The Evolution and Future of Mobile Communication Systems

Written by David G Ainscough
Copyright 2001 D.G.Ainscough

Chapter 2 : GSM (Global System for Mobile Communications)

2.1 Introduction (GSM)

The most successful mobile digital communications system in today's world is GSM, with networks in over 130 countries and more than 100 million users worldwide. Back at the start of the 1980's Europe was facing a big problem, there were many existing analogue mobile networks, which were based on similar standards, for example NMT 450, however they were all running on slightly different carrier frequencies. To avoid this problem in the second generation mobile phone system, the Groupe Spéciale Mobile (GSM) was created in 1982. Now the system developed by this group is known as global system for mobile communications (GSM).

The primary goal of GSM was to provide a mobile phone system that would allow it's users to use their mobile phone in any European country i.e. Roaming. This system would have to provide voice services comparable with ISDN and other PSTN systems. The initial specification details were over 5000 pages, with the new services in particular data services there are even more specification details.

GSM is a typical second generation system, replacing the old analogue first generation system, however it still does not offer worldwide high data rates but will be offered in the new third generation system UMTS. GSM was initially deployed in Europe using the 890 – 915 MHz band for the uplinks and the 935 – 960 MHz band for the downlinks. This version is commonly known as GSM 900, and later version GSM 1800 (1710 – 1785MHz uplink, 1805 – 1880MHz downlink) which commonly known as DCS (Digital Cellular System)

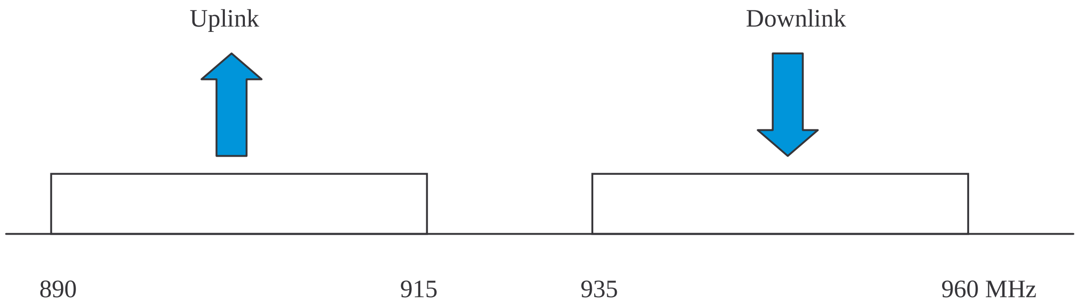

Figure 1 Uplink and Downlink frequencies for original GSM Spectrum

2.1.1 Mobile Services

The GSM system permits the integration of different voice and data services and the inter-working with existing networks. Services make a network flexible to users, i.e. they can choose one network over another. GSM has three different categories of services, bearer, tele and supplementary services And these are described in the following sections. Figure 3 shows a reference model for the GSM services.

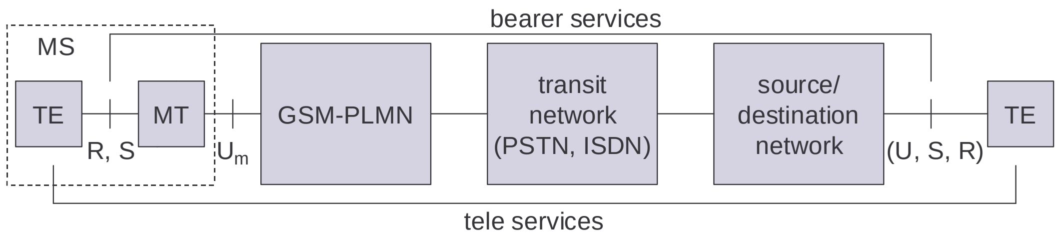

Figure 2 Bearer and tele services reference model

A mobile station (MS) is connected to the GSM Public Land Mobile Network (PLMN) via the Um interface. This network is connected to the Transit network, e.g. Integrated Services Digital Network (ISDN) or the traditional Public Switched Telephone Network (PSTN) though there might also be an additional network, the Source/destination network, before another Terminal (TE) is connected. Bearer services now comprise all services that enable the transparent transmission of data between the interfaces to the network, i.e., S in the case of the MS, and a similar interface for the other terminal. In the original GSM model, bearer services are connection-orientated and circuit or packet switched and these services only need the lower three layers of the ISO/OSI reference model.

Within the mobile station (MS), the mobile terminal (MT) performs all the network specific tasks (such as TDMA, FDMA, coding, etc) and also offers the interface for data transmission (S) to the terminal (TE), which can then be independent of the network. Depending on the capabilities of the TE, more interfaces may be needed, such as R, according to ISDN reference model (Halsall, 1996). Tele services are application specific and may need all seven layers of the ISO/OSI reference model, these services are specified end-to-end, i.e. from one terminal (TE) to another terminal.

2.1.1.1 Bearer Services

GSM specifies different mechanisms for data transmission for data transmission for the original GSM allowed for data rates up 9600 bit/s for non-voice services. Bearer services allow for both transparent and non-transparent, synchronous or asynchronous data transmission.

Transparent bearer services use only the functions of the physical layer (layer 1 ISO/OSI reference model) to transmit data; data transmission consequently has a constant delay and throughput, that is if no errors occur. The only mechanism of any use to try and increase the quality of the transmission is forward error correction (FEC). This mechanism codes redundancy into the data-stream and Depending on the FEC, data rate of 2.4, 4.8, or 9.6 kbit/s are possible.

Non-Transparent bearer services use protocols of the layers two and three to implement error correction and flow control. Non-transparent bearer services use the transparent bearer services, while adding a radio link protocol (RLP). This protocol uses mechanisms of high-level data link control (HDLC) (Halsall, 1996), and special selective-reject mechanisms to trigger retransmission of erroneous data. The achieved bit error rate is less than 10-7, but now throughput may vary, this depending on the transmission quality.

2.1.1.2. Tele Services

GSM is mainly focused on voice tele services and these comprise of encrypted voice transmission, message services, and basic data communication with terminals as known from the PSTN or ISDN (e.g. fax). However as the main service is telephony, the primary goal of GSM was to provide high-quality digital voice transmission, offering at least the typical audio bandwidth of 3.1 kHz (which was what the old analogue systems offered). Special codecs (coder/decoder) are used for voice transmission. Different codecs are used for the transmission of data for communication with traditional computer modems, e.g. fax machines or the internet.

Another tele service is the emergency number and this is the same number all over the GSM network in Europe and is also the same as the national emergency number. This is a mandatory service that all the network operators have to provide and is free of charge to the user. Another feature is that this service has the highest priority when connecting, possibly pre-empting other connections. Also, the network operators co-operate allowing users of any digital network to use any network to connect and furthermore this service will automatically put the user through to the nearest emergency centre.

A useful additional service that is offered is the short message service (SMS), which is a simple text message transfer service, offering transmission of messages up to about 160 characters. SMS messages do not use the data channels, but instead uses the unused capacity in the signalling channel. The use of the signaling channel means that the user can send and receive SMS messages during a voice or data transmission.

2.1.1.3. Supplementary Services

Further to bearer and tele services, GSM network operators can also offer supplementary services. These services offer enhancements to the standard telephony service and may differ from operator to operator, though typical services available to the user are caller location identifier (CLI), call forwarding, or redirection.

2.1.2 System Architecture

As with all telecommunications systems, GSM has a hierarchical and complex system architecture comprising of many entities, interfaces and acronyms figure 4 shows a simplified overview of the GSM system as specified in the ETSI (TS 101.622). GSM systems consist of three subsystems, the radio subsystem (RSS), the network and switching subsystem (NSS), and the operation subsystem (OSS). Generally a GSM user will only notice a very small portion of the whole network, commonly the mobile stations (MS) and some antenna masts of the base transceiver stations (BTS).

