GOA COLLEGE OF ENGINEERING

“Bhausaheb Bandodkar Technical Education Complex”

Tutorial No: 4

Q1) Which types of different services does GSM offer? Name some examples and give reasons why these services have been separated.

GSM provides 3 main categories of services. These are: 1. Bearer services
2. Teleservices
3. Supplementary services

Bearer services

Bearer services give the subscribers the capability to send and receive data to and from remote computers or mobile phones. Eg. Sending a data file such as a picture to a computer at the office that is connected to a public telephone network.

Teleservices

GSM provides both voice-oriented teleservices and non-voice teleservices. Eg Telehony(high quality digital voice transmission) and Fax.

Supplementary services

GSM provides supplementary services such as user identification, call redirection and for- warding of ongoing calls. In addition, standard ISDN features such as ’close user groups’ and multiparty’ communication are available.

Q2) Name the main elements of the GSM architecture and describe their functions. What are the advantages of specifying not only the radio interface but also all internal interfaces of the GSM system.

The main elements of the GSM architecture are :

The Radio Subsystem (RSS)

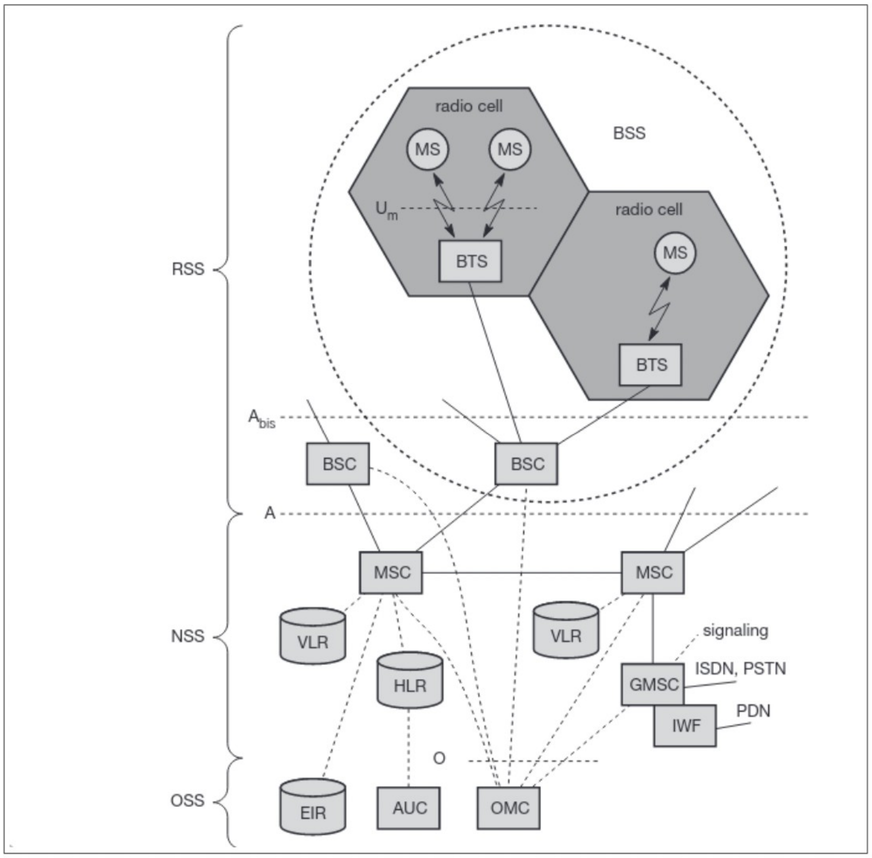

Figure 1

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). The 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 con- trolled 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.

- 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. 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. 3 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.

The Network and Switching Subsystem (NSS)

Also called the ”heart” of the GSM system is formed by the network and switching sub- system (NSS). The NSS connects the wireless network with standard public networks, per- forms 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.
- 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), sub- scribed services (e.g., call forwarding, roaming restrictions, GPRS), and the international mobile subscriber identity (IMSI).
- 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 Operation Subsystem (OSS).

The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The following entities have been defined:

- Operation and maintenance center (OMC): The OMC monitors and con- trols all other network entities Typical OMC management functions are traffic monitoring, status reports of net- work entities, subscriber and security management, or accounting and billing.
- Authentication centre (AuC): As the radio interface and mobile stations are par- ticularly 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. In theory an MS is useless as soon as the owner has reported a theft.

Q3) What are the reasons for a handover in GSM and the problems associated with it? Which are the typical steps of handover, what types of handovers can occur?

There are two basic reasons for a handover in GSM:

- 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) etc. – all these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.
- 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 typical steps of handover are:

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, BSC new. 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 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, BSC new. 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.

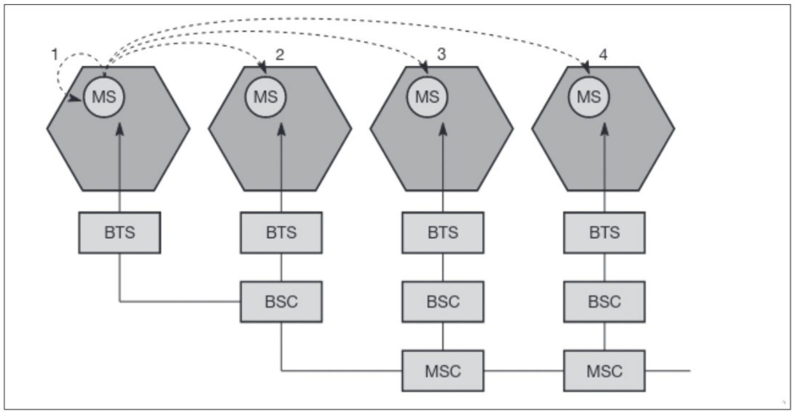

Figure 2

There are 4 possible types of handovers that can occur(shown in above figure):

- Intra-cell handover: Within a cell, narrow-band interference could make transmis- sion at a certain frequency impossible. The BSC could then decide to change the carrier frequency
- 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
- 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 differ- ent BSCs. This handover then has to be controlled by the MSC
- Inter MSC handover: A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together.

Q4) What are the functions of authentication and encryption in GSM? How is system security maintained?

Authentication

The purpose of authentication is to protect the network against unauthorised use. In the GSM context it helps protect the GSM subscribers by denying the possibility for intruders to impersonate authorised users. A GSM network operator can verify the identity of the subscriber, making it highly improbable to clone someone else’s mobile phone identity.

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 (the precise location of security functions for encryption, BTS and/or BSC are vendor dependent). Kc is generated using the individual key Ki and a random value by applying the algorithm A8.

Security

GSM offers several security services using confidential information stored in the AuC and in the individual SIM (which is plugged into an arbitrary MS). The SIM stores personal, secret data and is protected with a PIN against unauthorized use. (For example, the secret key Ki used for authentication and encryption procedures is stored in the SIM.) 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.
- 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. 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.