UNIT - II

Mobile Computing:

→ Mobile computing is a form of human–computer interaction by which a computer is expected to be transported during normal usage.
→ Mobile Computing is a technology that allows transmission of data, via a computer, without having to be connected to a fixed physical link.
→ Mobile Computing Systems are the computing systems that may be easily moved while they are being moved.

The term mobile is the ability to be on the move. There are two different kinds of mobility.

→ User mobility: Users communicate "anytime, anywhere, with anyone". In user mobility a user who has access the same or similar telecommunication services at different places.

Example:

- Simple call forwarding facility in telephone or desktops supporting roaming.
- read/write email on web browser.

→ Device portability: Devices can be connected anytime, anywhere to the network. With this, the communication device moves. Several techniques in the network guarantees that communication is even possible while the device is being moved.

Example:
Mobile phones (the system automatically directs the device from one base station to another, if the signal turns into weak signal).

Difference between Mobile and Wireless:

These terms both relate to a significant increase in productivity, there is a distinction between the two. Primarily the difference is one of focus: mobile relates to the portability of work, i.e. having the ability to perform tasks while out of the office; while wireless relates to being able to connect individual devices to one another or to a network without the need for cables.

Mobile computing simply means that computing tasks are performed outside the normal computing environment on a mobile computer (such as a laptop or notebook, or a PDA), rather than a computer that sits stationary on a desk in a room. Wireless computing means that data is sent from computer to computer through a wireless connection.

A communication device can exhibit one of the following characteristics.

- **Fixed and wired:** This configuration describes the typical desktop computer in an office. The devices use fixed networks for performance reasons.
- **Mobile and wired:** Many of today's laptops fall into this category; users carry the laptop from one hotel to the next, reconnecting to the company's network via the telephone network and a modem.
- **Fixed and wireless:** This mode is used for installing networks, e.g., in historical buildings to avoid damage by installing wires, or at trade shows to ensure fast network setup. Another

example is bridging the last mile to a customer by a new operator that has no wired infrastructure and does not want to lease lines from a competitor.

- **Mobile and wireless:** This is the most interesting case. No cable restricts the user, who can roam between different wireless networks. Today's most successful example for this category is GSM with more than 800 million users.

Applications:

➢ **Vehicles**

Today's cars already comprise some, but tomorrow's cars 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). For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity. For remote areas, satellite communication can be used, while the current position of the car is determined via the global positioning system (GPS). Cars driving in the same area build a local ad-hoc network for the fast exchange of information in emergency situations or to help each other keep a safe distance.

➢ **Emergencies**

If an ambulance connected with a high-quality wireless connection to a hospital, 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 cyclones or earthquakes. In the worst cases, only decentralized, wireless ad-hoc networks survive.

➢ **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. Wireless connections, e.g., via satellite, can help in this situation. Tradeshows need a highly dynamic infrastructure, but cabling takes a long time and frequently proves to be too inflexible. Many computer fairs use WLANs as a replacement for cabling. Other cases for wireless networks are computers, sensors, or information displays in historical buildings, where excess cabling may destroy valuable walls or floors. Wireless access points in a corner of the room can represent a solution.

➢ **Infotainment and more (Entertainment)**

Without wireless network 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. The travel guide might tell you something about the history of a building downloading information about a concert in the building at the same evening via a local wireless network. You

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 to enable.

➢ **Location dependent services**

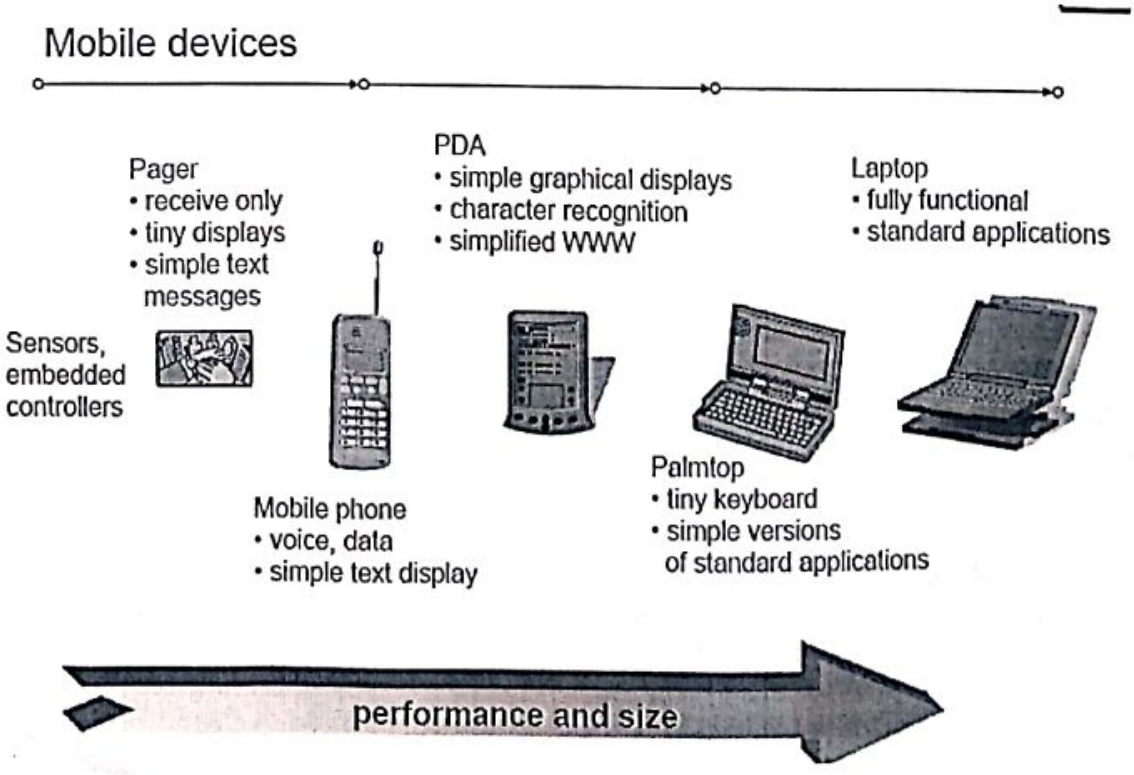
It is essential for an application to know something about the location or the user may require location information for future activities. Many services that depend on actual location are as follows.

