Definition:

GSM, which stands for Global System for Mobile communications, reigns as the world's most widely used cell phone technology. Cell phones use a cell phone service carrier's GSM network by searching for cell phone towers in the nearby area.

Introduction:

GSM (***Global System for Mobile communications: originally from Groupe Spécial Mobile***) is the most popular standard for mobile phones in the world. Its promoter, the GSM Association, estimates that ***80% 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 system. This has also meant that data communication was easy to build into the system. ***GSM EDGE is a 3G version of the protocol***.

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 travellers to connect to emergency services without knowing the local emergency number.

Newer versions of the standard were backward-compatible with the original GSM phones. For example, Release '97 of the standard added packet data capabilities, by means of General Packet Radio Service (GPRS). Release '99 introduced higher speed data transmission using ***Enhanced Data Rates for GSM Evolution (EDGE)***.

History:

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. Finally the system created by **SINTEF** lead by **Torleiv Maseng** was selected.

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.

GSM frequencies:

GSM networks operate in a number of different frequency ranges (separated into GSM frequency ranges for 2G and UMTS frequency bands for 3G). Most ***2G 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. Most ***3G GSM*** networks in Europe operate in the ***2100 MHz*** frequency band.

The rarer 400 and 450 MHz frequency bands are assigned in some countries 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 125 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 for all 8 channels 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.

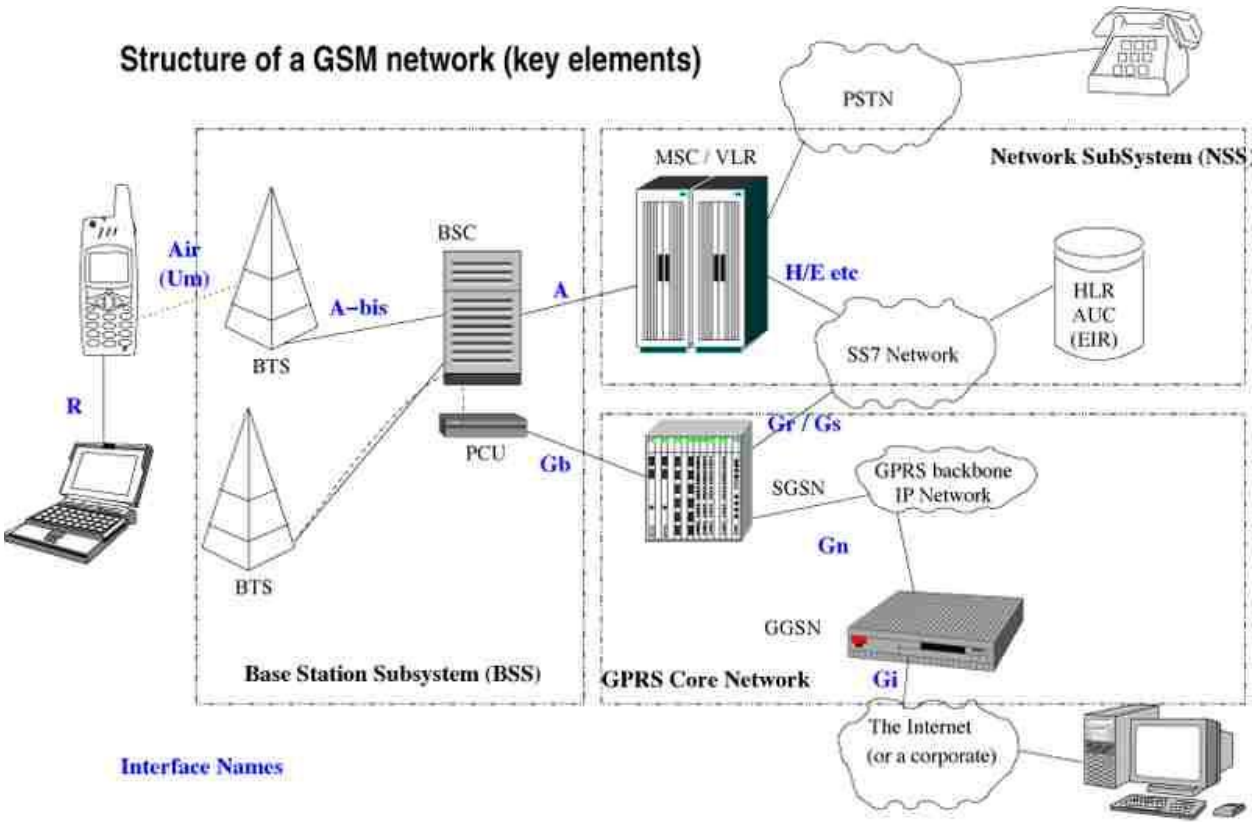
GSM Structure:

The network behind the GSM seen by the customer is large and complicated in order to provide all of the services which are required. It is divided into a number of sections and these are each covered in separate articles.

