5119 - PRIYADARSHINI ENGINEERING COLLEGE, VANIYAMBADI-635 751
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CS8601- MOBILE COMPUTING
UNIT II
MOBILE TELECOMMUNICATION SYSTEM

Introduction to Cellular Systems – GSM – Services & Architecture – Protocols – Connection Establishment – Frequency Allocation – Routing – Mobility Management – Security – GPRS- UMTS – Architecture – Handover – Security

INTRODUCTION TO CELLULAR SYSTEMS

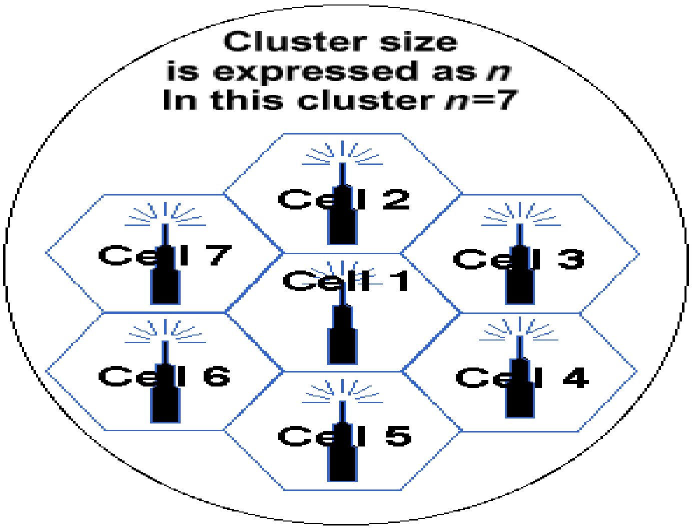
- Increases in demand and the poor quality of existing service led mobile service providers to research ways to improve the quality of service and to support more users in their systems.
- Because the amount of frequency spectrum available for mobile cellular use was limited, efficient use of the required frequencies was needed for mobile cellular coverage.
- In modern cellular telephony, rural and urban regions are divided into areas according to specific provisioning guidelines. Deployment parameters, such as amount of cell-splitting and cell sizes, are determined by engineers experienced in cellular system architecture.

Cells

- A cell is the basic geographic unit of a cellular system. The term cellular comes from the honeycomb shape of the areas into which a coverage region is divided.
- Cells are base stations transmitting over small geographic areas that are represented as hexagons. Each cell size varies depending on the landscape.
- Because of constraints imposed by natural terrain and man-made structures, the true shape of cells is not a perfect hexagon.

Clusters

A cluster is a group of cells. No channels are reused within a cluster. Figure illustrates a seven-cell cluster.

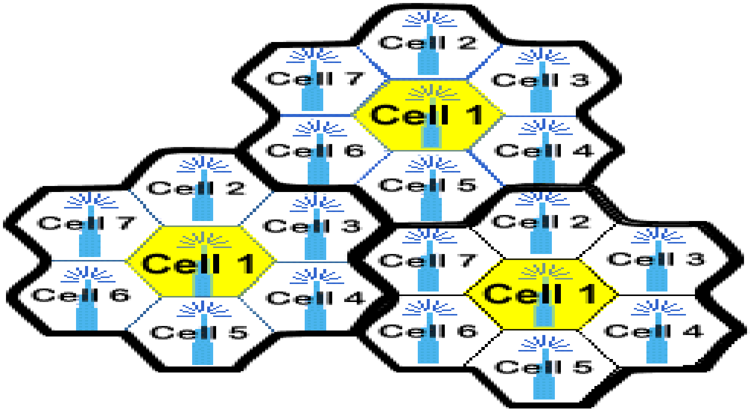


Frequency Reuse

- Because only a small number of radio channel frequencies were available for mobile systems, engineers had to find a way to reuse radio channels to carry more than one conversation at a time.
- The solution the industry adopted was called frequency planning or frequency reuse. Frequency reuse was implemented by restructuring the mobile telephone system architecture into the cellular concept.
- The concept of frequency reuse is based on assigning to each cell a group of radio channels used

within a small geographic area.

