RF & Microwave e-Academy Program
Powerful tools that keep you on top of your game

RFTD 101: GSM Basics

Agilent Technologies

Printed on Jan, 2004 5988-8498ENA

RFTD 101: GSM Basics

Welcome to RFTD 101 on GSM basics. In this module, we will introduce the architecture and working of the world's most popular cellular standard.

At the end of this module you should have a broad understanding of the GSM system, it's air interface and how a call is connected on a GSM network.

So let's go straight in. But first, a little history.

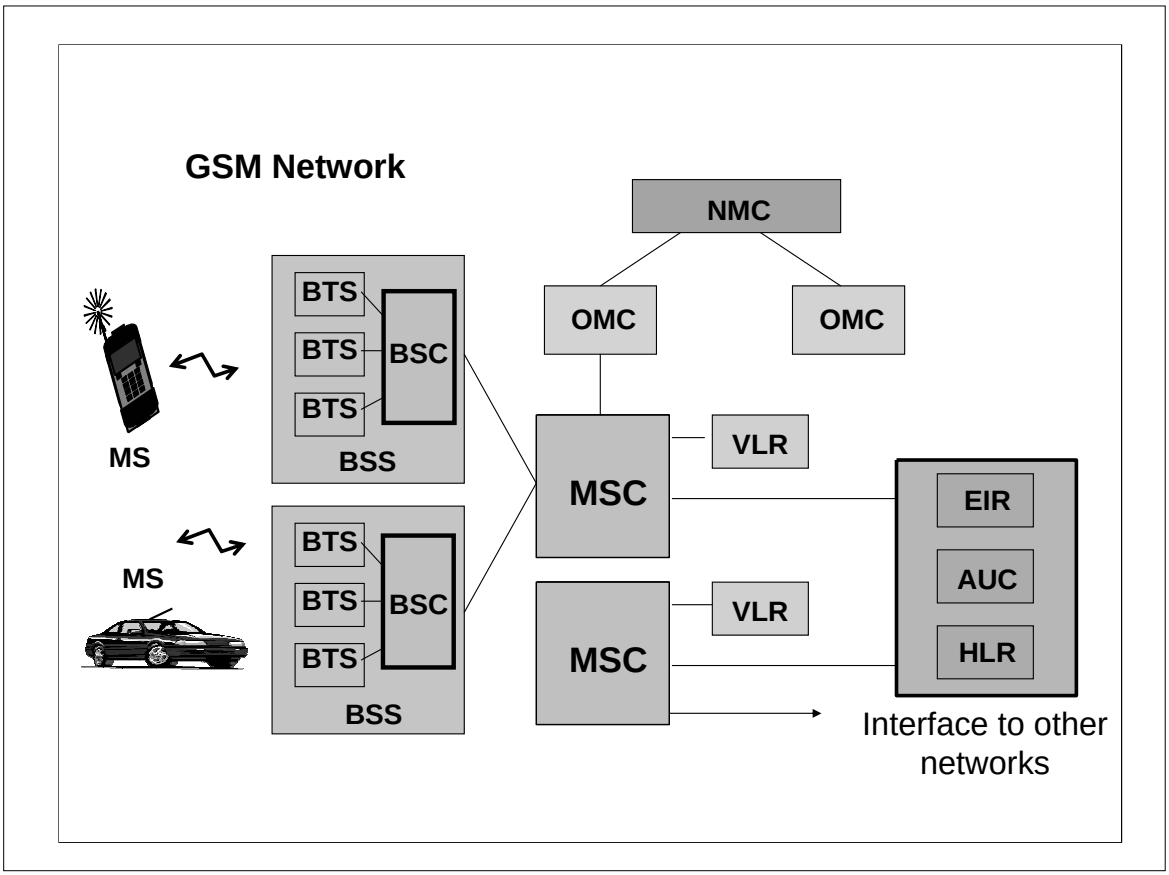
In 1981 analogue cellular was introduced and was a very successful communications technology. At about the same time there was a joint Franco-German study looking at digital cellular technology and the possibility of making a pan-European system.

In 1982 a special working committee, Groupe Spécial Mobile (GSM), was formed within the CEPT to look at and continue the Franco-German study. In 1986 the working committee was taken a step further by the establishment of a permanent nucleus of people to continue the work and create standards for a digital system of the future. About a year later, the memorandum of understanding, or MoU, as it is referred to, was signed by over 18 countries. It stated that they would participate in the GSM system and get it into operation by 1991.

In 1989 GSM was moved into the ETSI (European Telecommunications Standards Institute) organization. Once under the control of ETSI, the GSM system had it's name changed to Global System for Mobile communications. The committees working on the system changed from GSM to SMG (Special Mobile Group). These changes avoided confusion between the system name (GSM), and the people working on the specification (SMG). It also brought the naming in line with the official working language of ETSI (English).

In 1990 the GSM specification developed an offshoot - DCS1800. The Original DCS1800 specifications were developed simply as edited versions of the GSM900 documents. Interest in GSM quickly spread outside Europe. In 1992 Australia became the first non-European country to join the MoU. Since then, most Asian countries have adopted GSM. The Phase II specification for GSM has now been defined, merging GSM900 and DCS1800 documents, a number of new features are added to the system, along with many minor adjustments. Phase II+ defines the addition of specific new services such as data and fax to GSM and DCS1800.

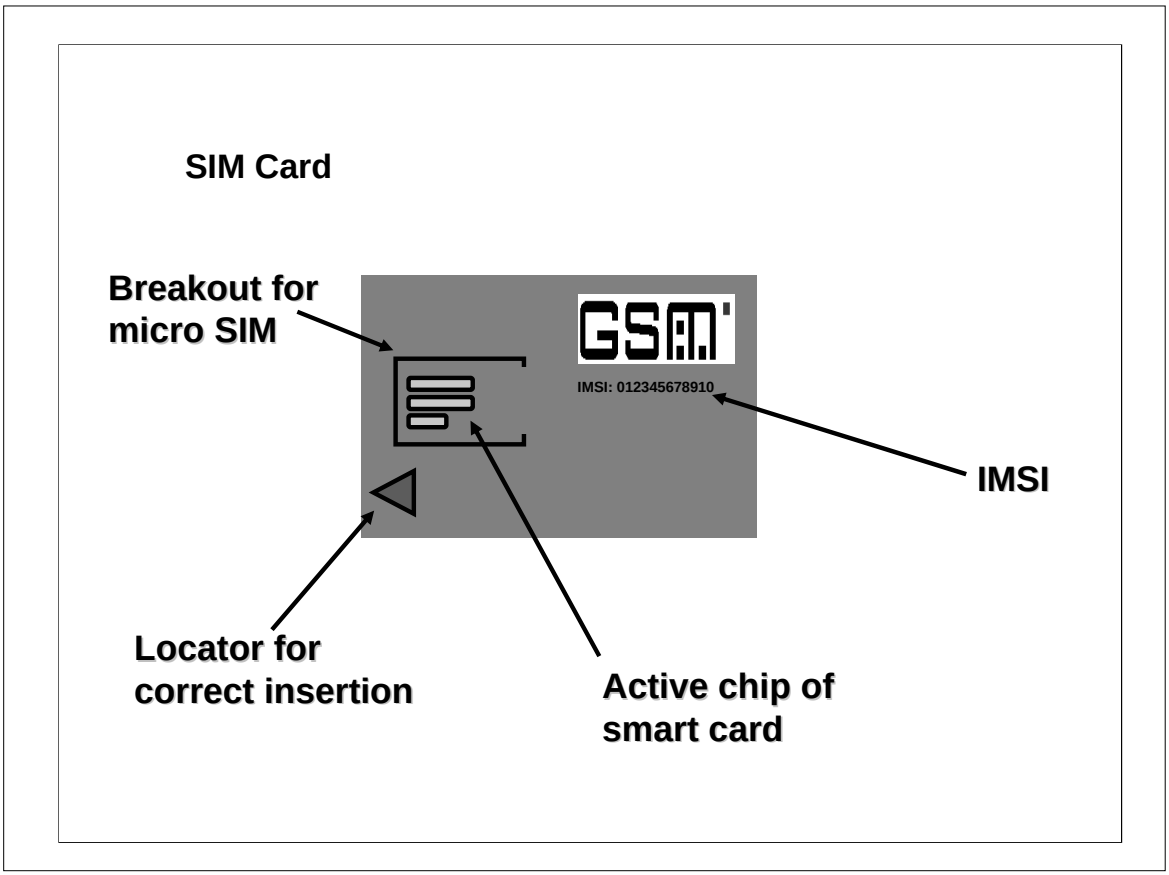
Today, GSM is by far the most popular cellular format. It has been deployed all across Europe, across most of Asia and in some countries in South America. A GSM variant, called PCS 1900, is deployed in North America. The need for more data capacity has added some extensions on GSM called GPRS and EDGE.



This is a simple representation of a GSM system. The Mobile Stations (MS) talk to the Base Station System (BSS) over the RF air interface. The Base Station System (BSS) consists of a Base Transceiver Station (BTS), and a Base Station Controller (BSC). It's typical for several BTS to be located at the same site, producing 2 to 4 sectored cells around a common antenna tower. BSC's are often connected to BTS via microwave links.

The BSC to BTS link is called the Abis interface. Typically 20 to 30 BTS will be controlled by one BSC. A number of BSS's would then report back to the Mobile Switching Center (MSC) which controls the traffic among a number of different cells. Each (MSC) will have a Visitors Location Register (VLR) in which mobiles that are out of their home cell will be listed, so that the network will know where to find them. The MSC will also be connected to the Home Location Register (HLR), the Authentication Center (AUC), and the Equipment Identity Register (EIR) so the system can verify that users and equipment are legal subscribers. This helps avoid the use of stolen or fraud mobiles. There are also facilities within the system for Operations and Maintenance (OMC) and Network Management (NMC) organizations. The Mobile Switching Center (MSC) also has the interface to other networks such as Private Land Mobile Networks (PLMN) and Public Switched Telephone Networks (PSTN) and ISDN networks.

