Part One

|  |
| --- |
| Chapter 1: GSM |

* 1. **Introduction to GSM**

Short for Global system for Mobile communication s, GSM is a digital cellular communication system. It was developed in order to create a common European mobile standard but it has been rapidly accepted worldwide. GSM is designed to provide comprehensive range of services and features to the users available on analog cellular networks and in my cases very much in advance of old public switched telephone network (PSTN). In addition to digital transmission, GSM incorporate many advanced services and features like worldwide roaming in other GSM networks.

* 1. **Services Provided by GSM**

Services in GSM can be distinguished into four classes,

– Bearer Services

– Teleservices

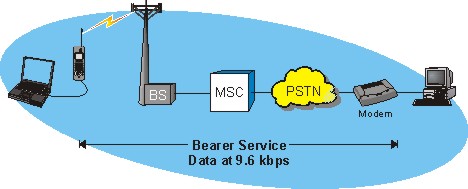
– Supplementary Services

– Value-added Services

**Bearer Services (BS)**

Bearer services are telecommunication services that are used to transfer user data and control signals between two pieces of equipment. Bearer services can range from the transfer of low speed messages (300 bps) to very high-speed data signals (10+ Gbps). Bearer services are typically categorized by their information transfer characteristics, methods of accessing the service, inter-working requirements (to other networks) and other general attributes. Information characteristics include data transfer rate, direction(s) of data flow, type of data transfer (circuit or packet) and other physical characteristics. The access methods determine what parts of the system control could be affected by the bearer service. Some bearer services must cross different types of networks (e.g. wireless and wired) and the data and control information may need to be adjusted depending on the type of network. Other general attributes might specify a minimum quality level for the service or special conditional procedures such as automatic re-establishment of a bearer service after the service has been disconnected due to interference. Some categories of bearer services available via the telephone system include synchronous and asynchronous data, packet data and alternate speech and data.

**Bearer Service Operation**



*Fig 1.1: Bearer Service Operation*

This figure shows a data transmission bearer service. In this diagram, a customer decides to send a data file to a computer that is connected to a public telephone network (at the office). In this example, the bearer service is 9.6 kbps circuit-switched data. The customer uses a modem to adapt their portable computer to the telephone network. The portable dials the office computer telephone number via the modem. The telephone system routes this call to a modem that connects the office computer to the telephone network. When the office computer modem accepts the call, the customer's modem begins to send data directly on the telephone line at channel at 28.8 kbps. Because the telephone system bearer service only provides 9.6 kbps data communication, the end-to-end transmission will be adjusted to 9.6 kbps.

**Teleservices or Telephony Services**

A Teleservice utilizes the capabilities of a Bearer Service to transport data, defining which capabilities are required and how they should be set up.

**Voice Calls**

The most basic Teleservices supported by GSM is telephony. This includes Full-rate speech at 13 Kbps and emergency calls, where the nearest emergency- service provider is notified by dialing three digits. A very basic example of emergency service is 911 service available in USA.

**Videotext and Facsimile**

Another group of teleservices includes Videotext access, Teletex transmission, Facsimile alternate speech and facsimile Group 3, Automatic facsimile Group 3 etc.

**Short Text Messages**

SMS (Short Messaging Service) service is a text messaging which allow you to send and receive text messages on your GSM Mobile phone. Services available from many of the world's GSM networks today - in addition to simple user generated text message services - include news, sport, financial, language and location based services, as well as many early examples of mobile commerce such as stocks and share prices, mobile banking facilities and leisure booking services.