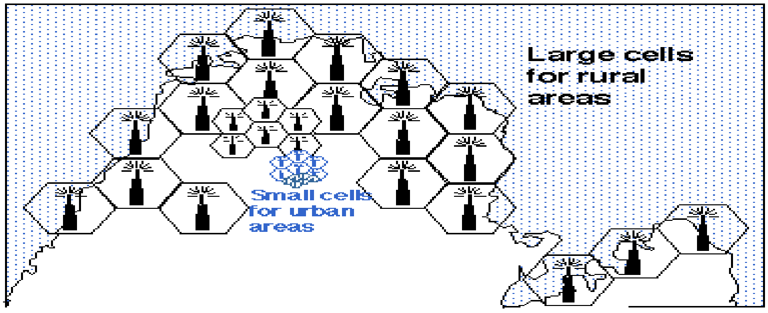
- Cells are assigned a group of channels that is completely different from neighboring cells. The coverage area of cells is called the footprint.
- This footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere.



Cells with the same number have the same set of frequencies. Here, because the number of available frequencies is 7, the frequency reuse factor is 1/7. That is, each cell is using 1/7 of available cellular channels.

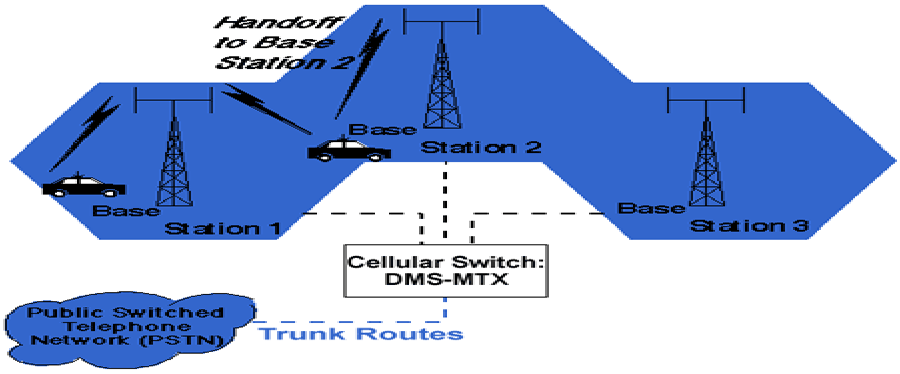
Cell Splitting

- Unfortunately, economic considerations made the concept of creating full systems with many small areas impractical.
- To overcome this difficulty, system operators developed the idea of cell splitting. As a service area becomes full of users, this approach is used to split a single area into smaller ones.
- In this way, urban centers can be split into as many areas as necessary to provide acceptable service levels in heavy-traffic regions, while larger, less expensive cells can be used to cover remote rural regions.



Handoff

- The final obstacle in the development of the cellular network involved the problem created when a mobile subscriber traveled from one cell to another during a call.
- As adjacent areas do not use the same radio channels, a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells.
- Because dropping the call is unacceptable, the process of handoff was created. Handoff occurs when the mobile telephone network automatically transfers a call from radio channel to radio channel as a mobile crosses adjacent cells.

