Chapter Publication

Domain: MOBILE COMPUTING

Subdomain: GSM

Author By:

Mr. Vivek T. Patil

Assistant Professor,

Dr. D. Y. Patil College of Engineering Akurdi Pune,

Teaching Experience: 6+ Years

PHD Perusing From Visvesvaraya Technological University

Publication Date: December 2018
Web: www.aspirepublishers.com
Email: info@aspirepublishers.com

INDEX

List of Figures

CHAPTER 1

GSM

1.1 GSM ARCHITECTURE

The GSM spec consists of 3 major subsystems:

Mobile Station (MS)

Base Station system (BSS)

Network and switch system (NSS)

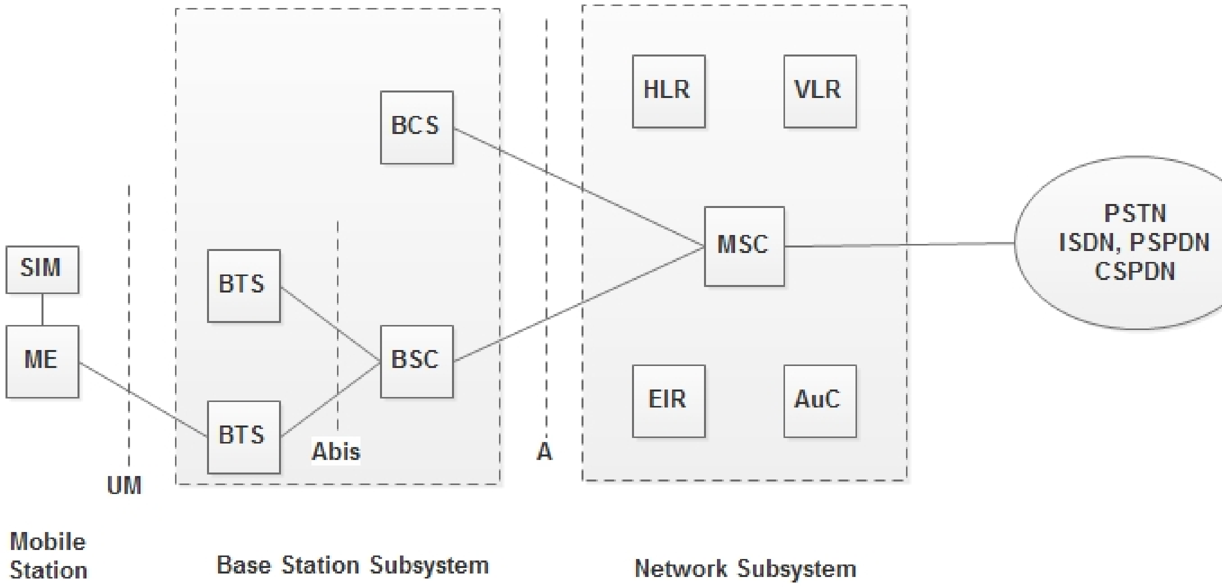

Figure 1.1: GSM ARCHITECTURE

The wireless link interface between the MS and the Base Transceiver Station (BTS), that may be a a part of BSS. several BTSs are controlled by a Base Station Controller (BSC). BSC is connected to the Mobile switch Center (MSC), that may be a a part of NSS. Figure shows the key useful parts within the GSM spec.

MOBILE STATION (MS):

A mobile station communicates across the air interface with a base station transceiver within the same cell during which the mobile subscriber unit is found. The MS communicates the data with the user and modifies it to the transmission protocols if the air-interface to communicate with the BSS. The user?s voice data is interfaced with the MS through a mike or microphone and speaker for the speech, keypad, and show for short messaging, and therefore the cable connection for alternative data terminals. The MS has 2 parts. The Mobile equipment (ME) refers to the physical device, that includes of transceiver, digital signal processors, and therefore the antenna. The second part of the MS is that the GSM is that the Subscriber Identity Module (SIM). The SIM card is exclusive to the GSM system. it's a memory of 32 KB.

BASE STATION SCHEME (BSS):

A base station scheme consists of a base station controller and one or additional base transceiver station. every Base Transceiver Station defines one cell. A cell will have a radius of between 100m to 35km, counting on the surroundings. A Base Station Controller is also connected with a BTS. it's going to management multiple BTS units and thus multiple cells. There are 2 main field parts within the BSS ? the base Transceiver system (BTS) and also the Base Station Controller (BSC). The interface that connects a BTS to a BSC is named the A-bis interface. The interface between the BSC and the MS is called the A interface, that is standardised inside GSM.

NETWORK AND SWITCH SCHEME (NSS)

The NSS is accountable for the network operation. It provides the link between the cellular network and therefore the Public switched telecommunicates Networks (PSTN or ISDN or knowledge Networks). The NSS controls handoffs between cells in several BSSs, authenticates user and validates their accounts, and includes functions for sanctioning worldwide roaming of mobile subscribers. specifically the switch scheme consists of:

- Mobile switch center (MSC)
- Home location register (HLR)
- Visitor location Register (VLR)
- Authentications center (Auc)
- Equipment Identity Register (EIR)

- Interworking Functions (IWF)

The NSS has one hardware, Mobile switching center and four software information element: Home location register (HLR), visitor location Register (VLR), Authentications center (Auc) and equipment Identity Register (EIR). The MS primarily performs the switch operate of the system by controlling calls to and from alternative telephone and information systems. It includes functions like network interfacing and customary channel signalling.

1.1.1 HLR:

The HLR is information software that handles the management of the mobile subscriber account. It stores the subscriber address, service kind, current locations, forwarding address, authentication/ciphering keys, and billings data. additionally to the ISDN number for the terminal, the SIM card is known with an international Mobile Subscribes Identity (IMSI) number that's completely totally different from the ISDN number. The HLR is that the reference information that for good stores knowledge associated with subscribers, together with subscriber?s service profile, location data, and activity standing.

1.1.2 VLR:

The VLR is temporary information software the same as the HLR identifying the mobile subscribers visiting within the coverage area of an msc. The VLR assigns a temporary mobile subscriber Identity (TMSI) that's wont to avoid using IMSI on the air. The visitor location register maintains data regarding mobile subscriber thatis presently physically within the range covered by the switch center. once a mobile subscriber roams from one LA (Local Area) to a different, current location is mechanically updated within the VLR. once a mobile station roams into afresh msc area, if the recent and new LA?s are under the control of 2 totally different VLRs, the VLR connected to the MS can request information regarding the mobile stations from the HLR. The entry on the recent VLR is deleted and an entry is made within the new VLR by repetition the information from the HLR.