# Supplementary Services

Supplementary services are provided on top of teleservices or bearer services, and include features such as caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

* **Multiparty Service or conferencing:** The multiparty service allows a mobile subscriber to establish a multiparty conversation. that is a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.
* **Call Waiting:** This service allows a mobile subscriber to be notified of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call. Call waiting is applicable to all GSM telecommunications services using a circuit-switched connection.
* **Call Hold:** This service allows a subscriber to put an incoming call on hold and then resume this call. The call hold service is only applicable to normal telephony.
* **Call Forwarding:** The Call Forwarding Supplementary Service is used to divert calls from the original recipient to another number, and is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost. A typical scenario would be a salesperson turns off his mobile phone during a meeting with customers, but does not wish to lose potential sales leads while he is unavailable.
* **Call Barring:** The concept of barring certain types of calls might seem to be a supplementary disservice rather than service. However, there are times when the subscriber is not the actual user of the Mobile Station, and as a consequence may wish to limit its functionality, so as to limit the charges incurred. Alternatively, if the subscriber and user are one and the same, the Call Barring may be useful to stop calls being routed to international destinations when they are routed. The reason for this is because it is expected that the roaming subscriber will pay the charges incurred for international re-routing of calls. So, GSM devised some flexible services that enable the subscriber to conditionally bar calls.
* **Number Identification:** There are following supplementary services related to number identification:
  + **Calling Line Identification Presentation:** This service deals with the presentation of the calling party's telephone number. The concept is for this number to be presented, at the start of the phone ringing, so that the called person can determine who is ringing prior to answering. The person subscribing to the service receives the telephone number of the calling party.
  + **Calling Line Identification Restriction:** A person not wishing their number to be presented to others subscribes to this service. In the normal course of event, the restriction service overrides the presentation service.
  + **Connected Line Identification Presentation:** This service is provided to give the calling party the telephone number of the person to whom they are connected. This may seem strange since the person making the call should know the number they dialled, but there are situations (such as forwardings) where the number connected is not the number dialled. The person subscribing to the service is the calling party.
  + **Connected Line Identification Restriction:** There are times when the person called does not wish to have their number presented and so they would subscribe to this person. Normally, this overrides the presentation service.
  + **Malicious Call Identification:** The malicious call identification service was provided to combat the spread of obscene or annoying calls. The victim should subscribe to this service, and then they could cause known malicious calls to be identified in the GSM network, using a simple command. This identified number could then be passed to the appropriate authority for action. The definition for this service is not stable.
* **Advice of Charge (AoC):** This service was designed to give the subscriber an indication of the cost of the services as they are used. Furthermore, those Service Providers who wish to offer rental services to subscribers without their own Subscriber Identity Module (SIM) can also utilize this service in a slightly different form. AoC for data calls is provided on the basis of time measurements.
* **Closed User Groups (CUGs):** This service is provided on GSM to enable groups of subscribers to only call each other. This type of service is being offered with special discount and is limited only to those members who wish to talk to each other.
* **Unstructured supplementary services data (USSD):** This allows operator-defined individual services.

**Value-added Services**

1. Missed Call Alerts is a service that allows an operator to notify their subscribers of calls they missed while their phone was off or unreachable. The notification is done through SMS messages listing the calling numbers and the time of the call attempts.
2. Outreach messaging solution is based on Roam ware SDS (Service Delivery System), and allows a Mobile Operator to send targeted messages using SMS.
3. Optimized Routing Service (OR) application will allow the operator’s subscribers and in-roamers to place calls to other in-roamers without the call being hauled over the international voice links. Based on the business decision of the operator, the mobile originated calls from the operator’s network can be optimally routed only to roamers in the same operator network or even to those who are on competitive networks in the same country.
4. Quick Info Service allows the users to send an SMS message to a particular number (e.g. 17777) with a short keyword like “nw” for news, “wh” for weather etc. The system then sends back an SMS message with the respective information as requested.
5. Multi-SIM MISM Service allows the users to use a unique MSISDN number in different SIM cards. This service consists of providing a specific number of secondary SIM cards to work on the same MSISDN number of the primary SIM card. Therefore, Subscribers can easily insert these SIM cards in different handsets and use them all without having to change SIMs between handsets.
6. Loyalty Management service enables mobile operators to deploy innovative rewards programs targeted at inbound and outbound roamers, creating a compelling incentive for roamers to actively choose their network. This service enables operators to attract and retain roamers to their network, enabling them to build a long-term and profitable relationship with their roamers.
7. Smart Call Assistance significantly makes local and international calls dialing easier for roamers by automatically correcting dialing mistakes introduced due to new and unfamiliar dialing codes and patterns in the visited network. This service essentially removes the hurdles faced by roamers in placing calls while roaming, and hence results in increased roaming calls directly driving roaming revenues for the operators.
   1. **GSM System Specification**

