell. Information transmitted in this channel is, e.g., the cell identifier, options available within this cell (frequency hopping), and frequencies available inside the cell and in neighboring cells. The BTS sends information for frequency correction via the frequency correction channel (FCCH) and information about time synchronization via the synchronization channel (SCH), where both channels are subchannels of the BCCH.

Common control channel (CCCH):

All information regarding connection setup between MS and BS is exchanged via the CCCH. For calls toward an MS, the BTS uses the paging channel (PCH) for paging the appropriate MS. If an MS wants to set up a call, it uses the random access channel (RACH) to send data to the BTS. The RACH implements multiple access (all MSs within a cell may access this channel) using slotted Aloha. This is where a collision may occur with other MSs in a GSM system. The BTS uses the access grant channel (AGCH) to signal an MS that it can use a TCH or SDCCH for further connection setup.

Dedicated control channel (DCCH):

While the previous channels have all been unidirectional, the following channels are bidirectional. As long as an MS has not established a TCH with the BTS, it uses the stand-alone dedicated control channel (SDCCH) with a low data rate (782 bit/s) for signaling. This can comprise authentication, registration or other data needed for setting up a TCH. Each TCH and SDCCH has a slow associated dedicated control channel (SACCH) associated with it, which is used to exchange system information, such as the channel quality and signal power level. Finally, if more signaling information needs to be transmitted and a TCH already exists, GSM uses a fast associated dedicated control channel (FACCH). The FACCH uses the time slots which are otherwise used by the TCH. This is necessary in the case of handovers where BTS and MS have to exchange larger amounts of data in less time.

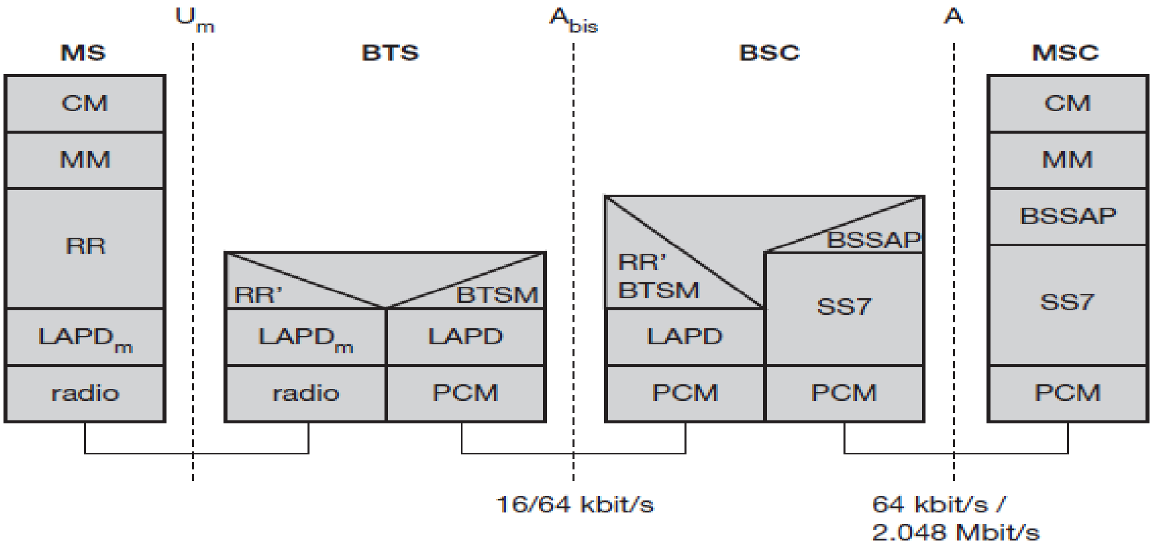
CS8601 -MOBILE COMPUTING

UNIT 2

MOBILE TELECOMMUNICATION SYSTEM

2.3. GSM Protocols:

The signaling protocol in GSM is structured into three general layers depending on the interface, as shown below. Layer 1 is the physical layer that handles all **radio**-specific functions. This includes the creation of bursts according to the five different formats, **multiplexing** of bursts into a TDMA frame, **synchronization** with the BTS, detection of idle channels, and measurement of the **channel quality** on the downlink. The physical layer at Um uses GMSK for digital **modulation** and performs **encryption/decryption** of data, i.e., encryption is not performed end-to-end, but only between MS and BSS over the air interface.



Protocol Architecture for Signaling

The main tasks of the physical layer comprise **channel coding** and **error detection/correction**, which is directly combined with the coding mechanisms. Channel coding makes extensive use of different **forward error correction (FEC)** schemes.

Signaling between entities in a GSM network requires higher layers. For this purpose, the LAPDm protocol has been defined at the Um interface for layer two. LAPDm has been derived from link access procedure for the D-channel (LAPD) in ISDN systems, which is a version of HDLC.

LAPDm is a lightweight LAPD because it does not need synchronization flags or checksumming for error detection. LAPDm offers reliable data transfer over connections, resequencing of data frames, and flow control.

The network layer in GSM, layer three, comprises several sublayers. The lowest sublayer is the radio resource management (RR). Only a part of this layer, RR', is implemented in the BTS, the remainder is situated in the BSC. The functions of RR' are supported by the BSC via the BTS management (BTSM). The main tasks of RR are setup, maintenance, and release of radio channels. Mobility management (MM) contains functions for registration, authentication, identification, location updating, and the provision of a temporary mobile subscriber identity (TMSI). Finally, the call management (CM) layer contains three entities: call control (CC), short message service (SMS), and supplementary service (SS).

SMS allows for message transfer using the control channels SDCCH and SACCH, while SS offers the services like user identification, call redirection, or forwarding of ongoing calls. CC provides a point-to-point connection between two terminals and is used by higher layers for call establishment, call clearing and change of call parameters. This layer also provides functions to send in-band tones, called dual tone multiple frequency (DTMF), over the GSM network. These tones are used, e.g., for the remote control of answering machines or the entry of PINs in electronic banking and are, also used for dialing in Data transmission at the modulation (PCM) systems. LAPD is used for layer two at Abis, BTSM for BTS management. Signaling system No. 7 (SS7) is used for signaling between an MSC and a BSC. This protocol also transfers all management information between MSCs, HLR, VLRs, AuC, EIR, and OMC. An MSC can also control a BSS via a BSS application part (BSSAP).

Localization and Calling

The fundamental feature of the GSM system is the automatic, worldwide localization of users for which, the system performs periodic location updates. The HLR always contains information about the current location and the VLR currently responsible for the MS informs the HLR about the location changes. Changing VLRs with uninterrupted availability is called roaming. Roaming can take place within a network of one provider, between two providers in a country and also between different providers in different countries.

To locate and address an MS, several numbers are needed:

Mobile station international ISDN number (MSISDN):- The only important number for a user of GSM is the phone number. This number consists of the country code (CC), the national destination code (NDC) and the subscriber number (SN).

International mobile subscriber identity (IMSI): GSM uses the IMSI for internal unique identification of a subscriber. IMSI consists of a mobile country code (MCC), the mobile network code (MNC), and finally the mobile subscriber identification number (MSIN).

Temporary mobile subscriber identity (TMSI):

To hide the IMSI, which would give away the exact identity of the user signalling over the air interface, GSM uses the 4 byte TMSI for local subscriber identification.

Mobile station roaming number (MSRN):

Another temporary address that hides the identity and location of a subscriber is MSRN. The VLR generates this address on request from the MSC, and the address is also stored in the HLR. MSRN contains the current visitor country code (VCC), the visitor national destination code (VNDC), the identification of the current MSC together with the subscriber number. The MSRN helps the HLR to find a subscriber for an incoming call. For a mobile terminated call (MTC), the following figure shows the different steps that take place.