1.1.3 AuC:

The auc information holds totally different algorithms that are used for authentication and encryptions of the mobile subscribers that verify the mobile user?s identity and make sure the confidentiality of every decision. The auc holds the authentication and encoding keys for all the subscribers in each the house and visitant location register.

1.1.4 EIR:

The EIR is another information that keeps the knowledge regarding the identity of mobile equipment such the International mobile equipment Identity (IMEI) that reveals the details regarding the manufacturer, country of production, and device kind. This data is employed to prevent calls from being ill-used, to forestall unauthorised or defective MSs, to report taken movables or check if the mobile phone is working consistent with the specification of its kind.

1.1.5 White list:

This list contains the IMEI of the phones who are allowed to enter within the network.

1.1.6 Black list:

This list on the contrary contains the IMEI of the phones who are not allowed to enter within the network, for instance because they're taken.

1.1.7 Grey list:

This list contains the IMEI of the phones momentarily not allowed to enter within the network, for instance as a result of the software version is just too recent or because they're in repair.

1.1.8 IWF-

Interworking Function: it's a system within the PLMN that permits for non speech between the GSM and the alternative networks. The tasks of an IWF are significantly to adapt transmission parameters and protocol conversions. The physical manifestations of an IWF is also through a modem that is activated by the msc obsessed on the bearer service and the destination network. The OSS (Operational Support Systems) supports operation and maintenance of the system and permits engineers to observe, diagnose, and troubleshoot each facet of the GSM network.[1]

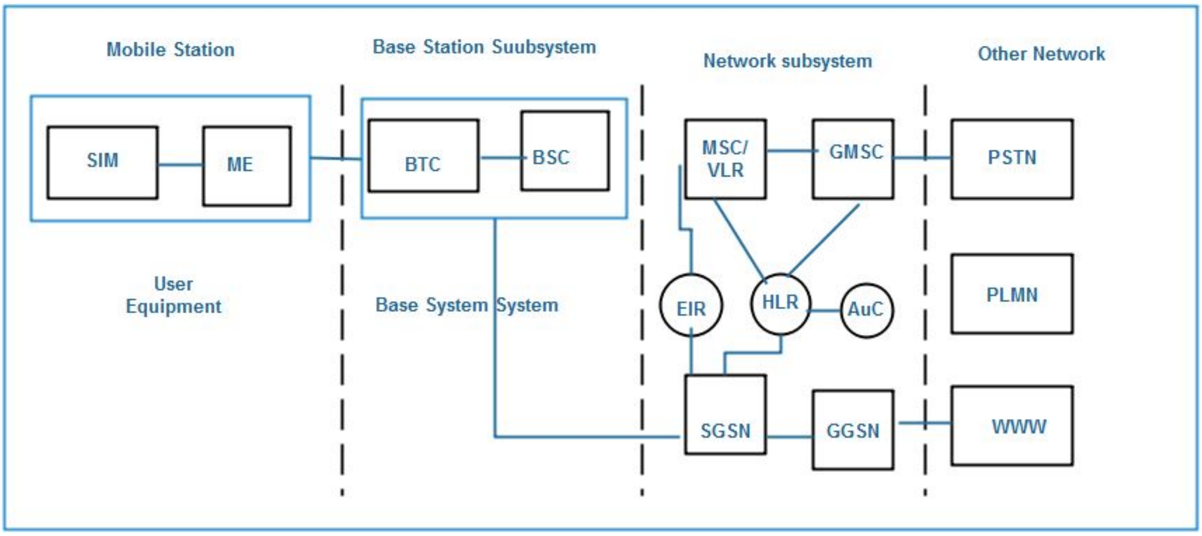

Figure 1.2: BLOCK AND ARCHITECTURE DIAGRAM

1.2 USER EQUIPMENT (UE)

These are the users .Number of users are controlled by one BTS

1. The mobile stations (MS) communicate with the base station system over the radio the radio interface.

2. The BSS referred to as as radio the system, provides and manages the radio transmission path between the mobile stations and the Mobile switching Centre(MSC).It additionally manages radio interface between the mobile stations and different subsystems of GSM.

3. every BSS contains several Base Station Controllers(BSC) that connect the

mobile station to the network and shift system (NSS) through the mobile shift center

4. The NSS controls the switching functions of the GSM system.It permits the mobile switching center to communicate with networks like PSTN, ISDN, CSPDN, PSPDN and different information networks.

5. The operation network (OSS) permits the operation and mantanance of the GSM system. It permits the system engineers to diagnose,troubleshoot and observe the parameters of the GSM systems.The OSS system interacts with the opposite subsystems and is provided for the GSM in operation company staff that gives service facilities for the network.

1.2.1 Base station(BSS)

the following stations subsystem contains of 2 parts:
1. Base Transceiver Station (BTS).
2. Base Station Controller(BSC).
The BSS consists several BSC that hook up with one master's degree. every BSC controls upto many hundred BTS.

1.2.2 Base Transreciver Station(BTS)-

It has radio transreciever that outline a cell and are capable of handelling communication system protocols with MS.
Functions of BTS are

1. Handelling radio link protocols

2. Providing FD communication to MS.

3. Interliving and de interliving.

Base station controller(BSC) IT manages radio resources for one or additional BTS.It controls many hundred BTS al are connected to single msc.
Functions of BTS are

- to manage BTS.
- Radio resource management
- handoff management and management
- Radio channel setup and frequency hoping

1.2.3 Network subsystem

1.It handels the switching of GSM calls between external networks and indoor BSC

2.It includes 3 totally different information bases for quality management as

- HLR (Home Location Register)
- VLR (Visitor Location Register)
- auc (Authentication center)

1.2.4 Mobile switching center (MSC)

It connects fix networks like ISDN ,PSTN etc. Following are the functions of msc

1. Call setup, supervising and relies
2. assortment OF billing data
3. decision handelling / routing
4. Management of signelling protocol
5. Record of VLR and HLR

1.2.5 HLR (Home Location Register)

Call roaming and decision routing capabilities of GSM are handeled.It stores all the adminstartive data of sub scriber registered within the networks.IT maintance distinctive international mobile subscriber identity.(IMSI).

1.2.6 VLR (Visitor Location Register)

it's a brief information base.It stores the IMSC number and costomer data for every roaming client visiting specific master's degree.

1.2.7 Authentication center

it's protected info .It maintance authentication keys and algorithms.It contain s areg-ister called as equipment Identity Register.