The system specifications for the GSM network are:

**Frequency band:** Uplink: 890MHz-915 MHz

Downlink: 935MHz-960MHz

**Extended GSM:** Uplink: 880MHz-890 MHz

Downlink: 925MHz-825MHz

**Duplex distance:** 45MHz

**Carrier separation:**  200KHz, (first career at 890.2MHz)

**Modulation:**  GMSK

**Air transmission rate:** 270kbps

**Access method:** TDMA

**Speech coder:** RPE-LTP-LPC (Regular pulse excitation

-Long Term prediction

-Linear Predictive coder)

**Adaptive Equalization**

For DCS networks the system specification is the same, except for the frequency band and duplex distance. The uplink is specified between 1780-1785 MHz and the downlink 1805-1880MHz. The duplex distance is 95MHz.

After it was decided that a digital system should be designed, the GSM group had to deal with the access method and the bandwidth.

**Access Method**

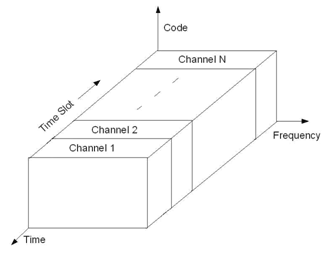
The digital system used TDMA (Time Division Multiple Access), where each carrier is divided into eight time slots. The mobile station sends and receives in the same time slot. This means that eight simultaneous conversations can take place on the same carrier.

In digital systems, continuous transmission is not required because users do not use the allotted bandwidth all the time. In such cases, TDMA is a complimentary access technique to FDMA. Global Systems for Mobile communications (GSM) uses the TDMA technique. In TDMA, the entire bandwidth is available to the user but only for a finite period of time. In most cases the available bandwidth is divided into fewer channels compared to FDMA and the users are allotted time slots during which they have the entire channel bandwidth at their disposal. [*Fig 1.2*]

TDMA requires careful time synchronization since users share the bandwidth in the frequency domain. The number of channels are less, inter channel interference is almost negligible. TDMA uses diﬀerent time slots for transmission and reception. This type of duplexing is referred to as Time division duplexing (TDD).

The features of TDMA include the following:

TDMA shares a single carrier frequency with several users where each user makes use of non-overlapping time slots. The number of time slots per frame depends on several factors such as modulation technique, available bandwidth etc. Data transmission in TDMA is not continuous but occurs in bursts. This results in low battery consumption since the subscriber transmitter can be turned OFF when not in use. Because of a discontinuous transmission in TDMA the handoﬀ process is much simpler for a subscriber unit, since it is able to listen to other base stations during idle time slots. TDMA uses diﬀerent time slots for transmission and reception thus duplexers are not required. TDMA has an advantage that is possible to allocate diﬀerent numbers of time slots per frame to diﬀerent users. Thus bandwidth can be supplied on demand to diﬀerent users by concatenating or reassigning time slot based on priority.

**

*Fig 1.2: The basic concept of TDMA.*

As discussed earlier, GSM is widely used in Europe and other parts of the world. GSM uses a variation of TDMA along with FDD. GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. It operates at either the 900 MHz or 1800 MHz frequency band. Since many GSM network operators have roaming agreements with foreign operators, users can often continue to use their mobile phones when they travel to different countries.

**Modulation**

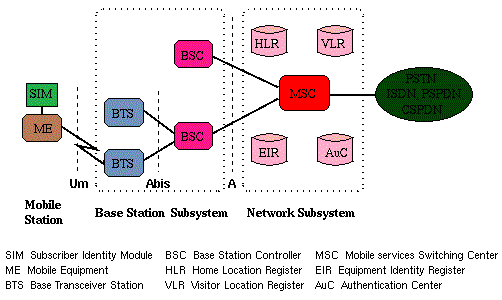
The chosen modulation method GMSK (Gaussian Minimum Shift Keying) is state of the art concerning modulations of digital signals. Further information on modulation method is referred to other literature.

