UNIT I
Introduction

Syllabus: Mobile Communications, Mobile Computing – Paradigm, Promises/Novel Applications and Impediments and Architecture; Mobile and Handheld Devices, Limitations of Mobile and Handheld devices.
GSM – Services, System Architecture, Radio Interfaces, Protocols, Localization, Calling, Handover, Security, New Data Services, GPRS.

Mobile Communications:

- A communication network (either public or private) which doesn't depend on any physical connection between two communication entities and have flexibility to be mobile during communication.
- There are two different kinds of mobility: **User mobility** and **Device portability**.
- **User mobility:**
  - A user who has access to the same or similar telecommunication services at different places, i.e., the user can be mobile, and the services will follow him or her.
  - Examples for mechanisms supporting user mobility are simple call-forwarding solutions known from the telephone or computer desktops supporting roaming
- **Device portability**:
  - The communication device moves (with or without a user). Many mechanisms in the network and inside the device have to make sure that communication is still possible while the device is moving.
  - A typical example for systems supporting device portability is the mobile phone system, where the system itself hands the device from one radio transmitter (also called a base station) to the next if the signal becomes too weak.
- Wireless communication means "way of accessing a network or other communication partners, i.e., without a wire. The wire is replaced by the transmission of electromagnetic waves through the air".
- A **communication device** can thus exhibit one of the following **characteristics**:
  - **Fixed and wired:** Typical desktop computer(fixed) connected with wired medium in home or office.
  - **Mobile and wired:** Laptops (movable) connected with wired medium.
  - **Fixed and wireless:** Fixed wireless refers to the operation of **wireless devices** or systems in **fixed** locations such as homes and offices.
  - **Mobile and wireless:** Mobile user roam between different wireless networks. example for this category is GSM.

Applications of Mobile Computing:

- Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.
- Mobile computing applications are,
    - Vehicles
    - Emergencies
    - Business
    - Replacement of wired networks
    - Infotainment and more
    - Location dependent services

Vehicles:

- Today's Vehicles will comprise many wireless communication systems and mobility aware applications.
- Music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB) with 1.5 Mbit/s.
- For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384 Kbit/s.
- For remote areas, satellite communication can be used, while the current position of the car is determined via the global positioning system (GPS).
- In case of an accident, not only will the airbag be triggered, but the police and ambulance service will be informed via an emergency call to a service provider.

Emergencies:

- If an ambulance with a high-quality wireless connection to a hospital, then vital information about injured persons can be sent to the hospital from the scene of the accident.
- All the necessary steps for this particular type of accident can be prepared and specialists can be consulted for an early diagnosis.
- Wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes.

Business:

- A travelling salesman today needs instant access to the company's database: to ensure that files on his or her laptop reflect the current situation, to enable the company to keep track of all activities of their travelling employees, to keep databases consistent etc.
- With wireless access, the laptop can be turned into a true mobile office, but efficient and powerful synchronization mechanisms are needed to ensure data consistency.

Replacement of wired networks:

- In some cases, wireless networks can also be used to replace wired networks, e.g., remote sensors, for tradeshows, or in historic buildings.

- Due to economic reasons, it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information. Wireless connections, e.g., via satellite, can help in this situation.

Infotainment and more:

- Internet everywhere? Not without wireless networks! Imagine a travel guide for a city.
- Static information might be loaded via CD-ROM, DVD, or even at home via the Internet. But wireless networks can provide up-to-date information at any appropriate location.
- We may choose a seat, pay via electronic cash, and send this information to a service provider.
- Another growing field of wireless network applications lies in entertainment and games.

Location dependent services:

- In many cases, however, it is important for an application to 'know' something about the location or the user might need location information for further activities.
- Several services that might depend on the actual location those are:
  1. Follow-on services
  2. Location aware services
  3. Privacy services
  4. Information services
  5. Support services

Limitations of Mobile Computing

- **Insufficient Bandwidth:**
  Mobile Internet access is generally slower than direct cable connections, using technologies such as GPRS and EDGE, and more recently 3G networks. These networks are usually available within range of commercial cell phone towers.
- **Security Standards:**
  When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards on the fleet. One can easily attack the VPN through a huge number of networks interconnected through the line.
- **Power consumption**:
  When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power.
- **Transmission interferences**:
  Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.

- **Potential health hazards:**
  People who use mobile devices while driving are often distracted from driving are thus assumed more likely to be involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
- **Human interface with device:**
  Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

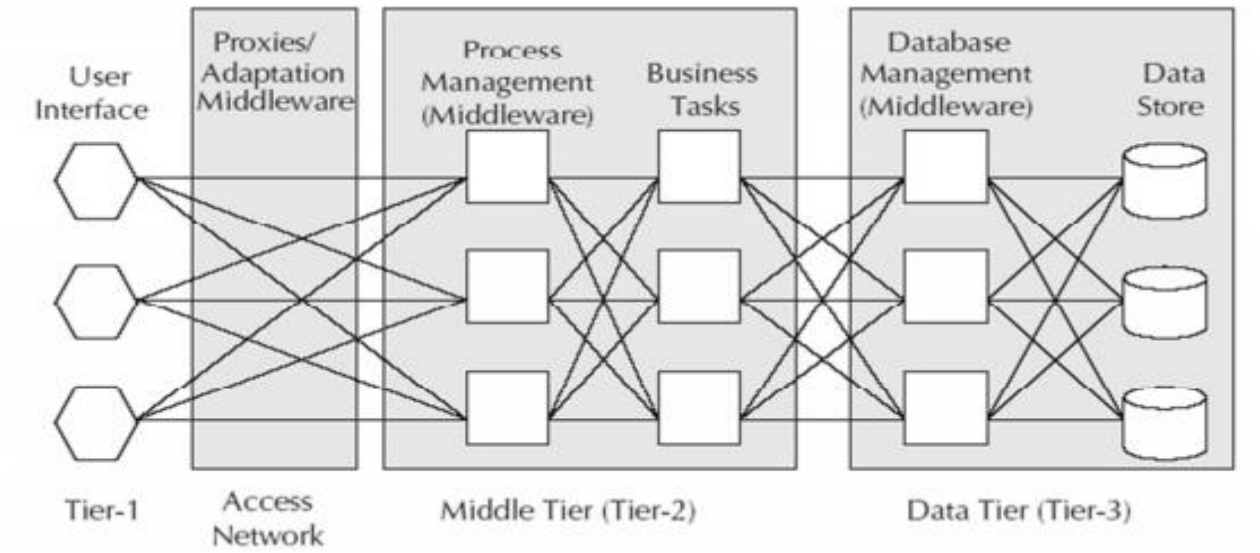
Mobile and Handheld Devices:

The following list gives some examples of mobile and wireless devices graded by increasing performance (CPU, memory, display, input devices etc.).

- **Sensor**:
  - A very simple wireless device is represented by a sensor transmitting state information. One example could be a switch sensing the office door.
  - If the door is closed, the switch transmits this to the mobile phone inside the office which will not accept incoming calls.
- **Embedded controllers**:
  - Many appliances already contain a simple or sometimes more complex controller. Keyboards, mice, headsets, washing machines, coffee machines, hair dryers and TV sets are just some examples.
- **Pager**:
  - As a very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages.
  - Pagers can even be integrated into watches. The tremendous success of mobile phones, has made the pager virtually redundant in many countries.
- **Mobile phones**:
  - The traditional mobile phone only had a simple black and white text display and could send/receive voice or short messages.
  - Today, mobile phones migrate more and more toward PDAs. Mobile phones with full color graphic display, touch screen, and Internet browser are easily available.
- **Personal digital assistant**:
  - PDAs typically accompany a user and offer simple versions of office software (calendar, note-pad, mail). The typical input device is a pen, with built-in character recognition translating handwriting into characters.
  - Web browsers and many other software packages are available for these devices.
- **Pocket computer**:
  - The next steps toward full computers are pocket computers offering tiny keyboards, color displays, and simple versions of programs found on desktop computers (text processing, spreadsheets etc.).
- **Notebook/laptop**:
  - Finally, laptops offer more or less the same performance as standard desktop computers; they use the same software – the only technical difference being size, weight, and the ability to run on a battery.