1.2.8 Operation subsystem

IT manages all mobile equipment within the system 1)management for charging and asking procedure 2)To maintain all hardware and network operations Interfaces used for GSM network : (ref fig 12)

1. UM Interface Used to communicate between BTS with MS
2. Abis Interface- wont to communicate BSC TO BTS
3. A Interface– wont to communicate BSC and msc
4. Singling protocol (SS 7)- wont to communicate msc with different network . [1]

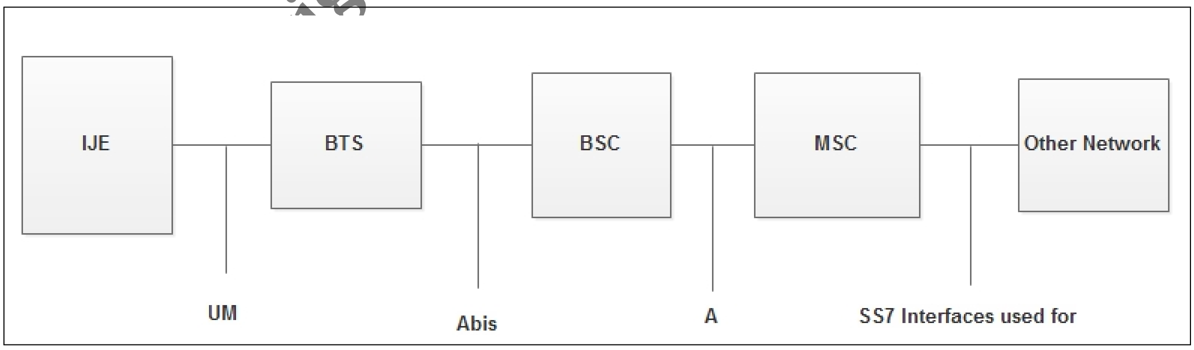

Figure 1.3: GSM NETWORK INTERFACE

1.3 IDENTIFIERS IN GSM

Following is the list of various identifiers used in GSM.

1. IMEI - International Mobile Equipment Identity
2. IMSI - International Mobile Subscriber Number
3. TMSI - Temporary Mobile Subscriber Identity
4. LMSI - Local Mobile Subscriber Identity
5. MSISDN - Mobile Subscriber International ISDN number
6. MSRN - Mobile Subscriber Roaming Number
7. LAI - Location Area Identity
8. CI - Cell Identifier
9. BSIC - Base Station Identity Code

1.3.1 IMEI - International Mobile Equipment Identity

Its an internationally-unique serial number allocated to Mobile Station (MS) hardware at the time of manufacture. It is registered by the network operator & stored in Authentication Center (AuC) for Validation purpose. This number consists of type approval code, final assembly code and serial number of the mobile station. The network stores the IMEI numbers in the Equipment Identity Register (EIR).

1.3.2 IMSI - International Mobile Subscriber Number

Each registered user is uniquely identified by its international mobile subscriber identity (IMSI). It is stored in the subscriber identity module (SIM). A mobile station can only be operated if a SIM with a valid IMSI is inserted into equipment with a valid IMEI.

1.3.3 There are following parts of an IMSI:

Mobile Country Code (MCC): 3 decimal places, internationally standardized.
Mobile Network Code (MNC): 2 decimal places, for unique identification of mobile network within the country.

Mobile Subscriber Identification Number (MSIN): Maximum 10 decimal places, identification number of the subscriber in the home mobile network.

1.3.4 TMSI

Temporary Mobile Subscriber Identity Its used to protect the true identity (IMSI) of a subscriber. It is issued by & stored within a VLR (not in the HLR) when an IMSI attach takes place or a Location Area (LA) updates takes place. The issues TMSI only has validity within a specific LA. The TMSI is used for security purposes, so that the IMSI of a subscriber does not have to be transmitted over the air interface. Its a temporary identity, which regularly gets changed.

1.3.5 LMSI - Local Mobile Subscriber Identity

The VLR can assign an additional searching key to each mobile station within its area to accelerate database access. This unique key is called the Local Mobile Subscriber Identity (LMSI). The LMSI is assigned when the mobile station registers with the VLR and is also sent to the HLR.

1.3.6 MSISDN - Mobile Subscriber ISDN Number

The real telephone number of a mobile station is the mobile subscriber ISDN number (MSISDN). It is assigned to the subscriber (his or her SIM, respectively), such that a mobile station set can have several MSISDNs depending on the SIM. The MSISDN categories follow the international ISDN number plan and therefore have the following structure: Country Code (CC) : Up to 3 decimal places. National Destination Code (NDC): Typically 2-3 decimal places. Subscriber Number (SN): Maximum 10 decimal places.

1.3.7 MSRN - Mobile Subscriber Roaming Number

It is temporary, location-dependent ISDN number issued by the parent VLR to all MSs within its area of responsibility. It is stored in VLR associated HLR but not in the MS. The MSRN is used by VLR associated MSC for call routing within MSC/VLR service area.

MRSN = CC + NDC + SN

LAI - Location Area Identity

Each location area within PLMN (Public Landline Mobile Network) has an associated Internationally unique identifier (LAI). The LAI is broadcasted regularly by the BTSs on the Broadcast Control Channel (BCCH), thus uniquely identify each cell within an associated location area (LA). It structure is as follows,

1.3.8 LAI = MCC + MNC + LAC

MCC= Mobile Country Code (of the visited country)

MNC= Mobile Network Code (of the serving PLMN)

LAC= Location Area Code

1.3.9 CI - Cell Identifier

Within an LA, the individual cells are uniquely identified with a cell identifier (CI), maximum 2 x 8 bits. Together with the global cell identity (LAI + CI) calls are thus also internationally defined in a unique way.

1.3.10 BSIC - Base Station Identity Code

Each BTS is issued with a unique identity, the BSIC is used to distinguish neighboring BTSs. It is needed to identify that the frequency strength being measured by the mobile station is coming from a particular base station.[2]

1.4 SPECTRUM ALLOCATION

Definition - What does Spectrum Allocation mean?

Spectrum allocation is that the method of regulation the utilization of the spectrum and dividing it among varied and generally competitory organizations and interests. This ensures that there's very little competition once employing a specific waveband, which may cause interference if constant waveband is used for various and unregulated functions. This regulation is controlled by varied governmental and international organizations.
Spectrum allocation is additionally called frequency allocation.

