CHAPTER 1
INTRODUCTION TO GSM
1.1 INTRODUCTION TO THE GSM

GSM (Global System for Mobile communications: originally from Groupe Spécial Mobile) is the most popular standard for mobile phones\(^1\) in the world. Its promoter, the GSM Association, estimates that 32% of the global mobile market uses the standard. GSM is used by over 3 billion people across more than 212 countries and territories. Its ubiquity makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world. GSM differs from its predecessors in that both signaling and speech channels are digital, and thus is considered a second generation (2G) mobile phone\(^1\) system. This has also meant that data communication was easy to build into the system.

The ubiquity of the GSM standard has been an advantage to both consumers (who benefit from the ability to roam and switch carriers without switching phones) and also to network operators (who can choose equipment from any of the many vendors implementing GSM). GSM also pioneered a low-cost, to the network carrier, alternative to voice calls, the Short message service (SMS, also called "text messaging"), which is now supported on other mobile standards as well. Another advantage is that the standard includes one worldwide Emergency telephone number, 112. This
makes it easier for international travelers to connect to emergency services without knowing the local emergency number.

GSM means an open, non-proprietary system that is constantly evolving. One of its great strengths is the international roaming capability. This gives consumers seamless and same standardized same number contact ability in more than 170 countries, GSM satellite roaming as extended service access to areas where terrestrial coverage is not available.

1.2 GSM HISTORY

The Europeans realized rapid growth of cellular communications early on, and in 1982. In 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Groupe Spécial Mobile (GSM) to develop a standard for a mobile telephone system that could be used across Europe. In 1987, a memorandum of understanding was signed by 13 countries to develop a common cellular telephone system across Europe.

In 1989, GSM responsibility was transferred to the European Telecommunications Standards Institute (ETSI) and phase I of the GSM specifications were published in 1990. The first GSM network was launched in 1991 by Radiolinja in Finland with joint technical infrastructure maintenance from Ericsson. By the end of 1993, over a million subscribers
were using GSM phone networks being operated by 70 carriers across 48 countries.

1.3 LIMITATIONS OF CONVENTIONAL MOBILE TELEPHONE SYSTEM

One of many reasons for developing a cellular mobile telephone system and deploying it in many cities is the operational limitations of conventional mobile telephone system limited service capability, poor service performance and inefficient frequency spectrum utilization.

1.3.1 LIMITED SERVICE CAPABILITY

A conventional mobile telephone system is usually designed by selecting one or more channels from a specific frequency allocation for use in autonomous geographic zones. The communications coverage area of each zone is normally planned to be as large as possible, which means that the transmitted power should be as high as the federal specification allows. The user who starts a call in one zone has to reinitiate the call when moving into a new zone because the call will be dropped. This is an undesirable radio telephone system since there is no guarantee that a call can be completed without a handoff capability.

The handoff is a process of automatically changing frequencies as the mobile unit moves into a different frequency zone so that conversation can be continued in a new frequency zone without redialing. Another
disadvantage of the conventional system is that the number of active users is limited to the number of channels assigned to a particular frequency.

1.4 GSM Family

- Basic GSM
- P-GSM, Standard or Primary GSM-900 Band
- E-GSM, Extended GSM-900 Band (includes Standard GSM-900 band)
- R-GSM, Railways GSM-900 Band (includes Standard and Extended GSM-900 band)
- T-GSM, TETRA-GSM
- High-Speed Circuit-Switched Data (HCSD)
- General Packet Radio System (GPRS)
- Enhanced Data GSM Environment (EDGE)
- Universal Mobile Telecommunications Service (UMTS)
- European Radio Messaging System (ERMES)
- Future Public Land Mobile Telecommunication System (FPLMTS),
- International Mobile Telecommunication (IMT-2)

1.5 TECHNICAL DETAILS OF GSM

GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in...
four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. Some countries in the Americas (including Canada and the United States) use the 850 MHz and 1900 MHz bands because the 900 and 1800 MHz frequency bands were already allocated.