Step 1: User dials the phone

Step 2: The fixed network (PSTN) identifies the number belongs to a user in GSM network and

forwards the call setup to the Gateway MSC (GMSC).

Step 3: The GMSC identifies the HLR for the subscriber and signals the call setup to HLR

Step 4: The HLR checks for number existence and its subscribed services and requests an MSRN from the current VLR.

Step 5: VLR sends the MSRN to HLR

Step 6: Upon receiving MSRN, the HLR determines the MSC responsible for MS and forwards the information to the GMSC

Step 7: The GMSC can now forward the call setup request to the MSC indicated

Step 8: The MSC requests the VLR for the current status of the MS

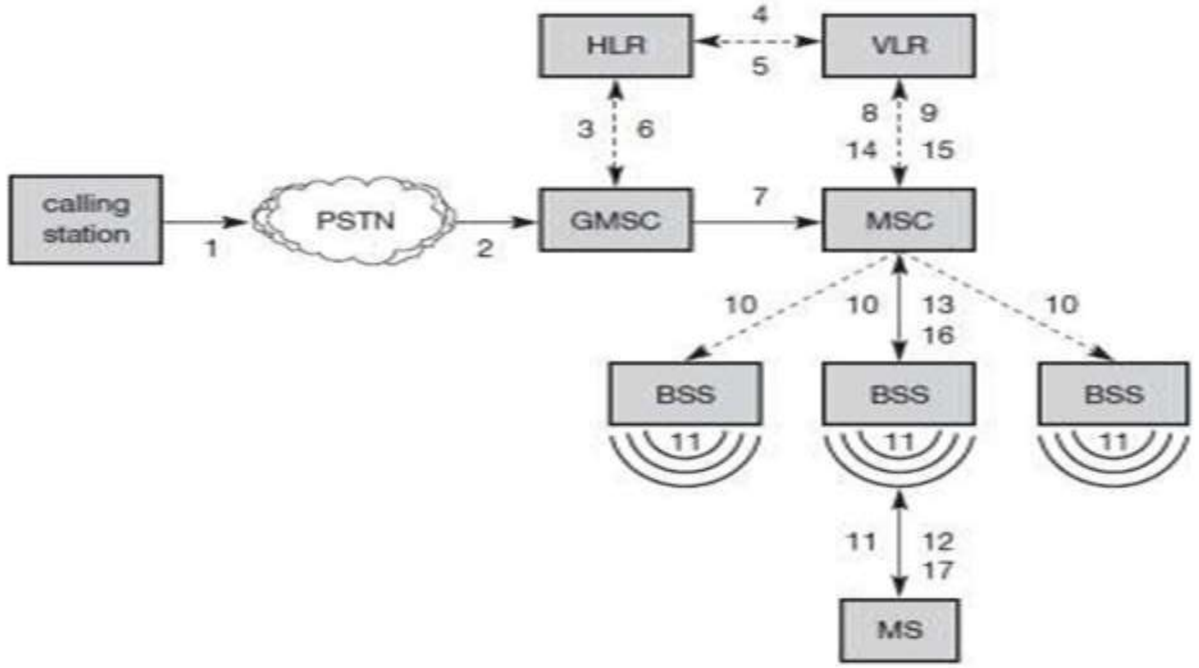
Step 9: VLR sends the requested information

Step 10: If MS is available, the MSC initiates paging in all cells it is responsible for.

Step 11: The BTSs of all BSSs transmit the paging signal to the MS

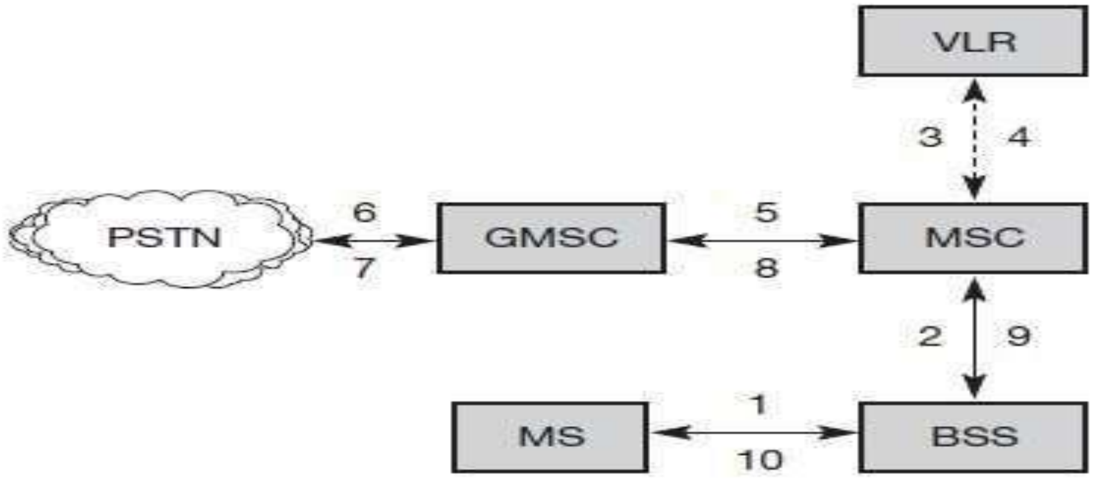
Step 12: Step 13: If MS answers, VLR performs security checks

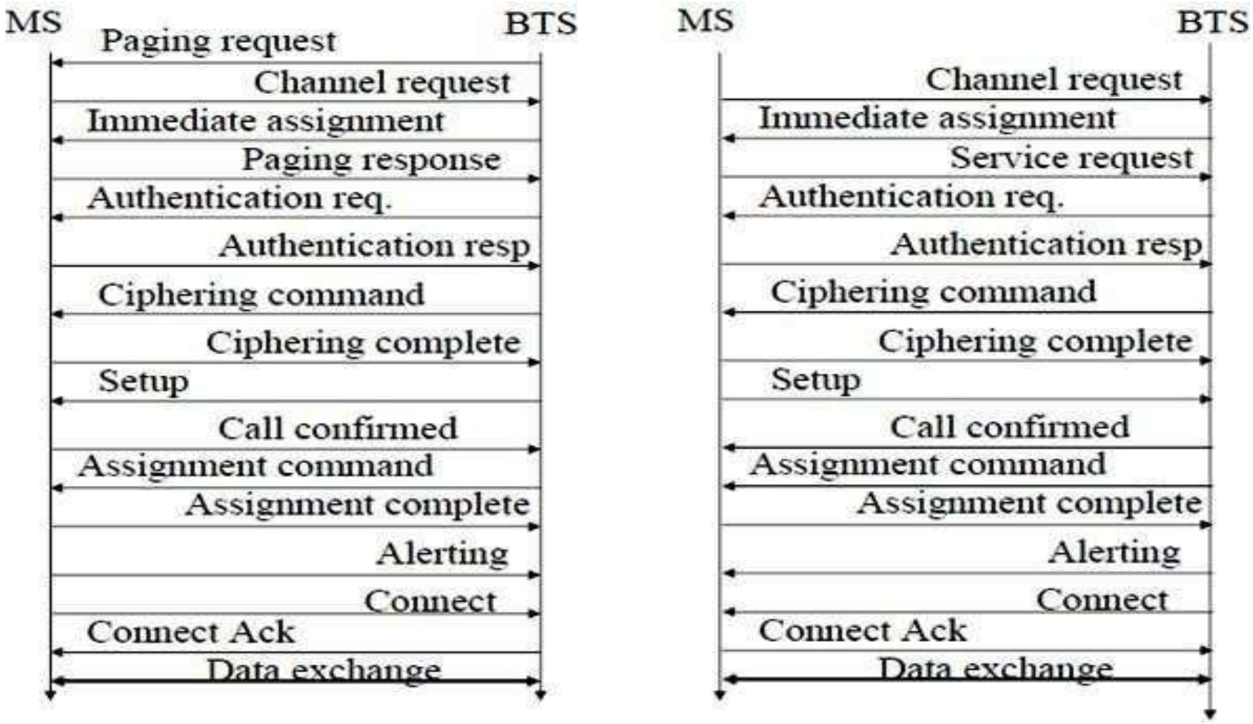
Step 15: Till step 17: Then the VLR signals to the MSC to setup a connection to the MS