- **Follow-on services:** The function of forwarding calls to the current user location is well known from the good old telephone system. Wherever you are, just transmit your temporary phone number to your phone and it redirects incoming calls.2 Using mobile computers, a follow-on service could offer, for instance, the same desktop environment wherever you are in the world. If someone wanted to reach you using a multimedia conferencing system, this call would be forwarded to your current location.
- **Location aware services:** Imagine you wanted to print a document sitting In big hotel using your laptop. If you drop the document over the printer icon, where would you expect the document to be printed? Certainly not by the printer in your office! However, without additional information about the capabilities of your environment, this might be the only thing you can do. For instance, there could be a service in the hotel announcing that a standard laser printer is available in the particular place or a color printer in a hotel meeting room etc.
- **Privacy:** The two service classes listed above immediately raise the question of privacy. You might not want video calls following you to dinner, but maybe you would want important e-mails to be forwarded. There might be locations and/or times when you want to exclude certain services from reaching you and you do not want to be disturbed. You want to utilize location dependent services, but you might not want the environment to know exactly who you are. Imagine a hotel monitoring all guests and selling these profiles to companies for advertisements.
- **Information services:** While walking around in a city you could always use your wireless travel guide to 'pull' information from a service, e.g., 'Where is the nearest Mexican restaurant?' However, a service could also actively 'push' information on your travel guide, e.g., the Mexican restaurant just around the corner has a special taco offer.
- **Support services:** Many small additional mechanisms can be integrated to support a mobile device. Intermediate results of calculations, state information, or cache contents could 'follow' the mobile node through the fixed network. As soon as the mobile node reconnects, all information is available again. This helps to reduce access delay and traffic within the fixed network.

➢ **Mobile and wireless devices**

Even though many mobile and wireless devices are available, there will be many more in the future. There is no precise classification of such devices, by size, shape, weight, or computing power. Currently, laptops are considered the upper end of the mobile device range. The following list gives some examples of mobile and wireless devices graded by increasing performance.

- **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. Without user interaction, the semantics of a closed door is applied to phone 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.
- **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.
- **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.



Simple Reference model (Architecture reference model of Mobile Computing):

The following figure shows the protocol stack implemented in the system according to the reference model. Here the End-systems are PDA and computer need a full protocol stack comprising the following layers.

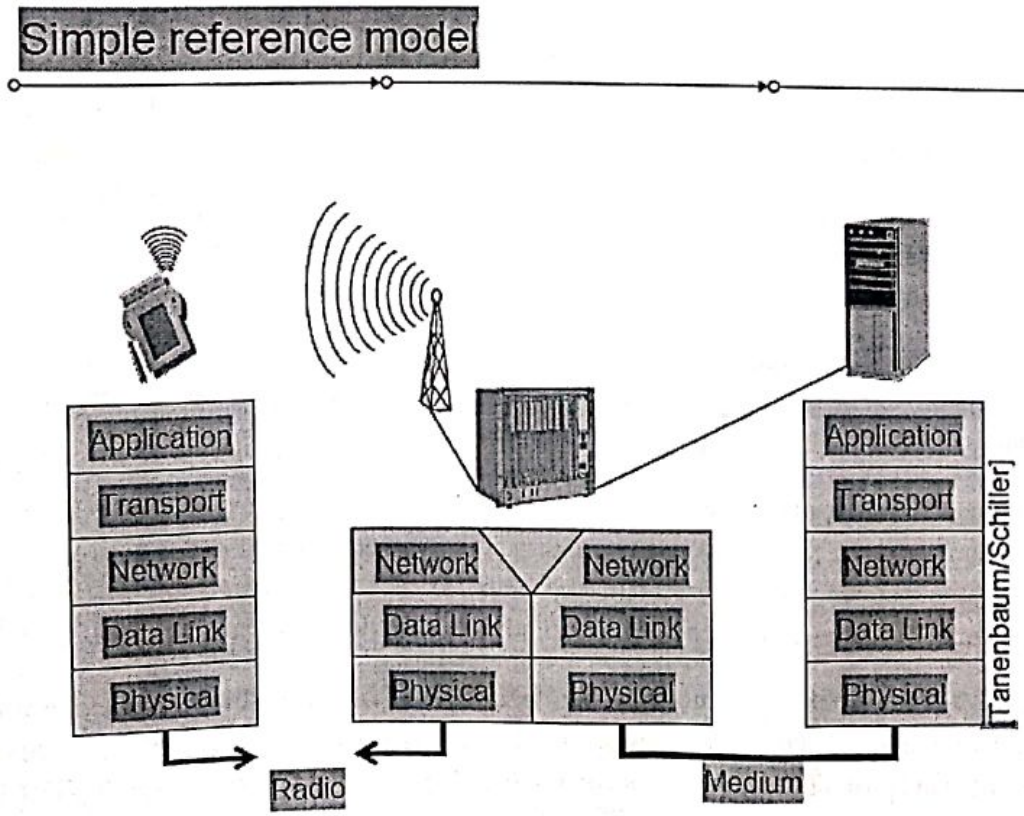
Physical layer: This is the lowest layer in a communication system and is responsible for the conversion of a stream of bits into signals that can be transmitted on the sender side. The physical layer of the receiver then transforms the signals back into a bit stream. For wireless communication, the physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection (although heavy interference may disturb the signal), modulation of data onto a carrier frequency and (depending on the transmission scheme) encryption.