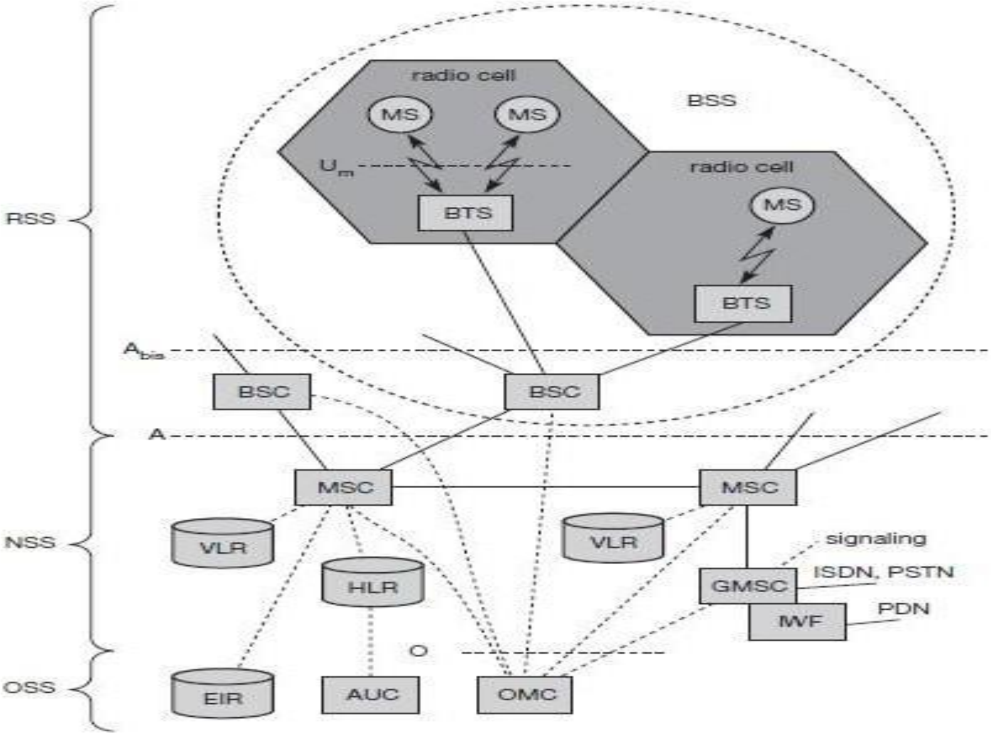


- During a call, two parties are on one voice channel. When the mobile unit moves out of the coverage area of a given cell site, the reception becomes weak.
- At this point, the cell site in use requests a handoff. The system switches the call to a stronger-frequency channel in a new site without interrupting the call or alerting the user.
- The call continues as long as the user is talking, and the user does not notice the handoff at all.

GSM

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).



Functional Architecture of a GSM System

<u>Network Switching Subsystem</u>: The NSS is responsible for performing call processing and subscriber related functions. The switching system includes the following functional units:

<u>Home location register (HLR)</u>: 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, he or she is registered in the HLR of that operator.

Visitor location register (VLR): It is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. VLR is always integrated with the MSC. When a MS roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later if the mobile station needs to make a call, VLR will be having all the information needed for call setup.

- 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).

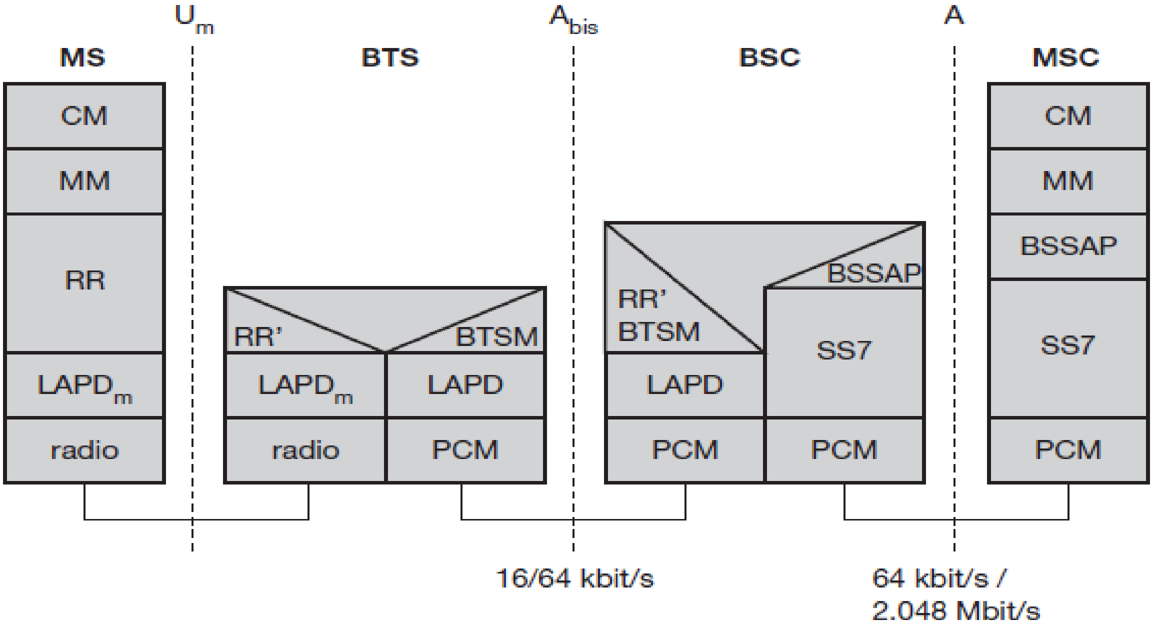
- Base station subsystem (BSS): A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS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