- If operated mainly via a sensitive display (touch sensitive or electromagnetic), the devices are also known as notepads or tablet PCs.

Mobile Computing Architecture:



Three-tier Architecture for Mobile Computing

Presentation Tier (Tier-1)

- This is the layer of agent applications and systems. These applications run on the client device and offer all the user interfaces.
- This tier is responsible for presenting the information to the end user. The visual presentation will relate to rendering on a screen. 'Presentation Tier' includes web browsers, WAP browsers and customized client programs.

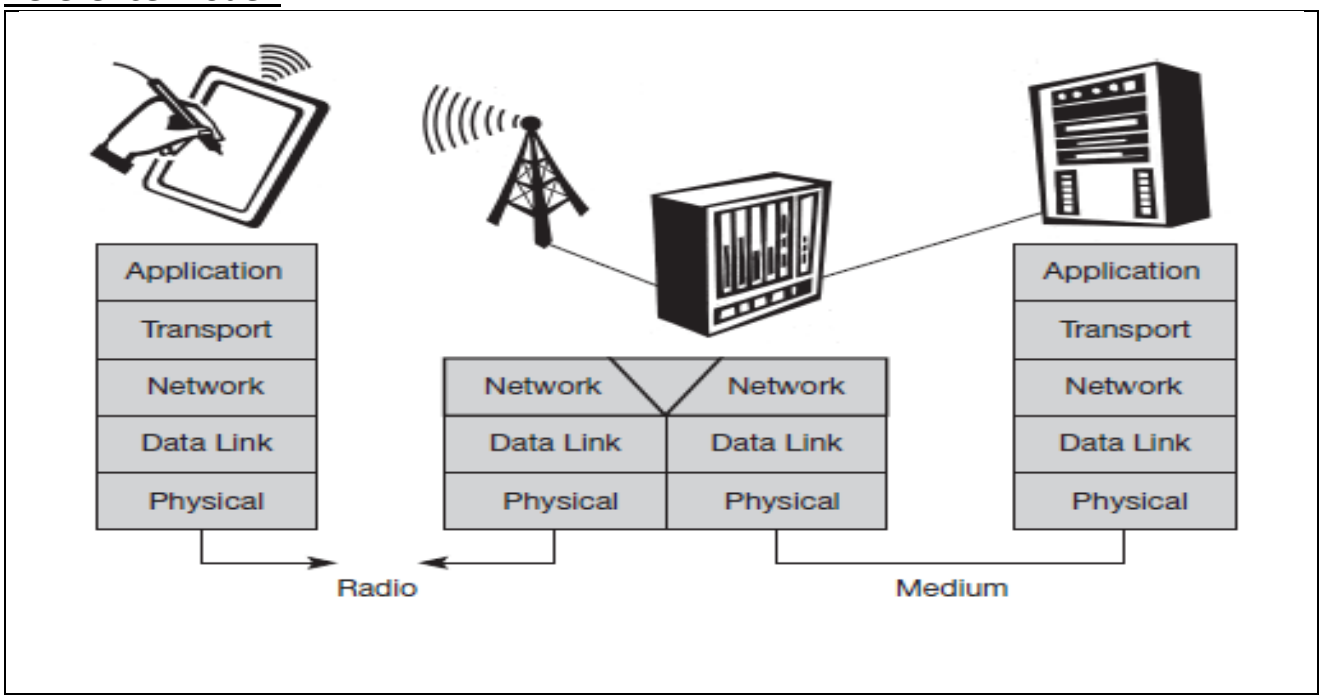
Application Tier (Tier-2)

- The application tier or middle tier is the "engine" of a ubiquitous application. It performs the business logic of processing user input, obtaining data and making decisions.
- In certain cases, this layer will do the transcoding of data for appropriate rendering in the Presentation Tier. The application tier may include technology lie CGIs, Java, JSP, .NET Services, PHP, etc. deployed in Apache, WebSphere, WebLogic, Pramati, etc.
- The application tier is presentation and database independent. A middleware framework is defined as a layer of software, which sits in the middle between the OS and the user facing software.

Data Tier (Tier-3)

- It is used to store data needed by the application and acts as a repository for both temporary and permanent data. The data can be stored in any form of data store or database.
- These can range from sophisticated relational database, legacy hierarchical database, to even simple text files.
- The data can also be stored in XML format for interoperability with other systems and data sources.
- A legacy application can also be considered as a data source or document through a communication middleware.

Reference Model:



- **Physical layer**:
  - This is the lowest layer in a communication system and is responsible for the conversion of a stream of bits into signals that can be transmitted on the sender side.
  - The physical layer of the receiver then transforms the signals back into a bit stream.
  - For wireless communication, the physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection, modulation of data onto a carrier frequency and encryption.
- **Data link layer**:
  - The main tasks of this layer include accessing the medium, multiplexing of different data streams, correction of transmission errors, and synchronization (i.e., detection of a data frame).
  - The data link layer is responsible for a reliable point-to-point connection between two devices or a point-to-multipoint connection between one sender and several receivers.

- **Network layer**:
  - This third layer is responsible for routing packets through a network or establishing a connection between two entities over many other intermediate systems.
- **Transport layer**:
  - This layer is used in the reference model to establish an end-to-end connection.
  - Topics like quality of service, flow and congestion control are relevant, especially if the transport protocols known from the Internet, TCP and UDP, are to be used over a wireless link.
- **Application layer**:
  - Finally, the applications are situated on top of all transmission oriented layers.
  - Topics of interest in this context are service location, support for multimedia applications, adaptive applications that can handle the large variations in transmission characteristics, and wireless access to the world wide web using a portable device.

Generations of Mobile Communications:

1G

- It is the first generation cellular network that existed in 1990's.
- It transfer data in analog wave, it has limitation because there are no encryption, the sound quality is poor and the speed of transfer is only 9.6 kbps.

2G

- It is the second generation, improved by introducing the concept of digital modulation, which means converting the voice into digital code and then into analog signals.
- Being over limitation 1G, such as it omits the radio power from handsets making life healthier, and it has enhanced privacy.

2.5G

- It is a transition of 2G and 3G.
- In 2.5G, the most popular services like SMS, GPRS, EDGE, high speed circuit switched data and more had been introduced.

3G

- It is the current generation of mobile telecommunication standards.
- It allows use of speech and data services and offers data rates up to 2 mbps, which provide services like video calls, mobile TV, mobile internet and downloading.
- There are bunch of technologies that fall 3G, like WCDMA, EV-DO, and HSPA etc.

4G

- It is the fourth generation of cellular wireless standards. It is a successor to the 3G and 2G families of standards.
- In 2008, the ITU-R organization specifies the IMT Advanced (International Mobile Telecommunication Advanced) requirements for 4G standards, setting peak speed requirements for 4G service at 100 Mbit/s for high mobility communication and 1 Gbit/s for low mobility communication.