Datalink layer: 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. The main tasks of this layer include accessing the medium, multiplexing of different data streams, correction of transmission errors, and synchronization.

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. Important topics are addressing, routing, device location, and handover between different networks.

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 and wireless access to the world wide web using a portable device.



Limitations of Mobile Computing:

- Mobile devices take more energy or power supply. The higher te functioning of the device, the faster it consumes the batteries. Hence the power supply has direct or indirect effect on mobile device.
- To make the device portable, interfaces with tiny Keypads are used, which makes typing complicate because of their limited key size.
- Small display despite with higher resolution does not support because the resolution capacity of human eye is the limiting factor.

GSM:

GSM (Global System for Mobile Communications, originally ***Groupe Spécial Mobile***), is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe technologies for second generation (or "2G") digital cellular networks. Developed as a replacement for first generation analog cellular networks, the GSM standard originally described a digital, circuit switched network optimized for full duplex voice telephony. The standard was expanded over time to include first circuit switched data transport, then packet data transport via GPRS. Packet data transmission speeds were later increased via EDGE. The GSM standard is succeeded by the third generation (or "3G") UMTS standard.

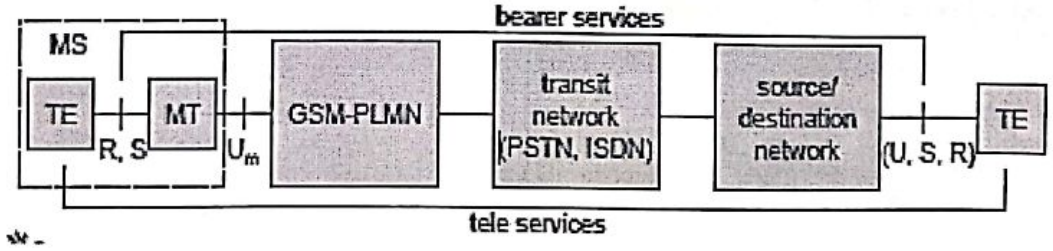
Mobile Services:

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

→ Bearer Services

→ Tele Services

→ Supplementary Services



Bearer Services

GSM specifies different mechanisms for data transmission. Bearer services permit transparent and non-transparent.

Transparent bearer services only use the functions of the physical layer (layer 1) to transmit data. The only mechanism to increase transmission quality is the use of **forward error correction (FEC),** which codesredundancy 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.

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.

Tele Services

→ Telecommunication services that enable voice communication via mobile phones
→ All these basic services have to obey cellular functions, security measurements etc.
→ Offered services

– Mobile Telephony

Primary goal of GSM was to enable mobile telephony offering the traditional bandwidth of 3.1 kHz

– Emergency Number

Common number throughout Europe (112); mandatory for all service providers; free of charge, without contract; connection with the highest priority (preemption of other connections possible)

Non-Voice-Teleservices

– Short Message Service (SMS)

Up to 160 character alphanumeric data transmission to/from the mobile terminal using the signaling channel, thus allowing simultaneous use of basic services and SMS

– group 3 fax
– voice mailbox (implemented in the fixed network supporting the mobile terminals)
– electronic mail (MHS, Message Handling System, implemented in the fixed network)

Supplementary Services

→ Services in addition to the basic services, cannot be offered stand-alone
→ Similar to ISDN services besides lower bandwidth due to the radio link
→ May differ between different service providers, countries and protocol versions
→ Important services