GSM PROTOCOLS

- The 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 qualit**y 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, re-sequencing 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 traditional analog telephone systems.
- Additional protocols are used at the Abis and A interfaces. Data transmission at the physical layer typically uses **pulse code 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

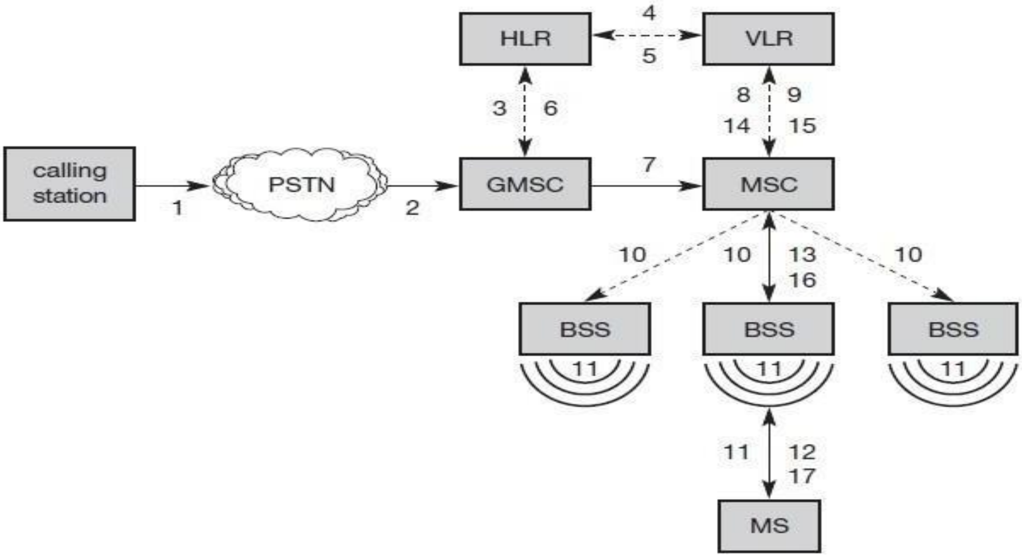
- The fundamental feature of the GSM system is the automatic, worldwide localization of users for which, the system performs periodic location updates.
- The HLR always contains information about the current location and the VLR currently responsible for the MS informs the HLR about the location changes.
- 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:



Mobile Terminated Call (MTC)

step 1: User dials the phone number of a GSM subscriber.

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

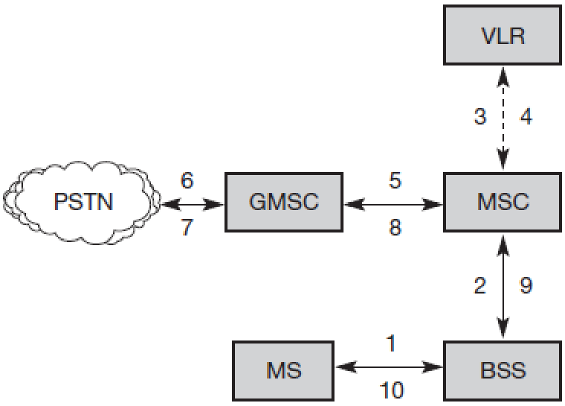
step 10: If MS is available, the MSC initiates paging in all cells it is responsible for.