* 1. **The GSM Network Architecture**

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements.

The GSM network can be divided into four main parts.

* The Mobile Station (MS)
* The Base Station Subscriber (BSS)
* The Network & Switching Subsystem (NSS)
* The Operation & Support Subsystem (OSS)



*Fig 1.2: Architecture of GSM Network*

**The mobile station (MS)**

A mobile station may be referred to as a handset, a mobile, a portable terminal or mobile equipment ME). It also includes a subscriber identity module (SIM) that is normally removable and comes in two sizes. Each SIM card has a unique identification number called IMSI (international mobile subscriber identity). In addition, each MS is assigned a unique hardware identification called IMEI (international mobile Equipment identity). In some of the newer applications (data communications in particular),a MS can also be a terminal that acts as a GSM interface, e.g. for a laptop computer. In this new application the MS does not look like a normal GSM telephone.

The seemingly low price of a mobile phone can give the (false) impression that the product is not of high quality. Besides providing a transceiver (TRX) for transmission and reception of voice and data, the mobile also performs a number of very demanding tasks such as authentication, handover, encoding and channel encoding.

**The base station subsystem (BSS)**

The base station subsystem (BSS) The base station subsystem (BSS) is made up of the base station controller (BSC) and the base transceiver station (BTS). The base transceiver station (BTS): GSM uses a series of radio transmitters called BTSs to connect the mobiles to a cellular network. Their tasks include channel coding/decoding and encryption/decryption. A

BTS is comprised of radio transmitters and receivers, antennas, the interface to the PCM facility, etc. The BTS may contain one or more transceivers to provide the required call handling capacity. A cell site may be omni directional or split into typically three directional cells. The base station controller (BSC): A group of BTSs are connected to a particular BSC which manages the radio resources for them. Today's new and intelligent BTSs have taken over many tasks that were previously handled by the BSCs. The primary function of the BSC is call maintenance. The mobile stations normally send a report of their received signal strength to the BSC every 480 MS. With this information the BSC decides to initiate handovers to other cells, change the BTS transmitter power, etc.

**The network subsystem (NSS)**

* The mobile switching center (MSC): Acts like a standard exchange in a fixed network and additionally provide all the functionality needed to handle a mobile subscriber. The main functions are registration, authentication, location updating, and handovers and call routing to a roaming subscriber. The signaling between functional entities (registers) in the network subsystem uses Signaling System 7 (SS7). If the MSC also has a gateway function for communicating with other Networks, it is called Gateway MSC (GMSC).
* The home location register (HLR): A database used for management of mobile subscribers. It stores the international mobile subscriber identity (IMSI), mobile station ISDN number (MSISDN) and current visitor location register (VLR) address. The main information stored there concerns the location of each mobile station in order to be able to route calls to the mobile subscribers managed by each HLR. The HLR also maintains the services associated with each MS. One HLR can serve several MSCs.
* The visitor location register (VLR): Contains the current location of the MS and selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. A VLR is connected to one MSC and is normally integrated into the MSC's hardware.
* The authentication center (AuC): A protected database that holds a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel. The
* AuC provides additional security against fraud. It is normally located close to each HLR within a GSM network.
* The equipment identity register (EIR): The EIR is a database that contains a list of all valid mobile station equipment within the network, where each mobile station is identified by its international mobile equipment identity (IMEI). The EIR has three databases: ± White list: for all known, good IMEIs ± Black list: for bad or stolen handsets ± Grey list: for handsets/IMEIs that are uncertain

**Operation and Maintenance Center (OMC)/ Operation and support Subsystem (OSS)**

The OMC is a management system that oversees the GSM functional blocks. The OMC assists the network operator in maintaining satisfactory operation of the GSM network. Hardware redundancy and intelligent error detection mechanisms help prevent network down-time. The OMC is responsible for controlling and maintaining the MSC, BSC and BTS. It can be in charge of an entire public land mobile network (PLMN) or just some parts of the PLMN.