->the Base Station Subsystem (the base stations and their controllers).

->the Network and Switching Subsystem (the part of the network most similar to a fixed network). This is sometimes also just called the core network.

->the GPRS Core Network (the optional part which allows packet based Internet connections).



->all of the elements in the system combine to produce many GSM services such as voice calls and SMS.

SIM:

One of the key features of GSM is the Subscriber Identity Module, commonly known as a SIM card. The SIM is a detachable smart card containing the user's subscription information and phone book. This allows the user to retain his or her information after switching handsets. Alternatively, the user can also change operators while retaining the handset simply by changing the SIM. Some operators will block this by allowing the phone to use only a single SIM, or only a SIM issued by them; this practice is known as SIM locking, and is illegal in some countries.

In Australia, North America and Europe many operators lock the mobiles they sell. This is done because the price of the mobile phone is typically subsidised with revenue from subscriptions, and operators want to try to avoid subsidising competitor's mobiles. A subscriber can usually contact the provider to remove the lock for a fee, utilize private services to remove the lock, or make use of ample software and websites available on the Internet to unlock the handset themselves. While most web sites offer the unlocking for a fee, some do it for free. The locking applies to the handset, identified by its International Mobile Equipment Identity (IMEI) number, not to the account (which is identified by the SIM card).

In some countries such as Bangladesh, Belgium, Costa Rica, Indonesia, Malaysia, Hong Kong, Pakistan and Singapore, all phones are sold unlocked. However, in Belgium, it is unlawful for operators there to offer any form of subsidy on the phone's price. This was also the case in Finland until April 1, 2006, when selling subsidized combinations of handsets and accounts became legal (3G phones only), though operators have to unlock phones free of charge after a certain period (at most 24 months).

In New Zealand, since May 2008, it is illegal for operators to lock handsets, and any phones purchased locked in the country before that date can be unlocked for free.

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 authenticates 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 ciphertext-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.

Accessing a GSM network

In order to gain access to GSM services, a user needs three things:

*1.A **subscription** with a mobile phone operator. This is usually either a Pay As You Go arrangement, where all GSM services are paid for in advance (commercially called "prepaid"), or a Pay Monthly option where a bill is issued each month for line rental, normally paid for a month in advance, and for services used in the previous month (commercially called "postpaid").*

*2.A **mobile phone** which is GSM compliant and operates at the same frequency as the operator. Most phone companies sell phones from third-party manufacturers.*

*3.A **SIM** ("Subscriber Identity Module") card which is activated by the operator once the subscription is granted. After activation the card is then programmed with the subscriber's MSISDN ("Mobile Subscriber Integrated Services Digital Network Number") (the telephone number). Personal information such as contact numbers of friends and family can also be stored on the SIM by the subscriber.*

After subscribers sign up, information about their identity (telephone number) and what services they are allowed to access are stored in a "SIM record" in the Home Location Register (HLR).

Once the SIM card is loaded into the phone and the phone is powered on, it will search for the nearest mobile phone mast, also called a Base Transceiver Station or BTS. If a mast can be successfully contacted, then there is said to be coverage in the area.

The key feature of a mobile phone is the ability to receive and make calls in any area where coverage is available. This is generally called roaming from a customer perspective, but also called visiting when describing the underlying technical process. Each geographic area has a database called the Visitor Location Register (VLR) which contains details of all the mobiles currently in that area. Whenever a phone attaches, or visits, a new area, the Visitor Location Register must contact the Home Location Register to obtain the details for that phone. The current cellular location of the phone (i.e. which BTS it is at) is entered into the VLR record and will be used during a process called paging when the GSM network wishes to locate the mobile phone.

Every SIM card contains a secret key, called the Ki, which is used to provide authentication and encryption services. This is useful to prevent theft of service, and also to prevent "over the air" snooping of a user's activity. The network does this by utilising the Authentication Center and is accomplished without transmitting the key directly.