Gen.	Definition	Throughput/ Speed	Technology	Features
1G (1970 to 1980)	Analog	14.4 Kbps (peak)	AMPS,NMT, TACS	• During 1G Wireless phones are used for voice only.
2G (1990 to 2000)	Digital Narrow band circuit data	9.6/14.4 Kbps	TDMA,CDMA	• 2G capabilities are achieved by allowing multiple users on a single channel via multiplexing. • During 2G Cellular phones are used for data also along with voice.
2.5G (2001 to 2004)	Packet Data	171.2 Kbps(peak) 20-40 Kbps	GPRS	• In 2.5G the internet becomes popular and data becomes more relevant.2.5G Multimedia services and streaming starts to show growth. • Phones start supporting web browsing through limited and very few phones have that.
3G (2004 to 2005)	Digital Broadband Packet Data	3.1 Mbps (peak) 500-700 Kbps	CDMA 2000 (1xRTT, EVDO) UMTS, EDGE	• 3G has Multimedia services support along with streaming are more popular.In 3G, Universal access and portability across different device types are made possible. (Telephones, PDA's, etc.)
3.5G (2006 to 2010)	Packet Data	14.4 Mbps (peak) 1-3 Mbps	HSPA	• 3.5G supports higher throughput and speeds to support higher data needs of the consumers.
4G (Now (Read more on Transition ing to 4G)	Digital Broadband Packet All IP Very high throughput	100-300 Mbps (peak) 3-5 Mbps 100 Mbps (Wi-Fi)	WiMax LTE Wi-Fi	• Speeds for 4G are further increased to keep up with data access demand used by various services. • High definition streaming is now supported in 4G. New phones with HD capabilities surface. It gets pretty cool. • In 4G, Portability is increased further. World-wide roaming is not a distant dream.

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.
- In the early 1980s, Europe had numerous coexisting analog mobile phone systems, which were often based on similar standards (e.g., NMT 450), but ran on slightly different carrier frequencies.
- To avoid this situation for a second generation fully digital system, the **Group Special Mobile (GSM)** was founded in 1982.
- This system was soon named the **Global System for Mobile Communications (GSM).**

GSM Services:

- GSM permits the integration of different voice and data services and the interworking with existing networks.
- GSM has defined three different categories of services:

- A reference model for GSM services. A **mobile station MS** is connected to the **GSM public land mobile network (PLMN)** via the Um interface. (GSM-PLMN is the infrastructure needed for the GSM network.)
- This network is connected to transit networks, e.g., **integrated services digital network (ISDN)** or traditional **public switched telephone network (PSTN)**.

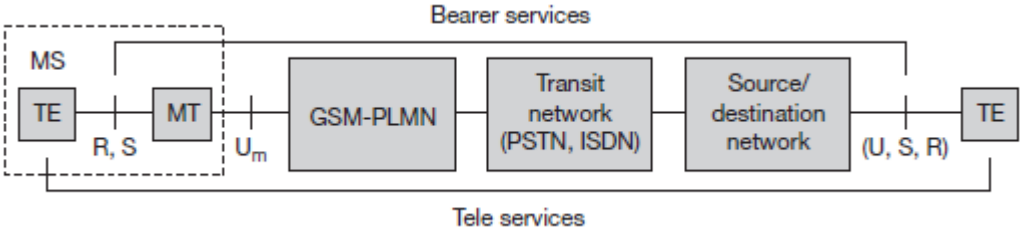


Fig: Bearer and tele services Reference model

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.

- The only mechanism to increase transmission quality is the use of **forward error correction (FEC)**.
- 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)**.
- 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

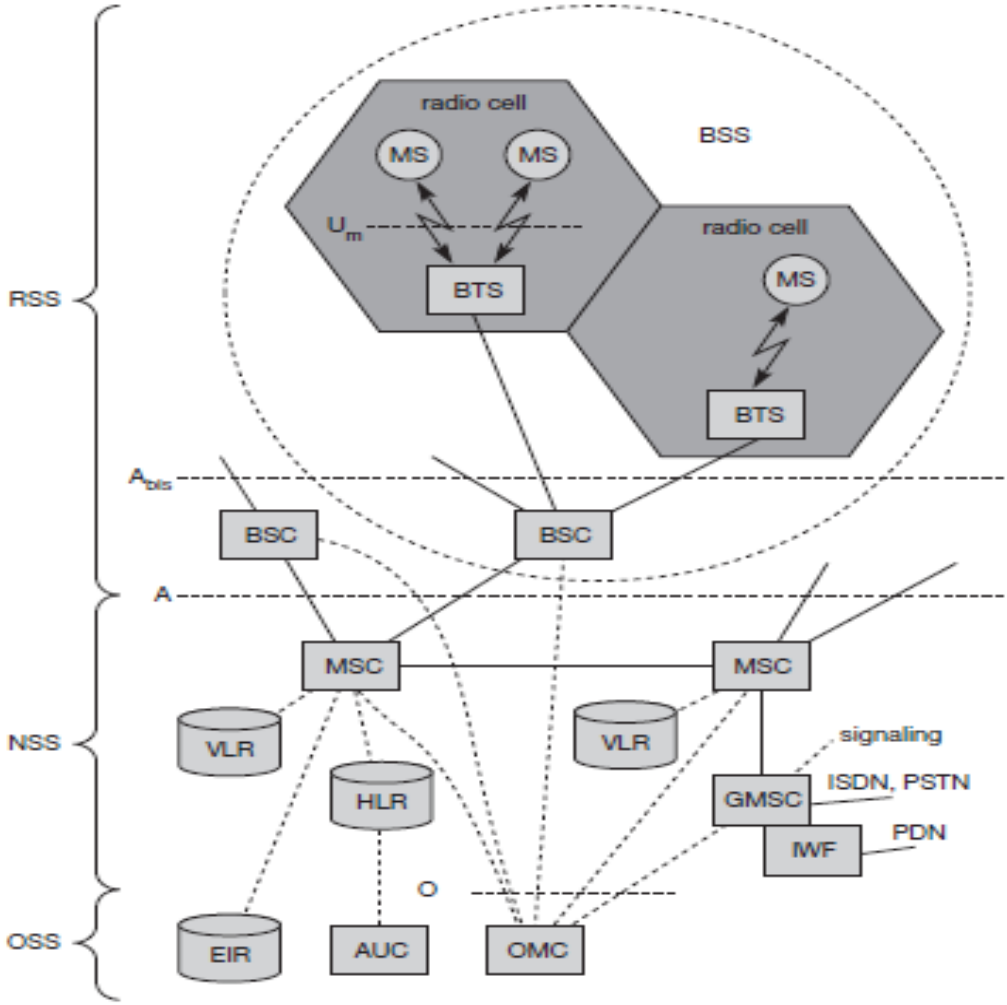
- GSM mainly focuses on voice-oriented tele services. These comprise encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN.
- However, as the main service is **telephony**, the primary goal of GSM was the provision of high-quality digital voice transmission, offering at least the typical bandwidth of 3.1 kHz of analog phone systems.
- 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**.
- A useful service for very simple message transfer is the **short message service (SMS)**, which offers transmission of messages of up to 160 characters.
- The successor of SMS, the **enhanced message service (EMS)**, offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures, small images and ring tones in a standardized.
- EMS never really took off as the **multimedia message service (MMS)** was available.
- **MMS** offers the transmission of larger pictures (GIF, JPG, WBMP), short video clips etc. and comes with mobile phones that integrate small cameras.

Supplementary services

- In addition to tele and bearer services, GSM providers can offer **supplementary services**.
- Similar to ISDN networks, 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. Standard ISDN features such as **closed user groups** and **multiparty** communication may be available.