Providing voice or data transmission quality over the radio link is only part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally, requiring standardized call routing and location updating functions in GSM networks. A public communications system also needs solid security mechanisms to prevent misuse by third parties. Security functions such as authentication, encryption and the use of Temporary Mobile Subscriber Identities (TMSIs) are an absolute must.

* 1. **Network Operations:**

In GSM five main functions can be defined, these are,

* Transmission
* Radio Resource Management(RRM)
* Mobility Management(MM)
* Communication Management(CM)
* Operation, Administration & Maintenance(OAM)

**Transmission**

This is transmission of data and signaling. This is not all the components of the GSM network are strongly related with both types of Tx. While the MSC BTS and BSC among others, are involved with data and signaling components such as HLR, VLR, or EIR registers are only concerned with signaling.

**Radio Resource Management (RRM)**

The role of RR function is to establish, maintain and release communication links between Mobile stations and MSC. The elements that are mainly concerned with the RR function are the MN and the BTS. However, since the RR component performs connection management also during cell handoff, it also affects the MSC which is the handoff management component.

The RR is also responsible for the management of frequency resources as well as varying radio interface conditions. Main component operations are:

* Channel assignment, Change and relies.
* Handoff
* Frequency Hopping.
* Power-level control.
* Discontinuous transmission and reception.
* Timing advance.

**Handoff**

Mobility and radio resource management plays a major role in Quality of Service provisioning for cellular communication systems. Due to the limited radio coverage of a cell, an ongoing call while being handed off may get dropped. We develop an effective and efficient handoff scheme using mobile controlled handoff and fractional guard channel techniques, where mobile station measures the signal strength from surrounding base stations and interference level on all channels. A handoff can be initiated if the signal strength of the serving base station is lower than that of other base station by certain threshold. Two models are proposed to calculate the blocking probability of new calls and the dropping probability of handoff calls, using call admission control scheme in a cellular system. Numerical analyses of both the models are carried out to investigate the impact on performance of the parameters and comparisons with conventional channel reservation schemes. [*Fig 1.3*]

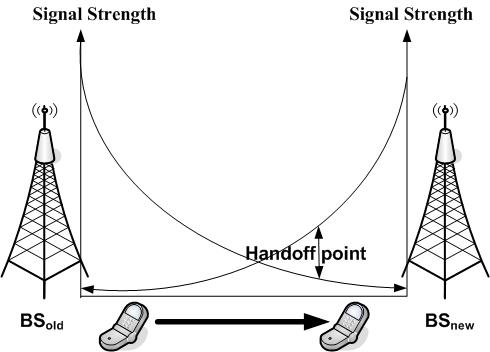
The user movement may change in the channel /cell, when the quality of the communication is degrading, which is known as handoff. Handoff occurs between:

* Channels within a cell.
* Cells controlled by the same BSC.
* Cells under the same MSC but controlled by different BSCs
* Cells controlled by different MSCs

Handoffs are mainly controlled by the MSCs. However to avoid unnecessary signaling, the first two types of handoffs are managed by the respective BSC (thus the MSC is only notified of the handoff).

The process of transferring a mobile user from one channel or base station to another –

* Important task in any cellular radio system.
* Must be performed successfully, infrequently and imperceptible to users.
* Identify a new base station.
* High priority than initiation request (block new calls rather than drop existing calls).



*Fig 1.3: Handoff*

To perform the handoff the mobile station controls continuously its own signal strength of the neighboring strength of the neighboring cells. The list of cells that must be monitored by the mobile station is given by the base station. Power measurements allow deicing which is the best cell in order to maintain the quality of the communication link.

Two basic algorithms are used for handoffs:

* The **minimum acceptance performance algorithm**. When the quality of the transmission degrades, the power level of the mobile is increased, until the increase of the power level has no effect on the quality of the signal. Upon this link layer hint, a handoff is initiated.
* The **power budget algorithm**. Here the hand off pre-empts the power increase to be obtain a good SIR.