For a mobile originated call (MOC), the following steps take place:

Step 1: The MS transmits a request for a new connection
Step 2: The BSS forwards this request to the MSC
Step 3: Step 4: The MSC then checks if this user is allowed to set up a call with the requested and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network. In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during connection setup (in either direction).





Message flow for MTC and MOC

CS8601 -MOBILECOMPUTING

UNIT 2

MOBILE TELECOMMUNICATIONSYSTEM

2.6.Handover &Security :

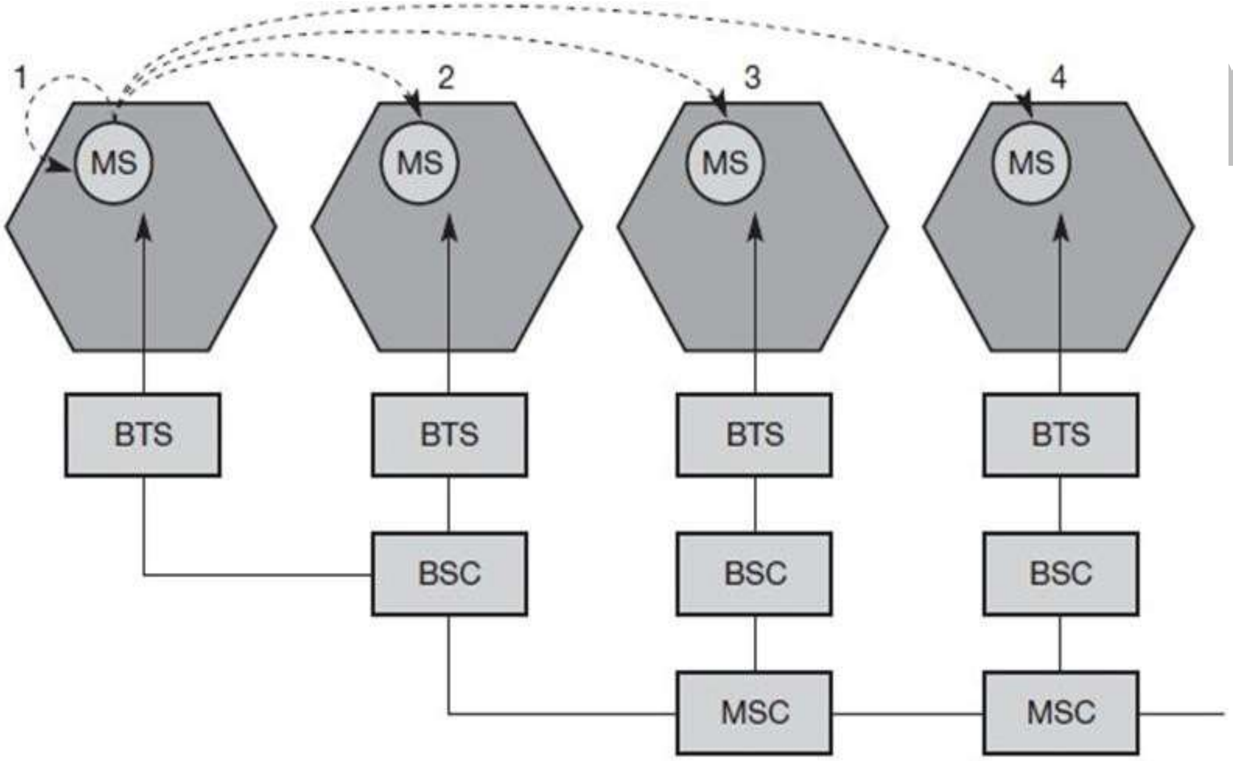
Handover

Cellular systems require **handover** procedures, as single cells do not cover the whole service area. However, a handover should not cause a cut-off, also called **call drop**. GSM aims atmaximum handover duration of 60 ms. There are two basic reasons for a handover:

The mobile station **moves out of the range** of a BTS, decreasing the received **signal level** increasing the **error rate** thereby diminishing the **quality of the radio link.**

Handover may be due to **load balancing,** when an MSC/BSC decides the traffic is too high in one cell and shifts some MS to other cells with a lower load.

The four possible handover scenarios of GSM are shown below:



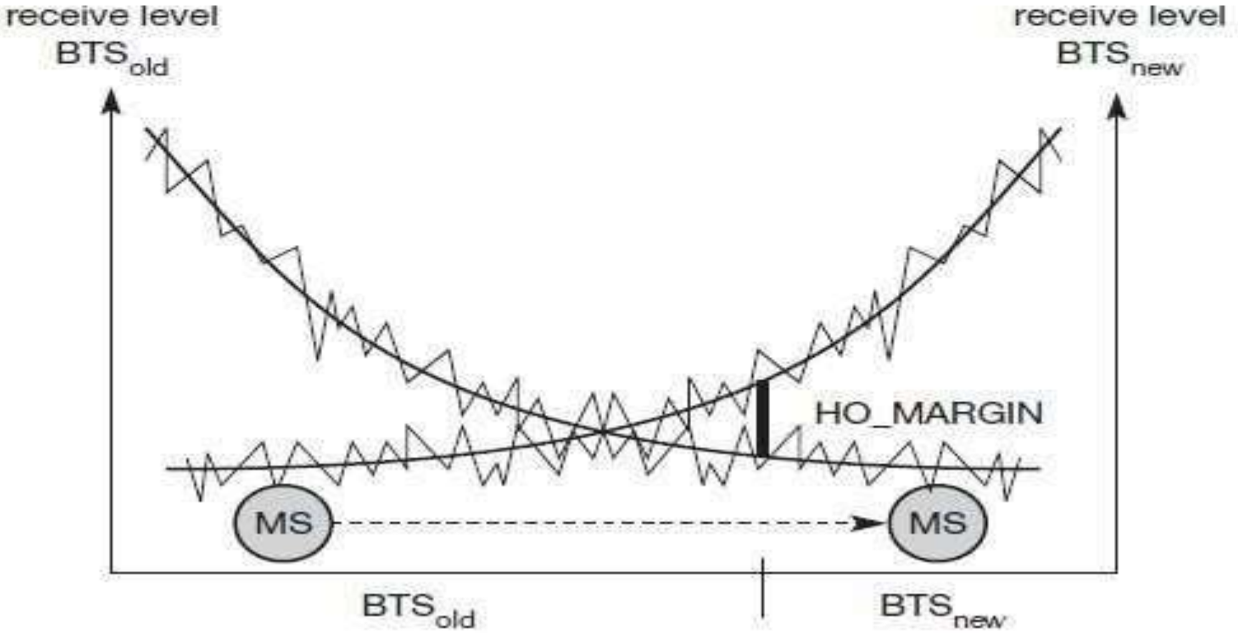
Intra-cell handover: With reference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).