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:

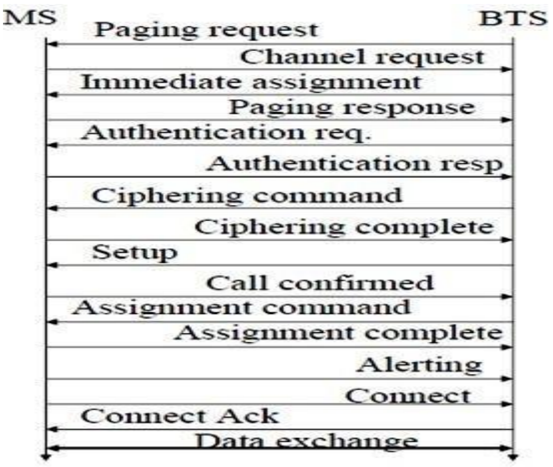


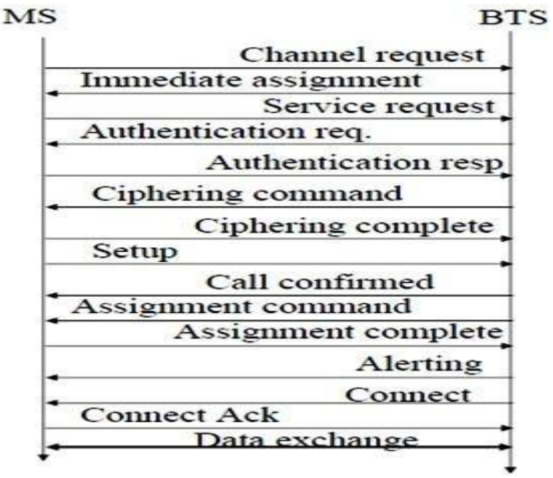
step 1: The MS transmits a request for a new connection

step 2: The BSS forwards this request to the MSC

step 3: 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).