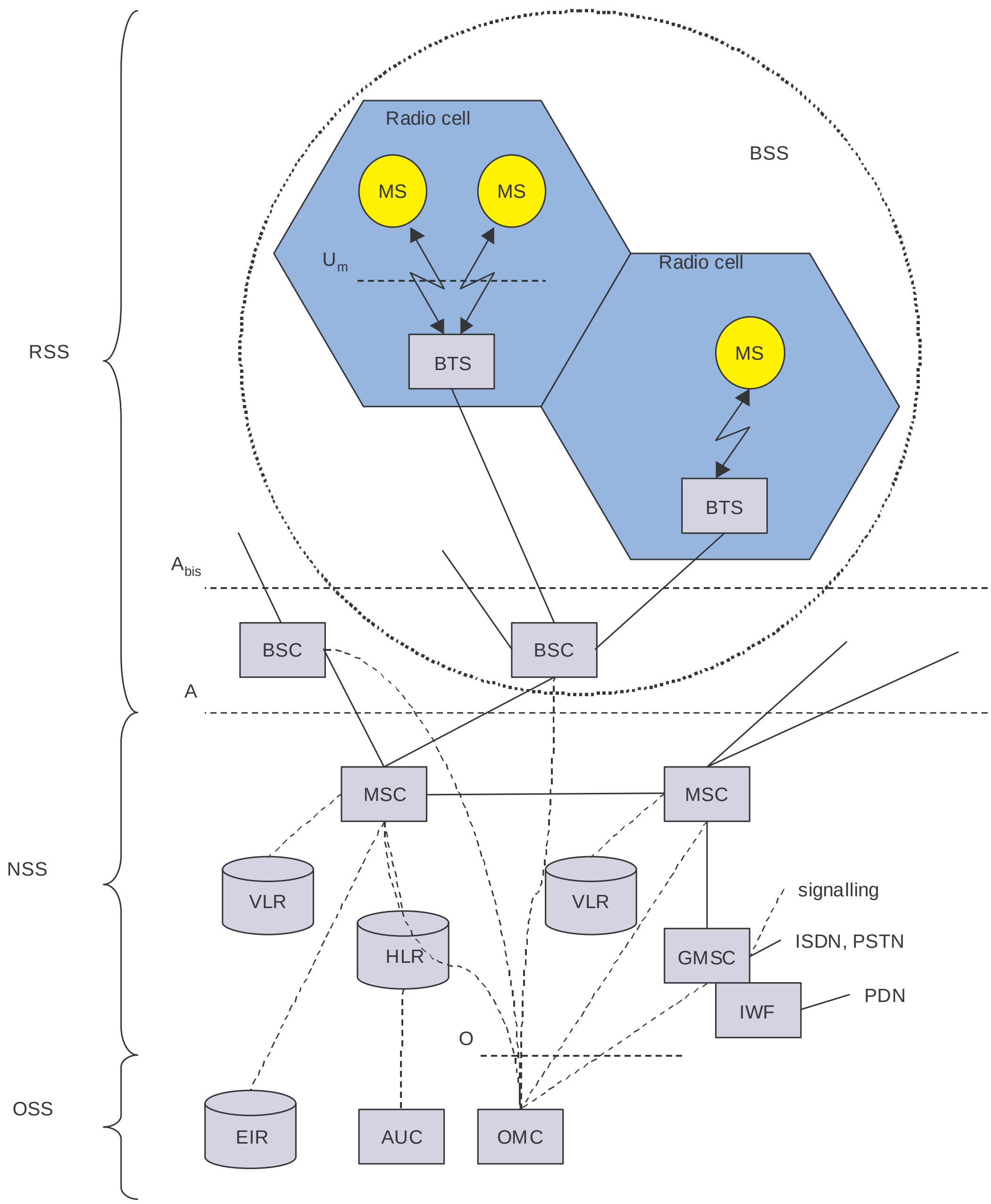

Figure 3 Functional Architecture of a GSM system

2.1.2.1 Radio Subsystem (RSS)

As suggested by the name, the radio subsystem is comprised of all the radio specific elements, i.e. the mobile stations (MS) and the base station subsystem (BSS). The connection between the RSS and the NSS (shown in figure x.ii) via the A interface (solid lines) and the connection to the OSS via the O interface (dashed lines). The A interface is generally based on a circuit-switched PCM-30 system (2.048 Mbit/s), carrying up to 30 X 64 kbit/s connections, whereas the O interface uses the Signalling System No. 7 (SS7) based on X.25 carrying system management data to/from the RSS.

Base Station Subsystem (BSS): A GSM network is made up of many BSSs, each one being controlled by a base station controller (BSC). The main function of the BSS is to maintain the radio connections to an MS, however, it does have several other functions such as the coding/decoding of voice, and rate adaptation to/from the wireless network part. As well as a BSC, the BSS contains several BTSs.

Base Transceiver Station (BTS): A BTS contains all the radio equipment (antennas, signal processing, amplifiers) necessary for radio transmission. A BTS can be used to form a radio cell, or if sectored antennas are used, several cells. The BTS is connected to the MS by the Um interface, and the BSC by the A_{bis} interface. The Um interface comprises of all the mechanisms necessary for wireless transmission (TDMA, FDMA). A_{bis} interface consists of 16 or 64 kbit/s connections. The area coverage from a GSM cell can vary from 100m and 35km depending on the expected traffic and the location environment.

Base Station Controller (BSC): Basically, the BSC controls the BTS The functions of the BSC include reserving radio frequencies, handling handovers from one BTS to another and performing the paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.

Function	BTS	BSC
Management of radio channels		X
Frequency hopping	X	X
Management of terrestrial channels		X
Mapping of terrestrial onto radio channels		X
Channel coding and decoding	X	
Rate adaptation	X	
Encryption/decryption	X	X
Paging	X	X
Uplink Signal measurement	X	
Traffic measurement		X
Authentication		X
Location registry, location update		X
Handover management		X

Mobile Station (MS) : The MS is the user equipment which contains the software required for communication with the GSM network. The MS consists of user independent hard/software and the subscriber identity module (SIM), which stores the user specific data. While an MS can be identified via the international mobile equipment identity (IMEI). Users can personalize their MS, by making use of the SIM.

2.1.2.2 Network and switching subsystem

At the centre of any GSM system there is the network and switching subsystem (NSS) that connects the GSM network with the public land network (i.e. a PSTN), performs the handovers between BSS's, comprises functions for worldwide localization of users and supports charging, accounting and roaming of users between different networks and in different countries. The NSS is comprised of the following switches and databases:

Mobile services switching centre (MSC): High-performance digital ISDN switches, that set up the connections between other MSC's and the BSC's, using the A interface. Hence the MSC's are the backbone of any GSM network. Normally one MSC will manage many BSC's in a geographical area. Some MSC's are gateway MSC (GMSC) that provide connections to other fixed networks (e.g. PSTN). Using additional functions such as the interworking functions (IWF) an MSC can also connect to public data networks (PDN) such as X.25.

Home Location Register (HLR): The most important database in a GSM network is the HLR as it stores all the relevant information about the users. Information such as the mobile station ISDN number (MSISDN), services subscribed to, and the authentication key Ki. Furthermore the HLR stores dynamic information like the LA (Location Area) of the MS. As the MS moves geographically around the GSM network, the HLR stores the location of the MS from the LA. This information is used to localize the user within the worldwide GSM network. All of these user specific information elements only exist once for each user in a single HLR. The HLR also supports charging and accounting.

Visitor Location Register (VLR): The VLR associated to each MSC is a very dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC. If a new MS comes into the LA then the VLR is responsible for it. The VLR copies all the relevant information for the MS from the HLR. The structure of the VLR and HLR avoids frequent updates and long-distance signaling of user information.

2.1.2.3 Operation Subsystem

The GSM system is broken up in to three parts, the first two parts have already been discussed, the third part of the GSM system is the operational subsystem (OSS). The OSS contains all the functions necessary for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signaling. The following section describes the entities:

Operation and Maintenance Centre (OMC): The OMC monitors and controls all other GSM network entities via the O interface (SS7 with X.25), typically the OMC functions are Traffic Monitoring, Status reports of the network entities, subscribers and security management, or accounting and billing.

Authentication Centre (AuC): The Radio Air interface and the MS's are particularly vulnerable, therefore a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication, the keys for encryption and generates the values needed for user authentication for the HLR.

Equipment Identity Register (EIR): EIR is a database for all IMEIs that stores all the device identifications registered for the GSM network. As MSs are mobile they can be stolen easily. If a user has a valid SIM of their own, then they can use any stolen MS. Hence the EIR has a 'black list' of stolen or locked devices so the MS on this list is useless as soon as the owner of the MS has reported it as stolen. Furthermore the EIR holds a list of valid IMEIs, and a list of malfunctioning devices.

2.1.3 Radio Air Interface

One of the most interesting interfaces in the GSM network is the Um, the Radio Air Interface because it comprises many of the mechanisms used for multiplexing and media access. GSM utilises SDMA (Space Division Multiple Access) using cells with BTS and assigns an MS to a BTS. What's more, FDD (Frequency Division Duplex) is used to separate the downlink and uplink as shown in Figure 5.