Spectrum Allocation

Spectrum allocation came to be owing to the rising and convergence of wireless telecommunications technology that created vast demands on the oftenness spectrum for varied services like high-speed knowledge transfer and communication. Therefore, the aim of varied spectrum policies and laws is that the regulation and management of the resource (the magnetic force spectrum) for the benefit of everyone using it. This essentially implies that spectrum allocation is completed to prevent major interference and chaos within the air waves, which might serve nobody in the least. Imagine a four-lane road that's quite tiny for route standards which there's no regulation wherever totally different vehicles square measure allowed to travel in. Now, contemplate that there's a fleet of enormous trucks moving along and driving at a slower speed for safety. while not regulation on that lane they'll drive in, the varied members of this fleet of trucks would use all four lanes, effectively block all alternative vehicles. This causes all alternative vehicles behind to travel at speeds slower than or capable those of the trucks since there's no approach for them to pass. this can be the aim of spectrum allocation, to easily place everything in its place, during this case in an exceedingly specific radio spectrum, to prevent interference and chaos.
Some standardization organizations acting on spectrum allocation and regulation:
European Conference of communication and Telecommunications Administrations

(CEPT)

International Telecommunication Union (ITU)

Inter - American Telecommunication Commission (CITEL)

Types of spectrum allocation

No one could transmit - Spectrum band is reserved for a particular use like radio astronomy so that there's no interference with radio telescopes

Anyone could transmit - As long as transmission power limits square measure revered

Only authorised users/organizations of the particular band could transmit - Examples are cellular and tv spectrums additionally as amateur oftenness allocations[3]

1.5 GSM CHANNELS

For long distances, Speech and Visual communications cannot be done. Such communications may be performed up to few kilometres using wire communication. therefore wireless communication is required for long distance Communication. If it's a wireless Communication, desires modulation and demodulation of the signal. Signals like speech, Music, news, pictures, scientific information, business transactions, military actions, entertainment, education, all may be handled electronically. Immediacy and flexibility makes transmission a basic key to success and progress. therefore wireless communication is speedy, versatile and secret. once a cellular phone is switched on, it instantly contacts the closest radio station. this can be known as location update . The station relays this data to the closest exchange, that stores the data. The radio stations are regularly broadcasting a number of data. This data is transmitted with the help of communication channels in GSM. additionally to the current, GSM Identities provides singularity to the user, on the bases of Subscriber, Location, and instrumentality.

1.5.1 GSM Physical Channels

A single GSM RF carrier will support up to eight MS subscribers simultaneously. every channel occupies the carrier for one eighth of the time. this can be a way known as Time Division Multiple Access. Time is split into separate periods known as timeslots. The timeslots are organized in sequence and area unit conventionally numbered zero to seven [4]. every repetition of this sequence is named a TDMA frame. every MS telephone call occupies one timeslot (07) inside the frame till the decision is terminated, or a relinquishing happens [2]. The TDMA frames are then designed into additional frame structures in keeping with the sort of channel. For such a system to figure properly, the temporal order of the transmissions to and from the mobiles is important. The MS or Base Station should transmit the knowledge associated with one call at precisely the right moment, or the timeslot are incomprehensible . The information carried in one timeslot is named a burst. Each data burst, occupying its allotted timeslot inside sequent TDMA frames, provides one

GSM physical channel carrying a varied variety of logical channels between the MS and BTS

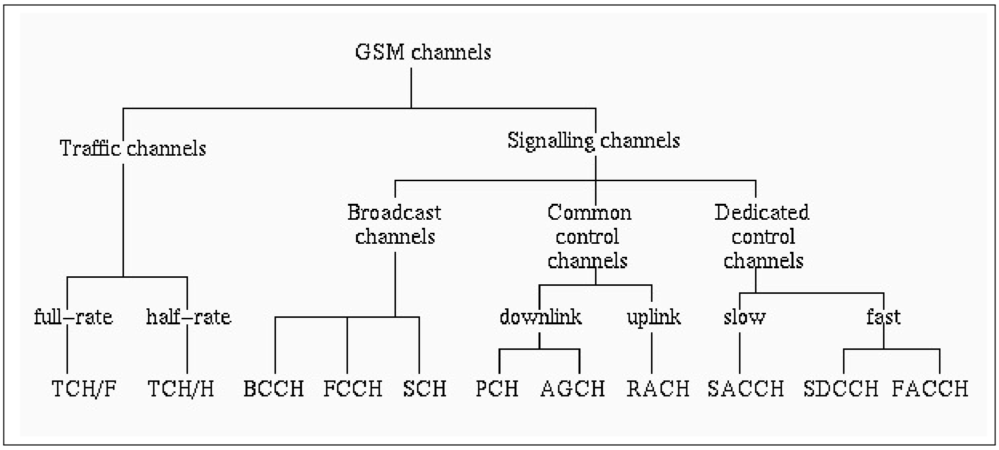

Figure 1.4: GSM CHANNELS

1.5.2 GSM Logical Channels

GSM Logical Channels consists of 2 types: control Channels and Traffic Channels.

1. control Channels

Control Channels additional consists of 3 groups specifically Broadcast control Channel, Common control Channel and Dedicated control Channel.

Broadcast control Channel (BCH)

the broadcast control Channels are downlink solely (BSS to MS) and it carries the CGI (Cell world Identity). It also sends control data to MS (Mobile Station). The information carried on the BCCH is monitored -by the MS periodically (at least each thirty sec), once it's switched on and not in a call.

Synchronization Channel (SCH)

The Synchronizing Channel (SCH) helps to synchronise TDMA Frame. It additionally sends the BSIC price to MS. The MS will monitor BCCH data from close cells and stores the knowledge from the most effective six cells. The SCH information on these cells is additionally hold on so the MS may quickly resynchronize once it enters a brand new cell.

Frequency Correction Channel (FCH)

Frequency Correction Channel (FCCH) permits the mobile to synchronize its own frequency thereto of the sending base site. It acts as a flag to the mobile to spot Timeslot 0 as a result of it should solely sent throughout slot zero on BCCH carrier frequency.

2. Common control Channel

The Common control Channel (CCCH) is accountable for transferring control data between all mobiles and therefore the BTS.

Random Access control Channel (RACH)

Random Access Channel (RACH) helps MS to assign with network and utilized by the mobile once it needs to realize access to the system. this happens once the mobile initiates a decision or responds to a page.

Paging control Channel (PCH)

Paging control Channel (PCH) helps network to assign with MS and additionally utilized by BTS (Base transceiver station) to page MS.

Access Grant control Channel (AGCH)

Access Grant control Channel (AGCH) is used by network to assign signalling upon successful decodation of Burst.

Cell Broadcast control Channel (CBCH)

Cell Broadcast control Channel (CBCH) tells from that BTS (Base Transceiver Station) we are getting coverage (RX Level) additionally MS has feature of Cell data display that display the name of website ID with that we are barred [4].

3. Dedicated control Channel

Dedicated control Channels are each uplink and Downlink and has additional categories: SDCCH, SACCH, and FACCH

Stand Alone Dedicated control Channel (SACH)

Stand Alone Dedicated control Channel (SDCCH) is used by MS for Location Updation, SMS, and Authentication.