Every GSM phone contains a unique identifier (different from the phone number), called the International Mobile Equipment Identity (IMEI). This can be found by dialling " *#06# ". When a phone contacts the network, its IMEI may be checked against the Equipment Identity Register to locate stolen phones and facilitate monitoring.

GSM Services:

GSM services are a standard collection of applications and features available to mobile phone subscribers all over the world. ***The GSM standards are defined by the 3GPP collaboration and implemented in hardware and software by equipment manufacturers and mobile phone operators***. The common standard makes it possible to use the same phones with different companies' services, or even roam into different countries. GSM is the world's most dominant mobile phone standard.

The design of the service is moderately complex because it must be able to locate a moving phone anywhere in the world, and accommodate the relatively small battery capacity, limited input/output capabilities, and weak radio transmitters on mobile devices.

1.Voice calls

Outgoing

Once a mobile phone has successfully attached to a GSM network as described above, calls may be made from the phone to any other phone on the global Public Switched Telephone Network.

The user dials the telephone number, presses the send or talk key, and the mobile phone sends a call setup request message to the mobile phone network via the nearest mobile phone mast (BTS).

The call setup request message is handled next by the Mobile Switching Center, which checks the subscriber's record held in the Visitor Location Register to see if the outgoing call is allowed. If so, the MSC then routes the call in the same way that a telephone exchange does in a fixed network.

If the subscriber is on a Pay As You Go tariff (sometimes known as Prepaid (for example, in Australia and India)), then an additional check is made to see if the subscriber has enough credit to proceed. If not, the call is rejected. If the call is allowed to continue, then it is continually monitored and the appropriate amount is decremented from the subscriber's account. When the credit reaches zero, the call is cut off by the network. The systems that monitor and provide the prepaid services are not part of the GSM standard services, but instead an example of intelligent network services that a mobile phone operator may decide to implement in addition to the standard GSM ones.

Incoming

Gateway MSC contact

When someone places a call to a mobile phone, they dial the telephone number (also called a MSISDN) associated with the phone user and the call is routed to the mobile phone operator's Gateway Mobile Switching Centre. The Gateway MSC, as the name suggests, acts as the "entrance" from exterior portions of the Public Switched Telephone Network onto the provider's network.

As noted above, the phone is free to roam anywhere in the operator's network or on the networks of roaming partners, including in other countries. So the first job of the Gateway MSC is to determine the current location of the mobile phone in order to connect the call. It does this by consulting the Home Location Register (HLR), which, as described above, knows which Visitor Location Register (VLR) the phone is associated with, if any.

Routing the call

When the HLR receives this query message, it determines whether the call should be routed to another number (called a divert), or if it is to be routed directly to the mobile.

If the owner of the phone has previously requested that all incoming calls be diverted to another number, known as the Call Forward Unconditional (CFU) Number, then this number is stored in the

Home Location Register. If that is the case, then the CFU number is returned to the Gateway MSC for immediate routing to that destination.

If the mobile phone is not currently associated with a Visited Location Register (because the phone has been turned off) then the Home Location Register returns a number known as the Call Forward Not Reachable (CFNRc) number to the Gateway MSC, and the call is forwarded there. Many operators may set this value automatically to the phone's voice mail number, so that callers may leave a message. The mobile phone may sometimes override the default setting.

Finally, if the Home Location Register knows that the phone is roaming in a particular Visited Location Register area, then it will request a temporary number (called an MSRN) from that VLR. This number is relayed back to the Gateway MSC, and then used to route the call to the MSC where the called phone is roaming.

Ringing the phone

When the call arrives at the Visiting MSC, the MSRN is used to determine which phone is being called. The MSC then pages all the mobile phone masts in the area in order to inform the phone that there is an incoming call for it. If the subscriber answers, a speech path is created through the Visiting MSC and Gateway MSC back to the network of the person making the call, and a normal telephone call follows.

It is also possible that the phone call is not answered. If the subscriber is busy on another call (and call waiting is not being used) the Visited MSC routes the call to a pre-determined Call Forward Busy (CFB) number. Similarly, if the subscriber does not answer the call after a period of time (typically 30 seconds) then the Visited MSC routes the call to a pre-determined Call Forward No Reply (CFNRy) number. Once again, the operator may decide to set this value by default to the voice mail of the mobile so that callers can leave a message.