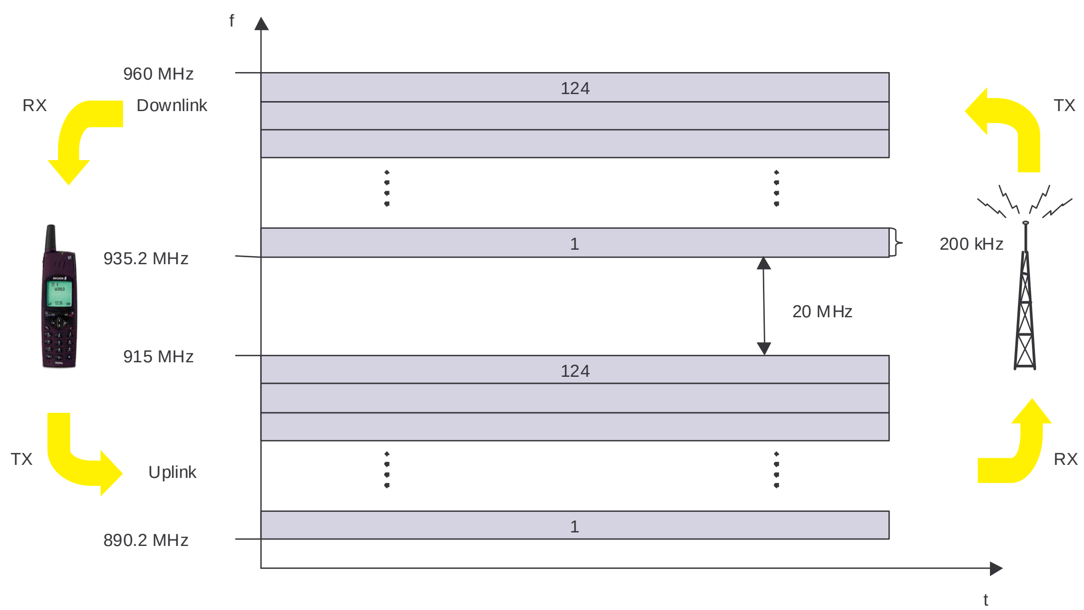

Figure 4 Frequency division multiplexing for multiple access and duplex

(NB. Figure 5, only show the frequency used by GSM as envisaged in GSM Phase 2)

Media access combines TDMA and FDMA. In GSM 900 there are 124 channels, each 200KHz wide and are used for FDMA, however in GSM 1800, there are 374 channels used. The following is an example based on the GSM 900 system, while figure x.iii shows the FDM in GSM. Figure 6 shows TDM in use. Each if the 248 channels is additionally separated in time by using a TDM GSM frame. i.e. each 200 kHz carrier is subdivided into frames that repeated continuously. The duration of a frame is 4.615 ms which is subdivided into 8 GSM time-slots, where each slot represents a TDM channel and lasts for 577 μs. Hence each TDM channel occupies the 200 kHz carrier for 577 μs every 4.615 ms.

Data is transmitted in small sections known as a 'burst' figure 6 shows a normal burst as used for data transmission inside a time slot. In this example (Figure 6) the burst is only 546.5 μs long and contains 148 bits of data. The remaining 30.5 μs is used as guard space which is done to prevent overlapping with other bursts due to the different path delays and to leave the transmitter time to turn on and off. However, if the full slot if filled with data that would allow the transmission of 148 bits within the 546.5 μs. So each physical TDM channel has a data rate of around 38.8 kbit/s, but each radio carrier transmits around 270 kbit/s over the Um interface.

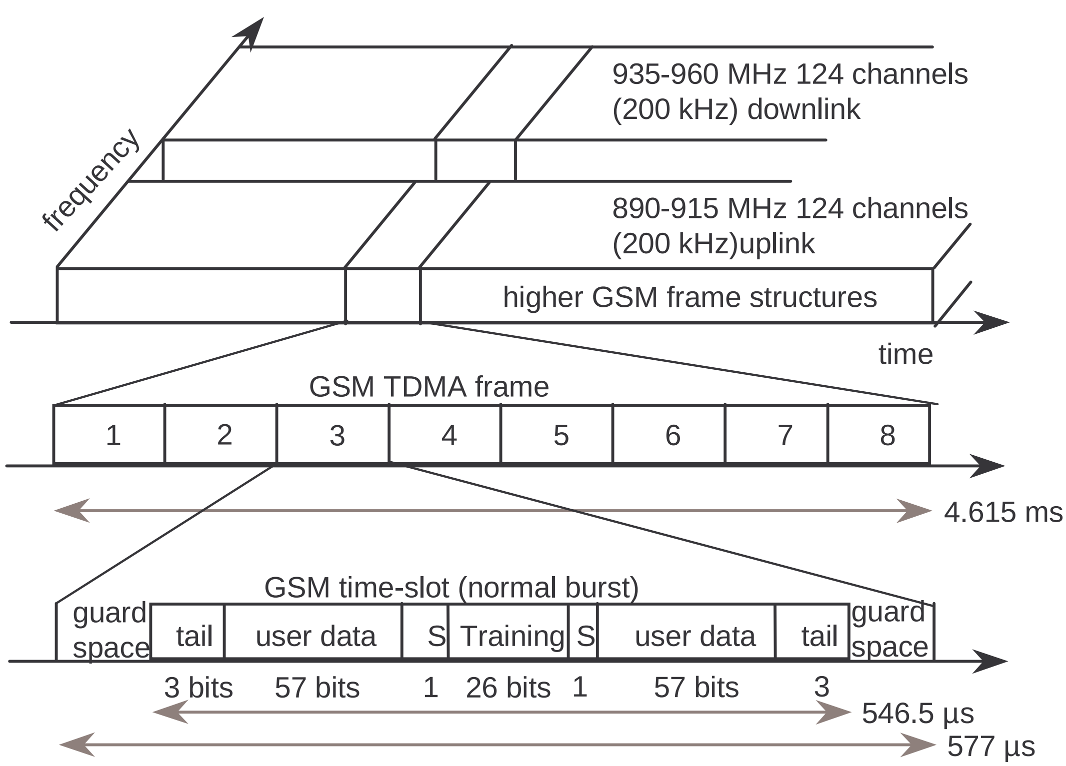

Figure 5 GSM TDMA frame, slots, and bursts

There are three bits at the start and finish of each burst these are known as the ‘tail’ and are set to 0 so they can be used to enhance the receiver performance. The training sequence in the middle of the burst is used to adapt the parameters of the receiver to the current path propagation characteristics and to select the strongest signal in the case of multi-path propagation (check this). The ‘S’ flag indicates whether the data field contains user or network control data.

Two factors allow for the use of simple transmitter hardware: on the one hand, the slots for uplink and downlink of a physical TDM channel are separated in frequency (45 MHz for GSM 900 and 95 MHz for GSM 1800 using FDD). On the other hand, the TDMA frames are shifted in time for three slots. i.e., if the BTS sends data at time t0 in slot one on the downlink, the MS access slot one on the uplink at time t0+3.577μs. An MS thus does not need a full-duplex transmitter, a simpler half-duplex transmitter switching between receiving and sending is enough. In order to avoid frequency selective fading, GSM specifies an optional slow frequency hopping mechanism. MS and BTS may change the carrier frequency after each frame, based on a common hopping sequence. An MS changes its frequency between up and downlink slots respectively.

2.1.3.1. Logical Channels and Frame Hierarchy

GSM specifies two basic groups of logical channel, they are the Traffic Channels and the Control Channels :

Traffic Channels (TCH): The GSM network uses a TCH to transmit user data (e.g. Voice). There are two basic TCHs and they are defined as Full Rate TCH (TCH/F) and Half Rate TCH (TCH/H). A TCH/F has a data rate of 28.8 kbit/s, whereas the data rate for TCH/H is 14.4 kbit/s. At the beginning of GSM standardisation the voice codecs only required 13 kbit/s, whereas the remaining capacity of TCH/H was used for error correction (TCH/FS). However, newer codecs allow for better voice coding and can make use of TCH/H. Making use of these TCH/Hs doubles the capacity of the GSM system for voice transmission, but reduces speech quality. For data transmission there are many different traffic channels, for example TCH/F4.8 for 4.8 kbit/s, TCH/F9.6 for 9.6 kbit/s, and in the newer specifications TCH/F14.4 for 14.4 kbit/s. It should be noted that that these logical channels differ in their coding and their level of error correction. However data throughput is < 2Kb/s.

Control Channels (CCH): The GSM network makes use of many different CCHs, for they control medium access, allocation of traffic channels or the mobility management. Three main groups of CCHs have been defined, each has their own sub-channels.

Broadcast Control Channel (BCCH): The BCCH is used by the BTS to signal all MSs within a cell. The sort of information transmitted in this channel is such as the cell identification, options available within this cell (frequency hopping), and the available frequencies within the cell and in neighbouring cells, known as the neighbour list. In addition to this, the

BTS sends information about frequency correction using the FCCH (Frequency Correction Channel), and also information about the time synchronisation via the SCH (Synchronisation Channel). Both of these channels, the FCCH and the SCH are sub channels of the BCCH.