Each block has an interlinking interface. The link between a mobile and the BTS is called the Um Interface, or more simply the air interface. The Abis interface links the BTS with the BSC, while the A interface links the BSC with the MSC. The links may be implemented as optical fibers or microwave links. The various interfaces are all defined in the GSM standard.



Without a SIM installed, all GSM mobiles are identical. It's the SIM card that gives a mobile its identity. If a user takes his SIM on a business trip and plugs it into the GSM mobile fitted to his rental car, the car's phone takes on the SIM's identity. The user's network access rights, his speed-dial memories and any other saved features, are transferred to the rental car phone. The really nice feature of SIMs is that they also carry your phone number. If the user's office want to call him, they simply dial his normal mobile number. The network knows the location of the phone with the user's SIM in it and so routes the call directly to the rental car.

The SIM card comes in two sizes:

- standard (credit card size) – this was used in older generation phones and is hardly ever used these days
- micro (postage stamp size)

SIMs (subscriber Identification Modules) plug into the GSM mobile. The SIM holds all the information related to a subscriber. For example:

- Unique subscriber number or IMSI (International Mobile Subscriber Identification)
- The networks and countries where service is entitled (MCC and MNC)
- Any other user specific information like speed dial numbers and memories

For test purposes, there are special Test-SIMs. Test SIMs allow mobiles to enter a special loop-back mode for receiver BER test.

GSM Channel Plans

	Phase 1 GSM900	Phase 2 GSM900	Phase 1 DCS1800	Phase 2 DCS1800	PCS1900
Uplink Frequency Range	890 to 915MHz	880 to 915MHz	1710 to 1785MHz	1710 to 1785MHz	1850 to 1910MHz
Downlink Frequency Range	935 to 960MHz	925 to 960MHz	1805 to 1880MHz	1805 to 1880MHz	1930 to 1990MHz
ARFCN Range	1 – 124	0 – 124 and 975 – 1023	512 – 885	512 – 885	512 – 810
Tx/Rx Spacing (MHz)	45	45	95	95	80

Each Base Transceiver Station (BTS) will be fitted with a number of TX/RX pairs or transceiver modules. The number will determine how many frequency channels can be used in the cell, and depends on the expected number of users. The link between the Base Station (BS) and the Mobile Station (MS) is called the Downlink and the link between MS and BS is the Uplink. These are separated by

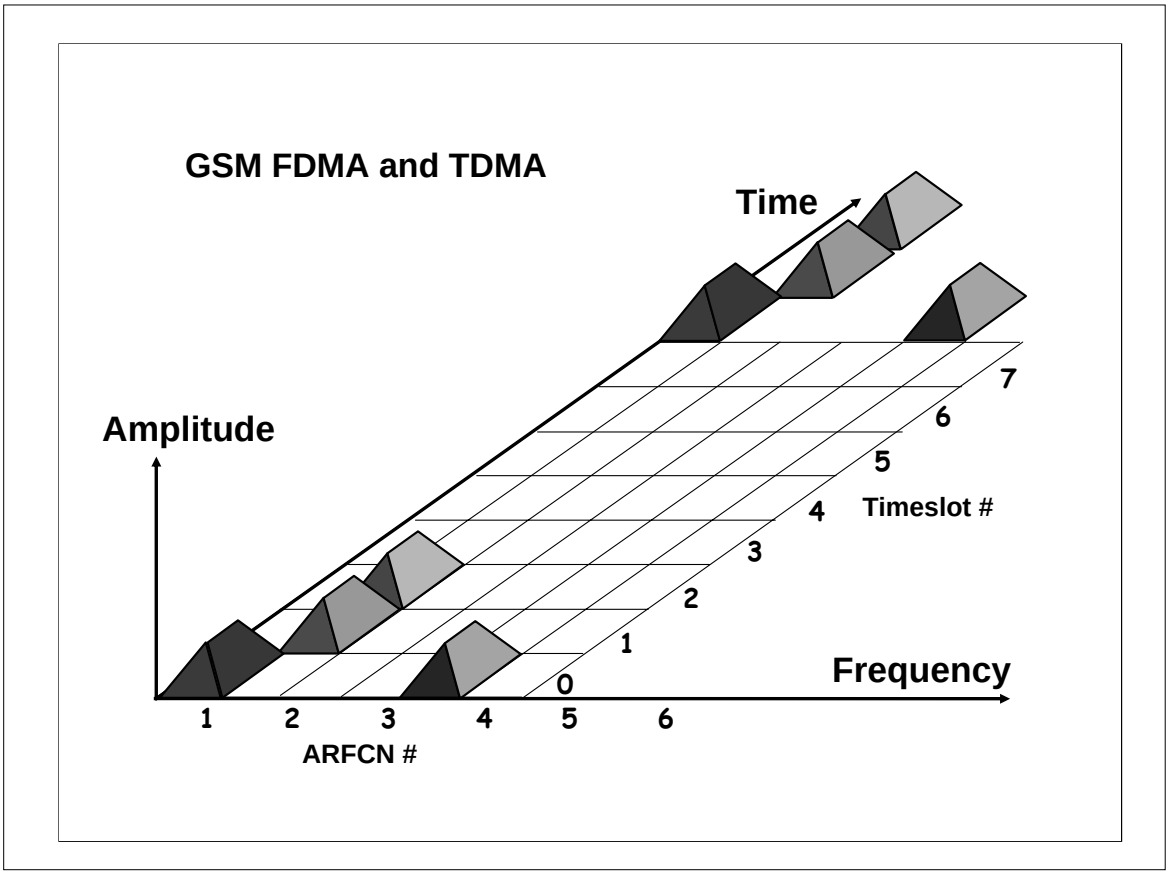
45 MHz in GSM

95 MHz in DCS

80 MHz in PCS

The table above shows the relative frequency plans of the three GSM networks: GSM900, DCS1800 and PCS1900.

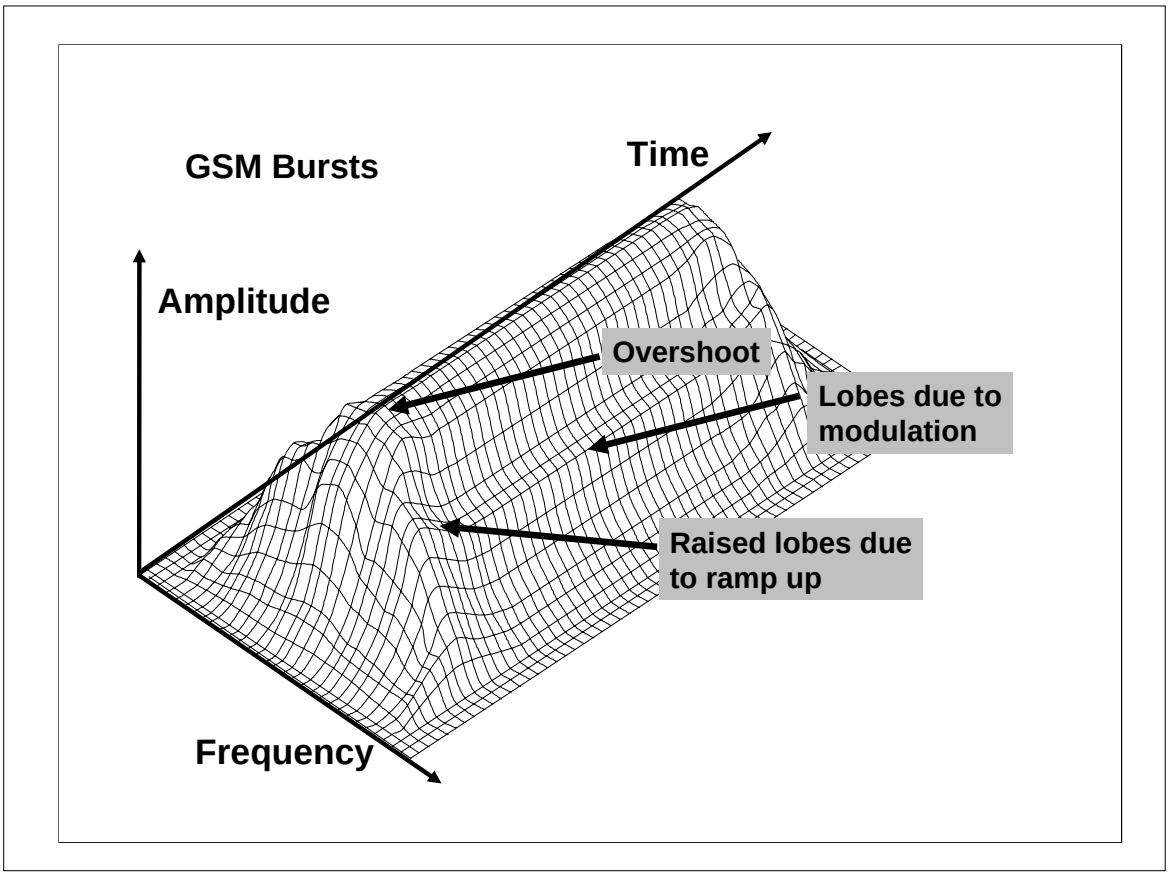
The frequency range of the Uplink and Downlink show how the two bands are split into the two directions, rather than an uplink being followed by a downlink 200kHz later. Another difference is that the channel numbers are different. Remember this if you write any test control software and want to port from one system to another, as the channel numbers must be changed for correct operation.