GSM System Architecture:

- GSM architecture consists of mainly 3-parts.
  - **RSS:** Radio Subsystem
  - **NSS:** Network and Switching Subsystem
  - **OSS:** Operation Subsystem



RSS: Radio Subsystem:

- The **radio subsystem (RSS)** comprises all radio specific entities, i.e.,
  - **Mobile stations (MS)**
  - **Base station subsystem (BSS)**.
- 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 transceiver station (BTS)**:
  - A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission.
  - A BTS can form a radio cell or, using sectorized antennas, several and is connected to MS via the **Um interface** (ISDN U interface for mobile use), and to the BSC via the **Abis interface**.
  - The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.) and will be discussed in more detail below.
  - The Abis interface consists of 16 or 64 kbit/s connections.
  - A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.
- **Base station controller (BSC)**:
  - The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS.
  - The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS)**:
  - The MS comprises all user equipment and software needed for communication with a GSM network.
  - MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is relevant to GSM.
  - While an MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself.
  - Device-specific mechanisms, e.g., theft protection, use the device specific IMEI.
  - Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a **personal identity number (PIN)**, a **PIN unblocking key (PUK)**, an **authentication key Ki**, and the **international mobile subscriber identity (IMSI)**.
  - The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM.
  - The MS stores dynamic information while logged onto the GSM system, such as, e.g., the **cipher key Kc** and the location information consisting of a **temporary mobile subscriber identity (TMSI)** and the **location area identification (LAI)**.

NSS: Network and Switching Subsystem:

- The "heart" of the GSM system is formed by the **network and switching subsystem (NSS)**.
- The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries.

- The NSS consists of the following switches and databases:

Mobile services switching center (MSC):

- MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system.
- Typically, an MSC manages several BSCs in a geographical region. A **gateway MSC (GMSC)** has additional connections to other fixed networks, such as **PSTN** and **ISDN**
- Using additional **interworking functions (IWF)**, an MSC can also connect to **public data networks (PDN)** such as X.25.
- MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs.
- The **standard signaling system No. 7 (SS7)** is used for this purpose. SS7 covers all aspects of control signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls).
- Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.

Home location register (HLR):

- The HLR is the most important database in a GSM system as it stores all user-relevant information.
- This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI)**.
- Dynamic information is also needed, e.g., the current **location area (LA)** of the MS, the **mobile subscriber roaming number (MSRN)**, the current VLR and MSC.
- As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network.
- HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.

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.
- The typical use of HLR and VLR for user localization will be described in section 4.1.5. Some VLRs in existence, are capable of managing up to one million customers.

OSS: Operation Subsystem:

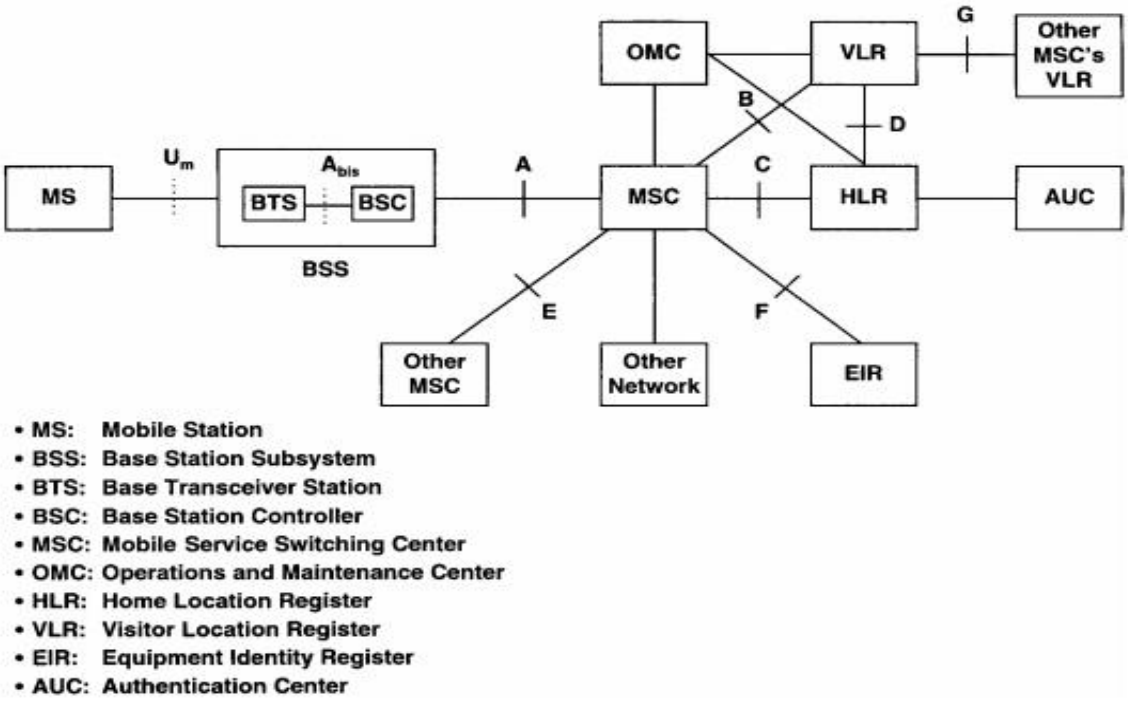
- The third part of a GSM system, the **operation subsystem (OSS)**, contains the necessary functions for network operation and maintenance.
- The OSS possesses network entities of its own and accesses other entities via SS7.

- **Operation and maintenance center (OMC)**:
  - The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.
  - OMCs use the concept of **telecommunication management network (TMN)** as standardized by the ITU-T.
- **Authentication center (AuC)**:
  - As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission.
  - The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR.
- **Equipment identity register (EIR)**:
  - The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network.
  - As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices.
  - The blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible.
  - The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

Radio Interfaces:

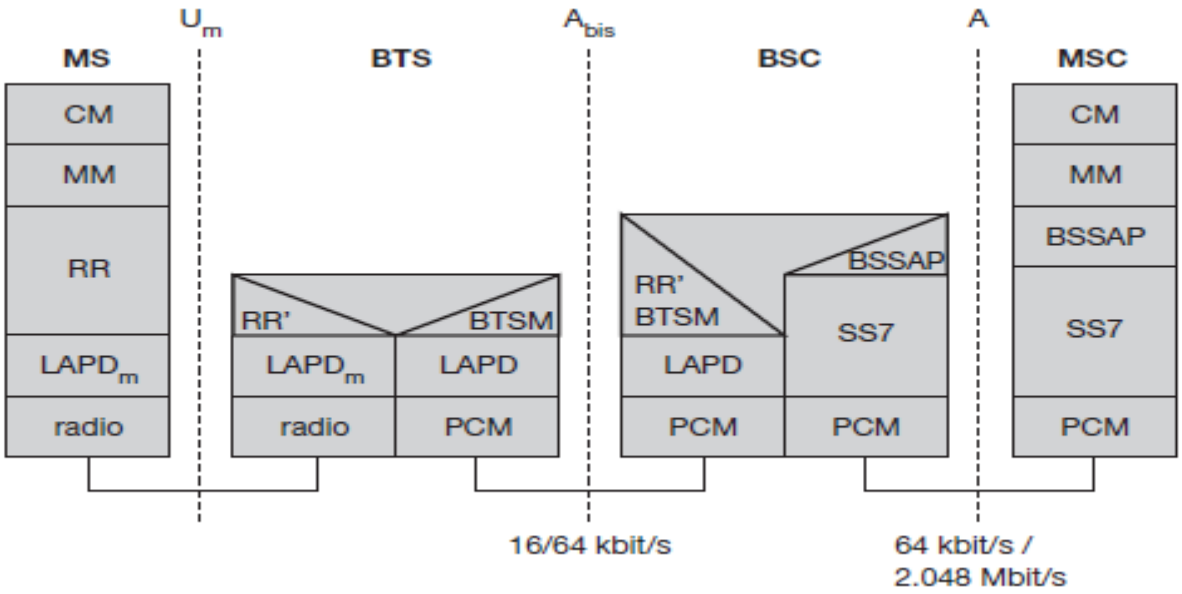
- The network structure is defined within the GSM standards. Additionally, each interface between the different elements of the GSM network is also defined.