Common Control Channel (CCCH): The CCCH is the channel where all information about connection set up between the MS and the BS is exchanged. For calls toward the MS, the BS uses the PCH (Paging Channel). However if a MS wants to set up a call, it uses the RACH (Random Access Channel) to send data to the BTS. The RACH implements multiple access to all MSs within a cell, and all MSs may access this channel. This however is where collisions may occur between MSs in the GSM system, so the BTS uses the AGCH (Access Grant Channel) to signal an MS that it can use the TCH or SDCCH for further connection set up.

Dedicated Control Channel (DCCH) : The previous two channels (BCCH and CCCH) are unidirectional, the DCCH and it’s sub channels are bi-directional. As long as an MS has not established a TCH with the BTS, it uses the SDCCH (Stand-alone Dedicated Control Channel) with a low data rate (782 bit/s) for signaling. The signaling is generally made up of authentication, registration and/or other data needed to set up the TCH. Each TCH and SDCCH has a SACCH (Slow Associated Dedicated Control Channel) associated with it. This channel is used to exchange system information such as the Channel Quality and the signal power level. Finally, if more signaling information needs to be transmitted and a TCH is already existing, GSM uses a FACCH (Fast Associated Dedicated Control Channel). The FACCH uses the time slots which are otherwise used by the TCH and is necessary, especially in the case of handovers where the BTS and the MS have to exchange larger amounts of data, in a smaller amount of time, known as layer 3 messages (not ISO/OSI reference model).

2.1.4 Protocols

Figure 7 shows the architecture of protocols used within the GSM system, with signaling protocols, interfaces as well as the entities already shown in Figure 5.

Again the main area of focus is in the Um interface, this is because the other interfaces occur between entities in a fixed network. The physical layer, Layer 1 handles all the radio specific functions. This layer includes the creation of bursts according to the five different formats, the multiplexing of bursts into TDMA frames, synchronisation with the BTS, detection of the idle channels and the measurement of the channel quality on the downlink. At Um, the physical layer uses GSMK (Gaussian Shift Minimum Keying) for the digital modulation and performs encryption/decryption of data This means that encryption is not performed end-to-end, but only between MS and BTS over the air interface.

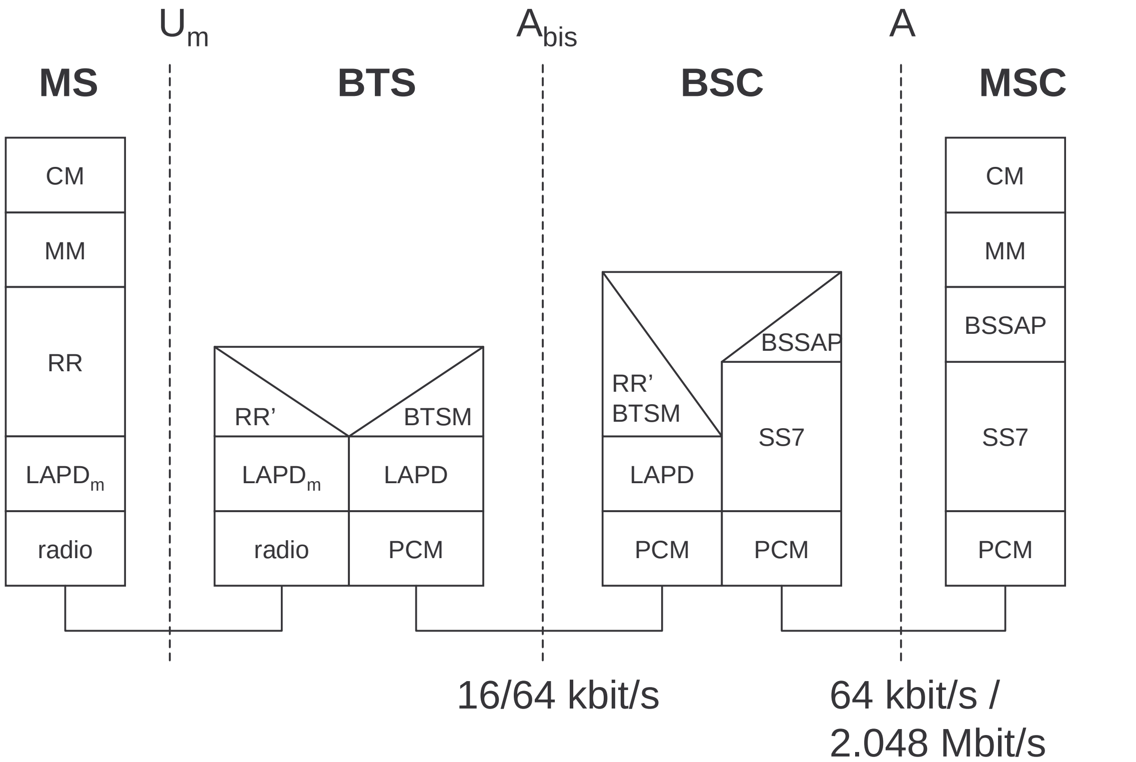

Figure 6 Protocol Architecture for signaling

The synchronisation also includes the correction of the individual path delay between the MS and the BTS, all MSs within a cell can use the same BTS and hence must be synchronised to the BTS. This is due to the fact that the BTS generated the time-structure of the frames and slots etc. This can be problematic since in this context there are different RTTs (Round Trip Time). *An MS that is close to the BTS has a very short RTT whereas an MS that is 35 km away has a RTT of around 0.23 ms.. If the MS 35 km away used the slot structure without correction, a large guard spaces would be required as 0.23 ms. are already 40% of the 0.577 ms available for each time slot.* (Wray Castle, GSM Appreciation, 1998.). Therefore the BTS sends the current RTT to MS, which then adjusts its access time so that all bursts reach the BTS within their limits. This mechanism ensures that the guard space is reduced to only 30.5 µs or 5%. See Figure 7. This means the adjustment of the access is controlled via the variable timing advance, where a burst can be shifted up to 63 bit times earlier, with the resulting bits having a duration of 3.69 µs, thus will result in the 0.23 ms needed.

The physical layer has several main tasks that comprise the channel coding, error detection/correction; this is directly combined with the coding mechanisms. FEC (Forward Error Correction) is used extensively in the coding channel, FEC adds redundancy to the user data, thus allowing for the detection and correction of selected errors. The power of the FEC scheme depends on the amount of redundancy, coding algorithm, and any further interleaving of data to minimise the effects of burst errors. Whatsmore the FEC is the reason that error detection/correction occurs in the physical layer. This differs to the ISO/OSI reference model where it occurs in layer two. The GSM physical layer tries to correct errors, however it does not deliver erroneous data to the higher layers.

GSM logical channels use different coding schemes with different correction capabilities, for example speech channels need the additional coding of voice data after analogue to digital conversion. This is in order to reach a data rate of 22.8 kbit/s (using the 13 kbit/s from the voice codec plus redundancy, CRC bits, and interleaving (Goodman, 1997). When GSM was envisaged it was assumed that voice would be the main service so the physical also contains special functions, for instance VAD (Voice Activity Detection), which transmits voice data only when there is a voice signal. In the duration between voice activity, the physical layer generates a comfort noise to fake a connection, however no actual transmission takes place.

All the interleaving in the voice channel is to minimise interference due to burst errors and the recurrence pattern of a logical channel generates a delay for transmission, although this delay is only about 60 ms for TCH/FS and about 100 ms for TCH/F9.6. These times have to be added to the transmission delay if the BTS is communicating with an MS rather than a standard fixed station (for example a stationary computer etc.) and this in turn may influence the performance of any of higher layer protocols, e.g.. for computer data transmission.

Signaling between the entities within the GSM network requires the use of the higher layers (see Figure 7). For this, the LAPDm (Link Access Procedure for the D-Channel) protocol has been defined at the Um interface for layer two. As the name already implies, it has been derived from link access procedure for the D-Channel (LAPD) in the ISDN system, which is a version of HDLC (Goodman, 1997), LAPDm is a lightweight version of LAPD, in that it does not require synchronisation flags or check summing for error detection, these are not needed as these functions are already performed in the physical layer of the GSM network. LAPDm, however offers reliable data transfer over connections, re-sequencing of data frames and flow control (ETSI, 1993, ETS 300 937), (ETSI, 1999) TS 100 938. Due to the fact that there is no buffering between layer one and two, the LAPDm has to obey the frame structures, recurrence patterns etc defined for the reassembly of data and acknowledged/unacknowledged data transfer.