GSM uses TDMA (Time Division Multiple Access) and FDMA (Frequency Division Multiple Access). The slide shows part of one of these bands. Each band is divided into 200kHz slots called ARFCN's (Absolute Radio Frequency Channel Numbers).

As well as dividing up the frequency, the ARFCN is also divided in time into 8 Timeslots (TS), each TS being used in turn by a different MS. The 8 TS's together are known as a Frame. The slide illustrates 4 TCH's (Traffic Channels). Each one of the TCH's uses a particular ARFCN and Timeslot. Two of the TCH's are on the same ARFCN, using different timeslots, the other two are on different ARFCN's.

The combination of a TS number and ARFCN is called a physical channel.

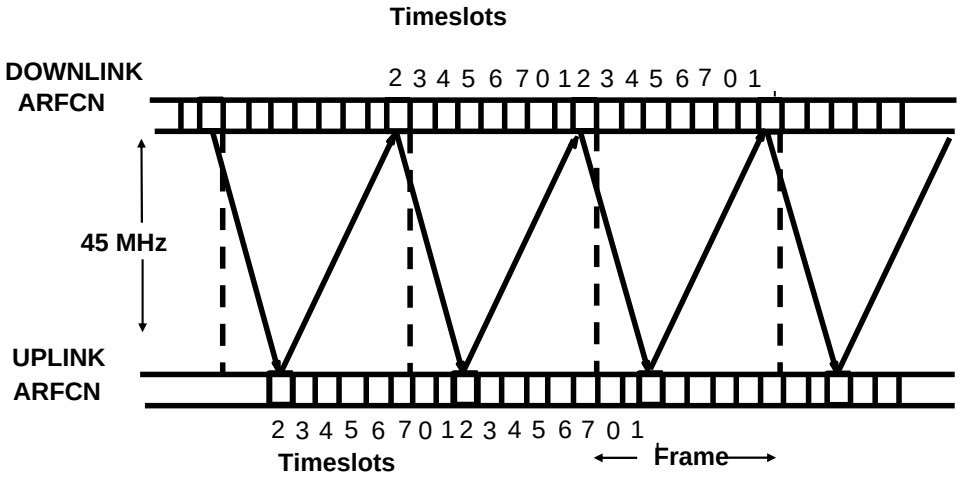


Above is a more detailed representation of a GSM burst. There are three areas to consider:

The overshoot that is caused by the fast ramp up of the burst
The lobes due to the ramp up
The lobes due to the modulation.

These are all specified by the GSM standard.

Downlink and Uplink



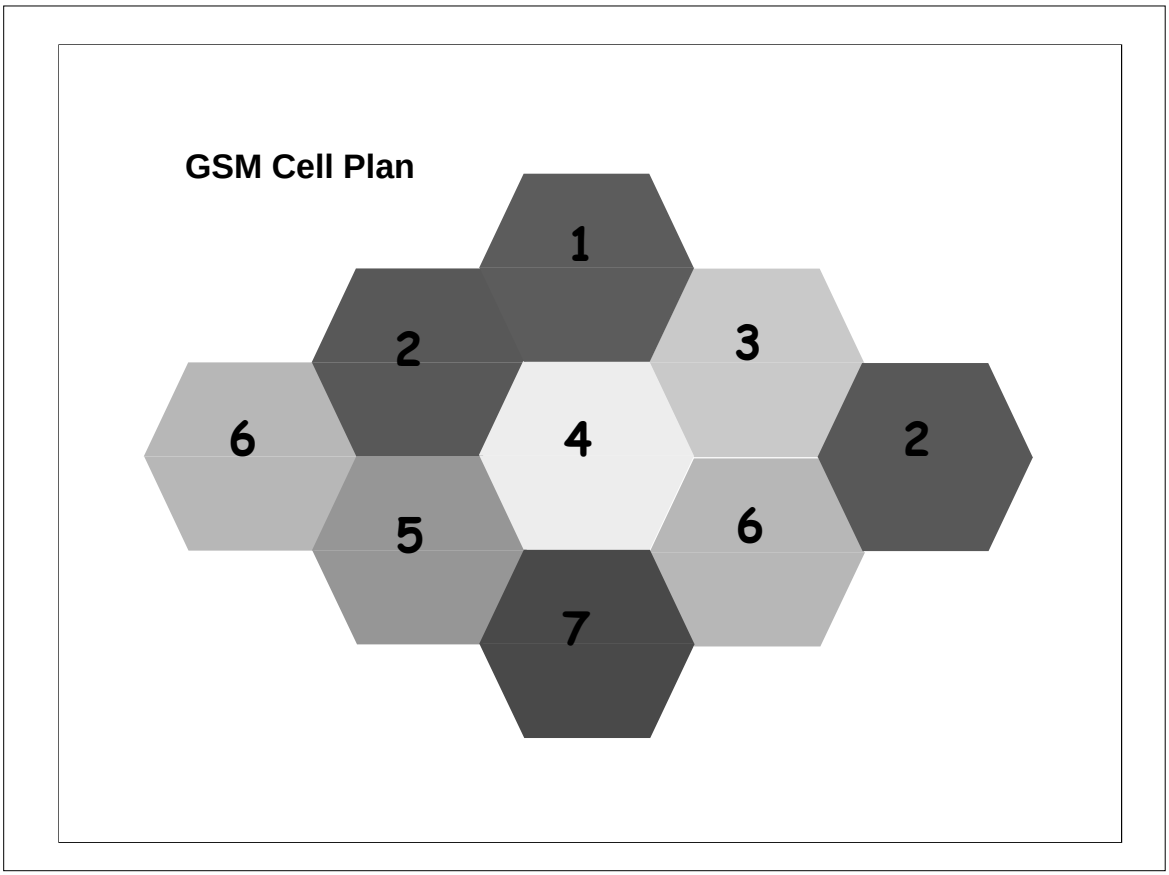
- **Uplink Lags Downlink by 3 Timeslot periods**
- **Uplink and Downlink use same Timeslot Number**
- **Uplink and Downlink use same Channel Number (ARFCN)**
- **Uplink and Downlink use different bands (45MHz apart for GSM900)**

To see how information is transmitted let's look at an example.

We have been assigned timeslot 2 and we're in a traffic mode, receiving and transmitting information to the base station. The downlink, on which we receive information, will be in the frequency range of 935 to 960MHz. The uplink, the frequency which the mobile will transmit information to the base station, will be in the frequency range of 890 to 915MHz.

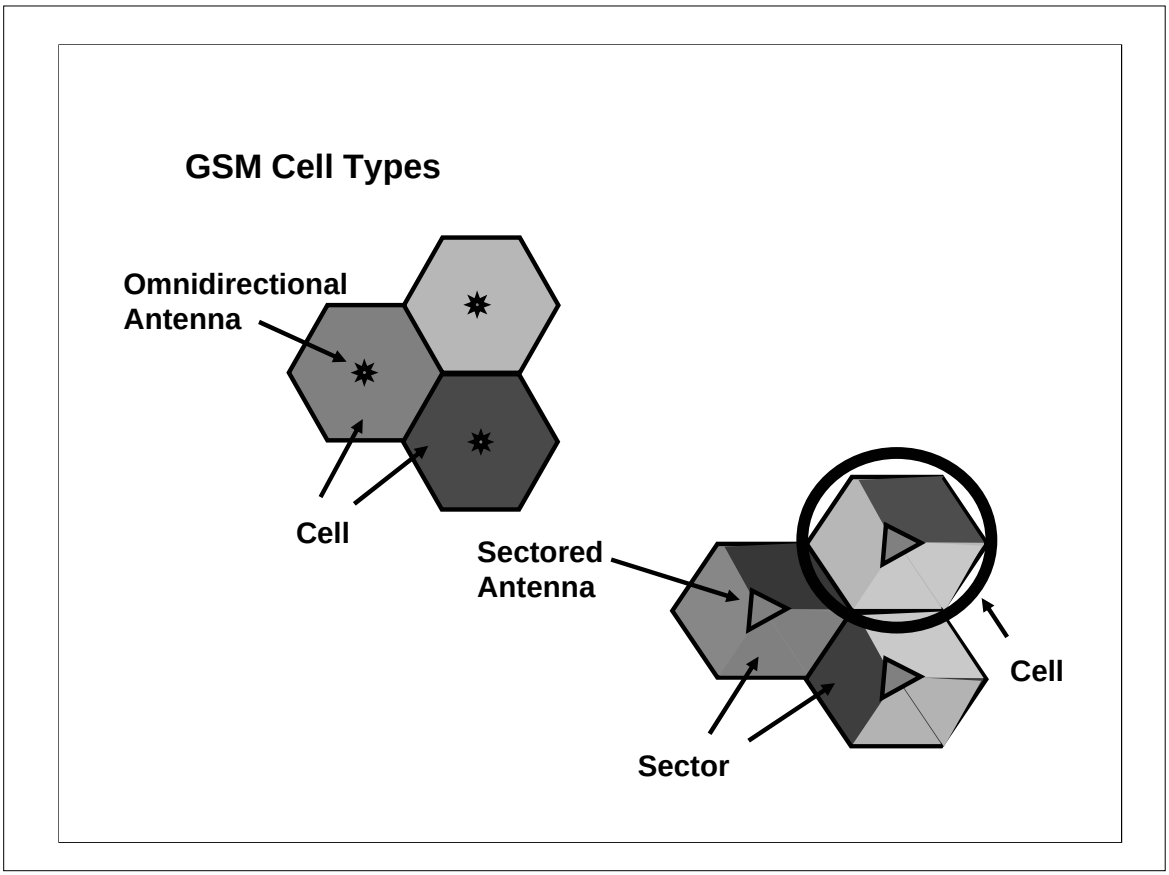
The uplink and the downlink make up a frequency pair, which for GSM900, is always separated by 45MHz.