1. ***Um interface***:The "air" or radio interface standard that is used for exchanges between a mobile (ME) and a base station (BTS / BSC). For signaling, a modified version of the ISDN LAPD, known as LAPDm is used.
2. ***Abis interface***: This is a BSS internal interface linking the BSC and a BTS, and it has not been totally standardized. The Abis interface allows control of the radio equipment and radio frequency allocation in the BTS.
3. ***A interface*** : The A interface is used to provide communication between the BSS and the MSC. The interface carries information to enable the channels, timeslots and the like to be allocated to the mobile equipments being serviced by the BSSs. The messaging required within the network to enable handover etc to be undertaken is carried over the interface.



4. ***B interface*** : The B interface exists between the MSC and the VLR . It uses a protocol known as the MAP/B protocol. As most VLRs are collocated with an MSC, this makes the interface purely an "internal" interface. The interface is used whenever the MSC needs access to data regarding a MS located in its area.
5. ***C interface:*** The C interface is located between the HLR and a GMSC or a SMS-G. When a call originates from outside the network, i.e. from the PSTN or another mobile network it ahs to pass through the gateway so that routing information required to complete the call may be gained.
6. ***D interface:*** The D interface is situated between the VLR and HLR. It uses the MAP/D protocol to exchange the data related to the location of the ME and to the management of the subscriber.
7. ***E interface:*** The E interface provides communication between two MSCs. The E interface exchanges data related to handover between the anchor and relay MSCs using the MAP/E protocol.
8. ***F interface:*** The F interface is used between an MSC and EIR. It uses the MAP/F protocol. The communications along this interface are used to confirm the status of the IMEI of the ME gaining access to the network.
9. ***G interface:*** The G interface interconnects two VLRs of different MSCs and uses the MAP/G protocol to transfer subscriber information, during e.g. a location update procedure.
10. ***H interface*** : The H interface exists between the MSC the SMS-G. It transfers short messages and uses the MAP/H protocol.
11. ***I interface:*** The I interface can be found between the MSC and the ME. Messages exchanged over the I interface are relayed transparently through the BSS.

GSM Protocols:



- The signaling protocol in GSM is structured into three general layers depending on the interface.
- 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.
- 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 **$LAPD_m$** protocol has been defined at the U_m interface for **layer two**.
- $LAPD_m$ has been derived from link access procedure for the D-channel (**LAPD**) in ISDN systems, which is a version of HDLC.
- $LAPD_m$ is a lightweight LAPD because it does not need synchronization flags or check summing for error detection. $LAPD_m$ 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.
- RR also directly accesses the physical layer for radio information and offers a reliable connection to the next higher layer.
- Finally, the call management (CM) layer contains three entities:
  - call control (CC),
  - short message service (SMS),
  - 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.
- 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:

- One of the main features of GSM system is the automatic, worldwide localization of its users.
- The GSM system always knows where a user is currently located, and the same phone number is valid worldwide.
- To have this ability the GSM system performs periodic location updates, even if the user does not use the MS, provided that the MS is still logged on to the GSM network and is not completely switched off.
- The HLR contains information about the current location, and the VLR that is currently responsible for the MS informs the HLR about the location of the MS when it changes.
- Changing VLRs with uninterrupted availability of all services is also called roaming.
- Roaming can take place within the context of one GSM service provider or between two providers in one country, however this does not normally happen but also between different service providers in different countries, known as international roaming.

- To locate an MS and to address the MS, several numbers are needed:
- **MSISDN (Mobile Station International ISDN Number)**: The only important number for the user of GSM is the phone number, due to the fact that the phone number is only associated with the SIM, rather than a certain MS.
- **IMSI (International Mobile Subscriber Identity)**: GSM uses the IMSI for internal unique identification of a subscriber.
- **TMSI (Temporary Mobile Subscriber Identity)**: To disguise the IMSI that would give the exact identity of the user which is signaling over the radio air interface, GSM uses the
  4-byte TMSI for local subscriber identification. The TMSI is selected by the VLR and only has temporary validity within the location area of the VLR. In addition to that the VLR will change the TMSI periodically.
- **MSRN (Mobile Station [Subscriber] Roaming Number)**: This is another temporary address that disguises the identity and location of the subscriber. The VLR generates this address upon request from the MSC and the address is also stored in the HLR.
- All the numbers described above are needed to find a user within the GSM system, and to maintain the connection with a mobile station.
- The following scenarios below shows a **MTC** (Mobile Terminate Call) and a **MOC** (Mobile Originated Call).

<u>MTC (Mobile Terminate Call):</u>

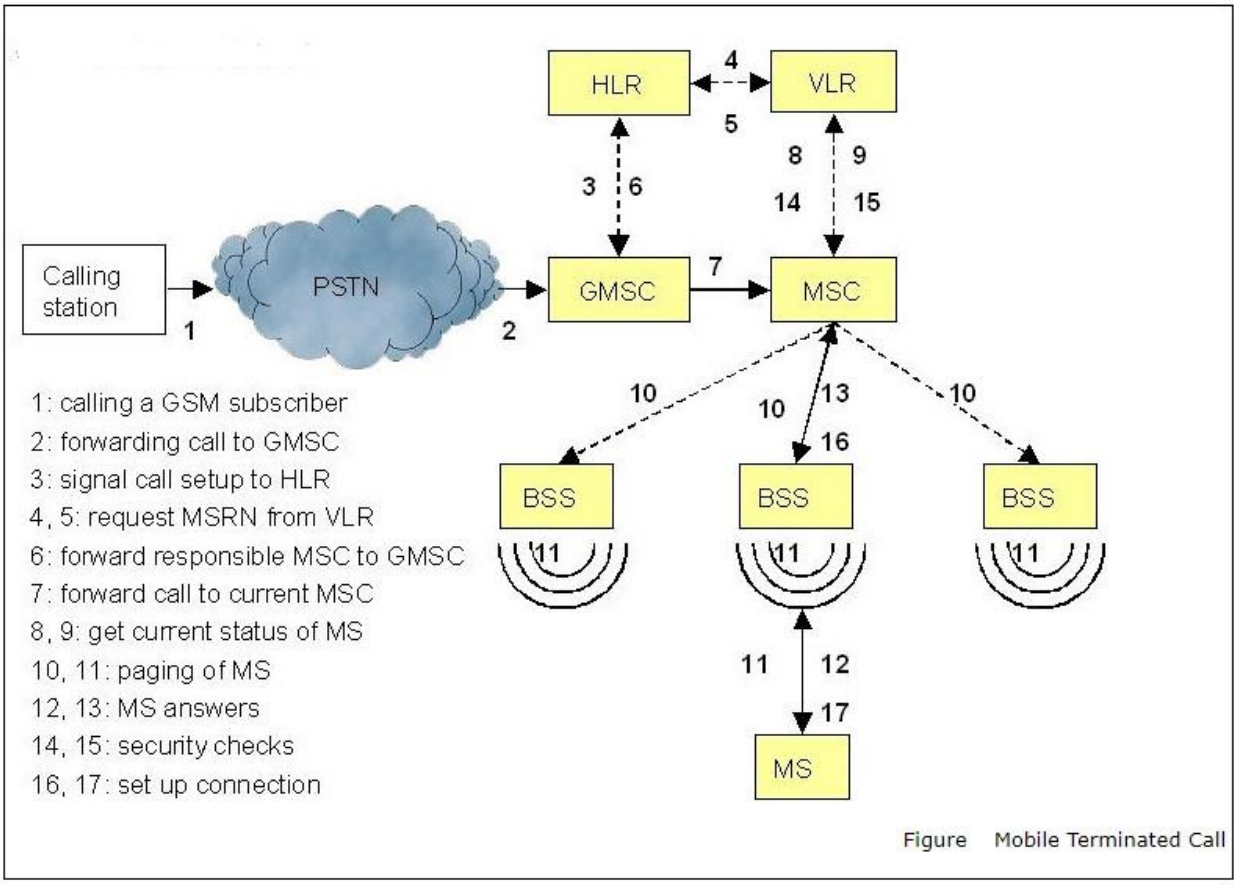


Figure Mobile Terminated Call

MOC (Mobile Originated Call):