The rarer 400 and 450 MHz frequency bands are assigned in some countries, notably Scandinavia, where these frequencies were previously used for first-generation systems.

GSM-900 uses 890–915 MHz to send information from the mobile station to the base station (uplink) and 935–960 MHz for the other direction (downlink), providing 124 RF channels (channel numbers 1 to 124) spaced at 200 kHz. Duplex spacing of 45 MHz is used. In some countries the GSM-900 band has been extended to cover a larger frequency range. This 'extended GSM', E-GSM, uses 880–915 MHz (uplink) and 925–960 MHz (downlink), adding 50 channels (channel numbers 975 to 1023 and 0) to the original GSM-900 band. Time division multiplexing is used to allow eight full-rate or sixteen half-rate speech channels per radio frequency channel. There are eight radio timeslots (giving eight burst periods) grouped into what is called a TDMA frame. Half rate channels use alternate frames in the same timeslot. The channel data rate is 270.833 kbit/s, and the frame duration is 4.615 ms.

The transmission power in the handset is limited to a maximum of 2 watts in GSM850/900 and 1 watt in GSM1800/1900.
GSM has used a variety of voice codecs to squeeze 3.1 kHz audio in between 5.6 and 13 kbit/s. Originally, two codecs, named after the types of data channel they were allocated, were used, called Half Rate (5.6 kbit/s) and Full Rate (13 kbit/s). These used a system based upon linear predictive coding (LPC). In addition to being efficient with bitrates, these codecs also made it easier to identify more important parts of the audio, allowing the air interface layer to prioritize and better protect these parts of the signal.

GSM was further enhanced in 1997 with the Enhanced Full Rate (EFR) codec, a 12.2 kbit/s codec that uses a full rate channel. Finally, with the development of UMTS, EFR was refactored into a variable-rate codec called AMR-Narrowband, which is high quality and robust against interference when used on full rate channels, and less robust but still relatively high quality when used in good radio conditions on half-rate channels.

There are five different cell sizes in a GSM network—macro, micro, pico, femto and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average roof top level. Micro cells are cells whose antenna height is under average roof top level; they are typically used in urban areas. Picocells are small cells whose coverage diameter is a few dozen meters; they are mainly used indoors. Femtocells are cells designed for use in residential or small business environments and connect to the service provider’s
network via a broadband internet connection. Umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells.

Cell horizontal radius varies depending on antenna height, antenna gain and propagation conditions from a couple of hundred meters to several tens of kilometres. The longest distance the GSM specification supports in practical use is 35 kilometres (22 miles). There are also several implementations of the concept of an extended cell, where the cell radius could be double or even more, depending on the antenna system, the type of terrain and the timing advance.

Indoor coverage is also supported by GSM and may be achieved by using an indoor picocell base station, or an indoor repeater with distributed indoor antennas fed through power splitters, to deliver the radio signals from an antenna outdoors to the separate indoor distributed antenna system. These are typically deployed when a lot of call capacity is needed indoors, for example in shopping centers or airports. However, this is not a prerequisite, since indoor coverage is also provided by in-building penetration of the radio signals from nearby cells.

The modulation used in GSM is Gaussian minimum-shift keying (GMSK), a kind of continuous-phase frequency shift keying. In GMSK, the signal to be modulated onto the carrier is first smoothed with a Gaussian low-pass filter prior to being fed to a frequency modulator, which greatly
reduces the interference to neighboring channels (adjacent channel interference).