Layer three in the GSM network is made up of several sublayers as shown in Figure 7, the lowest sublayer is the RR (Radio Resource Management). Only part of this layer the RR', is implemented in the BTS, the remainder of the RR is situated in the BSC. The BSC via the BTSM (Base Transceiver Station Management) are responsible for the functions of the RR'. The RR' has the function of setting up, maintenance and release of the radio channels. Also the RR' has direct access to the physical layer for radio information and offers a reliable connection to next higher layer.

MM (Mobility Management) encompasses the functions for registration, authentication, identification, location updating and the provision of TMSI (Temporary Mobile Subscriber Identity) that replaces the IMSI (International Mobile Subscriber Identity) and is needed to obscure the true identity of the MS over the radio air interface. Although the IMSI identifies the user, the TMSI is only valid within the location area of a VLR. MM also offers a reliable connection to the next higher layer.

Finally the CM (call management) layer contains three entities : CC (Call Control), SMS (Short Message Service) and SS (Supplementary Services). SMS allows for short messages transfer using the control channels SDCCH and SACCH, while SS offers the services described in section 2.1.1.3. CC provides a point-to-point connection between two terminals, the higher layers for call management use this, call clearing and change of call parameters. This layer also contains functions to send in-band tones, called DTMF (Dual Tone Multiple Frequency), over the GSM network.

Additional protocols are used at the A_{bis} and the A interfaces. Data transmission at the physical layer is typically done using PCM (Pulse Code Modulation) systems. Although PCM systems offer transparent 64 kbit/s channels, GSM allows for the sub-multiplexing of four 16 kbit/s channels into single 64 kbit/s (while remembering that 16kbit/s are enough for user data from an MS). At the physical layer, the A interface typically includes leased lines with a capacity of 2.048 Mbit/s. LAPD is used for layer two at A_{bis}, BTSM for the BTS management.

For signaling between the MSC and a BSC, the SS7 (Signaling System No, 7) is used. This protocol also transfers all the management information between MSC's, HLR, VLR's and OMC. Additionally, and MSC can control a BSS via the BSSAP (Base Station [Sub] System Application Part).

2.1.5 Localisation and Calling

One of the main features of GSM system is the automatic, worldwide localisation of it's users. The GSM system always knows where a user is currently located, and the same phone number is valid worldwide. To have this ability the GSM system performs periodic location updates, even if the user does not use the MS, provided that the MS is still logged on to the GSM network and is not completely switched off. The HLR contains information about the current location, and the VLR that is currently responsible for the MS informs the HLR about the location of the MS when it changes. Changing VLRs with uninterrupted availability of all services is also called roaming. Roaming can take place within the context of one GSM service provider or between two providers in one country, however this does not normally happen but also between different service providers in different countries, known as international roaming.

To locate an MS and to address the MS, several numbers are needed:

MSISDN (Mobile Station International ISDN Number)16. The only important number for the user of GSM is the phone number, due to the fact that the phone number is only associated with the SIM, rather than a certain MS. The MSISDN follows the E.164, this standard is also used in fixed ISDN networks.

IMSI (International Mobile Subscriber Identity). GSM uses the IMSI for internal unique identification of a subscriber.
TMSI (Temporary Mobile Subscriber Identity). To disguise the IMSI that would give the exact identity of the user which is signaling over the radio air interface, GSM uses the 4 byte TMSI for local subscriber

identification. The TMSI is selected by the VLR and only has temporary validity within the location area of the VLR. In addition to that the VLR will change the TMSI periodically.

MSRN (Mobile Station [Subscriber] Roaming Number)17. This is another temporary address that disguises the identity and location of the subscriber. The VLR generates this address upon request from the MSC and the address is also stored in the HLR. The MSRN is comprised of the current VCC (Visitor Country Code), the VNDC (Visitor National Destination Code) and the identification of the current MSC together with the subscriber number, hence the MSRN is essential to help the HLR to find a subscriber for an incoming call.

All the numbers described above are needed to find a user within the GSM system, and to maintain the connection with a mobile station. The following scenarios below shows a MTC (Mobile Terminate Call) and a MOC (Mobile Originated Call).