In the previous example we can see that the timeslots are offset by 3 between the downlink and the uplink. We receive information in timeslot two in the downlink we have two timeslots in which to switch to the uplink frequency and be ready to transmit information. Then, we have to get ready to receive our next time slot of information in the next frame.



GSM uses a number of channels in each cell. However, the same channels cannot be used in adjacent cells, as they would interfere with one another. This is Spatial Division Multiple Access (SDMA), a scheme that reuses the channels in distant geographical areas.

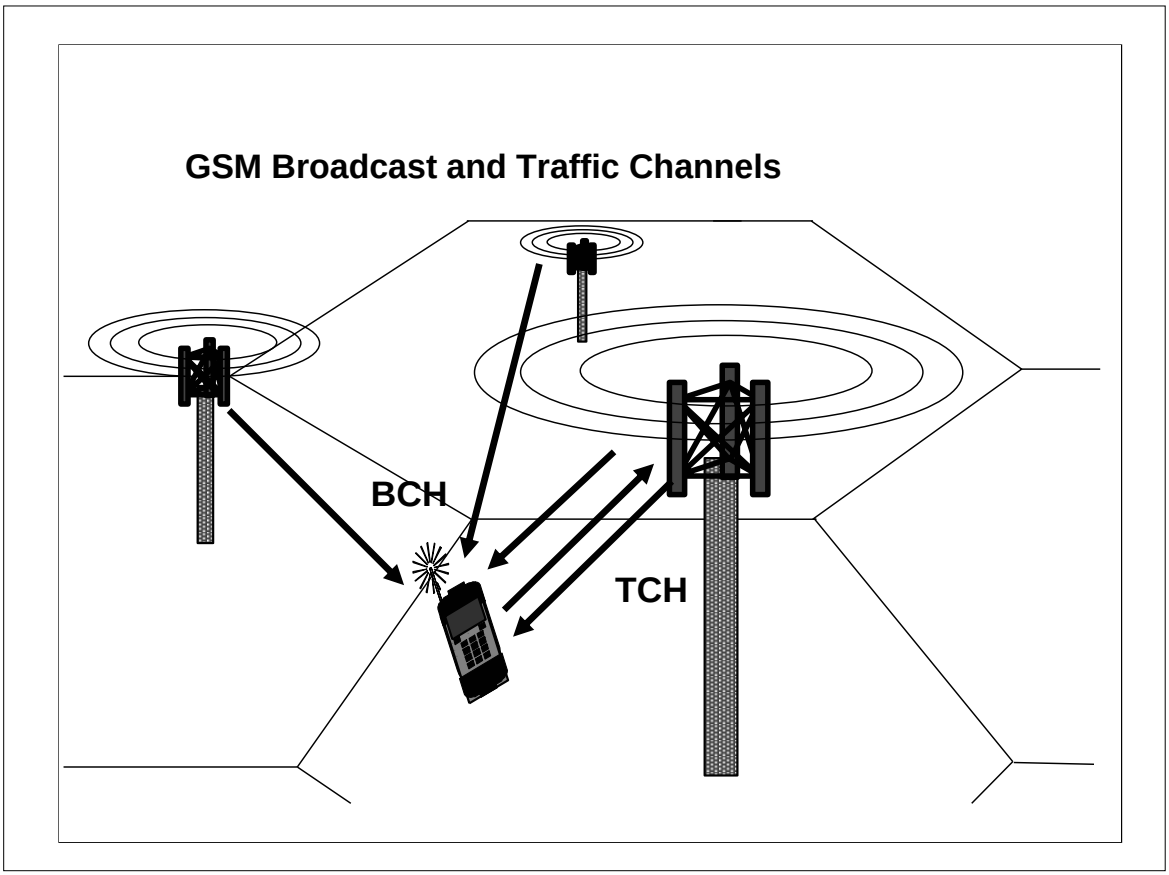
Above is a pattern known as an “N in 7”. In this example there is about three cells distance between reused channels. There are many other patterns used. These depend on output power and cell size.



One way for cells to be designed is using an omnidirectional antenna at the center. The whole cell uses the same channels.

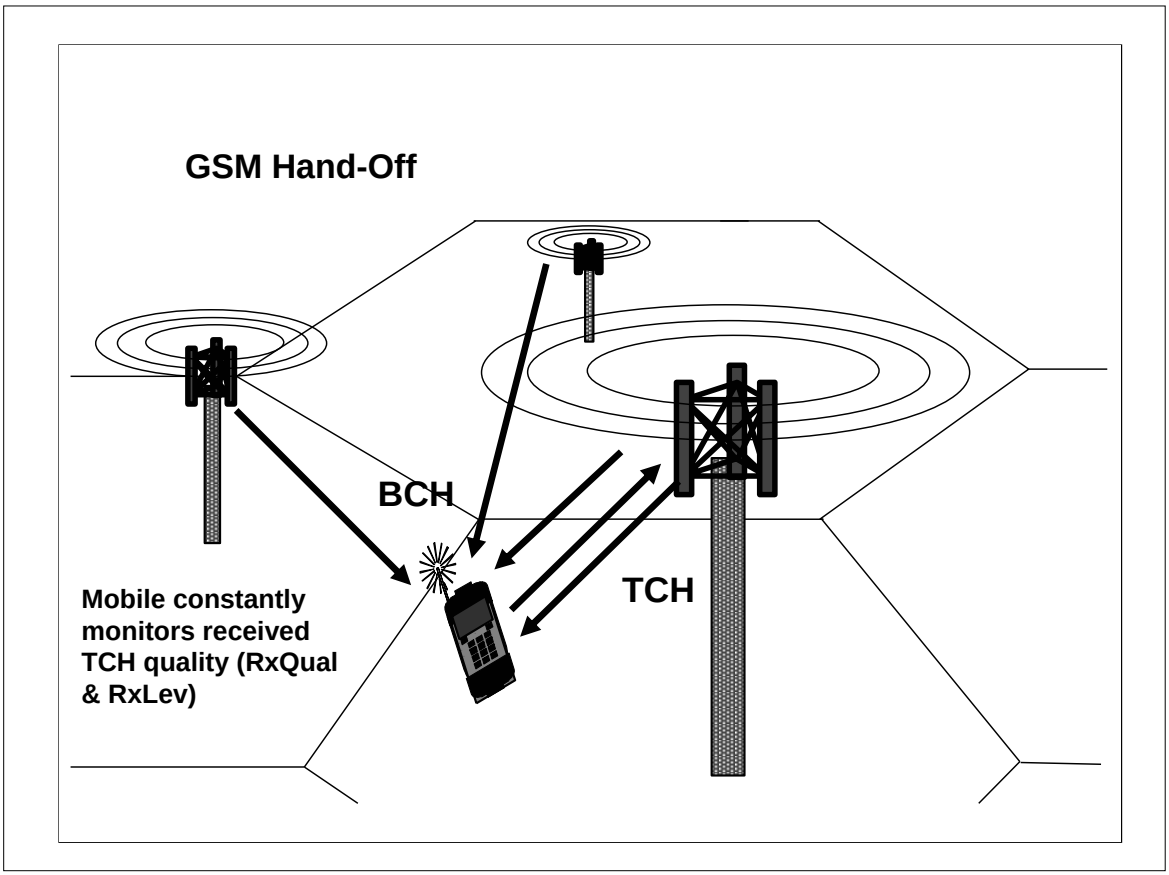
Another cell design is a sectored cell. This uses a beam antenna, which in the above example has a 120° beam width. This forms a three-sectored cell. There are other sector designs that can be used for other applications.

The are other types available but these are the most common. Another cell is the 'Umbrella' cell that is long and thin and is used to cover roadways in remote areas. This is used so that the valuable energy from the base station is not wasted on sides of the road that have no need for coverage. It also reduces handoff frequency.



All BTS produce a Broadcast Channel (BCH). The BCH is like a lighthouse or beacon. It's on all the time and allows mobile to find the GSM network. The network for a variety of user functions also uses the BCH signal strength. It's a useful way of telling which is the closest BTS to the mobile. It also has information coded onto it, such as the identity of the network (e.g. Mannesmann, Detecon, or Optus), paging messages for any mobiles needing to accept a phone call, and a variety of other information. Each mobile will monitor the power of adjacent cell BCH's to aid the network in making hand-off decisions.