1.6 OVERVIEW OF GSM

- TDMA structure 8 time slots carrier
- Time slot: 0.577ms
- Frame interval: 8 time slots = 4.615ms
- Radio carrier number 124 radio carrier (935-960MHZ Down Link, 890-915MHZ Up-Link)
- Modulation Scheme: Gaussian minimum shift keying with \( bt = 0.3 \)
- Frequency hopping: slow frequency hopping (217 hops / sec)
- Equalizer Equalization up to 16ms time dispersions.
- Maximum data rate: 9600 bit/s
- Maximum mobile terminal output power: 8 W
- Maximum hand-held mobile terminal output power: 2W
- Maximum cell radius: 30 km
- Minimum cell radius: 350 m
- Number of radio channels in each direction: 124
- Number of speech channels per radio channel: 8
- Frequency band—The frequency range specified for GSM is 1,850 to 1,990 MHz (mobile station to base station).
- Duplex distance—The duplex distance is 80 MHz. Duplex distance is the distance between the uplink and downlink frequencies. A channel has two frequencies, 80 MHz apart.
o channel separation—The separation between adjacent carrier frequencies. In GSM, this is 200 kHz.

o modulation—Modulation is the process of sending a signal by changing the characteristics of a carrier frequency. This is done in GSM via Gaussian minimum shift keying (GMSK).

o transmission rate—GSM is a digital system with an over-the-air bit rate of 270 kbps.

o access method—GSM utilizes the time division multiple access (TDMA) concept. TDMA is a technique in which several different calls may share the same carrier. Each call is assigned a particular time slot.

o speech coder—GSM uses linear predictive coding (LPC). The purpose of LPC is to reduce the bit rate. The LPC provides parameters for a filter that mimics the vocal tract. The signal passes through this filter, leaving behind a residual signal. Speech is encoded at 13 kbps.

1.7 GSM SPECTURM ALLOCATION

The mobile industry in India is divided between the two technologies GSM and CDMA. While the earlier service providers had adopted the GSM technology, the new players have been using CDMA technology and have
notched up a significant share of the Indian market.

Network operators in most of the world use the original GSM spectrum allocation i.e., 900 MHz (Only Vodafone uses 1800MHz). The frequency range allocated for cellular telephony purposes in the 1978 World Administrative Radio Conference (WARC) was 890-915 MHz for transmissions from mobile stations and 935-960 MHz for transmissions from fixed stations. In Europe the GSM networks generally use 900 MHz frequency band. 1800 MHz frequency is used in places where the capacity available at 900 MHz frequency band is not enough to cover the needs of the users.

Many modern European GSM phones are built as "dual band" phones, which can use both of those frequency bands, and automatically transparently to the user switch between those frequency bands as needed.

1.8 **ARCHITECTURE OF THE GSM NETWORK**

The GSM network\(^2\) is divided into three major systems: the switching system (SS), the base station system (BSS), and the operation and support system (OSS). The basic GSM network elements are shown in the Figure.1.1.
1.8.1 THE SWITCHING SYSTEM

The switching system (SS) is responsible for performing call processing and subscriber-related functions. The switching system includes the following functional units.

- **Home Location Register (HLR)**—The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the PCS operators, he or she is registered in the HLR of that operator.

- **Mobile Services Switching Center (MSC)**—The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others.

- **Visitor Location Register (VLR)**—The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile
station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

- **Authentication Center (AUC)**—A unit called the AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AUC protects network operators from different types of fraud found in today's cellular world.

- **Equipment Identity Register (EIR)**—The EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations. The AUC and EIR are implemented as stand-alone nodes or as a combined AUC/EIR node.

### 1.8.2 THE BASE STATION SUBSYSTEM

All radio-related functions are performed in the BSS, which consists of Base Station Controllers (BSCs) and the Base Transceiver Stations (BTSs).

- **BSC**—The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.

- **BTS**—The BTS handles the radio interface to the mobile station. The
BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlled by a BSC.

1.8.3 THE OPERATION AND SUPPORT SYSTEM (OSS)

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.

Other functional elements shown in Figure 1.1 are as follows:

- Message Center (MXE)—The MXE is a node that provides integrated voice, fax, and data messaging. Specifically, the MXE handles short message service, cell broadcast, voice mail, fax mail, e-mail, and notification.