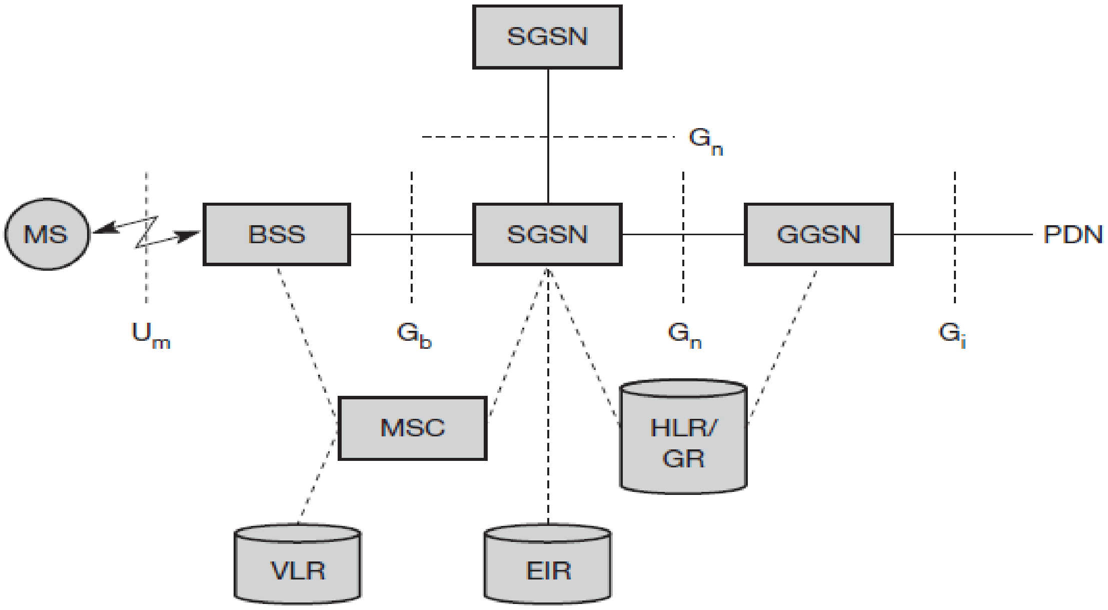




GPRS

- The **general packet radio service (GPRS)** provides packet mode transfer for applications that exhibit traffic patterns such as frequent transmission of small 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. All time 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 IP- based 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), and performs several security functions such as access control.
- The SGSN is connected to a BSC via frame relay and is basically on the same hierarchy level as an MSC. The GR, which is typically a part of the HLR, stores all GPRS-relevant data.

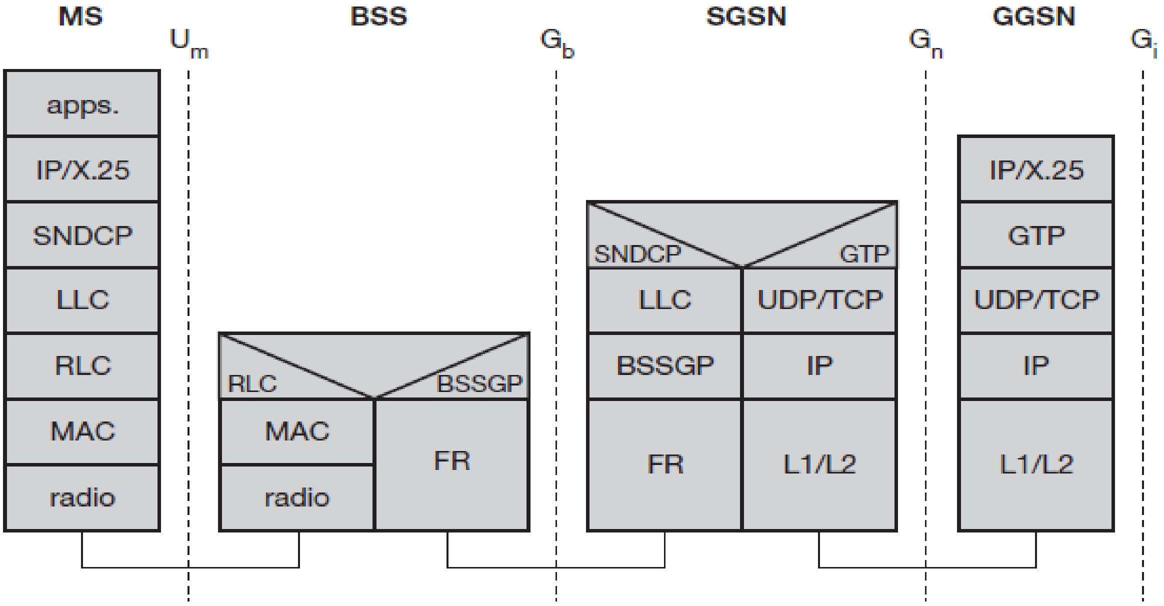


GPRS Architecture Reference Model

- 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 signalling 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