If the subscriber does not respond the the paging request, either due to being out of coverage, or their battery has gone flat/removed, then the Visited MSC routes the call to a pre-determined Call Forward Not Reachable (CFNRc) number. Once again, the operator may decide to set this value by default to the voice mail of the mobile so that callers can leave a message.

From the caller's point of view, it does not matter where the mobile subscriber is, as the technical process of connecting the call is the same. If a subscriber is roaming on a different company's network, the subscriber, instead of the caller, may pay a surcharge for the connection time. International roaming calls are often quite expensive, and as a result some companies require subscribers to grant explicit permission to receive calls while roaming to certain countries.

When a subscriber is roaming internationally and a call is forwarded to his or her voice mail, such as when his or her phone is off, busy, or not answered, he or she may actually be charged for two simultaneous international phone calls—the first to get from the GMSC to the VMSC and the second to get from the VMSC to the Call Forward Busy or Call Forward No Reply number (typically the voice

mailbox) in the subscriber's country. However, some networks' GMSCs connect unanswered calls directly, keeping the voice signal entirely within the home country and thus avoiding the double charge.

How speech is encoded during mobile phone calls

During a GSM call, speech is converted from analogue sound waves to digital data by the phone itself, and transmitted through the mobile phone network by digital means.

The digital algorithm used to encode speech signals is called a codec. The speech codecs used in GSM are called Half-Rate (HR), Full-Rate (FR), Enhanced Full-Rate (EFR) and Adaptive Multirate (AMR). All codecs except AMR operate with a fixed data rate and error correction level.

2.Data transmission

The GSM standard also provides separate facilities for transmitting digital data. This allows a mobile phone to act like any other computer on the Internet, sending and receiving data via the Internet Protocol.

The mobile may also be connected to a desktop computer, laptop, or PDA, for use as a network interface (just like a modem or Ethernet card, but using one of the GSM data protocols described below instead of a PSTN-compatible audio channel or an Ethernet link to transmit data). Some GSM phones can also be controlled by a standardised Hayes AT command set through a serial cable or a wireless link (using IrDA or Bluetooth). The AT commands can control anything from ring tones to data compression algorithms.

In addition to general Internet access, other special services may be provided by the mobile phone operator, such as SMS.

3.Circuit-switched data protocols

A circuit-switched data connection reserves a certain amount of bandwidth between two points for the life of a connection, just as a traditional phone call allocates an audio channel of a certain quality between two phones for the duration of the call.

Two circuit-switched data protocols are defined in the GSM standard: Circuit Switched Data (CSD) and High-Speed Circuit-Switched Data (HSCSD). These types of connections are typically charged on a per-second basis, regardless of the amount of data sent over the link. This is because a certain amount of bandwidth is dedicated to the connection regardless of whether or not it is needed.

Circuit-switched connections do have the advantage of providing a constant, guaranteed quality of service, which is useful for real-time applications like video conferencing.

4.General Packet Radio Service (GPRS)

The General Packet Radio Service (GPRS) is a packet-switched data transmission protocol which was incorporated into the GSM standard in 1997. It is backwards-compatible with systems that use pre-1997 versions of the standard. GPRS does this by sending packets to the local mobile phone mast (BTS) on channels not being used by circuit-switched voice calls or data connections. Multiple GPRS users can share a single unused channel because each of them uses it only for occasional short bursts.

The advantage of packet-switched connections is that bandwidth is only used when there is actually data to transmit. This type of connection is thus generally billed by the kilobyte instead of by the second, and is usually a cheaper alternative for applications that only need to send and receive data sporadically, like instant messaging.

GPRS is usually described as a 2.5G technology.

5.Short Message Service (SMS)

Short Messages (more commonly known as text messages) has become the most used data application on mobile phones, with 74% of all mobile phone users worldwide already as active users of SMS, or 2.4 billion people by the end of 2007. In many advanced countries, the users have shifted from considering the voice call being the most desired feature of a mobile phone, to considering SMS text messaging as the most desired feature.

SMS text messages may be sent by mobile phone users to other mobile users or external services that accept SMS. The messages are usually sent from mobile devices via the Short Message Service Centre using the MAP protocol.

The SMSC is a central routing hubs for Short Messages. Many mobile service operators use their SMSCs as gateways to external systems, including the Internet, incoming SMS news feeds, and other mobile operators (often using the de facto SMPP standard for SMS exchange).