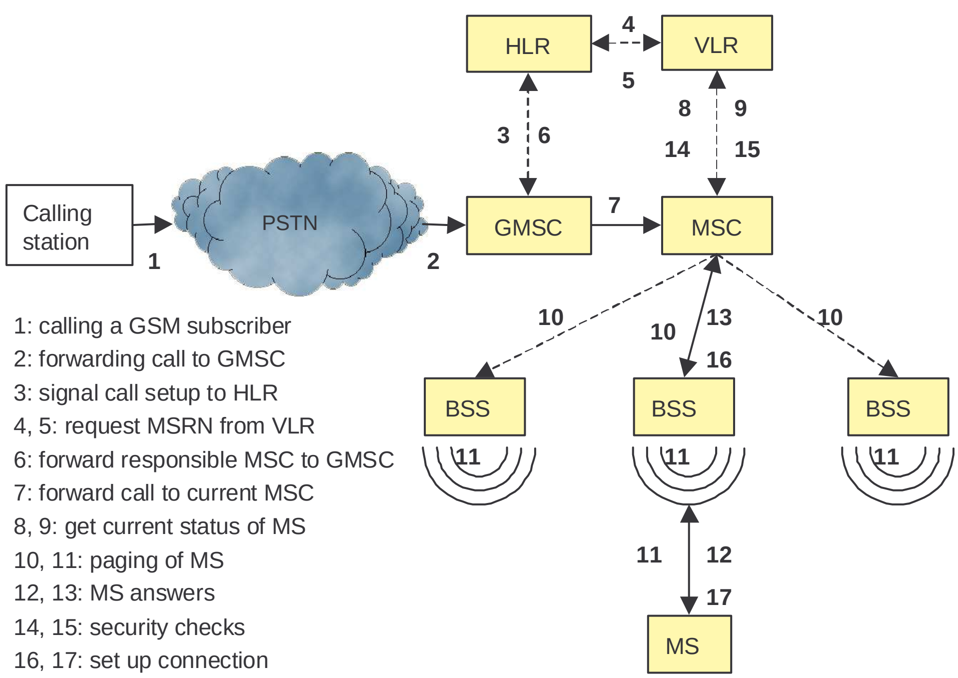

Figure 7 Mobile Terminated Call

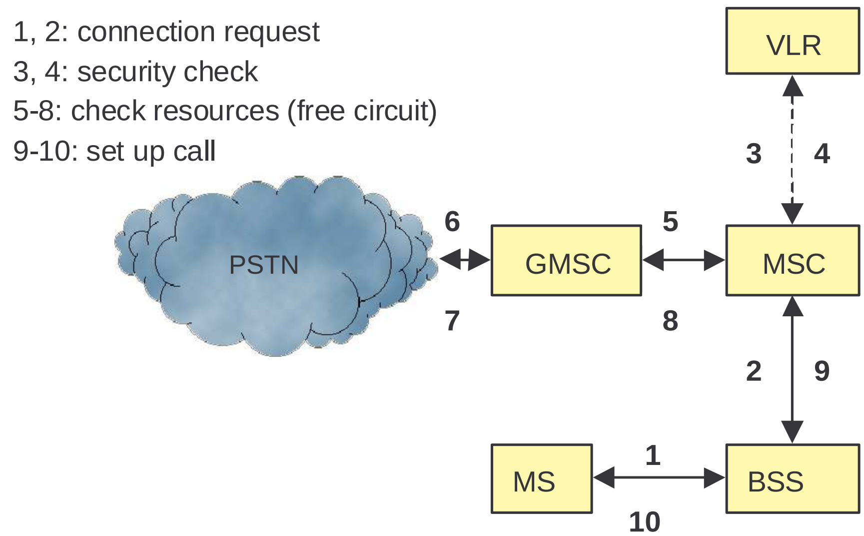

Figure 8 Mobile Originated Call

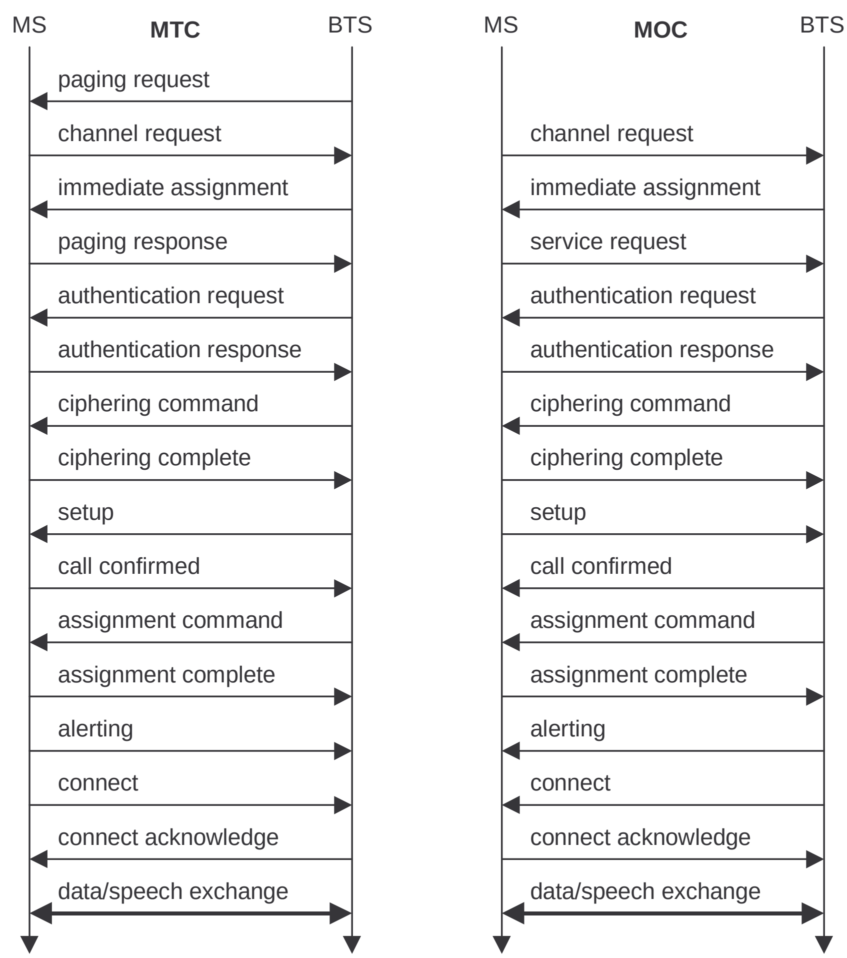

Figure 9 Message Flow for MTC and MOC

2.1.6 Handover

GSM systems require a procedure known as a Handover to maintain the continuity of the call. This is because a single cell does not cover the whole service area e.g. a whole city or country. However a single cell has a maximum service area of approximately 23 miles (35 km) for each antenna (Tripathi, et al. 1998). The smaller the size of the cell and the faster the movement of the MS through the cells (Up to 155 mph (250 kph) for GSM), the more handovers of ongoing calls are required, but a handover should not cause the a call drop. Basically there are two main reasons for handovers, however the GSM Specification identifies 40 reasons.

The MS moves out of coverage of the serving BTS thus the signal level becomes lower continuously until it falls beneath the minimal requirements for communications. Or the error rate may grow due to interference, the distance to the BTS may be do high. All these effects may diminish the quality of the radio link and make transmission impossible in the near future.

The wired infrastructure i.e. the MSC, BSC may decide that the traffic in one cell is too high thus introducing congestion and hence decides to shift some MSs to other cells with a lower level of traffic, if that is possible. Thus, handovers can be used as a method of controlling traffic through load balancing to relieve localised congestion.

Figure 11 shows four possible handover scenarios with in the GSM system.

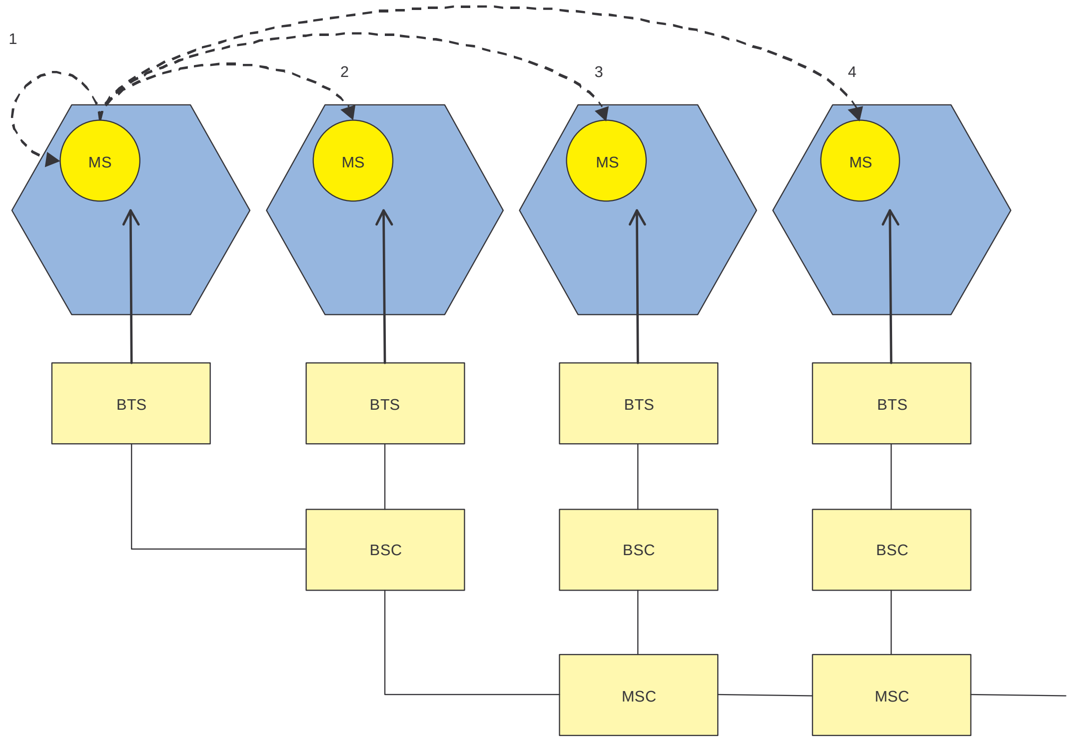

Figure 10 Types of handover within a GSM system

1. Intra Cell Handover : This happens when within a cell, when narrowband interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency. (1)

2. Inter Cell, intra BSC handover : This type of handover is a typical handover within the GSM system and occurs when the MS moves from one BTS to another but stays within the control of same BSC. The BSC performs the handover and assigns a new radio channel in the new BTS, then releases the old BTS. (2)

3. Inter BSC, Intra MSC handover : Since a BSC controls a limited number of BTSs, the GSM system has to perform handovers between BSCs. This form of handover is controlled by the MSC. (3)

4. Inter MSC handover : A handover could also be required between two BTSs that belong to two different MSCs, now both MSCs perform the handover together. (4)

In order to provide all the information necessary for a handover due to a weak link, the MS and the BSC both perform periodic measurements of the downlink and the uplink quality respectively. The link quality measurement is made up from receive signal level (RxLev) and the bit error rate (BER) and form part of the layer 3 messaging function. Measurement reports are sent by the MS about every 0.5 seconds and these contain the quality of the current link used for transmission as well as the quality of certain channels in neighbouring cells (the BCCHs).

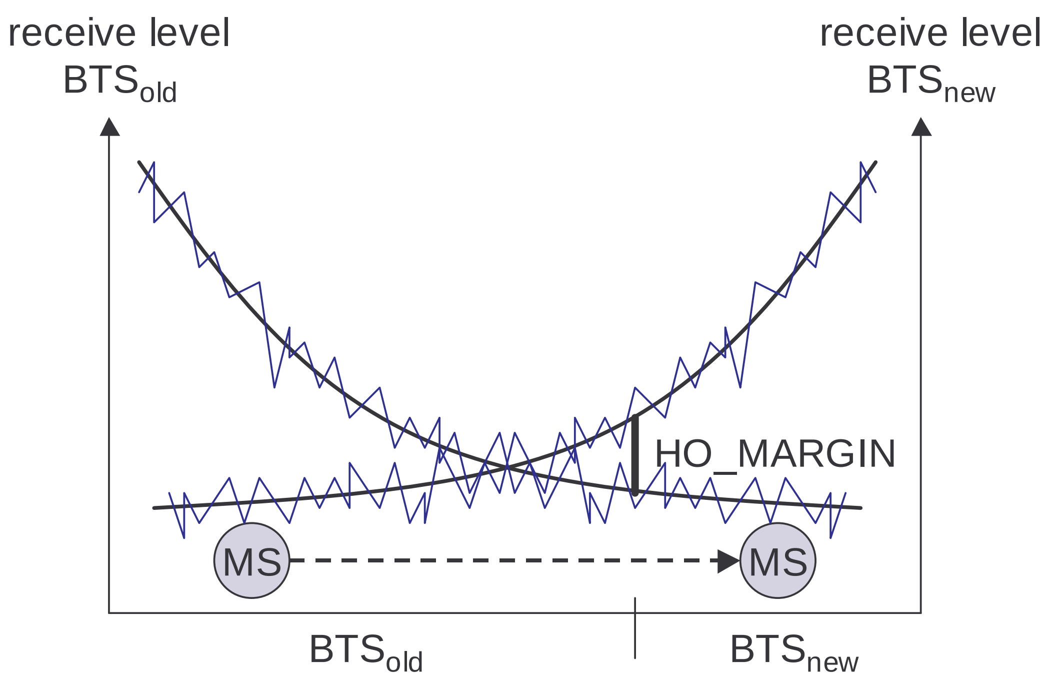

Figure 11 A Typical Handover decision, made depending on the RxLev

Figure 12 shows a handover decision, using the RxLev as the MS moves away from the BTS_{old} (BTS_{old} is the serving cell) towards another BTS

(BTS_{new}). In the handover decision shown in figure 12, the handover decision is made not purely on the instantanious value of the receive signal level, but on the average value.