Inter-cell, intra-BSC handover: This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2).

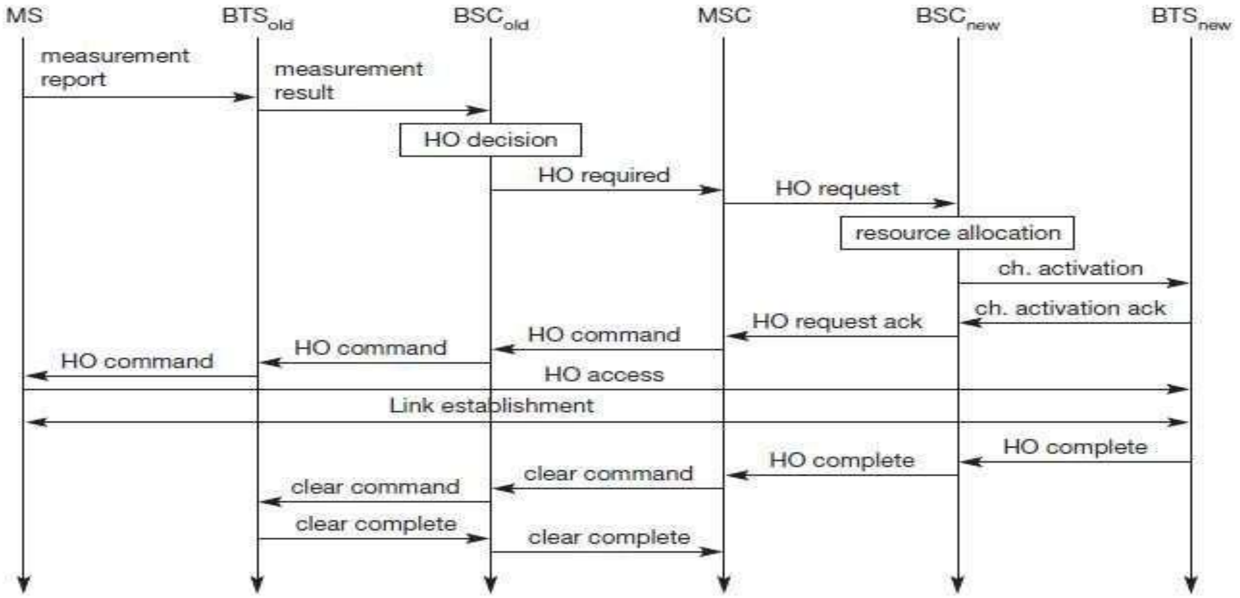
Inter-BSC, intra-MSC handover: As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).

Inter MSC handover: A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

To provide all the necessary information for a handover due to a weak link, MS and BTS both perform periodic measurements of the downlink and uplink quality respectively. Measurement reports are sent by the MS about every half-second and contain the quality of the current link used for transmission as well as the quality of certain channels in neighboring cells (the BCCHs).



Handover decision depending on receive level



Intra-MSC handover

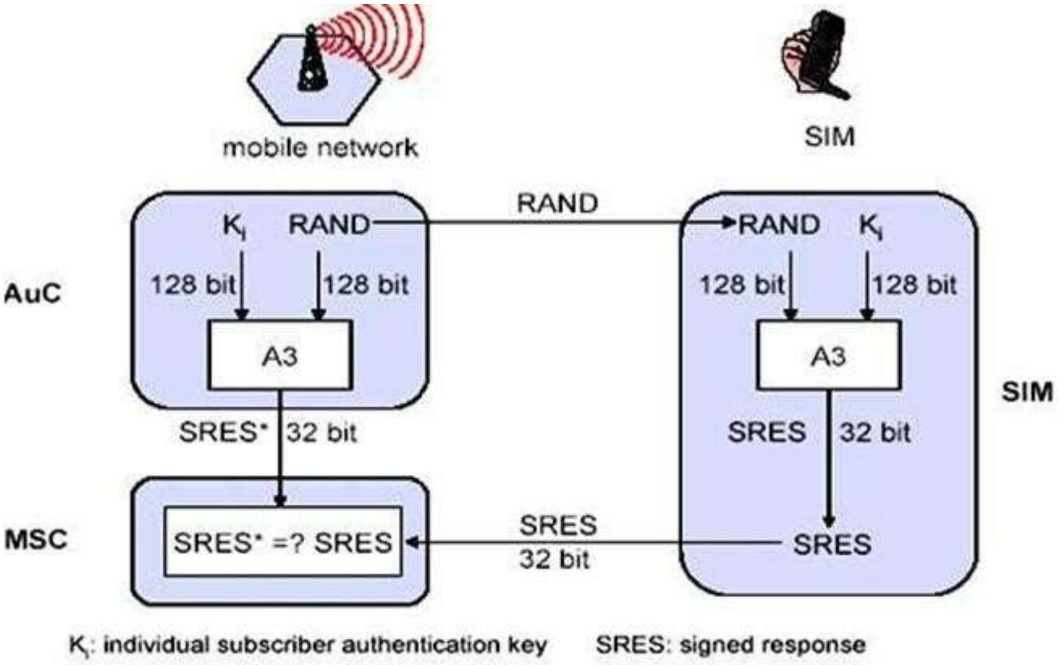
More sophisticated handover mechanisms are needed for seamless handovers betweendifferent systems.

Security

GSM offers several security services using confidential information stored in the AuCand in the individual SIM. The SIM stores personal, secret data and is protected with a PIN against unauthorized use. Three algorithms have been specified to provide security services in GSM. **Algorithm A3** is used for **authentication**, **A5** for **encryption**, and **A8** for the **generation of a cipher key**. The various security services offered by GSM are:

Access control and authentication: The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriberauthentication. This step is based on a challenge-response scheme as shown below:

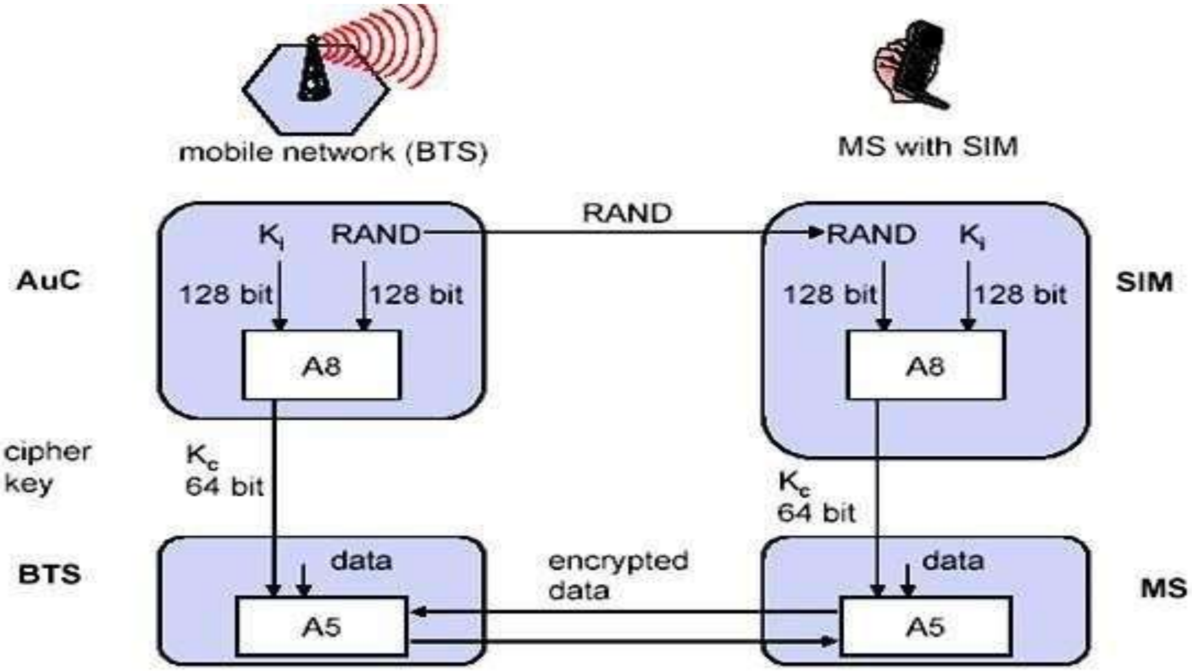
Authentication is based **authentication key Ki**, the **user identification IMSI**, and the algorithm used for authentication **A3**. The AuC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR. The current VLR requests the appropriate values for RAND, SRES, and **Kc** from the HLR. For authentication, the VLR sends the random value RAND to the SIM. Both sides, network and subscriber module, perform the same operation with RAND and the key **Ki**, called **A3**. The MS sends back the SRES generated by the SIM; the VLR can now compare both values. If they are the same, the VLR accepts the subscriber, otherwise the subscriber is rejected.