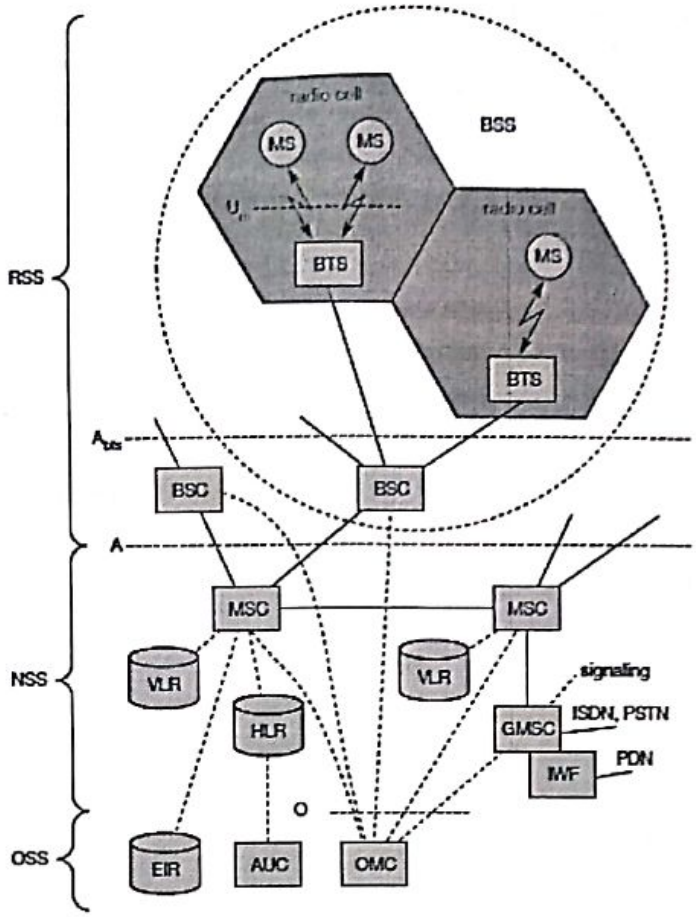
– identification: forwarding of caller number
– suppression of number forwarding
– automatic call-back
– conferencing with up to 7 participants
– locking of the mobile terminal (incoming or outgoing calls)

GSM System Architecture:

As with all systems in the telecommunication area, GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms. A GSM system consists of three subsystems, the **radio sub system (RSS)**, the **network and switching subsystem (NSS)**, and the **operation subsystem (OSS)**.

Radio Subsystem:

As the name implies, the **radio subsystem (RSS)** comprises all radio specific entities, i.e., the **mobile stations (MS)** and the **base station subsystem (BSS)**. Above 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 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 cells , 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.). A GSM cell can measure between some 100 m and 35 km depending on the environment.

• **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.

• **Mobile station (MS)**: The MS comprises all user equipment and software needed for communication with a GSM network. An 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. 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.

MS can also offer other types of interfaces to users with display, loudspeaker, microphone, and programmable soft keys. Further interfaces comprise computer modems, IrDA, or Bluetooth.

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.

- **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. An 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.

- **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.

- **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. If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR.

Operation Sub system:

The third part of a GSM system, the **operation subsystem (OSS)**, contains the necessary functions for network operation and maintenance.

- **Operation and maintenance center (OMC)**: The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing.

- **Authentication centre (AuC)**: 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.

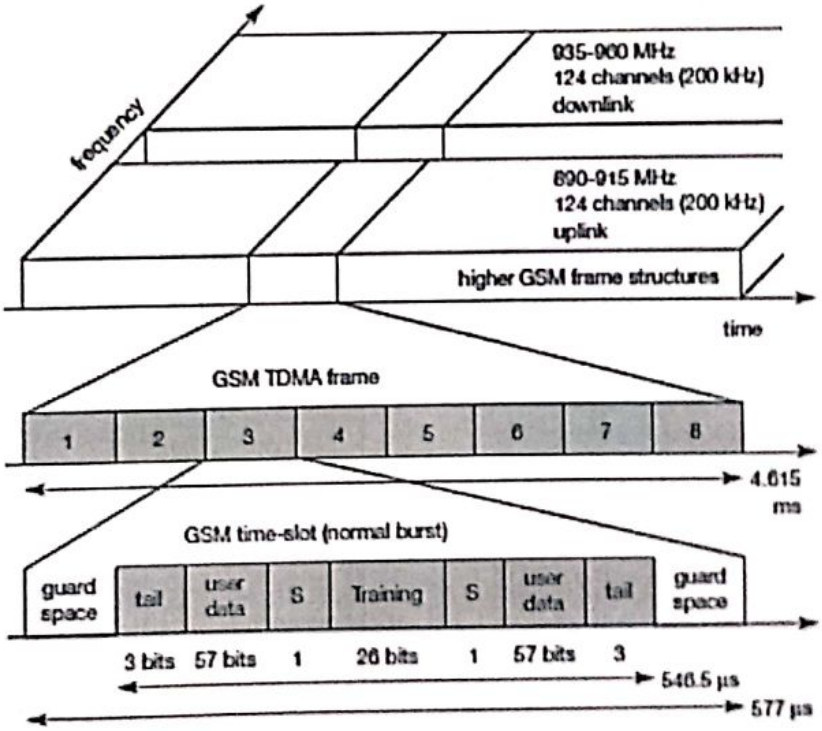
- **Equipment identity register (EIR)**: The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS.

Radio Interface:

The most interesting interface in a GSM system is Um, the radio interface. GSM implements SDMA using cells with BTS and assigns an MS to a BTS. Furthermore, FDD is used to separate downlink and uplink. In GSM 900, 124 channels, each 200 kHz wide, are used for FDMA, whereas GSM 1800 uses, 374 channels. Due to technical reasons, channels 1 and 124 are not used for transmission in GSM 900. Typically, 32 channels are reserved for organizational data; the remaining 90 are used for customers.

The following figure shows the TDM used. 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**. Below shows a so called **normal burst** as used for data transmission inside a time slot (user and signaling data). In the diagram, 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.



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 strongest signal in case of multi-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 neighboring 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.