Slow Associated control Channel (SACCH)

Slow Associated control Channel (SACCH) sends control information (Power Control) in downlink and mensuration reports (Link Quality Reports) in uplink.

fast Associated control Channel (FACCH)

Fast Associated management Channel is transmitted rather than a TCH. The FACCH steals the TCH (Traffic control Channel) burst and inserts its own data. The FACCH is employed to hold out user authentication, handovers and immediate assignment.

2. Traffic Channels

The traffic channel carries speech or information data. It is further of 2 types: Full Rate and half Rate that are of once more of 2 sorts specifically internet Rate and Gross Rate

A. Full Rate/ half Rate

In Full Rate, one Subscriber uses one interval which implies in TDMA Frame there are total eight Subscribers whereas case of half Rate, one interval is used by two Subscribers on sharing bases that means sixteen Subscribers in one TDMA Frame [2].

B. net Rate/ Gross Rate

Net Rate refers to the information Rate before Channel writing whereas Gross Rate refers to rate when channel coding.

1.6 GSM BURST

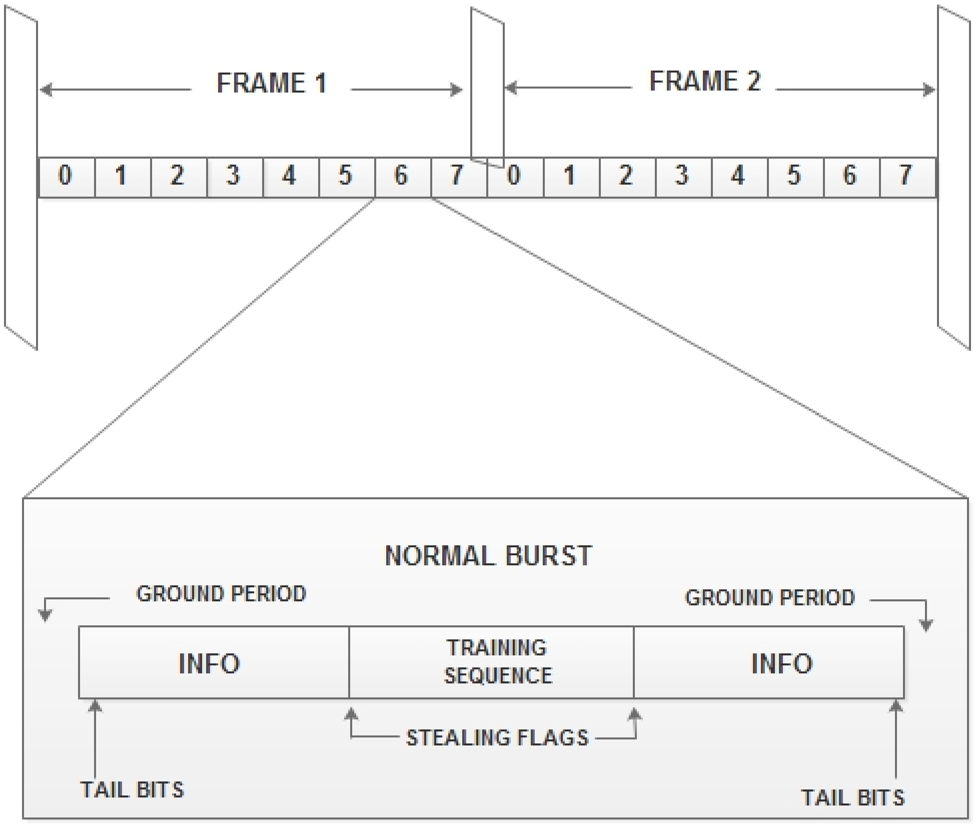

Figure 1.5: GSM BURST ARCHITECTURE

Info

This is the world in which the speech, knowledge or control info is held.

Guard period

The BTS and MS will solely receive the burst and decrypt it, if it's received inside the timeslot selected for it. The timing, therefore, should be extraordinarily correct, however the structure will yield atiny low margin of error by incorporating a guard period as shown within the diagram. To be precise, the timeslot is 0.577 ms long, whereas the burst is simply 0.546 ms long, thus there's a time distinction of 0.031 ms to modify the burst to hit the timeslot.

Stealing Flags

These 2 bits area unit set once a traffic channel burst has been stolen by a FACCH (the quick Associated management Channel). One bit set indicates that half the block has been taken.

Training Sequence

This is employed by the receivers equalizer because it estimates the transfer characteristic of the physical path between the BTS and also the MS. The coaching sequence is twenty six bits long.

Tail Bits

These are wont to indicate the beginning and end of the burst.

Burst types

The diagram below shows the 5 forms of burst utilized within the GSM air interface. All bursts, of no matter kind, have to be compelled to be regular in order that they're received inside the acceptable timeslot of the TDMA frame.
The burst is that the sequence of bits transmitted by the BTS or MS, the timeslot is that the distinct amount of real time inside that it should arrive so as to be properly decoded by the receiver:

Normal Burst

The normal burst carries traffic channels and every one forms of management channels.

Frequency Correction Burst

This burst carries FCCH downlink to correct the frequency of the MSs local oscillator, effectively protection it to it of the BTS.

Synchronization Burst

So called because its perform is to hold SCH downlink, synchronizing the temporal arrangement of the MS to it of the BTS.

Dummy Burst

Used once there's no info to be carried on the unused timeslots of the BCCH Carrier (downlink only).

Access Burst

This burst is of a lot of shorter length than the opposite varieties. The increased guard amount is important as a result of the timing of its transmission is unknown. once this burst is transmitted, the BTS doesn't know the placement of the MS and so the timing of the message from the MS can't be accurately accounted for. (The Access Burst is uplink solely.)

1.7 GSM FRAME

1.7.1 GSM FRAME STRUCTURE

GSM frame structure uses slots, frames, multiframes, superframes and hyperframes to convey the specified structure and timing to the info transmitted.

The GSM system has a outlined GSM frame structure to modify the orderly passage of data. The GSM frame structure establishes schedules for the preset use of times-lots.

By establishing these schedules by the use of a frame structure, each the mobile and the base station are able to communicate not solely the voice information, but also signalling info while not the various forms of information becoming intermixed and each ends of the transmission knowing specifically what forms of info are being transmitted.

The GSM frame structure provides the idea for the varied physical channels used among GSM, and consequently it's at the center of the system.

Basic GSM frame structure

The basic component within the GSM frame structure is that the frame itself. This contains the eight slots, every used for various users among the TDMA system. As mentioned in another page of the tutorial, the slots for transmission and reception for a given mobile are offset in time in order that the mobile doesn't transmit and receive at a similar time.