So what's happening. The BTS collects all the values (RxLev and BER from the uplink and downlink) from the BTS and MS, then calculates the average values. These values are then compared to the Handover Margin (HO Margin). The HO Margin includes a hysteresis level to avoid the "*ping-pong*" effect (Wong, 1997). (*Without hysteresis, even short-term interference, e.g. shadowing due to a building, could cause a handover*). However, even with the HO Margin some ping-pong can still occur. If the HO Margin is set to high then this could cause dropped calls due to low RxLev, and if it is set to low then there will be many handovers in a short period, hence the ping-pong effect and a significant reduction in the quality of the service.

The HO Margin will change between rural and urban areas, but typically will be set at –8db.

The following three figures shows the typical measurement reports, and cell details for a handover. These measurements were taken using TEMS Investigation 2.02, supplied by Ericcson.

Typical Measurement reports for a Handover

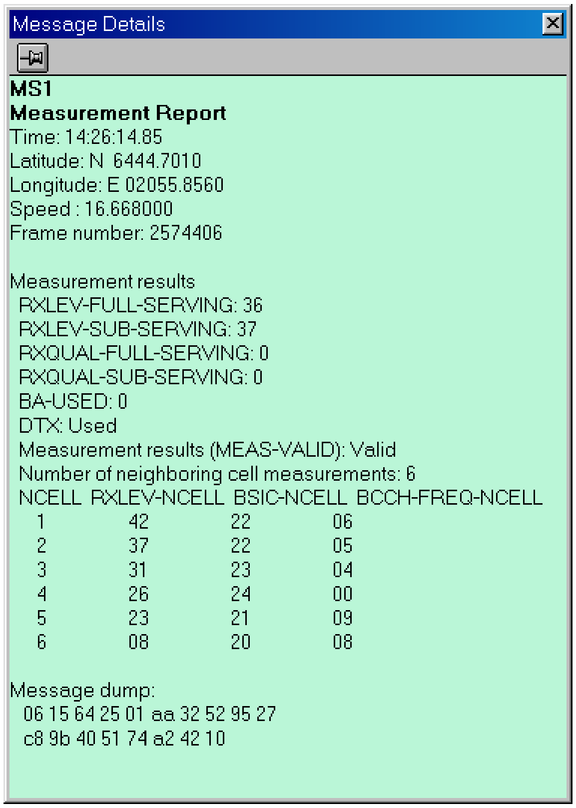

Figure 12 Measurement Reports Before Handover

(Source Ericsson Network Optimization Solutions, TEMS Investigation 2.02)

Message Details

MS1
Handover Command
Time: 14:26:14.95
Latitude: N 6444.7010
Longitude: E 02055.8560
Speed : 16.668000
Frame number: 2574428

Cell description
 PLMN colour code (NCC): 2
 BS colour code (BCC): 2
 BCCH ARFCN: 32
Channel description
 Channel type: TCH/F + ACCHs
 Timeslot number (TN): 6
 Training sequence code (TSC): 2
 Hopping channel: Single RF channel
 FB-NO: Band 0
 Absolute RF channel number (ARFCN): 32
Handover reference value: 174
Power level: 5
Synchronization indication (SI): Non-synchronized
Report Observed Time difference (ROT): Mobile time difference IE shall not be included in the HANDOVER COMPLETE message
Normal Cell Indication (NCI): Out of range timing advance is ignored
Channel mode: Speech full rate or half rate version 2

Message dump:
06 2b 12 20 0e 40 20 ae 05 d0
63 21

Figure 13 Handover Command

(Source Ericsson Network Optimization Solutions, TEMS Investigation 2.02)

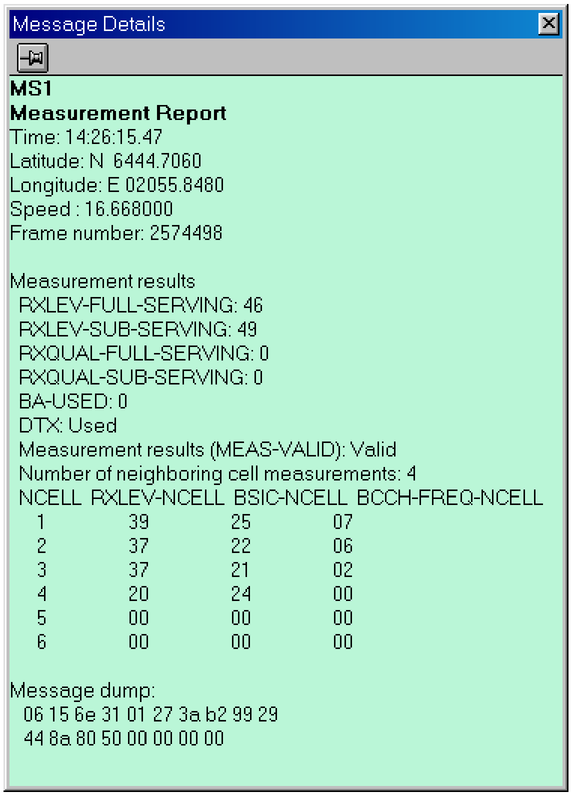

Figure 14 Measurement Report after Handover

(Source Ericsson Network Optimization Solutions, TEMS Investigation 2.02)

2.1.7 Security

The GSM system has several security services for security, these security services use confidential information that is stored in the AuC and in the customers SIM (Subscriber Identity Module) chip. The SIM chip may be plugged into any MS, however for the SIM chip to allow access to the MS the user must enter a PIN (Personal Identification Number), the SIM chip contain personal, secret data. The following are the security services offered by GSM:

Authentication and Access Control : For any MS to be used on the GSM network a number of events have to take place, the first event includes the authentication of a valid user for the SIM, the user enters their secret PIN to access the SIM. Then the MS contacts the AuC (See Figure 16 (Authentication Request)).

Confidentiality : All data that is related to the user is encrypted, after authentication the BTS and MS apply encryption to data, voice and signaling. This confidentiality only exist between the BTS and MS, however it does not exist end-to-end or within the whole fixed GSM/telephone network.

Anonymity : The GSM system also provides a level of anonymity, all of the data is encrypted before transmission, and user identifiers that would show the identity of a user are not used over the air. Instead the GSM system uses a temporary identitfier (TMSI), this is newly assigned by the VLR after each location update. Further more the VLR can change the TMSI at any time.

The GSM system uses three different algorithms to provide security services, the A3 algorithm is used primarily for authentication, A5 is used for the encryption/decryption and A8 which is used for the generation of a cipher key. Out of the three algorithms A5 was the only one that was publicly available, where as A3 and A8 were secret, but standard with open interfaces. However that change in 1998 when A3 and A8 were published on the internet.

2.1.7.1 Authentication

As I have already stated before any user can access the GSM system they must be authenticated as a valid user and this authentication is done by use of the PIN on the SIM. The SIM stores the users Individual Authentication Key K_i, the user identification IMSI and used the A3 algorithm for identification.

The authentication method that is used is challenge – response : the access control will generate a random number RAND as a challenge, and the SIM within the MS has to answer with a signed responses SRES as response. The AuC performs the basic generation of the RAND, signed responses SRES, and cipher key K_c for each IMSI, then forward this information to the HLR, then current VLR then requests the suitable values for the RAND, SRES and the K_c from the HLR.