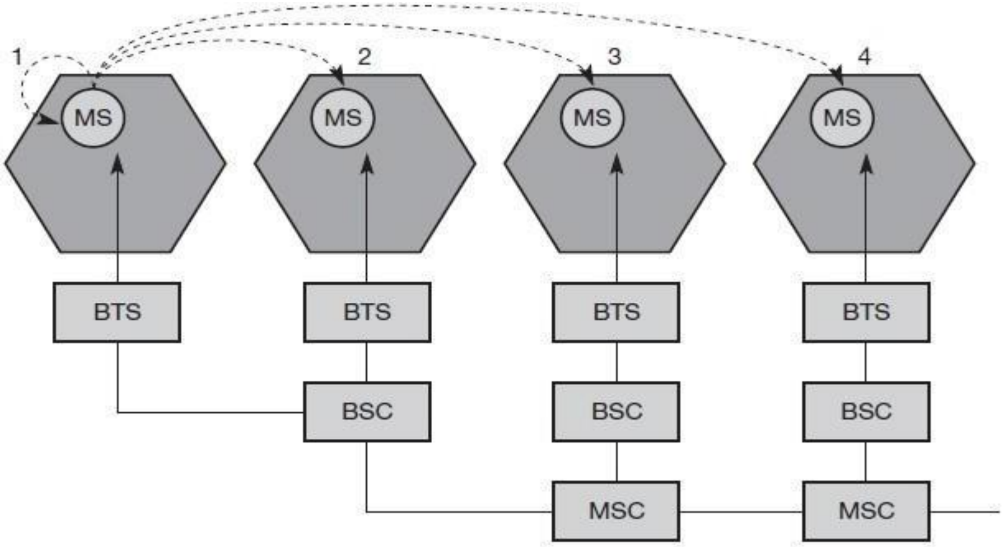
- A base station subsystem GPRS protocol (BSSGP) is used to convey routing and QoS- related information between the BSS and SGSN.
- BSSGP does not perform error correction and works on top of a frame relay (FR) network.
- Finally, radio link dependent protocols are needed to transfer data over the Um 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.

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 at maximum handover duration of 60 ms. There are two basic reasons for a handover:

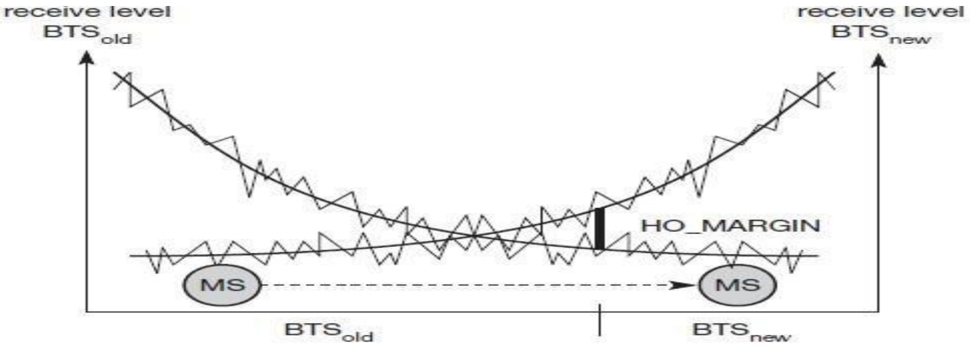
1. The mobile station **moves out of the range** of a BTS, decreasing the received **signal level** increasing the **error rate** thereby diminishing the **quality of the radio link.**
2. Handover may be due to **load balancing,** when an MSC/BSC decides the traffic is too high in one cell and shifts some MS to other cells with a lower load.

The four possible handover scenarios of GSM are shown below:

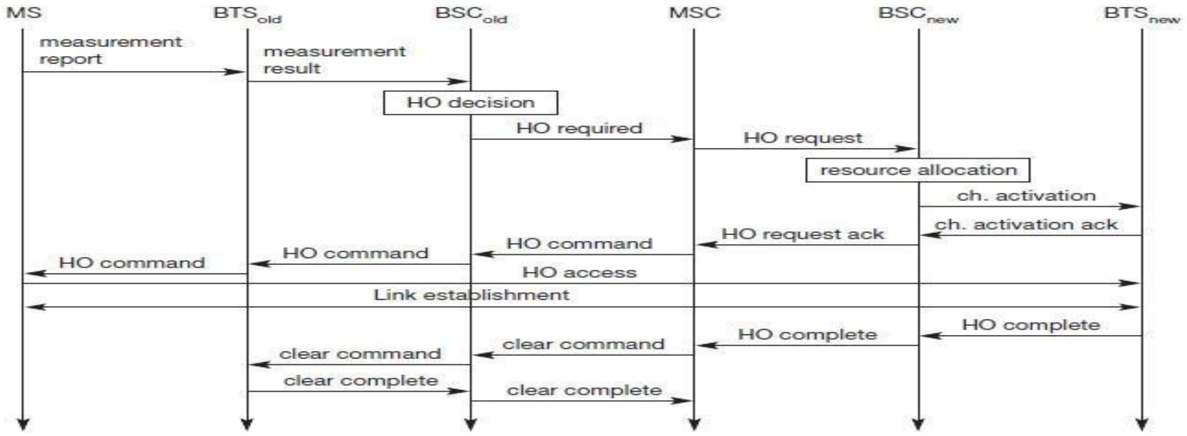


- **Intra-cell handover:** Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).
- **Inter-cell, intra-BSC handover:** This is a typical handover scenario. The mobile station moves from 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