Logical channels and Frame hierarchy:

GSM specifies two basic groups of logical channels, i.e., traffic channels and control channels:

- **Traffic channels (TCH):** GSM uses a TCH to transmit user data (e.g., voice, fax). Two basic categories of TCHs have been defined, i.e., **full-rate TCH (TCH/F)** and **half-rate TCH (TCH/H)**. A TCH/F has a data rate of 22.8 kbit/s, whereas TCH/H only has 11.4 kbit/s. With the voice codecs available at the beginning of the GSM standardization, 13 kbit/s were required, whereas the remaining capacity of the TCH/F (22.8 kbit/s) was used for error correction (**TCH/FS**). Data transmission in GSM is possible at many different data rates, e.g., **TCH/F4.8** for 4.8 kbit/s, **TCH/F9.6** for 9.6 kbit/s, and, as a newer specification, **TCH/F14.4** for 14.4 kbit/s.

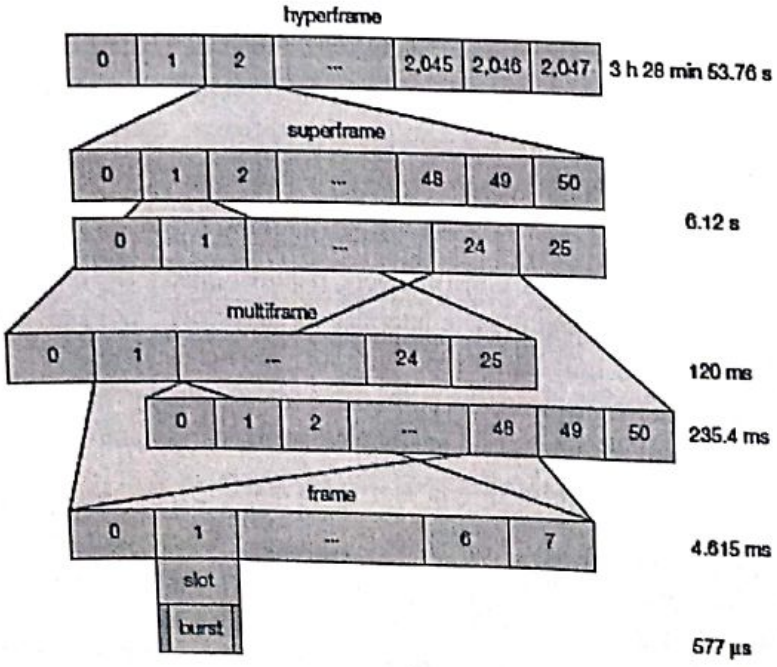
- **Control channels (CCH):** Many different CCHs are used in a GSM system to control medium access, allocation of traffic channels or mobility management. Three groups of control channels have been defined, defined, each again with sub channels.

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. Sub channels are **frequency correction channel (FCCH), synchronization channel (SCH).**

Common control channel (CCCH): All information regarding connection setup between MS and BS is exchanged via the CCCH. Sub channels are **paging channel (PCH), random access channel (RACH), access grant channel (AGCH).**

Dedicated control channel (DCCH): While the previous channels have all been unidirectional, the following channels are bidirectional. Sub channels are **stand-alone dedicated control channel (SDCCH), slow associated dedicated control channel (SACCH), fast associated dedicated control channel (FACCH).**

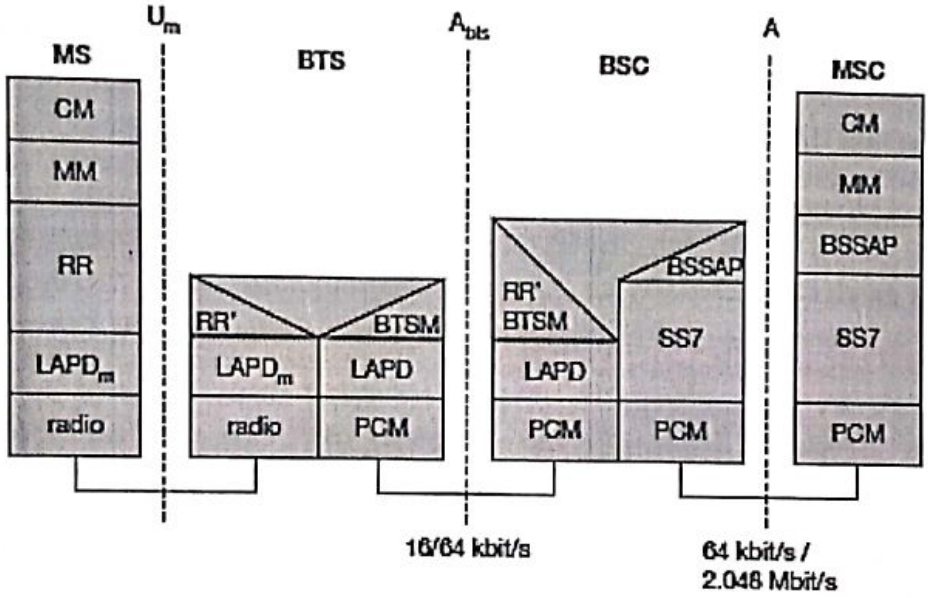
The following figure shows the logical combination of 26 frames (TDMA frames with duration of 4.615 ms) to a multiframe with a duration of 120 ms.