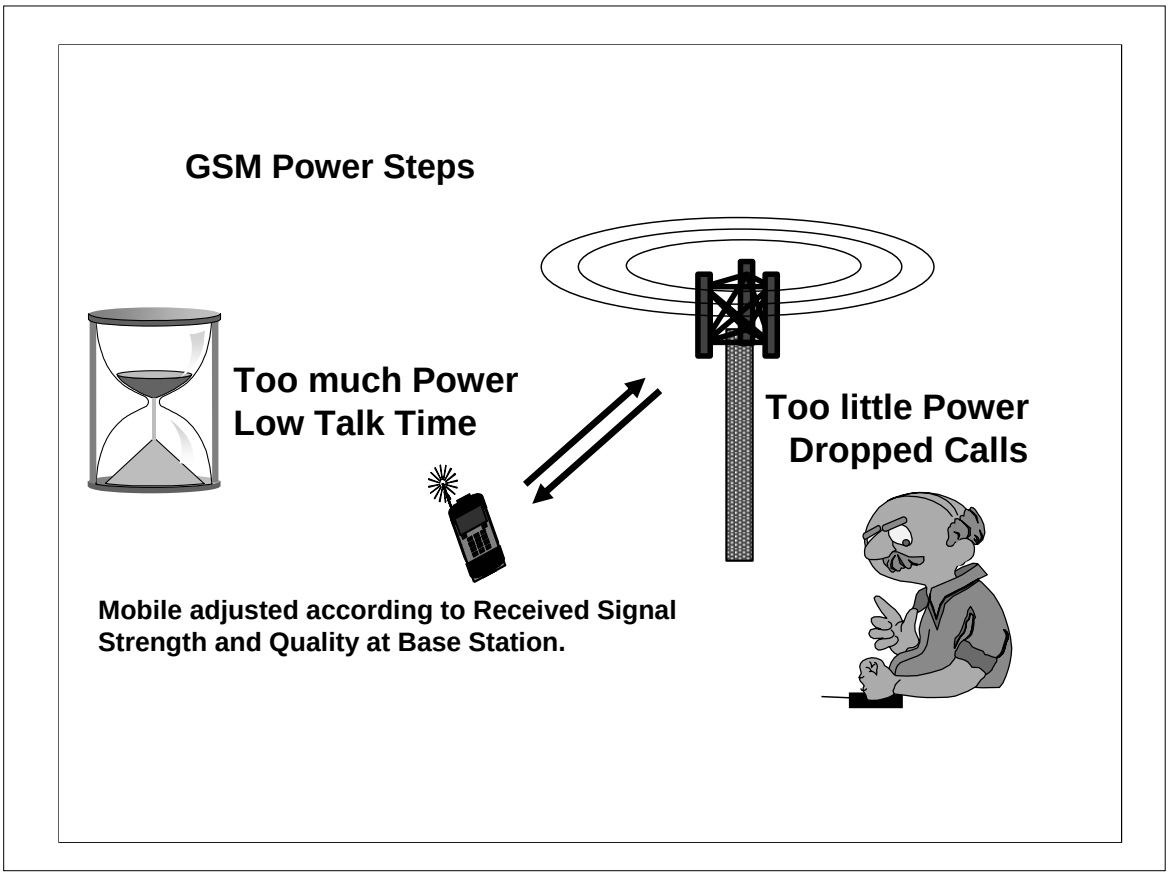
Mobiles on a call use a Traffic Channel (TCH). The TCH is a two way channel used to exchange speech information between the mobile and base-station. It's interesting to note that while the TCH uses a frequency channel in both the uplink and downlink, the BCH occupies a channel in the downlink band only. The corresponding channel in the uplink is effectively left clear. The mobile can use this for unscheduled or Random Access Channels (RACH). When the mobile wants to grab the attention of the base station (perhaps to make a call).



When the MS is on a call, it is constantly monitoring the Received Signal Quality (a bit error rate measurement known as RxQual) and the Received Signal Level (a power measurement call RxLev). These are constantly being sent back to the BS on a Slow Associated Control Channel (SACCH). When the levels cannot be maintained by adjustments in power level by the BS, it will instruct the MS to start a hand-off. As mentioned earlier, the MS is also monitoring the surrounding cells' BCH's, this helps the BS decide which is the best cell to hand-off to.

Besides receiving and transmitting information, the mobile must switch frequency and get ready to receive and measure the level of the adjacent cell's broadcast channels. It then reports this (RxLev) information to its own base station in order to establish when a handoff is appropriate between cells. Again, information is received on timeslot 2, we switch 45MHz to transmit information and then, need to switch back 45MHz +/- a few MHz to monitor and measure the level of the adjacent cell's broadcast channels. This information will be reported back to the base station at least every 30 seconds so that the base station can determine the appropriate time to do a handoff. The RxLev information is reported back to the base-station on the uplink SACCH (Slow Associated Control CHannel).

The mobile uses a list of ARFCN in the BA (Base Allocation) table to know which BCH frequencies to go out and measure. The BA table is coded onto the BCH, and also the downlink SACCH.



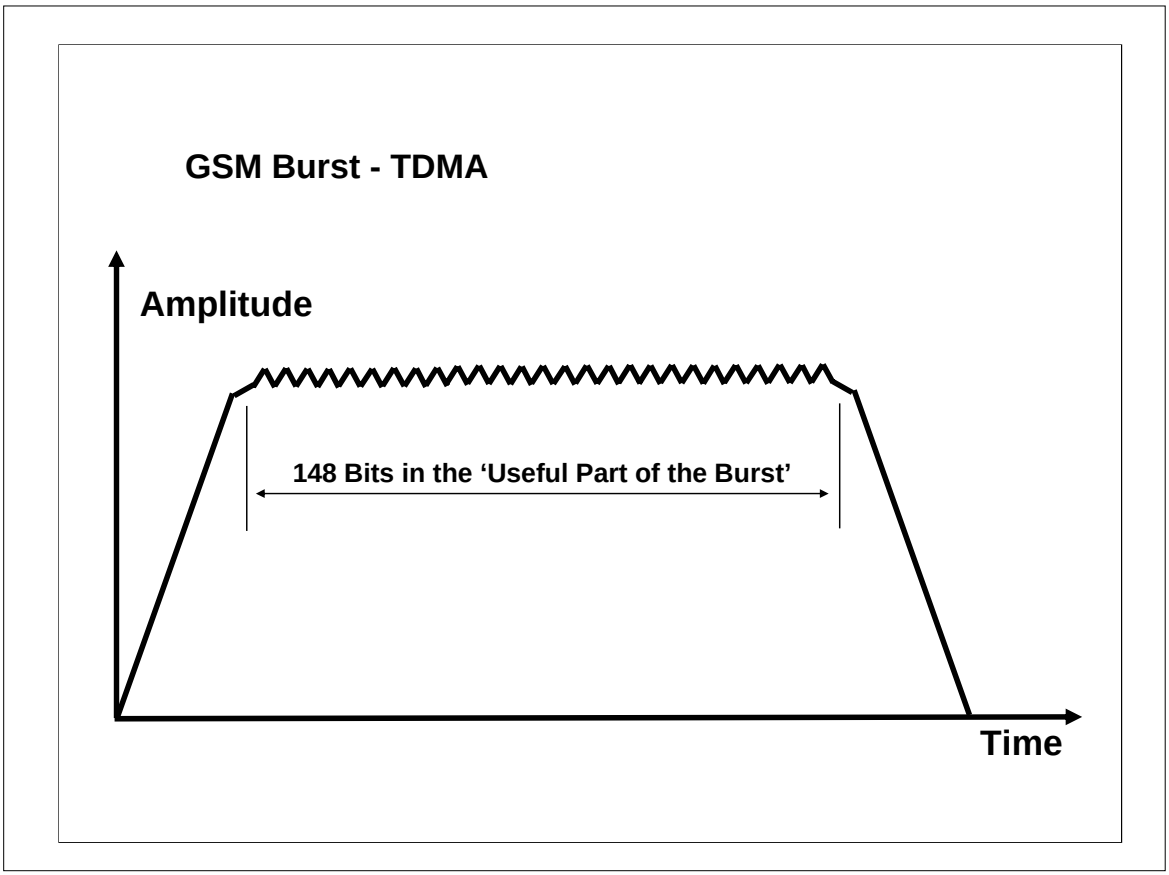
As the mobile moves around the cell, its transmitter power needs to be varied. When it's close to the base station, power levels are set low to reduce the interference to other users. When the mobile is further from the base station, its power level needs to increase to overcome the increased path loss. However, if too much power is used, the user's battery will run down too quickly.

All GSM mobiles are able to control their output power in 2dB steps. The base station commands the mobile to a particular MS TX Level (power level) by watching the power level of the received signal at the BS.

Mobile Power Levels

	Phase 1 GSM900	*Phase 2 GSM900*	*Phase 1 DCS1800*	*Phase 2 DCS1800*	*PCS1900*
Mobile Max Power	20W (8W used) 43dBm/39dBm	8W / 39dBm	1W / 30dBm	4W / 36dBm	2W / 33dBm
Mobile Min Power	20mW /13dBm	3mW / 5dBm	1mW/ 0dBm	1mW / 0dBm	1mW / 0dBm
Mobile Power Control Steps	0 - 15	2 - 19	0 - 13	0 - 15	0-15 ,30,31

The table above shows the maximum and minimum power levels on the mobiles in different systems. The final row shows the power steps, which are all numbered, and how they relate to the max and min powers.