Subscriber Authentication

Confidentiality:

All user-related data is encrypted. After authentication, BTS and MS apply encryption tovoice, data, and signalling as shown below.



To ensure privacy, all messages containing user-related information are encrypted in GSM over the air interface. After authentication, MS and BSS can start using encryption by applying the cipher key **Kc**, which is generated using the individual key Ki and a random value by applying the algorithm A8. Note that the SIM in the MS and the network both calculate the same **Kc** based on the random value RAND. The key Kc itself is not transmitted over the air interface. MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key Kc.

Anonymity:

To provide user anonymity, all data is encrypted before transmission, and user identifiers are not used over the air. Instead, GSM transmits a temporary identifier (TMSI), which is newly assigned by the VLR after each location update. Additionally, the VLR can change the TMSI at any time.

To enhance the data transmission capabilities of GSM, two basic approaches are possible.As the basic GSM is based on connection-oriented traffic channels, e.g., with 9.6 kbit/s each, several channels could be combined to increase bandwidth. This system is called **HSCSD {high speed circuit switched data}.** A more progressive step is the introduction of packet oriented traffic in GSM, i.e., shifting the paradigm from connections/telephone thinking to packets/internet thinking. The system is called **GPRS {general packet radio service}**.

HSCD:

A straightforward improvement of GSM's data transmission capabilities is high speed circuit switched data (HSCSD) in which higher data rates are achieved by bundling several TCHs. An MS requests one or more TCHs from the GSM network, i.e., it allocates several TDMA slots within a TDMA frame. This allocation can be asymmetrical, i.e. more slots can be allocated on the downlink than on the uplink, which fits the typical user behaviour of downloading more data compared to uploading. A major disadvantage of HSCD is that it still uses the connection-oriented mechanisms of GSM, which is not efficient for computer data traffic.

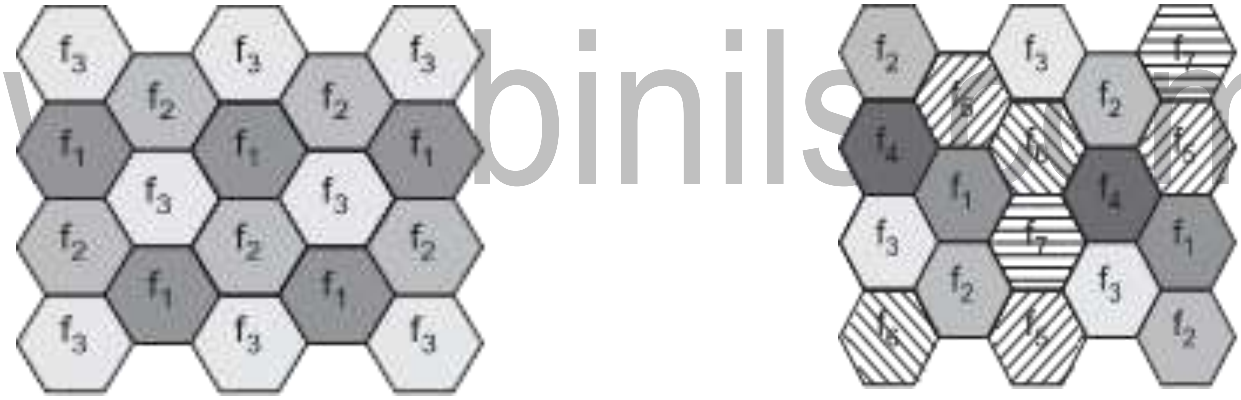
CS8601 -MOBILE COMPUTING

UNIT 2

MOBILE TELECOMMUNICATION SYSTEM

2.1. CELLULAR SYSTEMS

Cellular systems for mobile communications implement SDM. Each transmitter, typically called a base station, covers a certain area, a cell. Cell radii can vary from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the countryside. The shape of cells are never perfect circles or hexagons (as shown in Figure), but depend on the environment (buildings, mountains, valleys etc.), on weather conditions, and sometimes even on system load. Typical systems using this approach are mobile telecommunication systems , where a mobile station within the cell around a base station communicates with this base station and vice versa.



Cellular system with three and seven cell clusters

Advantages of cellular systems with small cells are the following:

- ***Higher capacity:*** Implementing SDM allows frequency reuse. If one transmitter is far away from another, i.e., outside the interference range, it can reuse the same frequencies. As most mobile phone systems assign frequencies to certain users (or certain hopping patterns), this frequency is blocked for other users. But frequencies are a scarce resource and, the number of concurrent users per cell is very limited. Huge cells do not allow for more users. On the contrary, they are limited to less possible users per km2. This is also the reason for using very small cells in cities where many more people use mobile phones.

- ***Less transmission power:*** While power aspects are not a big problem for base stations, they are indeed problematic for mobile stations. A receiver far away from a base station would need much more transmit power than the current few Watts. But energy is a serious problem for mobile handheld devices.

- ***Local interference only:*** Having long distances between sender and receiver results in even more interference problems. With small cells, mobile stations and base stations only have to deal with 'local' interference.

- ***Robustness:*** Cellular systems are decentralized and so, more robust against the failure of single components. If one antenna fails, this only influences communication within a small area.

Small cells also have **some disadvantages**:

- **Infrastructure needed:** Cellular systems need a complex infrastructure to connect all base stations. This includes many antennas, switches for call forwarding, location registers to find a mobile station etc, which makes the whole system quite expensive

- **Handover needed:** The mobile station has to perform a handover when changing from one cell to another. Depending on the cell size and the speed of movement, this can happen quite often.