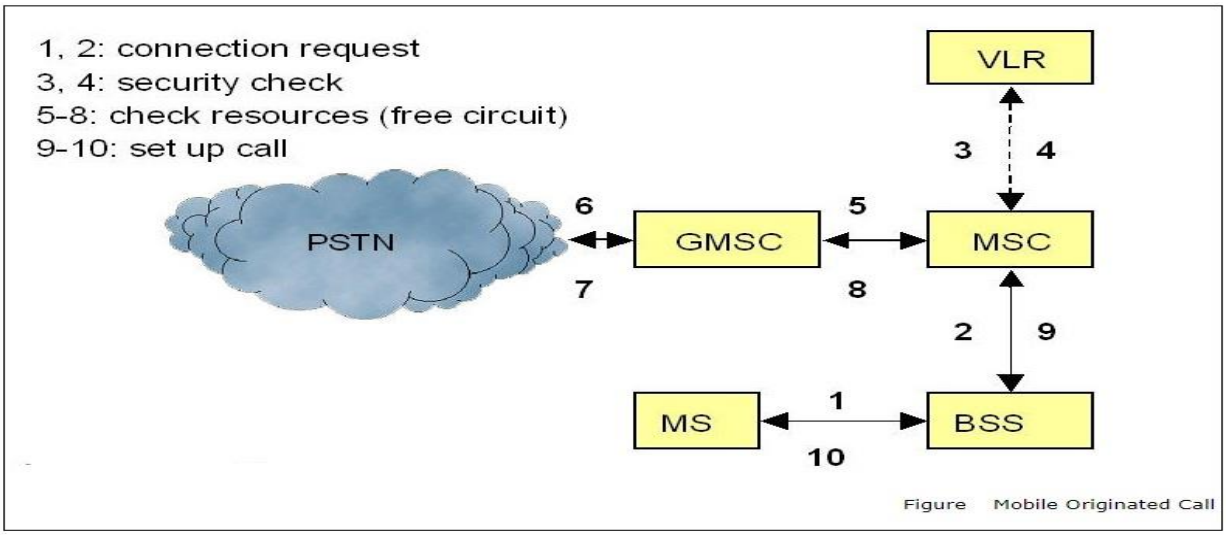


Figure Mobile Originated Call

Message Flow for MTC and MOC:

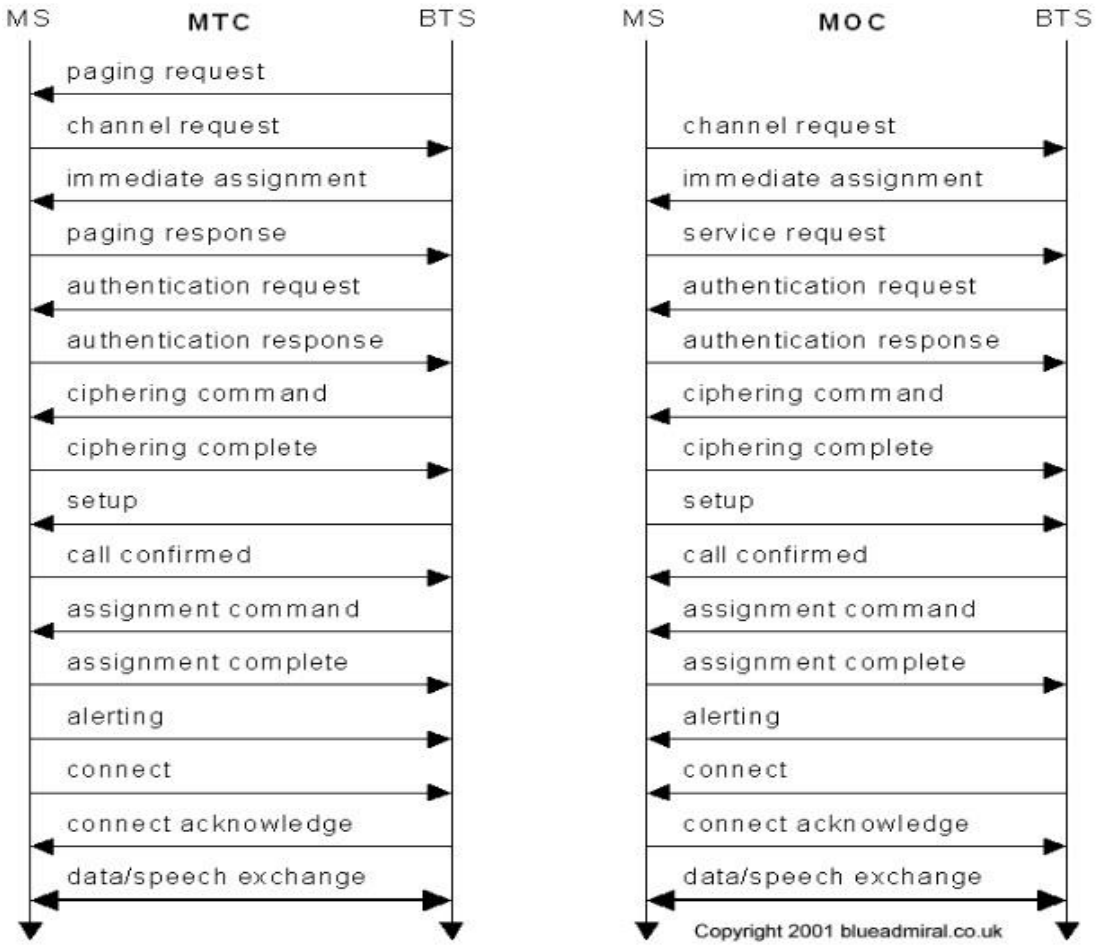
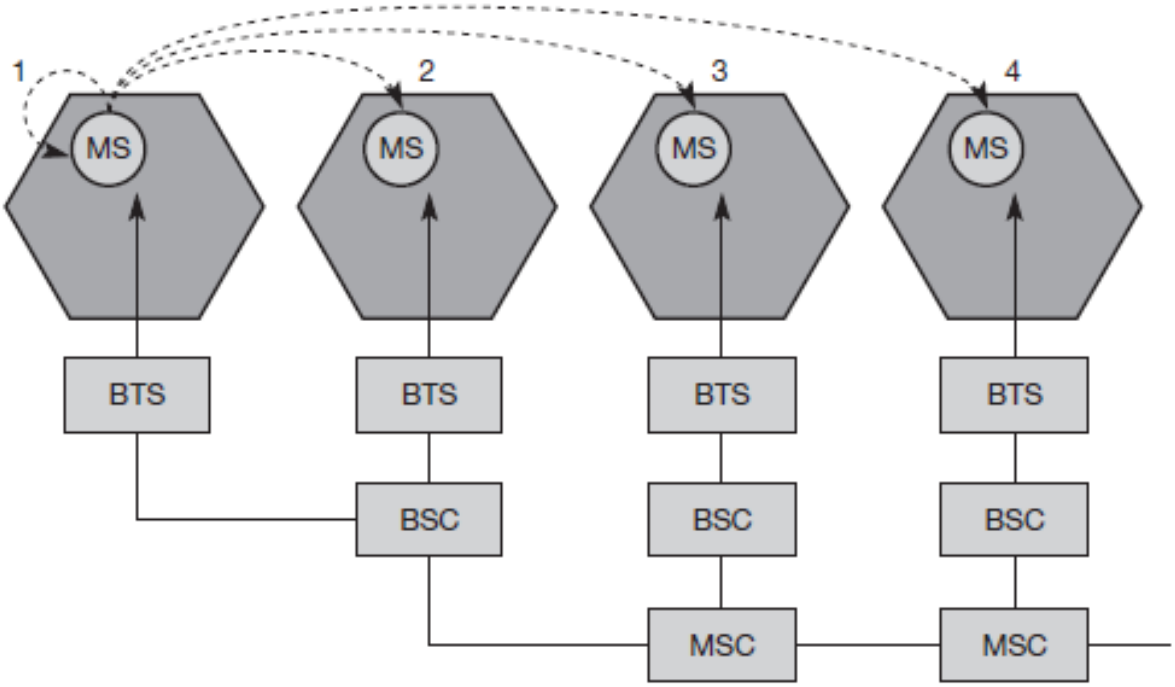