This logical frame hierarchy continues, combining 26 multiframes with 51 frames or 51 multiframes with 26 frames to form a **superframe**. 2,048 superframes build a **hyperframe** with a duration of almost 3.5 hours. Altogether, 2,715,648 TDMA frames form a hyperframe.

Protocols:

The following figure shows the protocol architecture of GSM with signaling protocols, interfaces, as well as the entities. The main interest lies in the Um interface, as the other interfaces occur between entities in a fixed network. **Layer 1**, the physical layer, 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. Different logical channels of GSM use different coding schemes with different correction capabilities. Speech channels need additional coding of voice data after analog to digital conversion, to achieve a data rate of 22.8 kbit/s.

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, as the name already implies, has been derived from link access procedure for the D-channel (**LAPD**) in ISDN systems. LAPDm offers reliable data transfer over connections, re-sequencing of data frames, and flow control. Further services provided by LAPDm include segmentation and reassembly of data and acknowledged/unacknowledged data transfer.

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)** that replaces the **international mobile subscriber identity (IMSI)** and which hides the real identity of an MS user over the air interface.

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.

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. While PCM systems offer transparent 64 kbit/s channels, GSM also allows for the submultiplexing of four 16 kbit/s channels into a single 64 kbit/s channel. **Signaling system No. 7 (SS7)** is used for signaling between an MSC and a BSC. An MSC can also control a BSS via a **BSS applicationpart (BSSAP).**

Localization and calling:

One fundamental feature of the GSM system is the automatic, worldwide localization of users. The system always knows where a user currently is, and the same phone number is valid worldwide. To provide this service, GSM performs periodic location updates even if a user does not use the mobile station.

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

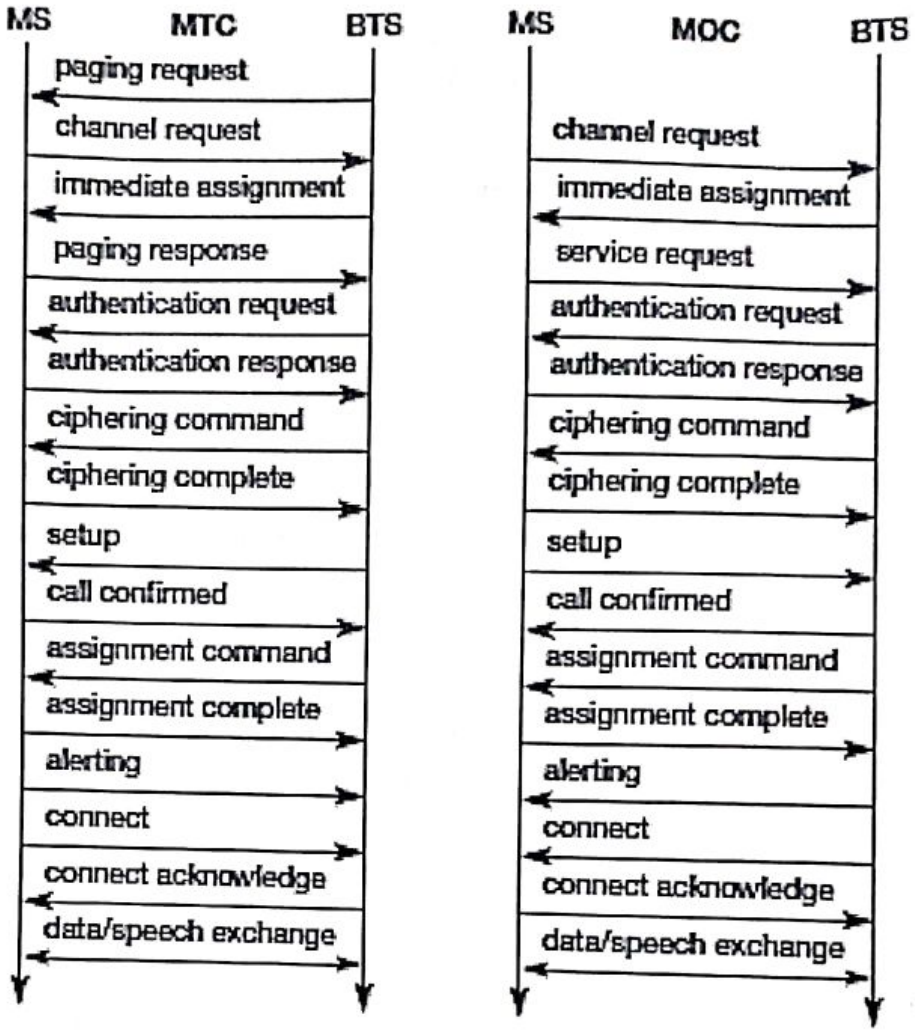
- **Mobile station international ISDN number (MSISDN):** The only important number for a user of GSM is the phone number. Remember that the phone number is not associated with a certain device but with the SIM, which is personalized for a user. This number consists of the **country code (CC),** the **national 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 signaling over the air interface. TMSI is selected by the current VLR and is only valid temporarily and within the location area of the VLR.

- **Mobile station7 roaming number (MSRN):** Another temporary address that hides the identity and location of a subscriber is MSRN. 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.