6.Supplementary Services

GSM supports a comprehensive set of supplementary services that complement and support the telephony and data services described above. They are all defined in GSM standards. A partial listing of supplementary services follows:

Call forwarding:This service gives the subscriber the ability to forward incoming calls to another number if the called mobile unit is not reachable, if it is busy, if there is no reply, or if call forwarding is allowed unconditionally.

Barring of Outgoing Calls: This service makes it possible for a mobile subscriber to prevent all outgoing calls.

Barring of Incoming Calls: This function allows the subscriber to prevent incoming calls. The following two conditions for incoming call barring exist: baring of all incoming calls and barring of incoming calls when roaming outside the home PLMN.

Advice Of Charge (AoC): The AoC service provides the mobile subscriber with an estimate of the call charges. There are two types of AoC information: one that provides the subscriber with an estimate of the bill and one that can be used for immediate charging purposes. AoC for data calls is provided on the basis of time measurements.

Call Hold: This service enables the subscriber to interrupt an ongoing call and then subsequently reestablish the call. The call hold service is only applicable to normal telephony.

Call Waiting: This service enables the 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.

Multiparty service: The multiparty service enables a mobile subscriber to establish a multiparty conversation - that is, a simultaneous conversation between three and six subscribers. This service is only applicable to normal telephony.

Calling Line Identification presentation/restriction: These services supply the called party with the integrated services digital network (ISDN) number of the calling party. The restriction service enables the calling party to restrict the presentation. The restriction overrides the presentation.

Closed User Groups (CUGs): CUGs are generally comparable to a PBX. They are a group of subscribers who are capable of only calling themselves and certain numbers.

Explicit Call Transfer (ECT): This service allows a user who has two calls to connect these two calls together and release its connections to both other parties.

Advantages of GSM:

1.GSM is already used worldwide with over 450 million subscribers.

2.International roaming permits subscribers to use one phone throughout Western Europe. CDMA will work in Asia, but not France, Germany, the U.K. and other popular European destinations.

3.GSM is mature, having started in the mid-80s. This maturity means a more stable network with robust features. CDMA is still building its network.

4.GSM's maturity means engineers cut their teeth on the technology, creating an unconscious preference.

5.The availability of Subscriber Identity Modules, which are smart cards that provide secure data encryption give GSM m-commerce advantages.

Comparision between GSM AND CDMA

1.International Roaming with GSM and CDMA

Where international business travel is an issue, GSM leaps forward in the race for the title of "Most Accessible." Because GSM is used in more than 74% of the markets across the globe, users of tri-band or quad-band handsets can travel to Europe, India, and most of Asia and still use their cell phones. CDMA offers no multiband capability, however, and therefore you can't readily use it in multiple countries.

2.Data Transfer Methods in GSM vs. CDMA

Another difference between GSM and CDMA is in the data transfer methods. GSM's high-speed wireless data technology, GPRS (General Packet Radio Service), usually offers a slower data bandwidth for wireless data connection than CDMA's high-speed technology (1xRTT, short for single carrier radio transmission technology), which has the capability of providing ISDN (Integrated Services Digital Network)-like speeds of as much as 144Kbps (kilobits per second). However, 1xRTT requires a dedicated connection to the network for use, whereas GPRS sends in packets, which means that data calls made on a GSM handset don't block out voice calls like they do on CDMA phones.

3.Interaction between GSM and CDMA

In cities and densely populated areas, there are often high concentrations of GSM and CDMA connection bases. In theory, GSM and CDMA are invisible to one another and should "play nice" with one another. In practice, however, this is not the case. High-powered CDMA signals have raised the "noise floor" for GSM receivers, meaning there is less space within the available band to send a clean signal. This sometimes results in dropped calls in areas where there is a high concentration of CDMA technology. Conversely, high-powered GSM signals have been shown to cause overloading and jamming of CDMA receivers due to CDMA's reliance upon broadcasting across its entire available band.

The result of this little cross-broadcasting joust has led some cities to pass ordinances limiting the space between cell towers or the height they can reach, giving one technology a distinct advantage over the other. This is something to note when choosing a wireless provider. The distance between towers will severely affect connectivity for GSM-based phones because the phones need constant access to the tower's narrow band broadcasting.

4.Prevalence of CDMA vs. GSM

GSM is a lot more widespread in Europe and Asia. In the United States, Sprint and Verizon networks are CDMA whereas AT&T and T-Mobile are on GSM. In India, Hutch, Bharti and BSNL are on GSM whereas Reliance and Tata Tele are on CDMA networks.