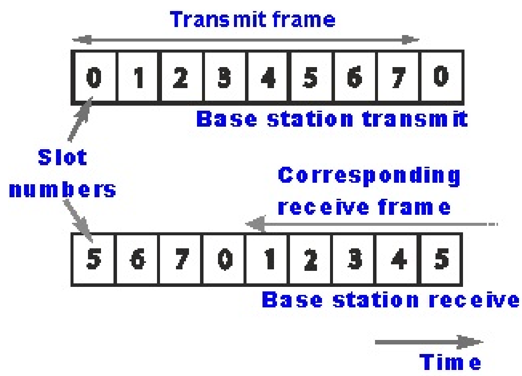

Figure 1.6: GSM FRAME STRUCTURE

Eight slot GSM frame structure

The basic GSM frame defines the structure upon that all the timing and structure of the GSM messaging and signalling relies. the basic unit of time is named a burst period and it lasts for roughly 0.577 ms (15/26 ms). Eight of those burst periods are sorted into what is known as a TDMA frame. This lasts for roughly 4.615 ms (i.e.120/26 ms) and it forms the essential unit for the definition of logical channels. One physical channel is one burst amount allotted in every TDMA frame. In simplified terms the bottom station transmits 2 forms of channel, specifically traffic and control. consequently the channel structure is unionized into 2 differing types of frame, one for the traffic on the most traffic carrier frequency, and therefore the different for the management on the beacon frequency.

GSM multiframe

The GSM frames are sorted along to create multiframes and in this way it's possible to establish a time schedule for their operation and therefore the network are often synchronized.

There are many GSM multiframe structures:

Traffic multiframe: The Traffic Channel frames are organised into multiframes consisting of 26 bursts and taking 120 ms. during a traffic multiframe, twenty four bursts square measure used for traffic. These square measure numbered zero to eleven and thirteen to twenty four. one among the remaining bursts is then wont to accommodate the SACCH, the remaining frame remaining free. the particular position used alternates between position 12 and 25.

Control multiframe:

the control Channel multiframe that contains 51 bursts and occupies 235.4 ms. This invariably occurs on the beacon frequency in time interval zero and it should also occur among slots two, four and six of the beacon frequency still. This multiframe is divided into logical channels that square measure time-scheduled. These logical channels and functions embrace the following:

Frequency correction burst

Synchronisation burst

Broadcast channel (BCH)

Paging and Access Grant Channel (PACCH)

Stand Alone Dedicated control Channel (SDCCH)

GSM Superframe

Multiframes are then made into superframes taking 6.12 seconds. These carries with it 51 traffic multiframes or 26 control multiframes. because the traffic multiframes are 26 bursts long and therefore the control multiframes are 51 bursts long, the various variety of traffic and control multiframes among the superframe, brings them into line once more taking exactly the same interval.

GSM Hyperframe

Above this 2048 superframes (i.e. 2 to the power 11) are grouped to form one hyperframe which repeats every 3 hours 28 minutes 53.76 seconds. It is the largest time interval within the GSM frame structure. Within the GSM hyperframe there is a counter and every time slot has a unique sequential number comprising the frame number and time slot number. This is used to maintain synchronisation of the different scheduled operations with the GSM frame structure. These include functions such as:

Frequency hopping:

Frequency hopping is a feature that is optional within the GSM system. It can help reduce interference and fading issues, but for it to work, the transmitter and receiver must be synchronised so they hop to the same frequencies at the same time.

Encryption:

The encryption process is synchronised over the GSM hyperframe period where a counter is used and the encryption process will repeat with each hyperframe. However, it is unlikely that the cellphone conversation will be over 3 hours and accordingly it is unlikely that security will be compromised as a result.

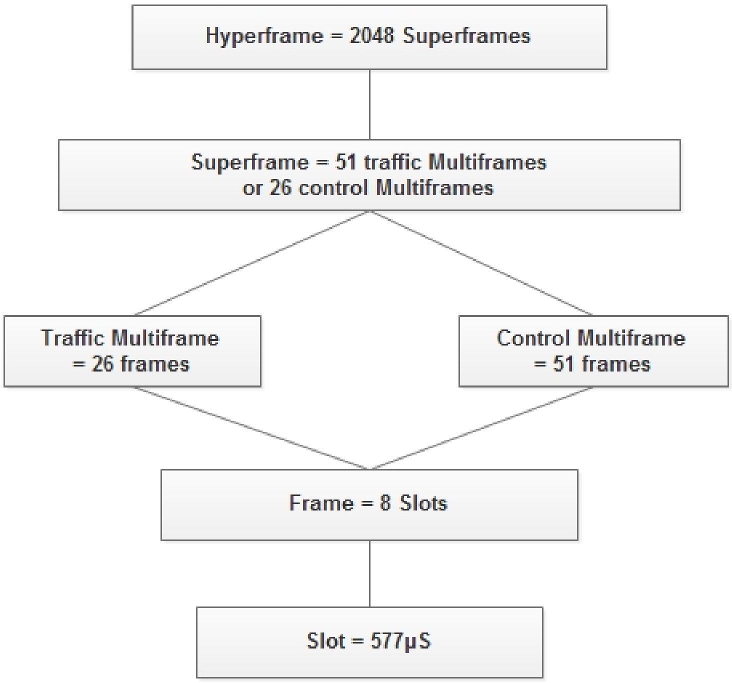

Figure 1.7: GSM FRAME STRUCTURE

1.8 GPRS

GPRS design works on a similar procedure like GSM network, but, has extra entities that permit packet information transmission. This information network overlaps a second-generation GSM network providing packet information transport at the rates from nine.6 to 171 kbps. in conjunction with the packet information transport the GSM network accommodates multiple users to share a similar air interface resources at the same time. GPRS tries to reprocess the existing GSM network parts as much

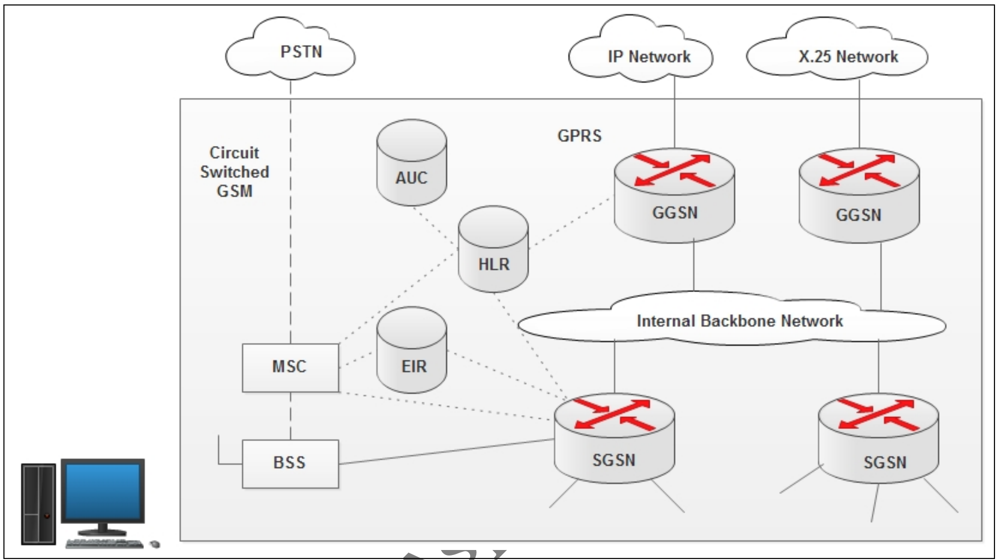

Figure 1.8: GPRS ARCHITECTURE

as doable, however to effectively build a packet-based mobile cellular network, some new network parts, interfaces, and protocols for handling packet traffic ar needed.