**Mobility Management (MM)**

The MM component management handles:

* **Location management:** Location is managed through periodically or on-demand. At power on lime, the MH signals an IMSI attach. On-demand location updates are signaled when the MN moves to a different PLMN or new location area (LA). The signal is sent to a new MSC/VLR, which forwards it to the subscriber’s HLR. Upon authorization in the new MSC/VLR. If after the update time interval, the MN at the old MSC/VLR. If after the update time interval, the MN has not registered, it is then deregistered. On power-off, the MN performs an IMSI detach.
* **Security and Authorization:** Authorization involves the SIM card and the Authentication center. A secret key, stored in the SIM and the AuC together with a ciphering algorithm called A3, are used to authenticate the user. The MN and AuC compute a SRES through A3 using the secret key and nonce generated by the AuC. If the two computed SRES are the same, the subscriber is checked. Now the security check is performed in the equipment identity (IMEI). If the IMEI number is of the mobile is authorized in the EIR, the mobile station is registered with a Temporary Mobile Subscriber Identity (TMSI) after the first location update procedure. Enciphering is another option to guarantee a very strong security.

**Communication Management (CM):**

The CM component manages:

* Call Control (CC) it controls call setup, management and tear-down in relation to management of type of service. Call routing is the primary task for this component. To reach the mobile subscriber, a user dials the mobile subscriber ISDN(MISDN) which includes :
* A country code
* A national destination code, this identifies the subscriber’s operator
* A code mapping to the subscriber’s HLR.
* The call is passed to GSMSC (if the call is originated from the fixed network) that knows the HLR for call routing information. The HLR requests this information from subscriber’s current VLR. This VLR allocates temporarily a mobile station routing number (MSRN) for the call. The MSRN number is the information returned by the HLR to GMSC. It is latter that routes the call through the MSRN number, LA, the mobile is paged.
* Supplementary Services Management: This in involves the MN and the HLR.

SMS management: here the GMS network contents the short message service center through two following interfaces:

* SMS-GMSC for mobile terminating Short Messages (SMS-MT/PP). It has the same role as the GMSC.
* SMS-IWMSC for mobile originating Short message (MSM-MO/PP).

**Operation, Administration and Maintenance (OAM)**

The OAM component allows the operator to monitor and control the system as well as modify the configuration of the elements of the system. Not only the OSS is part of the OAM, but also the BSS and NSS participate in the function such as:

* Provide the operator with all the information it needs. The info. is forward to the OSS to control the network.
* Perform self-test tasks in addition to the OAM function.
* Control of Multiple BTSs by the BSS.

Teletalk Bangladesh LTD started their network upgrade from GPRS network. EDGE (known as 2.75G) network is set up after GPRS. In the beginning of 2013 they launched their 3G network based on Circuit switching.

* 1. **GSM Development Evolution**

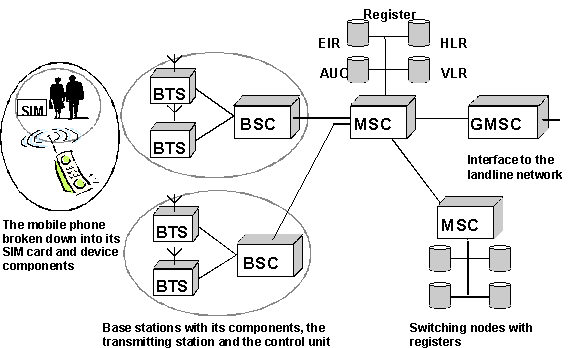
Teletalk Bangladesh Ltd. started their network upgrade from GPRS network. EDGE (known as 2.75G) network is set up after GPRS. In the beginning of 2013 they launched their 3G network based on circuit switching. [*Fig 1.4*]

*Fig 1.4: Data rate of EDGE and GPRS*

* 1. **Call Flow In GSM Networks**

GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. 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. Pico cells are small cells whose coverage diameter is a few dozen meters; they are mainly used indoors. Femto cells 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.

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).



*Fig 1.5: Call Flow*