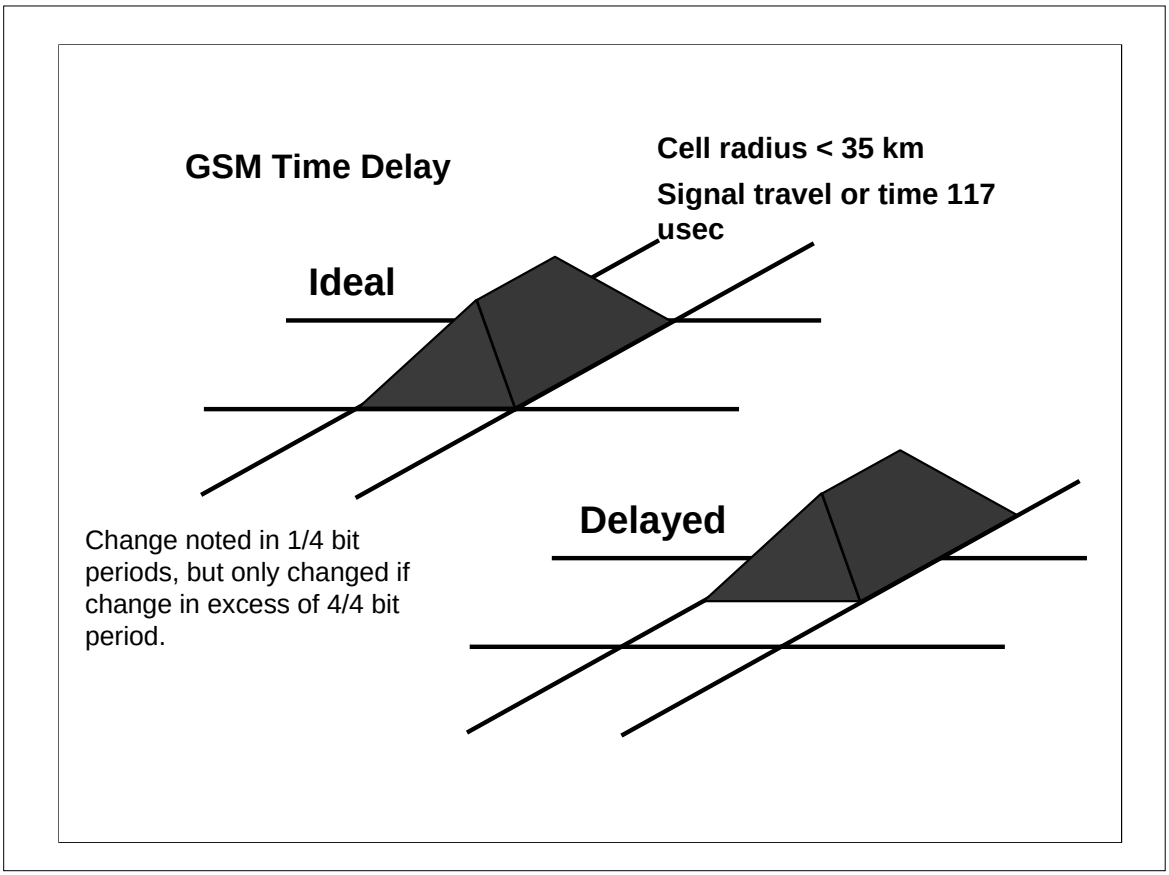


The burst can be divided into three distinct areas:

- Ramp Up
- Useful Part of the Burst
- Ramp Down

All of these levels are controlled by the GSM standard.

The Useful Part of the Burst is the area where the modulated data is present. There are 148 bits (each bit is represented by a single symbol in 0.3GMSK modulation) which will be examined more closely in a later section.



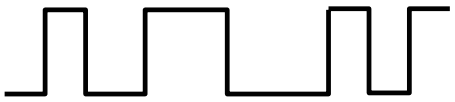
In GSM, because it uses TDMA with cells up to 35 km radius, a radio signal will take a finite period of time to travel from the mobile to the base-station. There must be some way to make sure the signal arrives at the base-station at the correct time.

If the burst arrives at the correct time, it will fit into its physical channel and not disturb any other burst that may follow it in the next timeslot. However, if it is delayed, due to a long distance to travel, it may arrive late and impact the following burst from another user. In this case the mobile is instructed by the BS to burst earlier which will correctly align the burst in the timeslot. The message sent by the BS is called the Timing Advance.

The base station monitors the burst to see when it arrives at the base station. If it arrives late or early, the base station will note how many times it has changed since the last Timing Advance adjustment, and if there have been more than 4 x ¼ bit periods change in one direction, the adjustment will be made again.

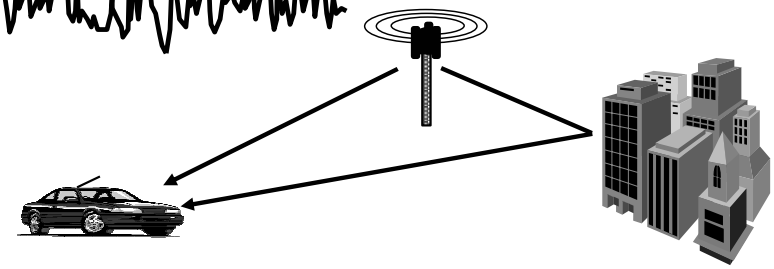
Midamble or Training Bits

- **8 Midamble Patterns (Colour Codes) of 26 bits**
- **Equalizer Estimates Channel Impulse Response From Midamble**
- **Mathematically Construct Inverse Filter**
- **Uses Inverse to Decode Data Bits**



Reference Color Code (Midamble)

Actual Received Signal



The GSM burst may not arrive at the radio without first bouncing off a number of objects. This can cause multipath signals that will add together and distort the signal. Part of the burst data is called the midamble. The midamble (color code) is known by the MS and BS. The mobile, as part of its design, knows what the received signal's midamble should look like. If it does not see what is expected, the equalizer will set an inverse filter to counter the effects of the environment on the transmitted signal.

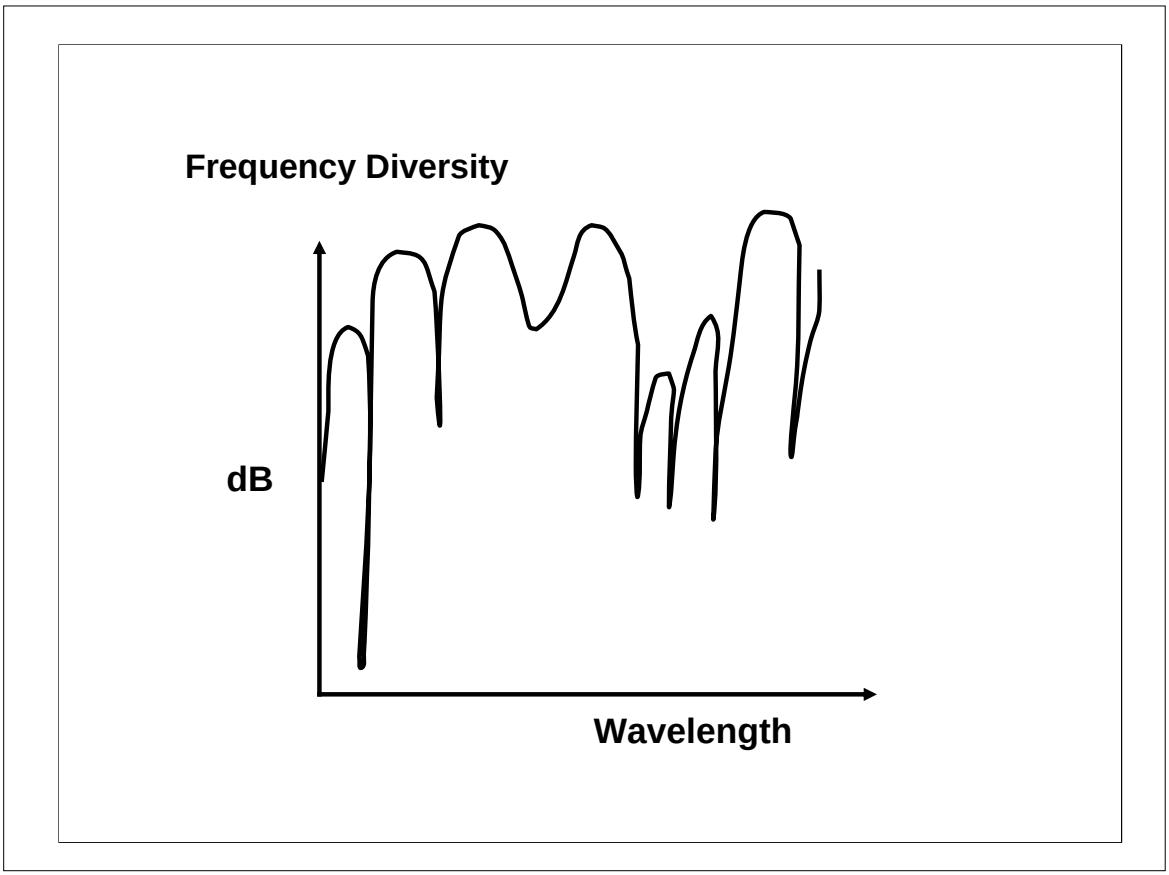
The middle 26 bits of the data in the useful part of the burst are the midamble or a training sequence. For a normal burst this mid-amble will consist of 8 base station color codes and these are numbered 0 through 7. They are 26 bits long.

Midambles are placed in the center of the burst to minimize the time difference from to any bit in the burst. The midamble has a number of different uses; the most important is equalization to improve bit error rate.

The mobile knows the midamble it should be receiving (part of the information the MS gets when assigned to a BS).

This is a pre-defined sequence is 26 bits in the case of a traffic channel. It receives the mid-amble and compares the it to what it should have been. From the difference it can estimate the impulse response of the transmission path at that instant in time. Once it knows the impulse response it can mathematically calculate an inverse filter, it can apply this filter to the data bits on each side of the mid-amble and clean them up, reducing the chance of detecting a bit wrong.

This is referred to as equalization or the equalizer within the radio. Equalizer mechanisms are a closely guarded design feature of most mobiles. It's a key area of competition between mobile manufacturers.