1.8.1 GPRS Mobile Stations

New Mobile Stations (MS) ar needed to use GPRS services because existing GSM phones don't handle the improved air interface or packet information. a spread of MS will exist, as well as a high-speed version of current phones to support high-speed information access, a replacement personal organiser device with Associate in Nursing embedded GSM phone, and laptop cards for laptop computer computers. These mobile stations ar backward compatible for creating voice calls exploitation GSM.

1.8.2 GPRS Base Station subsystem

Each BSC needs the installation of 1 or additional Packet control Units (PCUs) and a package upgrade. The PCU provides a physical and logical information interface to the bottom Station scheme (BSS) for packet information traffic. The BTS can even need a package upgrade however generally doesn't need hardware enhancements.

When either voice or information traffic is originated at the subscriber mobile, it's transported over the air interface to the BTS, and from the BTS to the BSC within the same approach as a typical GSM decision. However, at the output of the BSC, the traffic is separated; voice is distributed to the Mobile switching Center (MSC) per commonplace GSM, and information is distributed to a replacement device known as the SGSN via the PCU over a Frame Relay interface.

1.8.3 GPRS Support Nodes

Following 2 new elements, known as entree GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) ar added:

1.8.4 Gateway GPRS Support Node (GGSN)

The entree GPRS Support Node acts as an interface and a router to external networks. It contains routing info for GPRS mobiles, that is employed to tunnel packets through the ip based internal backbone to the right Serving GPRS Support Node. The GGSN also collects charging info connected to the use of the external information networks and may act as a packet filter for incoming traffic.

1.8.5 Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is liable for authentication of GPRS mobiles, registration of mobiles within the network, quality management, and collection info on charging for the use of the air interface.

1.8.6 Internal Backbone

The internal backbone is an ip based network wont to carry packets between totally different GSNs. Tunnelling is employed between SGSNs and GGSNs, therefore the internal backbone doesn't would like any info concerning domains outside the GPRS network. Signalling from a GSN to a msc, HLR or EIR is finished using SS7.

1.8.7 Routing space

GPRS introduces the construct of a Routing space. this idea is comparable to Location space in GSM, except that it usually contains fewer cells. as a result of routing areas are smaller than location areas, less radio resources are used whereas broadcasting a page message.

1.9 GSM SPEECH ENCODING AND DECODING

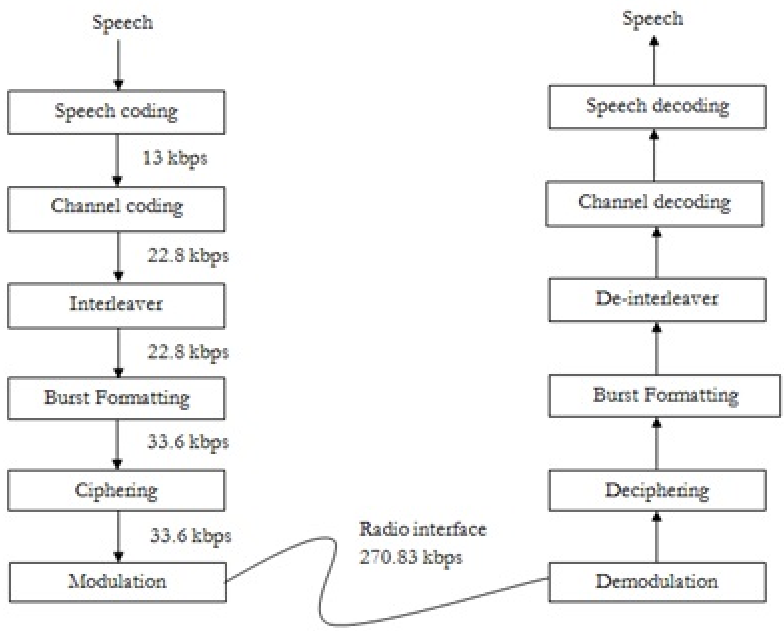

Fig: GSM Signal Processing

Figure 1.9: GSM Speech Encoding and decoding REF:http://www.ques10.com/p/11998/explain-gsm-speech-processing-in-detail/

A. Speech coding:

GSM speech coder is RELP (Residually Excited Predictive Coder), which is enhanced by including a Long Term Predictor (LTP). The coder provides 260 bits for 20ms blocks of speech, which yields a bit rate of 13kbps.

GSM system operates in Discontinuous Transmission mode (DTX) by incorporating a Voice Activity Detector (VAD) in speech coder. This mode provides a longer battery life and reduces instantaneous radio interference since GSM transmitter is not active during silent periods. A Comfort Noise Subsystem (CNS) is used at receiver which adds background acoustic noise to compensate for the annoying switched muting which occurs due to DTX.

B. Channel coding:

The outputs of the speech coder are ordered into for error protection, based upon their significance in contributing groups to speech quality. Out of 260 bits in a frame, the most important 50 bits called type Ia bits, have 3 parity check (CRC) bits added to them to detect non-correctable errors at the receiver. The next 132 bits with first 53 are appended by 4 trailing zero bits, thus providing a data block of 189 bits. This block is then encoded for error protection using a rate convolution encoder with constant length K=5, thus providing a sequence of 378 bits. The least important 78 bits do not have error protection and concatenated to existing sequence to form a block of 456 bits in 20ms frame, data rate of speech signal becomes 22.8kbps.

C. Interleaving:

To minimize the effect of sudden fades on the received data, the total of 456 encoded bits within each 20ms speech frame or control message frame are broken into eight 57 bits sub blocks and they are numbered even odd according to block number. These eight consecutive blocks are spread over eight consecutive TCH time slot. If a burst is lost due to interference or fading, channel coding ensures that enough bits will still be received correctly to allow the error correction to work. Each TCH time slot carries two 57 bits blocks of data from two different 20ms speech blocks. Time slot of first 4 frames contains even data blocks of present speech frame and odd data block of previous speech frame. Time slot of next 4 frames contains odd blocks of present speech frame and even data block of next speech frame.