All these numbers are needed to find a subscriber and to maintain the connection with a mobile station. The interesting case is the **mobile terminated call (MTC),** i.e., a situation in which a station calls a mobile station. It is much simpler to perform a **mobile originated call (MOC)** compared to a MTC. In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during connection setup.



Handover:

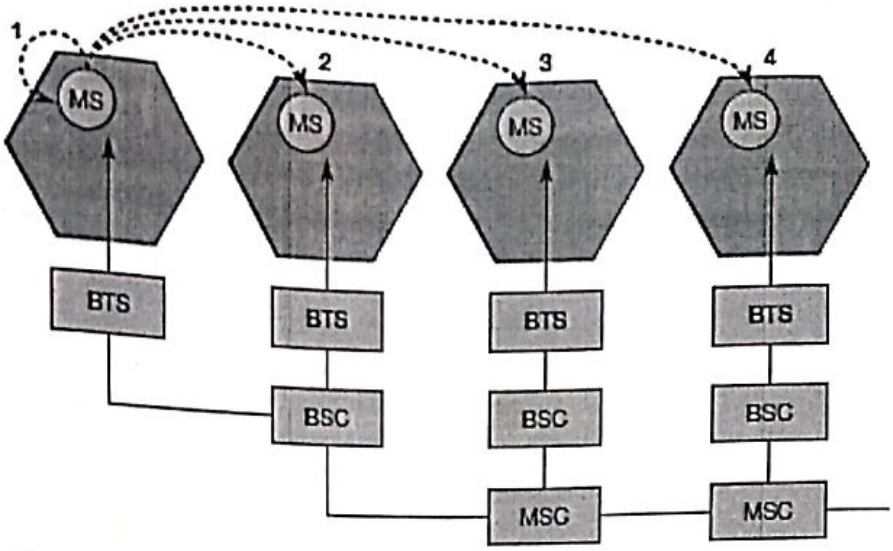
Cellular systems require **handover** procedures, as single cells do not cover the whole service area, but, e.g., only up to 35 km around each antenna on the countryside and some hundred meters in cities. However, a handover should not cause a cut-off, also called **call drop**. GSM aims at maximum handover duration of 60 ms.

There are two basic reasons for a handover

- 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 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**.

The following figure shows four possible handover scenarios in GSM.



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).

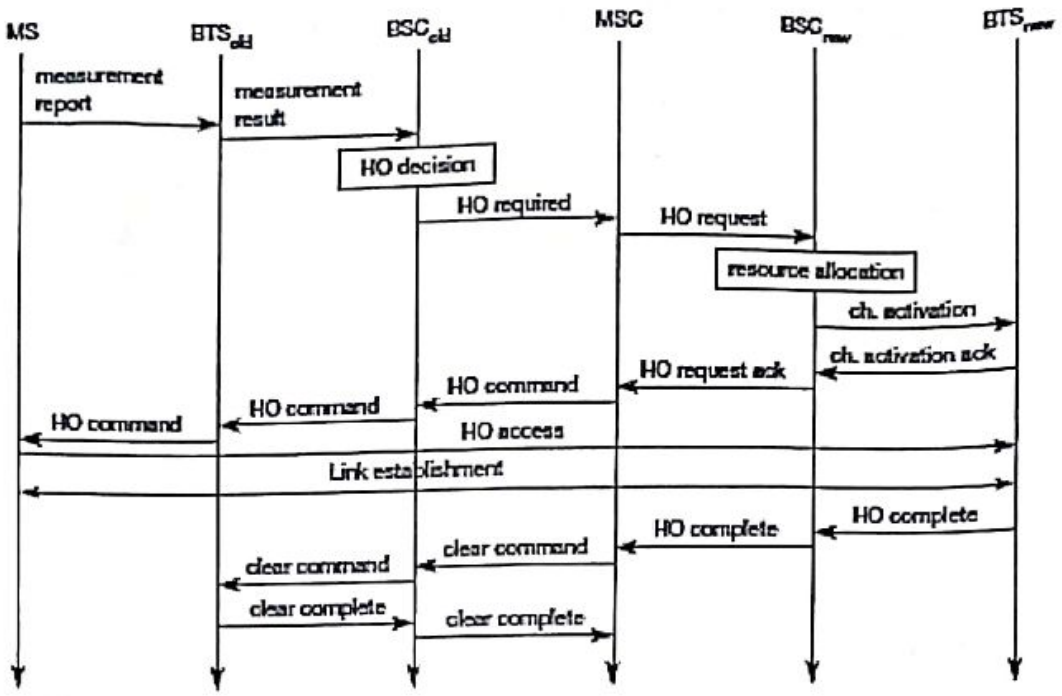
Inter-BSC, intra-MSC handover: As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).

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

The following figure shows the typical signal flow during an inter-BSC, intra-MSC handover. The MS sends its periodic measurements reports, the BTSold forwards these reports to the BSCold together with its own measurements. Based on these values and, e.g., on current traffic conditions, the BSCold may decide to perform a handover and sends the message HO_required to the MSC. The task of the MSC then comprises the request of the resources needed for the handover from the new BSC, BSCnew. This BSC checks if enough resources (typically frequencies or time slots) are available and activates a physical channel at the BTSnew to prepare for the arrival of the MS.

The BTSnew acknowledges the successful channel activation, BSCnew acknowledges the handover request. The MSC then issues a handover command that is forwarded to the MS. The MS now breaks its old radio link and accesses the new BTS. The next steps include the establishment of the link (this includes layer two link establishment and handover complete messages from the MS).