Figure Message Flow for MTC and MOC

Handover:

- In cellular telecommunications, the terms handover or handoff refer to the process of transferring an ongoing call or data session from one channel connected to the core network to another channel.
- There are two basic reasons for a handover
  - The mobile station **moves out of the range** of a BTS or a certain antenna of a BTS respectively. The received **signal level** decreases continuously until it falls below the minimal requirements for communication. The **error rate** may grow due to interference, the distance to the BTS may be too high (max. 35 km).
  - The wired infrastructure (MSC, BSC) may decide that the **traffic in one cell is too high** and shift some MS to other cells with a lower load (if possible). Handover may be due to **load balancing**.

1) **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).
2) **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).
3) **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).
4) **Inter MSC handover:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

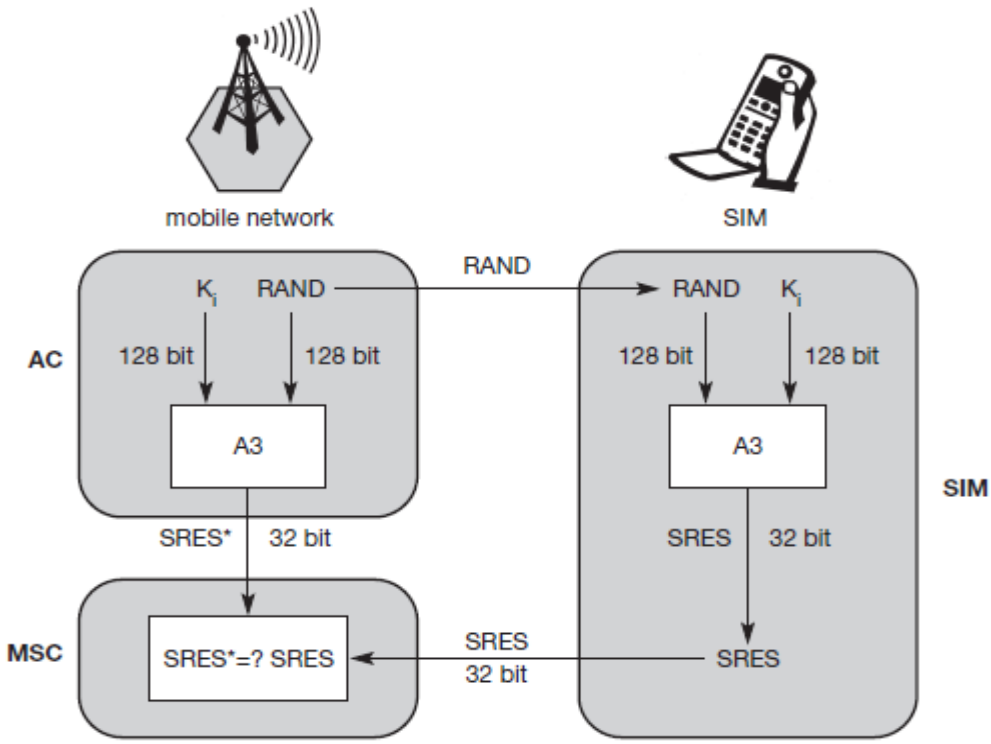


GSM Security:

- 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.
- The security services offered by GSM are explained below:

Access control and authentication:

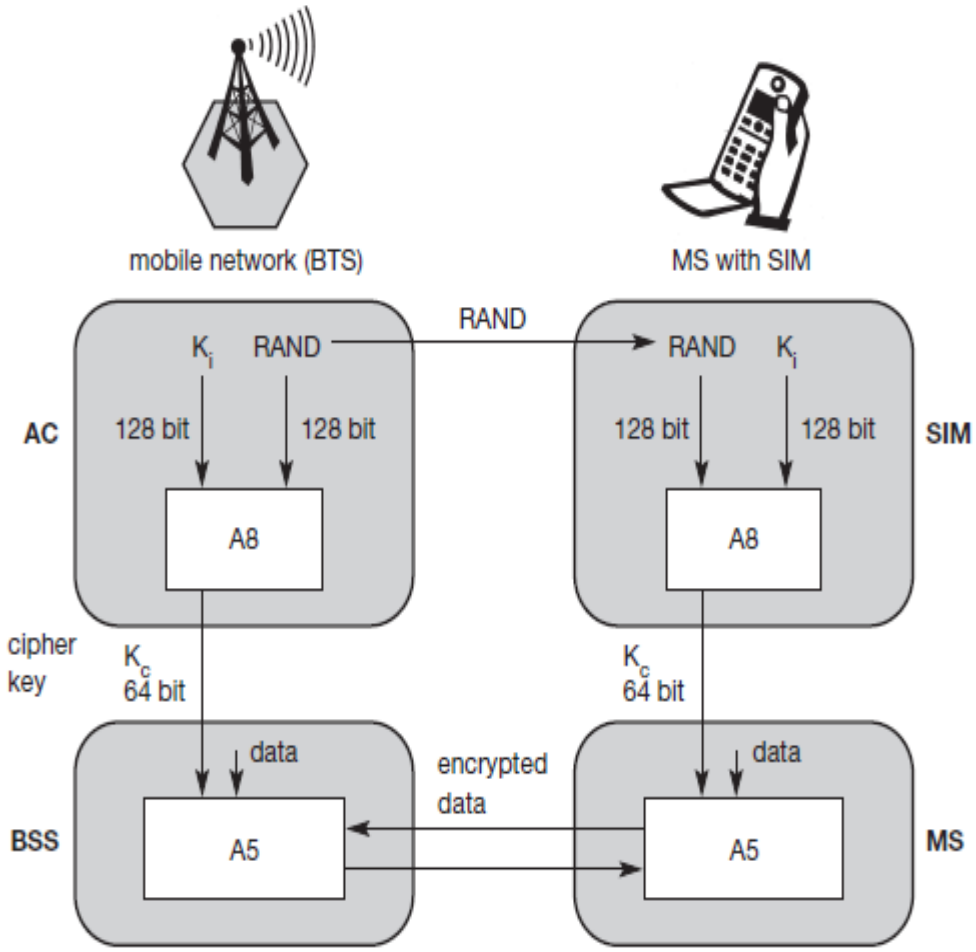
- The first step includes the authentication of a valid user for the SIM. The user needs a secret PIN to access the SIM. The next step is the subscriber **authentication**.
- This step is based on a challenge-response scheme as shown below.