For authentication the VLR sends the random value RAND to the SIM. Each side, the GSM network and the subscriber module, must perform the same operation with the RAND and the K_i. The MS sends back the SRES generated by the SIM, the VLR can now compare both values. If the value produced by the SIM and the VLR match then the user is granted to access the GSM network, however if they do not match then the subscriber is refused access to the network. This process is shown in Figure 16

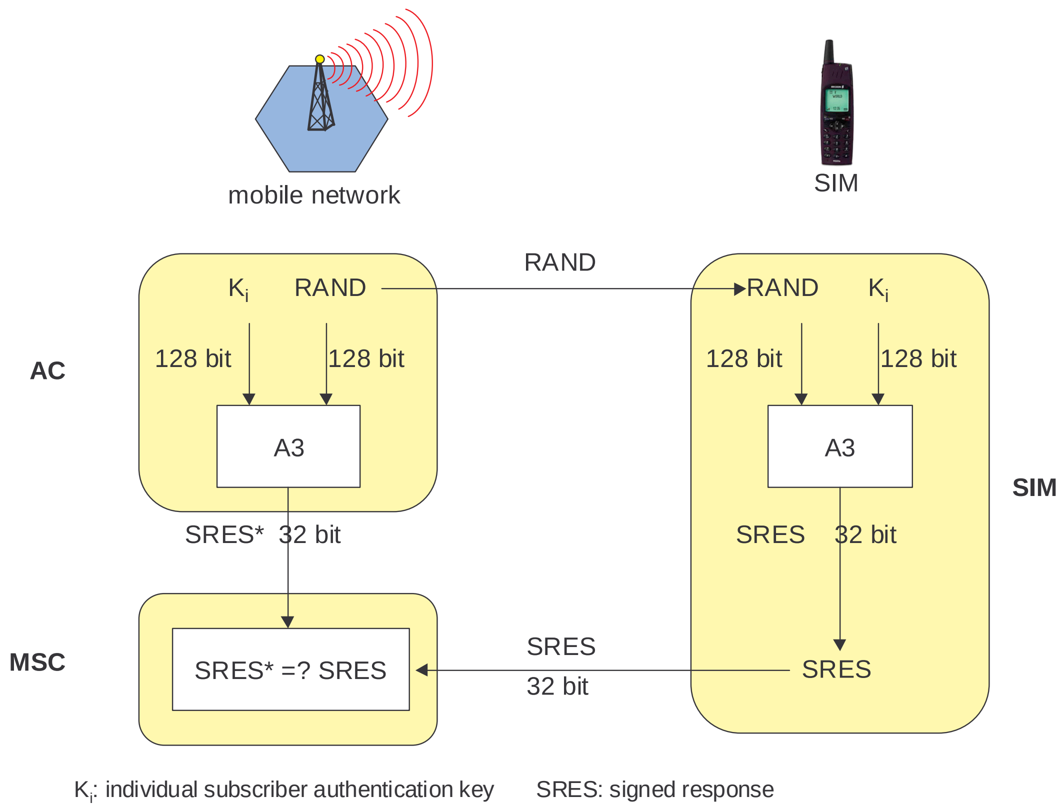

Figure 15 Subscriber Authentication

2.1.7.2 Encryption.

In the GSM system there is a large amount of user related information transmitted over the air interface and since this is the weakest part of GSM system it uses encryption to ensure privacy. After the user has been authenticated, the MS and the BTS can start using encryption by applying the cipher key K_c. K_c is generated using the individual key K_i and a RAND by applying the A8 algorithm. However it should be noted that that the SIM in the MS and the network both create the same value K_c based on the RAND. The K_c itself is not transmitted over the air interface.

The MS and the BTS can now encrypt and decrypt data using the A5 algorithm and the K_c. You can see the encryption and decryption process in Figure 17, K_c should be a 64 bit key – this however this level of encryption is not very strong, but provides enough protection to stop simple eavesdropping.

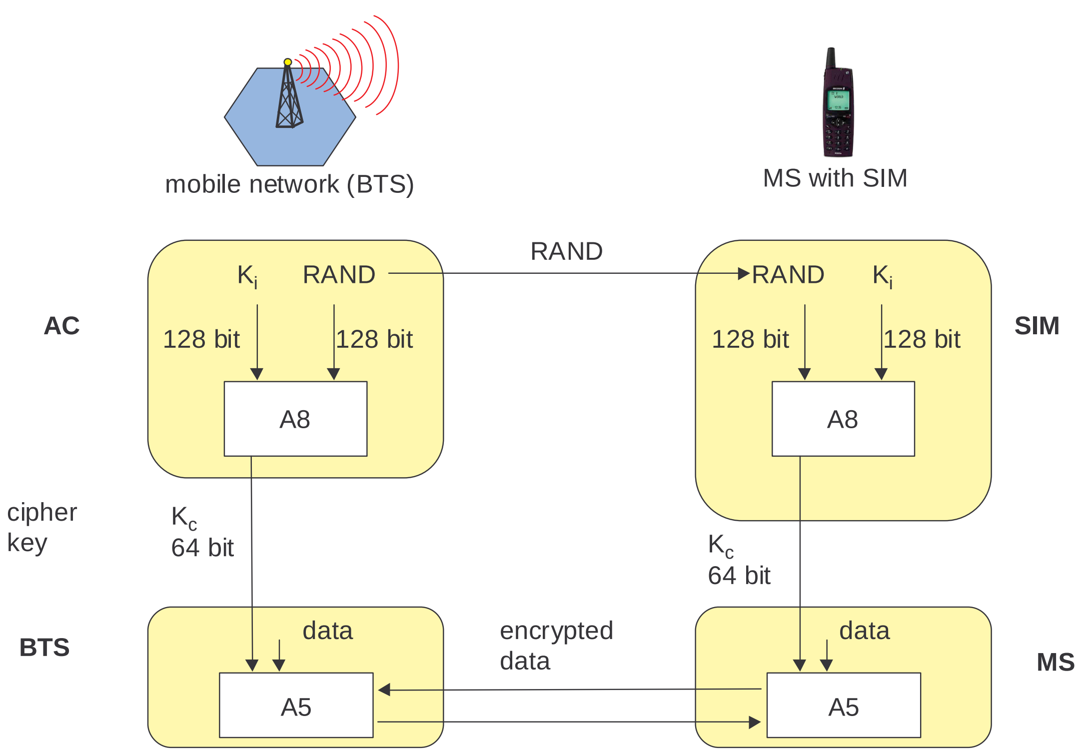

Figure 16 Data Encryption

Since the publication of the algorithm's A3 and A8 on the Internet, it has show that there are certain limitations for example 10 of the 64bits are always set to 0, hence the real length of the key is only 54 bits. The consequence of this is that the encryption is much weaker.

Chapter Summary and key Points

With the increase in demand for the need for communications whist away from a fixed line, GSM specifications were developed in order to provide greater capacity, improved quality and significantly greater security. Also the need to be able to use your mobile phone in other countries became of paramount importance.

GSM provided significantly greater capacity by the use of a combination of FDMA and TDMA. Whereas in previous technologies such as TACS and MTN the modulation technique was analogue and thus not very secure, GSM utilizes digital encoded modulation (See section 2.1.7.2), thus making it virtually impossible for interception by the casual eaves dropper. As a result of this certain Government agencies found it impossible to intercept calls and decode them in real time (DEA, See Appendix 2). However, in recent years details of the encryption algorithms have been made available to these agencies, and then leaked on the internet, thus reducing the security of the GSM system.

A further security improvement brought about by GSM was the use of SIM cards. The SIM card holds data relating to the user, authentication codes, and billing details.

The GSM radio air interface (Abis) is split into two levels, Physical Channels which are the radio bearers and Logical Channels which contain all the control and speech information in data streams. These logical channels are described in GSM Section 2.1.3.1. The net outcome is that speech only occupies a small amount of these data streams, hence the use of TDMA on the FDMA radio bearers.

Mobility means that the MS is moving from one location to another. Thus the system has to know where the MS is in order to direct calls. The MS continually provides a location update so that the network knows where to find the MS. Also because the MS is moving the network has to handover from BSC to another BSC, or another sector in the BSC. Consequently the MS has to continually measure the signal levels and quality in order to know which BSC has the appropriate availability in terms of capacity and quality. In this way the network is able to maintain connectivity and quality of service to the user.

With this increased mobility, users started to demand the ability to send data from their PCs and thus the mobile internet was born. In earlier technologies data transmission was achieved by the use of an analogue modems, but with GSM digital modems are now incorporated into the some MSs, thus providing greater data throughput.

The success of GSM data transmissions has meant that users require faster and faster speeds. On fixed lines the technique known as packet switched data transmission was available, but this was no use for GSM as the human ear cannot tolerate the delays introduced by such a technology. Initially data on the GSM network used a technique known as circuit switched (GSM-CS), which meant that the MS was permanently connected to a specific circuit, which was necessary for speech transmission. In order to increase the data rate a new technology based around packet switching had to be developed and thus the evolution of the GSM network continues into EDGE.