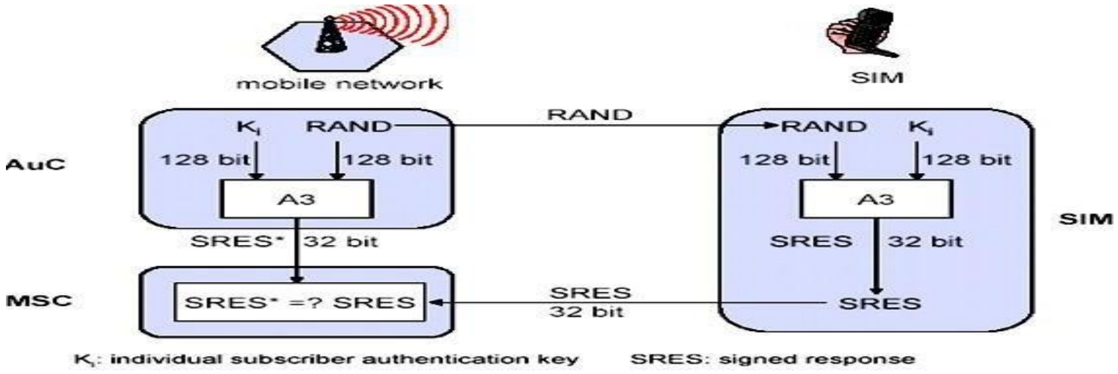
Intra-MSChandover

More sophisticated handover mechanisms are needed for seamless handovers between different systems.

SECURITY

- GSM offers several security services using confidential information stored in the AuC and 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:

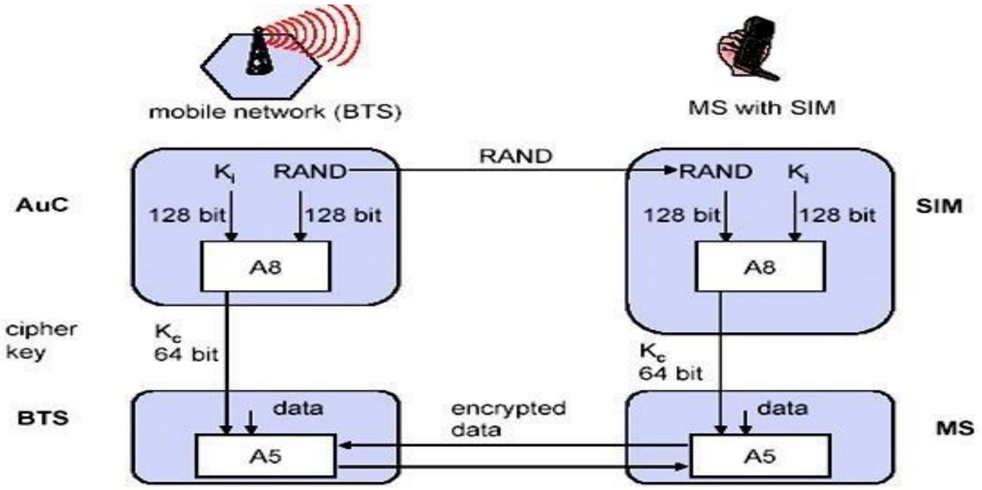
Access control and authentication: The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber authentication. This step is based on a challenge-response scheme as shown below:



Subscriber Authentication

- Authentication is based on the SIM, which stores the **individual 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.

Confidentiality: All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, 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.