- Authentication is based on the SIM, which stores the **individual authentication key Ki**, the **user identification IMSI**, and the algorithm used for authentication **A3**.
- Authentication uses a challenge-response method: the access control AC generates a random number **RAND** as challenge, and the SIM within the MS answers with **SRES** (signed response) as response 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:

- After authentication, BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network.
- 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.
- Kc 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. As above figure shows, Kc should be a 64 bit key – which is not very strong, but is at least a good protection against simple eavesdropping.

Anonymity:

- To provide user anonymity, all data is encrypted before transmission, and user identifiers (which would reveal an identity) 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.

New Data Services:

- The standard bandwidth of 9.6 kbit/s (14.4 kbit/s with some providers) available for data transmission is not sufficient for the requirements of today's computers.
- When GSM was developed, not many people anticipated the tremendous growth of data communication compared to voice communication.
- At that time, 9.6 kbit/s was a lot, or at least enough for standard group 3 fax machines. But with the requirements of, e.g., web browsing, file download, or even intensive e-mail exchange with attachments, this is not enough.
- To enhance the data transmission capabilities of GSM, two basic approaches are possible.

HSCSD: High Speed Circuit Switched Data

- In this system, higher data rates are achieved by bundling several TCHs (Traffic Channels). An MS requests one or more TCHs from the GSM network, i.e., it allocates several TDMA slots within a TDMA frame.

GPRS: General Packet Radio Service

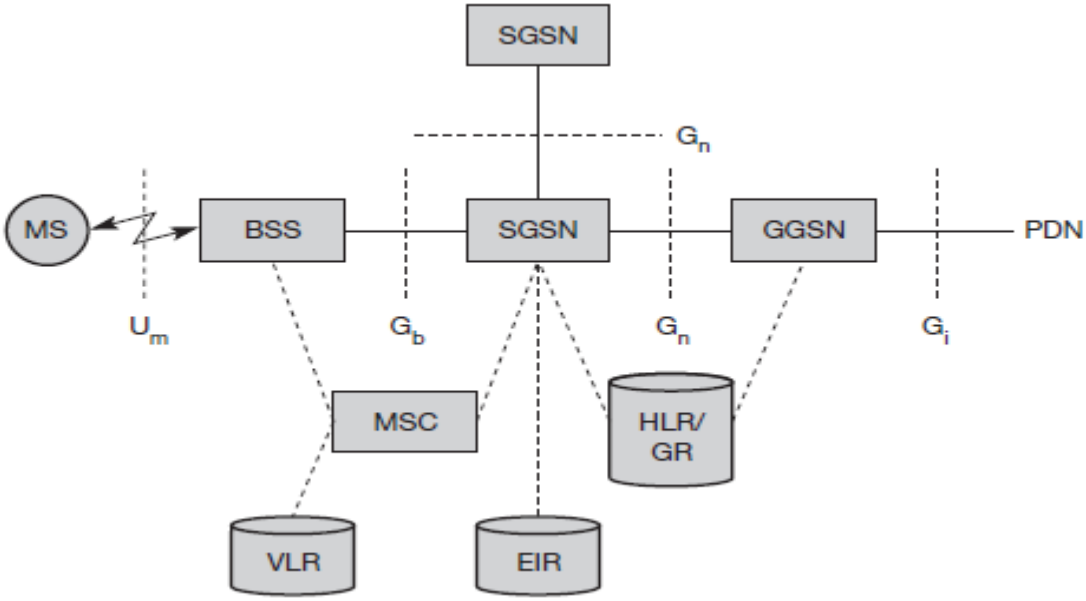
- The more progressive step is the introduction of packet-oriented traffic in GSM, i.e., shifting the paradigm from connections/telephone thinking to packets/internet thinking. The system, called GPRS.

GPRS(General Packet Radio Service):

- **GPRS** provides packet mode transfer for applications that exhibit traffic patterns according to the requirement specification such as
    - frequent transmission of small volumes
    - infrequent transmissions of small or medium volumes (e.g., typical web responses)
- 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.
- The GPRS concept is independent of channel characteristics and of the type of channel, and does not limit the maximum data 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.

GPRS Architecture:

- 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.



Gateway GPRS Support Node (GGSN):

- It 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).

Serving GPRS Support Node (SGSN):

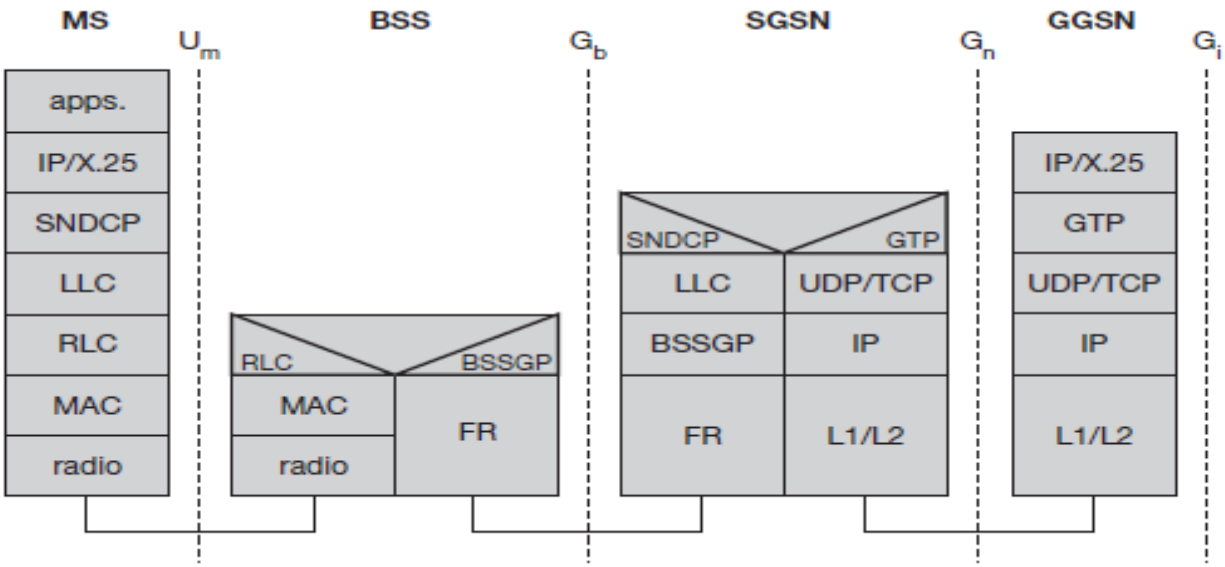
- The SGSN,
  - Requests user addresses from the **GPRS register (GR)**
  - Keeps track of the individual MS's location
  - Responsible for collecting billing information (e.g., counting bytes)
  - Performs several security functions such as access control.
- The SGSN is connected to a BSC via frame 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.
- GGSNs and SGSNs can be compared with home and foreign agents, respectively, in a mobile IP network.

PDN(Public Data Network): Packet data is transmitted from a PDN, via the GGSN and SGSN directly to the BSS and finally to the MS.

MSC(Mobile Switching Center): MSC is responsible for data transport in the traditional circuit-switched GSM, is only used for signaling in the GPRS scenario.

GPRS Protocols:

- The protocol architecture shows the transmission plane for GPRS. Architectures for the signaling planes can be found in ETSI (1998b).
- All data within the GPRS backbone, i.e., between the GSNs, is transferred using the **GPRS tunneling protocol (GTP)**.
- GTP can use two different transport protocols,
    - reliable **TCP** (needed for reliable transfer of X.25 packets)
    - non-reliable **UDP** (used for IP packets)
- The network protocol for the GPRS backbone is **IP** (using any lower layers).
- 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.



- 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.
- The **MAC** controls access with signaling 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).
- However, several new logical channels and their mapping onto physical resources have been defined. For example, one MS can allocate up to eight **packet data traffic channels (PDTCHs)**.

****