D. Burst formatting:

Burst formatting adds binary data to the data block to help synchronization and equalization of the received signal.

E. Ciphering:

Ciphering modifies the contents of the eight interleaved blocks by encryption techniques known only to the particular mobile station and base transceiver station. The A3 ciphering algorithm is used to authenticate each mobile by verifying the user password within the SIM with the cryptographic key at the MSC. The A5 ciphering algorithm is used for encryption. It provides scrambling for 114 coded bits sent in each TS. The A8 is used for ciphering key.

F. Modulation:

The modulation scheme used by GSM system is 0.3GMSK where 0.3 describes 3db bandwidth of the Gaussian pulse shaping filter. The channel data rate of GSM is 270.833 kbps which is four times the RF frequency shift. This minimizes bandwidth of the modulation spectrum and hence improves channel capacity. MSK modulated signal is then passed through Gaussian filter to smooth the rapid frequency transitions which would otherwise spread energy in adjacent channels.

G. Demodulation:

The portion of the transmitted forward channel signal which is of interest to a particular user is determined by the assigned TS and ARFCN. The appropriate TS is demodulated with aid of synchronization data provided by the burst formatting.

After demodulation the binary information is deciphered, de-interleaved, channel decoded and speech decoded.

1.10 HANDOVER

One of the key components of a mobile phone or cellular telecommunications system, is that the system is split into several tiny cells to supply smart frequency re-use and coverage. but because the mobile moves out of 1 cell to a different it should be attainable to retain the association. the method by that this occurs is known as handover or handoff. The term handover is additional wide used inside Europe, whereas football play tends to be use additional in North America. Either way, handover and handoff are a similar process.
GSM systems need a procedure referred to as a handover to keep up the continuity of the call. this is often because one cell doesn't cover the complete place e.g. an entire town or country. but one cell incorporates a most place of approximately 23 miles (35 km) for every antenna . The smaller the dimensions of the cell and also the quicker the movement of the MS through the cells (Up to 155 mph (250 kph) for GSM), the additional handovers of in progress calls ar needed, however a relinquishment shouldn't cause the a decision drop. primarily there ar 2 main reasons for handovers, but the GSM Specification identifies forty reasons.
The MS moves out of coverage of the serving BTS so the amplitude becomes lower incessantly till it falls to a lower place the minimal needs for communications. Or the error rate could grow thanks to interference, the gap to the BTS could also be do high. of these effects could diminish the standard of the communication system and create transmission not possible within the close to future. The wired infrastructure i.e. the MSC, BSC could decide that the traffic in one cell is just too high so introducing congestion and thus decides to shift some MSs to alternative cells with a lower level of traffic, if that's attainable. Thus, handovers will be used as a way of dominant traffic through load leveling to alleviate localised congestion.

1. Intra Cell handover : This happens once inside a cell, once narrowband interference might create transmission at a precise frequency not possible. The BSC might then plan to amendment the carrier frequency. (1)
2. Inter Cell, intra BSC handover : this kind of handover could be a typical handover inside the GSM system and happens once the MS moves from one BTS to a different

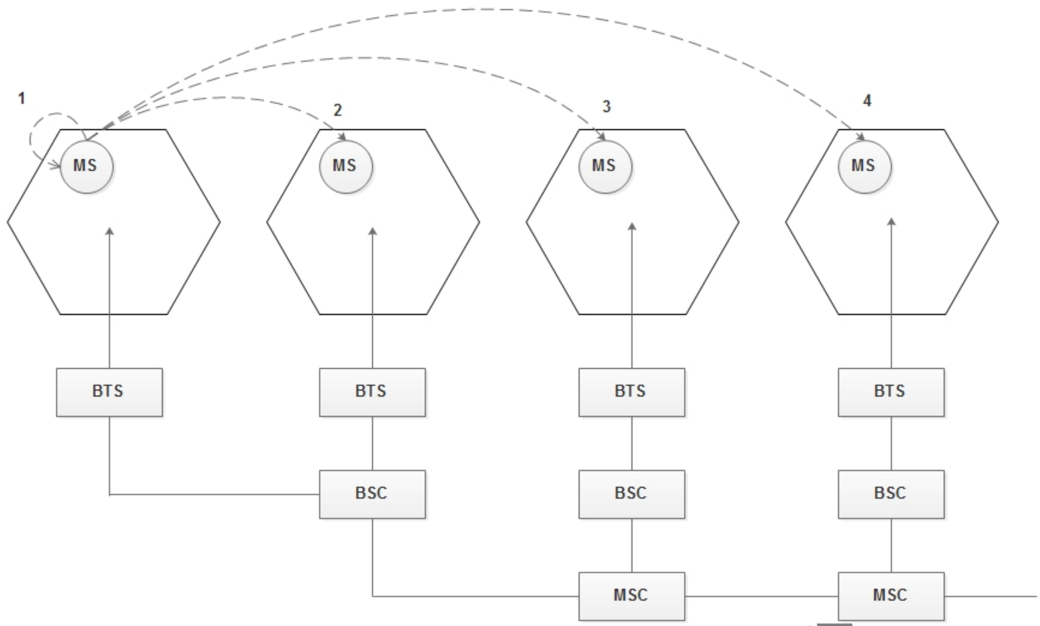

Figure 1.10: HANDOVER PROCESS

however stays inside the control of same BSC. The BSC performs the handover and assigns a replacement radio channel within the new BTS, then releases the previous BTS. (2)

3. Inter BSC, Intra MSc handover : Since a BSC controls a restricted range of BTSs, the GSM system needs to perform handovers between BSCs. this kind of relinquishment is controlled by the MSc. (3)

4. inter msc handover : A handover might even be needed between 2 BTSs that belong to 2 totally different MSCs, currently each MSCs perform the handover along.(4)

REFERENCES

http://www.ques10.com/p/2599/gsm-explain-gsm-architecture-with-a-neat-block-dia/

https://www.queryhome.com/tech/52933/identifiers-in-gsm

https://www.techopedia.com/definition/9492/spectrum-allocation

https://www.slideshare.net/hi2mohdnazir/channel-in-gsm

http://www.althos.com/tutorial/gsm-tutorial-control-channels.html

http://www.teletopix.org/gsm/what-is-burst-in-gsm-and-burst-types-in-gsm/

1 https://www.radio-electronics.com/info/cellulartelecomms/gsmtechnical/frames-structure-super-hyper.php