Basically, the MS has then finished the handover, but it is important to release the resources at the old BSC and BTS and to signal the successful handover using the handover and clear complete messages as shown.



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.

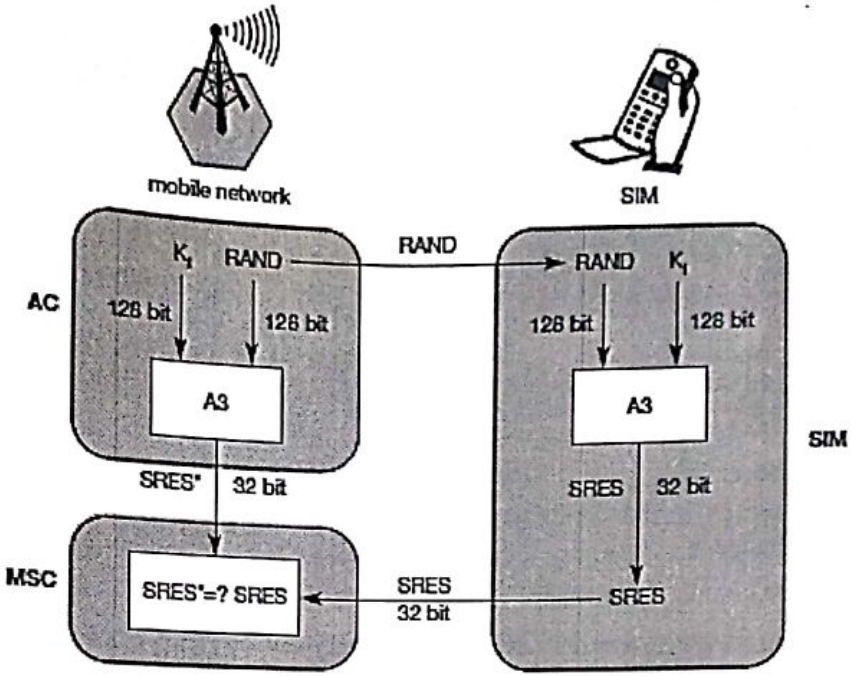
- **Confidentiality:** All user-related data is encrypted. After authentication, BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS, but it does not exist end-to-end or within the whole fixed GSM/telephone network.

- **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.

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.**

Authentication:

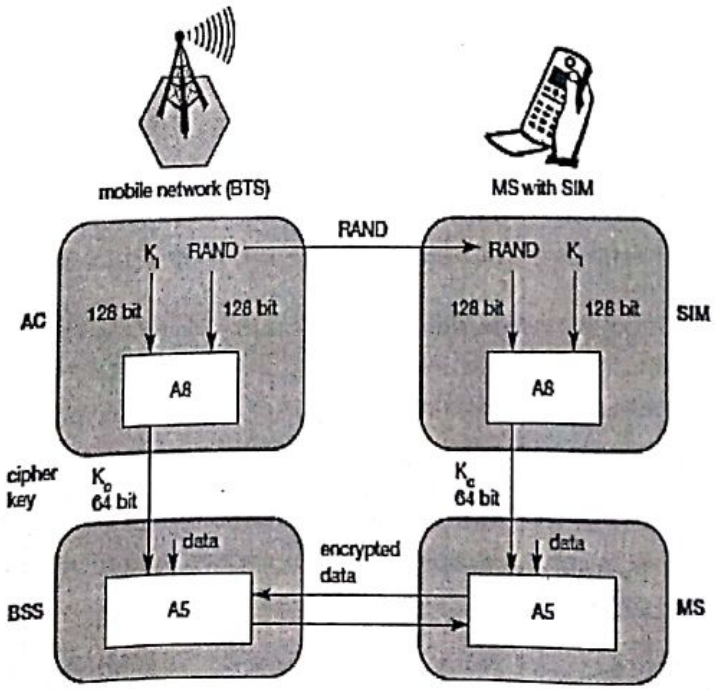
Before a subscriber can use any service from the GSM network, he or she must be authenticated. Authentication is based on the SIM, which stores the **individual authentication key Ki,** the **user identification IMSI,** and the algorithm used for authentication **A3.**



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.

Encryption:

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.

New data services:

As mentioned above, 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. 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 and is presented in the following.

HSCSD (High Speed Circuit Switched Data):

In this system, 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. HSCSD exhibits some major disadvantages. It still uses the connection-oriented mechanisms of GSM. While downloading a larger file may require all channels reserved, typical web browsing would leave the channels idle most of the time.

AIUR	TCH / F4.8	TCH / F9.6	TCH / F14.4
4.8 kbit/s	1	–	–
9.6 kbit/s	2	1	–
14.4 kbit/s	3	–	1
19.2 kbit/s	4	2	–
28.8 kbit/s	–	3	2
38.4 kbit/s	–	4	–
43.2 kbit/s	–	–	3
57.6 kbit/s	–	–	4

For *n* channels, HSCSD requires *n* times signaling during handover, connection setup and release. Each channel is treated separately. The probability of blocking or service degradation increases during handover.

GPRS **(General Packet Radio Service):**

The more flexible and powerful data transmission avoids the problems of HSCSD by being fully packet-oriented.