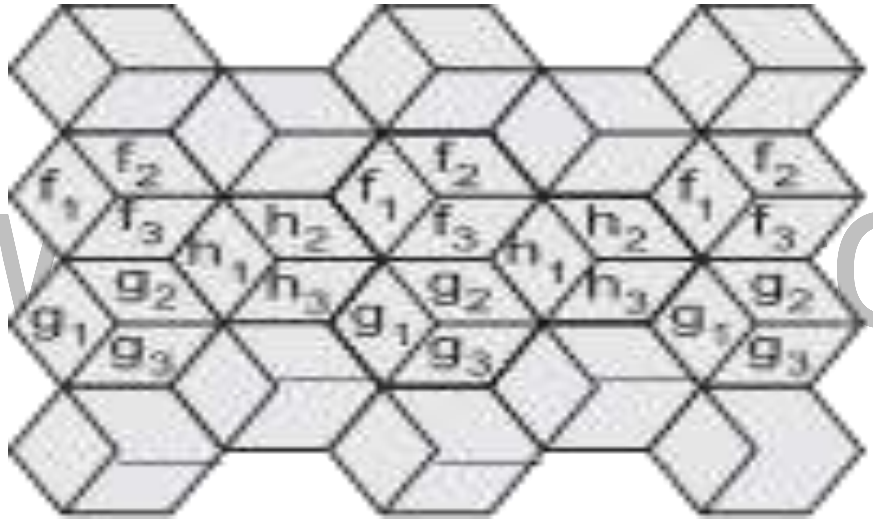
- **Frequency planning:** To avoid interference between transmitters using the same frequencies, frequencies have to be distributed carefully. On the one hand, interference should be avoided, on the other, only a limited number of frequencies is available.

To avoid interference, different transmitters within each other's interference range use FDM. If FDM is combined with TDM (see Figure), the hopping pattern has to be coordinated. The general goal is never to use the same frequency at the same time within the interference range (if CDM is not applied). Two possible models to create cell patterns with minimal interference are shown in Figure. Cells are combined in clusters – on the left side three cells form a cluster, on the right side seven cells form a cluster. All cells within a cluster use disjointed sets of frequencies. On the left side, one cell in the cluster uses set f1, another cell f2, and the third cell f3. In real-life transmission, the pattern will look somewhat different. The hexagonal pattern is chosen as a simple way of illustrating the model. This pattern also shows the repetition of the same frequency sets. The transmission power of a sender has to be limited to avoid interference with the next cell using the same frequencies.

To reduce interference even further (and under certain traffic conditions, i.e., number of users per km2) sectorized antennas can be used. Figure shows the use of three sectors per cell in a cluster with three cells. Typically, it makes sense to use sectorized antennas instead of omni-directional antennas for larger cell radii.

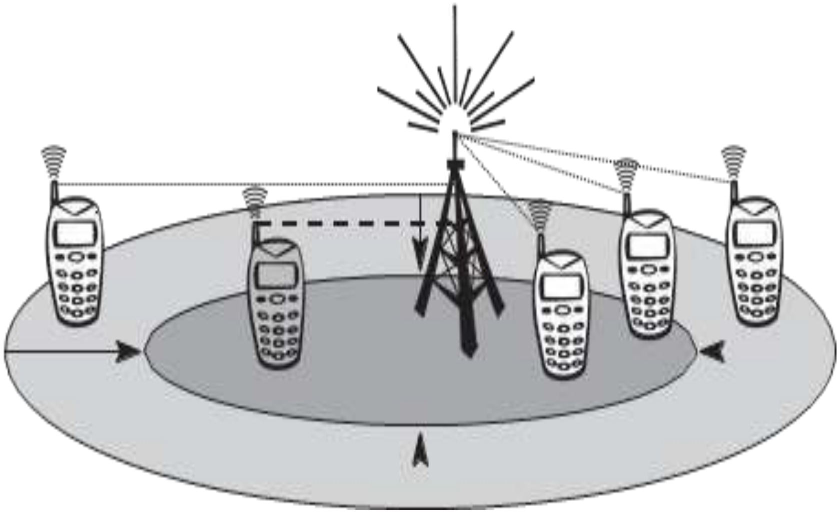
The fixed assignment of frequencies to cell clusters and cells respectively, is not very efficient if traffic load varies. For instance, in the case of a heavy load in one cell and a light load in a neighboring cell, it could make sense to 'borrow' frequencies. Cells with more traffic are dynamically allotted more frequencies. This scheme is known as **borrowing channel allocation (BCA)**, while the first fixed scheme is called **fixed channel allocation (FCA)**. FCA is used in the GSM system as it is much simpler to use, but it requires careful traffic analysis before installation.

A **dynamic channel allocation (DCA)** scheme has been implemented in DECT .In this scheme, frequencies can only be borrowed, but it is also possible to freely assign frequencies to cells. With dynamic assignment of frequencies to cells, the danger of interference with cells using the same frequency exists. The 'borrowed' frequency can be blocked in the surrounding cells.



Cellular system with three cell clusters and three sectors per cell

Cellular systems using CDM instead of FDM do not need such elaborate channel allocation schemes and complex frequency planning. Here, users are separated through the code they use, not through the frequency. Cell planning faces another problem – the cell size depends on the current load. Accordingly, CDM cells are commonly said to 'breathe'. While a cell can cover a larger area under a light load, it shrinks if the load increases. The reason for this is the growing noise level if more users are in a cell. The higher the noise, the higher the path loss and the higher the trans- mission errors. Finally, mobile stations further away from the base station drop out of the cell. (This is similar to trying to talk to someone far away at a crowded party.) Figure illustrates this phenomenon with a user transmit- ting a high bit rate stream within a CDM cell. This additional user lets the cell shrink with the result that two users drop out of the cell. In a real-life scenario this additional user could request a video stream (high bit rate) while the others use standard voice communication (low bit rate).



Cell breathing depending on the current load

CS8601 -MOBILE COMPUTING

UNIT 2

MOBILE TELECOMMUNICATION SYSTEM

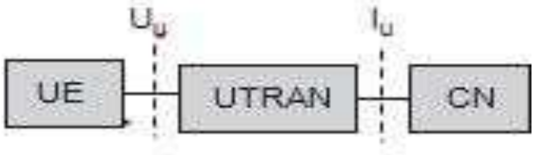
2.5. UMTS [UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM]

Figure shows the very simplified UMTS reference architecture which applies to both UTRA solutions (3GPP, 2000). The UTRA network (UTRAN) handles cell level mobility and comprises several radio network subsystems (RNS). The functions of the RNS include radio channel ciphering and deciphering, hand-over control, radio resource management etc. The UTRAN is connected to the user equipment (UE) via the radio interface Uu (which is comparable to the Um inter-face in GSM). Via the Iu interface (which is similar to the A interface in GSM),

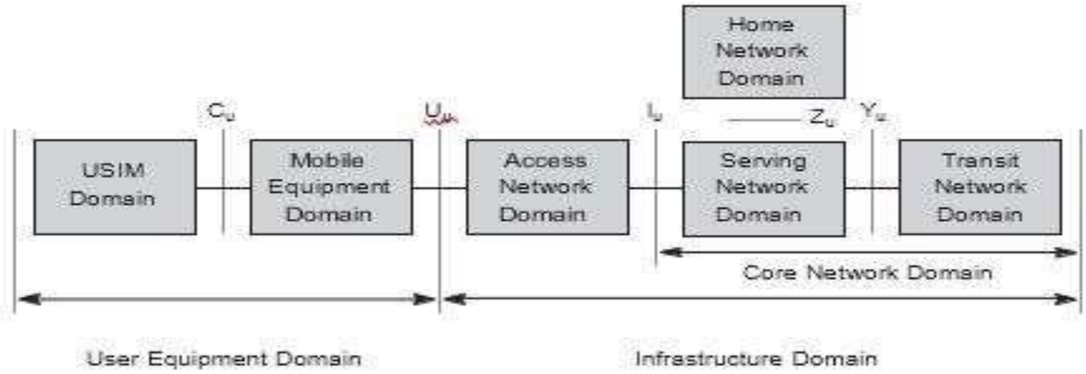
UTRAN communicates with the core network (CN). The CN contains functions for inter-system handover, gateways to other networks (fixed or wireless), and performs location management if there is no dedicated connection between UE and UTRAN.