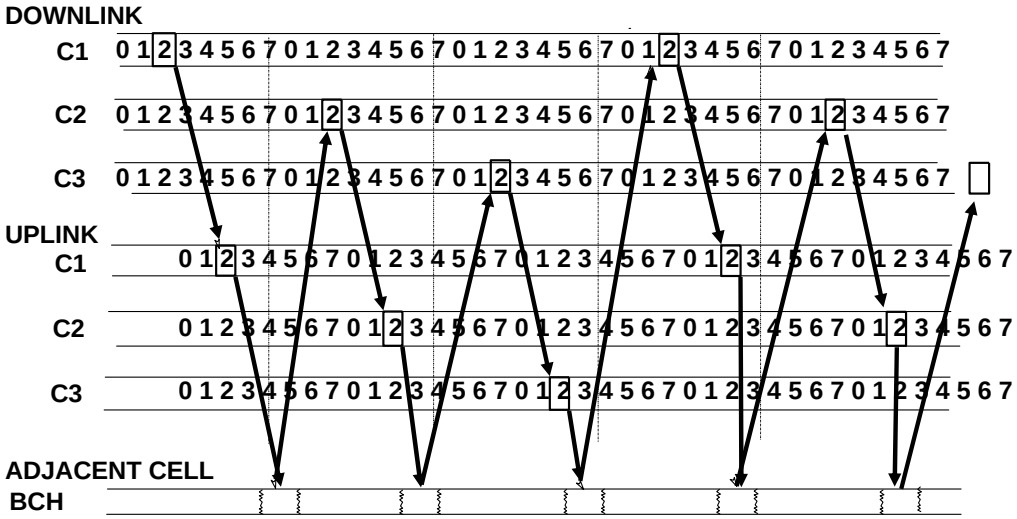


If there is an area that has bad multipath, such as urban areas with lots of reflections from buildings, the cell may have many fades. A fade is where the multipath signals destructively adds and produce a low level signal. The graph above shows these fades as a function of wavelength. If a mobile moves into a fade it can drop a call. There are two ways to avoid this problem:

1. Stop mobile moving into fades
2. Move the fades around so that a mobile may only be in one for a very short and insignificant period of time

Restricting the use of a mobile is impossible, as it would require an exact mapping of the fades in a cell and warning signs around them! The more practical method is to move the fade. Changing the wavelength of the signal does this. By doing this you will see that the above graph would expand and compress along the x-axis and hence the fade would move. This is done by a system called 'frequency hopping.' So the cell would need to be defined as a hopping cell.

Hopping Sequences



All mobiles must have the capability of hopping. However, not all cells will be hopping cells. In this example, there are three frequency pairs to hop among. The mobile still needs to go out and measure the adjacent cells' broadcast channel (BCH). In the first frame, the mobile receives information on channel 1 downlink, then switches to the uplink for channel 1 (45MHz away), transmits it's information, and finally monitors one of the adjacent cells to measure its level. The mobile must move to the downlink for channel 2 and receive information in timeslot 2, switch 45MHz, and transmit on the uplink for channel 2. Then it monitors another cell's broadcast channel and measures its level. This continues through the sequence of frequencies that have been assigned to the cell. The CA (Cell Allocation) and MA (Mobile Allocation) tables define the hopping sequence. The CA table is a master list of all the hop frequencies available in a particular cell. It's sent to the mobile on the BCH and also the downlink SACCH. The MA table is an index into the CA table, and gives a hopping sequence for a particular mobile. The MA table is sent to the mobile as part of the handoff or channels assignment process.

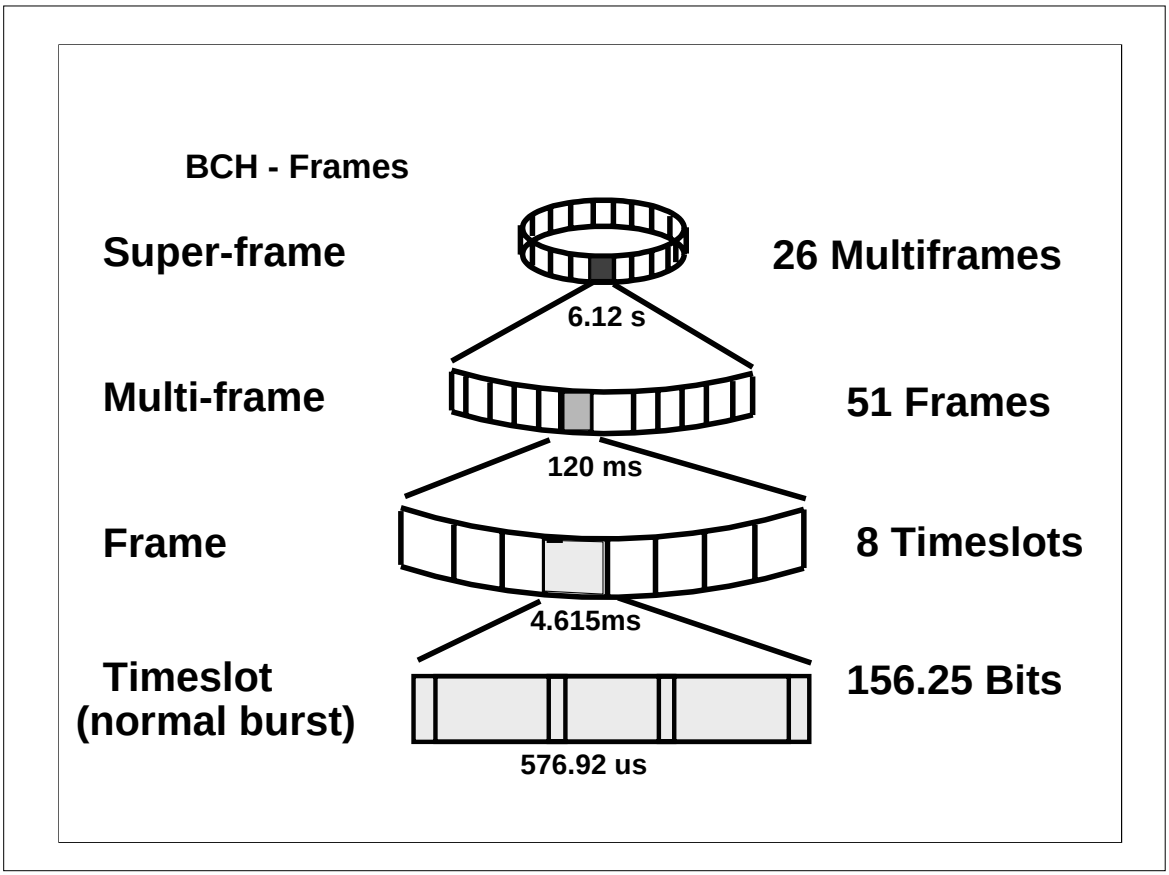
Hopping Sequences

- **Control Channels NEVER hop**
- **Can employ cyclic or pseudo-random hopping sequences**
- **Different mobiles in a cell have different MAIO's (Mobile Allocation Index Offset)**

There are a few things to know about hopping cells. The BCH never hops. As the hopping process is a highly synchronized operation, and the mobiles that are not camped to the system are not synchronized, we would end up with a catch 22 situation. The mobile cannot hop because it is not synchronized, it is not synchronized because it is not camped, it cannot camp because it is not synchronized and it cannot synchronize because it cannot hop!

There are pseudo-random sequences defined in cells, as they tend to better reduce the affects of multipath signals. However, there is still the need for cyclic hopping in a sequence.

If there are 8 users on a channel and the channel is hopping amongst three channel, as in the example, they must not arrive in the same timeslot on the same channel. The timeslot is defined on call set up, however this does not account for two users in the same timeslot on different channels. The mobiles would be given a channel offset (starting point) of 0, 1 or 2 so that they stayed in the correct part of the channel sequence while hopping.



We're going to be introduced to a new term now, frames. In order to understand frames, we must first get a grip on what is happening in the timeslots.

The digital signal is transmitting bits. We will see when we examine the speech path from the mobile to the base station that the bits do not form complete messages. It's a little like sending a shuffled deck of cards through the mail in different envelopes and then sorting them all at the destination. In order to make sure that he sorting can take place, we must synchronize all the timeslots into frames. These are just repeating patterns. Later we will see that the pattern repeats not every 8 slots but after many slots.

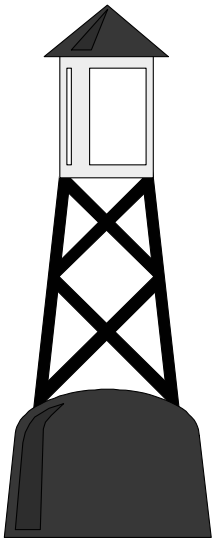
We use frames to make sure that everyone starts in the correct place. Part of the GSM standard defines a frame counter, which every mobile must know before it can accurately transmit and receive.

We will start with the Broadcast Channel and then move on to the Traffic Channel later.

A timeslot is 577 microseconds long and serves a single user, or represent a single Broadcast Channel (of which there is only 1 in a cell). Including guard bits it is 156.25 bits long (remember that time can be represented by bit periods).

As we know 8 timeslots make up all the users on a channel. Together these are known as frames. 51 frames make up a multiframe and 26 multiframes, a superframe. The largest is a hyperframe and is 2048 superframes and lasts exactly 3 hours 28 minutes' 53 seconds 760 milliseconds. This is the master clock of the system and is also what gives GSM such security: A repeating pattern only happens 7 or 8 times every day! The mobile has to synchronize and find its place in the frame in order to operate.