- Mobile Service Node (MSN)—The MSN is the node that handles the mobile intelligent network (IN) services.
Gateway Mobile Services Switching Center (GMSC)—A gateway is a node used to interconnect two networks. The gateway is often implemented in an MSC. The MSC is then referred to as the GMSC.

GSM Inter Working Unit (GIWU)—The GIWU consists of both hardware and software that provides an interface to various networks for data communications. Through the GIWU, users can alternate between speech and data during the same call. The GIWU hardware equipment is physically located at the MSC/VLR.

1.9 GSM NETWORK AREAS

The GSM network\(^2\) is made up of geographic areas. As shown in Figure 1.2, these areas include cells, location areas (LAs), MSC/VLR service areas, and public land mobile network (PLMN) areas.

The cell is the area given radio coverage by one base transceiver station. The GSM network identifies each cell via the cell global identity (CGI) number assigned to each cell. The location area is a group of cells. It is the area in which the subscriber is paged. Each LA is served by one or more base station controllers, yet only by a single MSC shown in Figure 1.3. Each LA is assigned a location area identity (LAI) number.

An MSC/VLR service area represents the part of the GSM network that is covered by one MSC and which is reachable, as it is registered in the VLR of the MSC shown in Figure 1.4.
The PLMN service area is an area served by one network operator shown in Figure 1.5.

1.10 GSM SECURITY

GSM was designed with a moderate level of security. The system was designed to authenticate the subscriber using a pre-shared key and challenge-response. Communications between the subscriber and the base station can be encrypted. The development of UMTS introduces an optional USIM, that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user - whereas GSM only authenticated the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non-repudiation. GSM uses several cryptographic algorithms for security. The A5/1 and A5/2 stream ciphers are used for ensuring over-the-air voice privacy. A5/1 was developed first and is a stronger algorithm used within Europe and the United States; A5/2 is weaker and used in other countries. Serious weaknesses have been found in both algorithms: it is possible to break A5/2 in real-time with a cipher text-only attack, and in February 2008, Pico Computing, Inc revealed its ability and plans to commercialize FPGAs that allow A5/1 to be broken with a rainbow table attack. The system supports multiple algorithms so operators may replace that cipher with a stronger one.
1.11 GSM SUBSCRIBER SERVICES

- There are two basic types of services offered through GSM: telephony (also referred to as teleservices) and data (also referred to as bearer services). Telephony services are mainly voice services that provide subscribers with the complete capability (including necessary terminal equipment) to communicate with other subscribers. Data services provide the capacity necessary to transmit appropriate data signals between two access points creating an interface to the network. In addition to normal telephony and emergency calling, the following subscriber services are supported by GSM:
  - dual-tone multifrequency (DTMF) — DTMF is a tone signaling scheme often used for various control purposes via the telephone network, such as remote control of an answering machine. GSM supports full-originating DTMF.
  - facsimile group III — GSM supports CCITT Group 3 facsimile. As standard fax machines are designed to be connected to a telephone using analog signals, a special fax converter connected to the exchange is used in the GSM system. This enables a GSM-connected fax to communicate with any analog fax in the network.
  - short message services — A convenient facility of the GSM network is the 1/9/2006 short message service. A message consisting of a
maximum of 160 alphanumeric characters can be sent to or from a mobile station. This service can be viewed as an advanced form of alphanumeric paging with a number of advantages. If the subscriber's mobile unit is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has reentered the coverage area of the network. This function ensures that the message will be received.

- **cell broadcast**—A variation of the short message service is the cell broadcast facility. A message of a maximum of 93 characters can be broadcast to all mobile subscribers in a certain geographic area. Typical applications include traffic congestion warnings and reports on accidents.

- **voice mail**—This service is actually an answering machine within the network, which is controlled by the subscriber. Calls can be forwarded to the subscriber's voice-mail box and the subscriber checks for messages via a personal security code.

- **fax mail**—With this service, the subscriber can receive fax messages at any fax machine. The messages are stored in a service center from which they can be retrieved by the subscriber via a personal security code to the desired fax number.