UMTS further subdivides the above simplified architecture into so-called domains (see Figure). The user equipment domain is assigned to a single user and comprises all the functions that are needed to access UMTS services. Within this domain are the USIM domain and the mobile equipment domain. The USIM domain contains the SIM for UMTS which performs functions for encryption and authentication of users, and stores all the necessary user-related data for UMTS. Typically, this USIM belongs to a service provider and contains a microprocessor for an enhanced program execution environment (USAT, UMTS SIM application toolkit). The end device itself is in the mobile equipment domain. All functions for radio transmission as well as user interfaces are located here.

The infrastructure domain is shared among all users and offers UMTS services to all accepted users. This domain consists of the access network domain, which contains the radio access networks (RAN), and the core network domain, which contains access network independent functions. The core network domain can be separated into three domains with specific tasks. The serving network domain comprises all functions currently used by a user for accessing UMTS services. All functions related to the home network of a user, e.g., user data look-up, fall into the home network domain. Finally, the transit network domain may be necessary if, for example, the serving network cannot directly contact the home network. All three domains within the core network may be in fact the same physical network. These domains only describe functionalities.



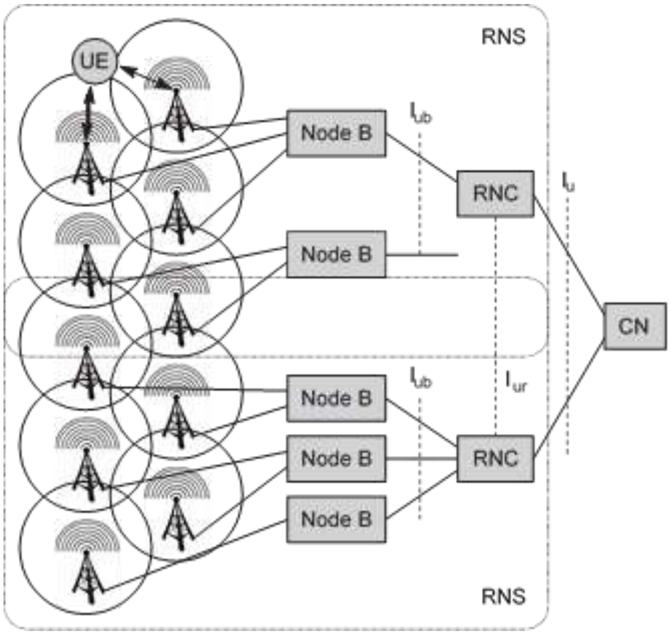
Main components of the UMTS reference architecture



UMTS domains and interfaces

UTRAN

Figure above shows the basic architecture of the UTRA network. This consists of several radio network subsystems (RNS). Each RNS is controlled by a radio network controller (RNC) and comprises several compo- nents that are called node B. An RNC in UMTS can be compared with the BSC; a node B is similar to a BTS. Each node B can control several antennas which make a radio cell. The mobile device, UE, can be connected to one or more antennas as will subsequently be explained in the context of handover. Each RNC is connected with the core network (CN) over the interface Iu (similar to the role of the A interface in GSM) and with a node B over the interface Iub. A new interface, which has no counterpart in GSM, is the interface Iur connecting two RNCs with each other. The use of this interface is explained together with the UMTS handover mechanisms.



Basic architecture of the UTRA network

Radio network controller

An RNC in UMTS has a broad spectrum of tasks as listed in the following:

- ***Call admission control:*** It is very important for CDMA systems to keep the interference below a certain level. The RNC calculates the traffic within each cell and decides, if additional transmissions are acceptable or not.

- ***Congestion control:*** During packet-oriented data transmission, several stations share the available radio resources. The RNC allocates bandwidth to each station in a cyclic fashion and must consider the QoS requirements.

- ***Encryption/decryption:*** The RNC encrypts all data arriving from the fixed network before transmission over the wireless link (and vice versa).

- ***ATM switching and multiplexing, protocol conversion:*** Typically, the connections between RNCs, node Bs, and the CN are based on ATM. An RNC has to switch the connections to multiplex different data streams. Several protocols have to be converted – this is explained later.

- ***Radio resource control:*** The RNC controls all radio resources of the cells connected to it via a node B. This task includes interference and load measurements. The priorities of different connections have to be obeyed.

- ***Radio bearer setup and release:*** An RNC has to set-up, maintain, and release a logical data connection to a UE (the so-called UMTS radio bearer).

- ***Code allocation:*** The CDMA codes used by a UE are selected by the RNC. These codes may vary during a transmission.

- ***Power control:*** The RNC only performs a relatively loose power control (the outer loop). This means that the RNC influences transmission power based on interference values from other cells or even other RNCs. But this is not the tight and fast power control performed 1,500 times per second. This is carried out by a node B. This outer loop of power control helps to minimize interference between neighbouring cells or controls the size of a cell.

- ***Handover control and RNS relocation:*** Depending on the signal strengths received by UEs and node Bs, an RNC can decide if another cell would be better suited for a certain connection. If the RNC decides for handover it informs the new cell and the UE as explained in subsection 4.4.6. If a UE moves further out of the range of one RNC, a new RNC responsible for the UE has to be chosen. This is called RNS relocation.

- ***Management:*** Finally, the network operator needs a lot of information regarding the current load, current traffic, error states etc. to manage its net- work. The RNC provides interfaces for this task, too.

Node B:

The name node B was chosen during standardization until a new and better name was found. However, no one came up with anything better so it remained. A node B connects to one or more antennas creating one or more cells (or sectors in GSM speak), respectively. The cells can either use FDD or TDD or both. An important task of a node B is the inner loop power control to mitigate near-far effects. This node also measures connection qualities and signal strengths. A node B can even support a special case of handover, a so-called softer handover which takes place between different antennas of the same node B .

User equipment:

The UE shown in Figure is the counterpart of several nodes of the architecture.

- ✓ As the counterpart of a node B, the UE performs signal quality measurements, inner loop power control, spreading and modulation, and rate matching.
- ✓ As a counterpart of the RNC, the UE has to cooperate during handover and cell selection, performs encryption and decryption, and participates in the radio resource allocation process.
- ✓ As a counterpart of the CN, the UE has to implement mobility management functions, performs bearer negotiation, or requests certain services from the network.

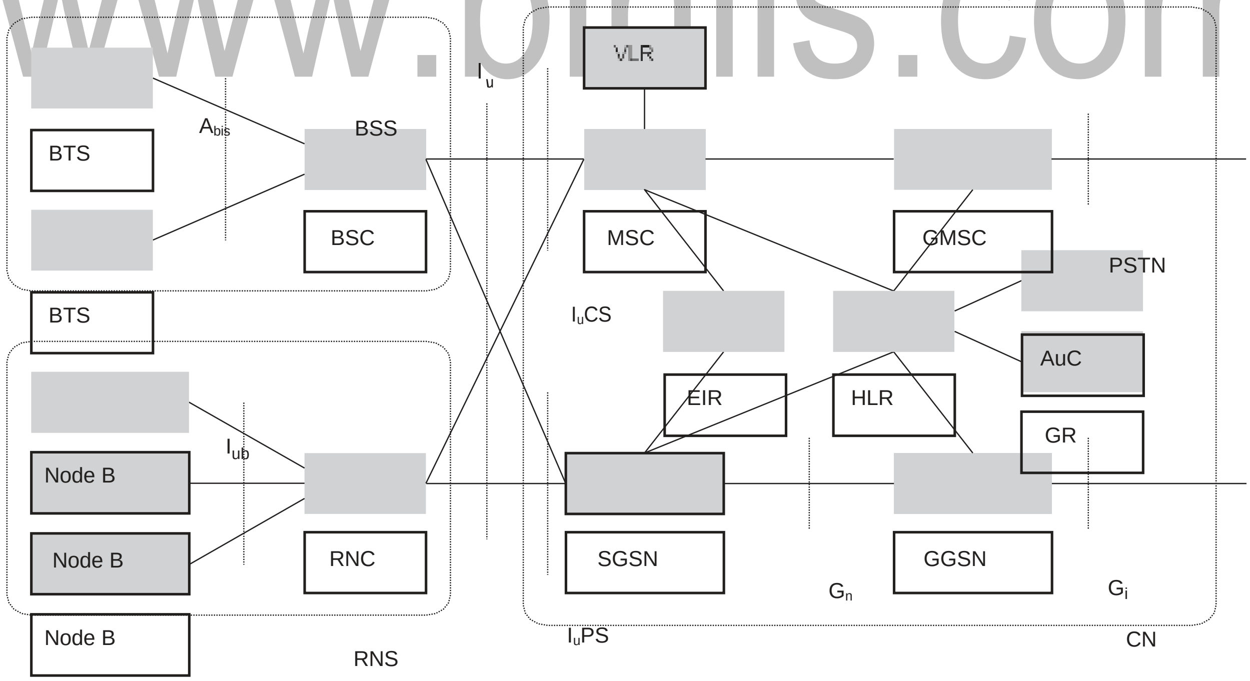
This list of tasks of a UE, which is not at all exhaustive, already shows the complexity such a device has to handle. Additionally, users also want to have organizers, games, cameras, operating systems etc. and the stand-by time should be high.

Core network:

Figure below shows a high-level view of the UMTS release 99 core network architecture together with a UTRAN RNS and a GSM BSS. This shows the evolution from GSM/GPRS to UMTS. The core network (CN) shown here is basically the same as already explained in the context of GSM and GPRS . The circuit switched domain (CSD) comprises the classical circuit switched services including signaling. Resources are reserved at connection setup and the GSM components MSC, GMSC, and VLR are used. The CSD connects to the RNS via a part of the Iu interface called IuCS. The CSD components can still be part of a classical GSM network connected to a BSS but need additional functionalities (new protocols etc.).

The packet switched domain (PSD) uses the GPRS components SGSN and GGSN and connects to the RNS via the IuPS part of the Iu interface. Both domains need the data-bases EIR for equipment identification and HLR for loca- tion management (including the AuC for authentication and GR for user specific GPRS data).

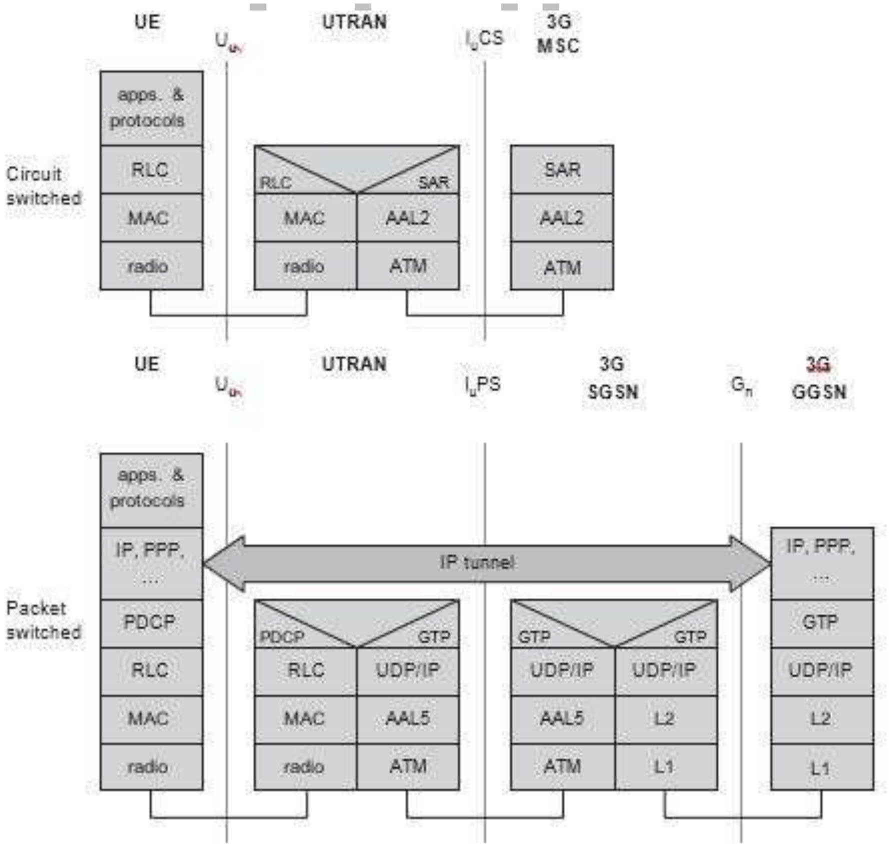
Reusing the existing infrastructure helps to save a lot of money and may convince many operators to use UMTS if they already use GSM. The UMTS industry pushes their technology with the help of the market dominance of GSM. This is basically the same as cdma2000, which is a evolution of cdmaOne. The real flexible core network comes with releases 5 and 6, where the GSM circuit switched part is being replaced by an all-IP core.



UMTS core network together with a 3G RNS and a 2G BSS

Figure below shows the protocol stacks of the users planes of the circuit switched and packet switched domains, respectively. The CSD uses the ATM adaptation layer 2 (AAL2) for user data transmission on top of ATM as trans- port technology. The RNC in the UTRAN implements the radio link control (RLC) and the MAC layer, while the physical layer is located in the node B. The AAL2 segmentation and reassembly layer (SAR) is, for example, used to segment data packets received from the RLC into small chunks which can be transported in ATM. AAL2 and ATM has been chosen, too, because these protocols can transport and multiplex low bit rate voice data streams with low jitter and latency (compared to the protocols used in the PSD).

In the PSD several more protocols are needed. Basic data transport is per- formed by different lower layers (e.g., ATM with AAL5, frame relay). On top of these lower layers UDP/IP is used to create a UMTS internal IP network. All packets (e.g., IP, PPP) destined for the UE are encapsulated using the GPRS tunneling protocol (GTP). The RNC performs protocol conversion from the combination GTP/UDP/IP into the packet data convergence protocol (PDCP). This protocol performs header compression to avoid redundant data transmission using scarce radio resources. In UMTS the RNC handles the tunneling protocol GTP, while in GSM/GPRS GTP is used between an SGSN and GGSN only. The BSC in GSM is not involved in IP protocol processing.



User plane protocol stacks (circuit and packet switched)

The radio layer (physical layer) depends on the UTRA mode . The medium access control (MAC) layer coordinates medium access and multiplexes logical channels onto transport channels. The MAC layers also help to identify mobile devices and may encrypt data. The radio link control (RLC) layer offers three different transport modes. The acknowledged mode transfer uses ARQ for error correction and guarantees one- time in-order delivery of data packets.The unacknowledged mode transfer does not perform ARQ but guarantees at least one-time delivery of packets with the help of sequence numbers. The transparent mode transfer simply forwards MAC data without any further processing. The system then has to rely on the FEC which is always used in the radio layer. The RLC also performs segmentation and reassembly and flow control. For certain services the RLC also encrypts.