GSM BCH



Broadcast Channel

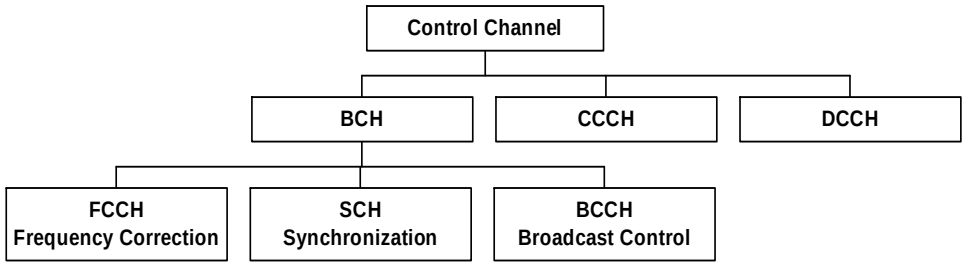
- **One BCH on all the time, in every cell**
- **BCH Information carried in Timeslot 0**
- **Identifies Network Carries, Paging and other Control Information**

The concept of a Broadcast Channel (BCH) is very simple; the BCH acts like a beacon, or lighthouse. It's on all the time and is the first thing the mobile looks for when it's trying to find service. The BCH ARFCN has to be active in all timeslots to allow mobiles synchronized to other cells to measure its power. The useful BCH information is always carried in timeslot 0. The other timeslots are filled with dummy bursts, or are available for TCH.

There are a number of sub-channels on the BCH. A sub channels has a operation to do with establishing the mobile as part of the network. In real terms it is just dividing up the received bit into groups and saying that they have different functions.

This is a little like saying that the deck of cards that we talked of earlier has different uses between the four suits, Spade, club, heart and diamond. Together they are a deck of cards, unless you previously define what the suits mean.

Control Channel Organization



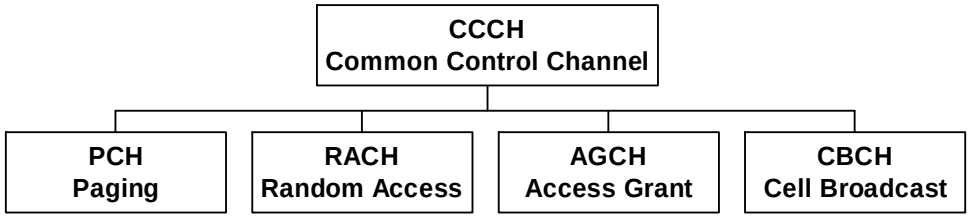
Although we refer to the main control channel as the Broadcast Channel, this is really only one of its uses. There is also a Common Control Channel (CCCH) and a Dedicated Control Channel (DCCH). We will discuss them in detail later.

The Broadcast Channel (BCH) has three sub-channels. The FCCH is like a flag, it allows the mobile know that it has found a GSM BCH. Once it has established this, it will then use the SCH to work out how fast the system clock is 'ticking'. Now that it can get some useful information, it will examine the BCCH to find out which network, or even networks, that it has found. It then uses other information to make a choice of which network to camp on to.

The SCH is sometimes known as the S burst. It is a complete message in itself and does not need multiple messages to be sorted, in order to be used. It appears at regular intervals and from its position, much of the order of the frame can be deduced. Once the position of the burst is known, the mobile knows that it will see a FCCH in the next frame. The midamble is a little longer than a normal burst as the mobile has a harder time trying to find it. The midamble is fixed and never changes, as this would make finding it nearly impossible for the mobile.

The FCCH is a very specially designed burst. Again it is a message in a single timeslot. What the message is, is the ticking of a clock. Remember from Analog and Digital Technology Course that a pattern of all 0's will cause the signal to look like a sine wave. This is the message. A constant frequency sine wave (1625/24 kHz higher than the channel center frequency), with which the mobile can synchronize its internal clock.

Common Control Channel Organization



So now we have synchronized to a network and we know which one, what next?

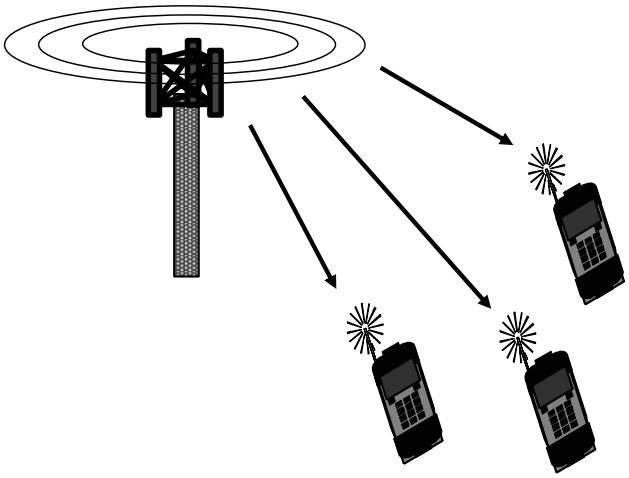
Next we need to be able to make and receive calls. The mobile will monitor the Common Control Channel. This is so called, as all the mobiles will watch the same common place. It is a little like a message board at an airport, everyone looks at the same board but only act if there is a message for them.

The Paging Channel, as its name suggests, is where mobiles are paged to proceed on a call. This is true even if it wants to make a call, as it will send a Random Access Channel and wait to be paged back on the PCH.

Once it has answered a page, it waits for a channel on the Access Grant Channel and then proceeds on the call.

The Cell Broadcast Channel is where Short Messages are sent to an entire cell, not individual users.

SMS Cell Broadcast

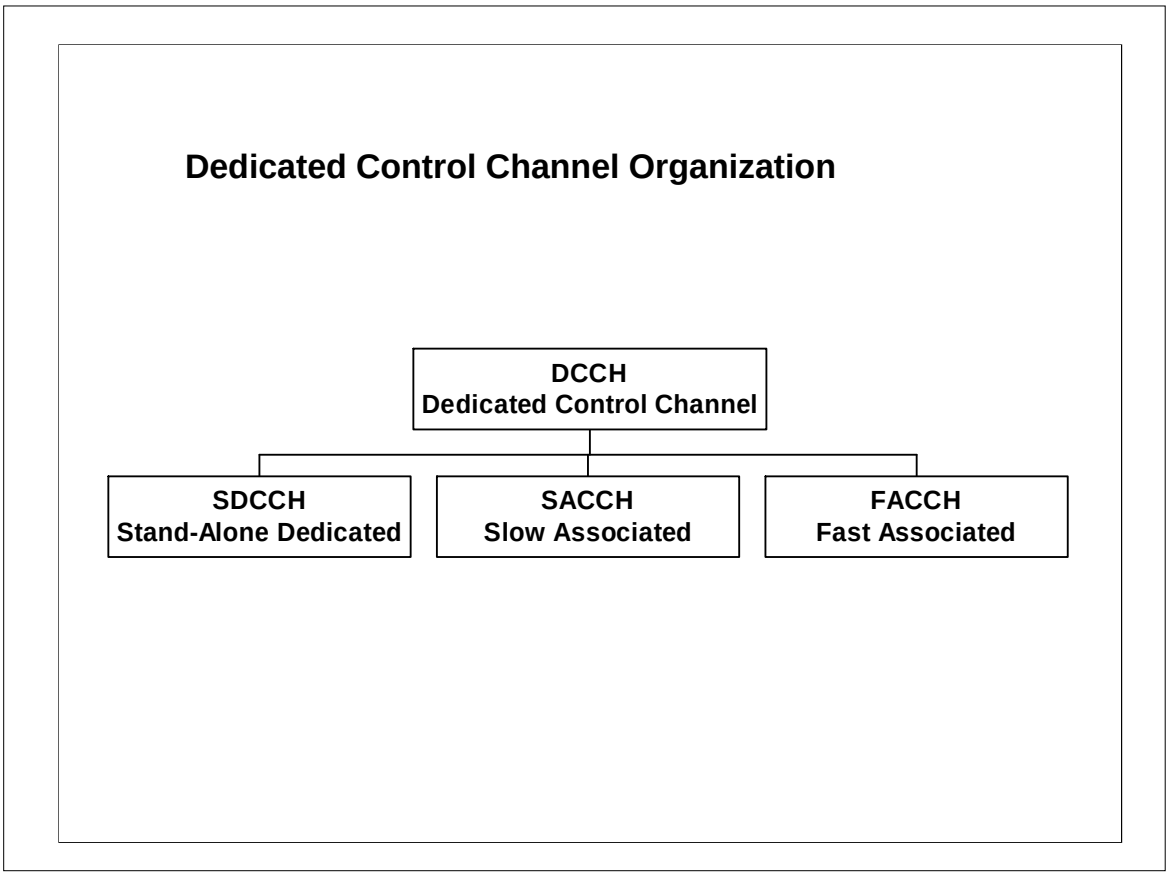


All mobiles in a cell receive the same message from the base station

SMS (Short Message Service) Cell Broadcast is a method by which all user in a cell will receive the same text message on the display of their mobiles. Why would this be useful? Take an example of a tariff that allows cheaper calls in certain dialing code areas. By displaying the codes of that particular cell, the user can decide whether to make the call. A message to say that the cell is undergoing maintenance could also be useful. This message is carried on the CBCH.

Another messaging system that we will mention here is the SMS Point-to-Point message. This is addressed to a single user, rather than a whole cell. It does not work in the same way as the SMS Cell Broadcast, and does not use the CBCH. We mention it here so as to keep all SMS discussions together.

The message is sent from a Service Center in much the same way as a call. If a call is in progress, the message is sent on a FACCH, but otherwise is sent on a Stand Alone Dedicated Control Channel (SDCCH) which we will look at next.



The Dedicated Control Channel (DCCH) is the only part of the Control Channel used during calls and call set up. We mentioned earlier that the mobile does not look at the CCCH during calls, it does however look at the DCCH. Remember that another way of describing a mobile on a call is it is in Dedicated Mode. This may be on the same frequency as the BCH, TCH or another altogether depending on how the system is configured.

The Stand-Alone Dedicated Control Channel (SDCCH) is used during call set up as a stepping stone to the Traffic Channel. It is also used to pass signaling when the mobile is in IDLE mode. This is used for example for SMS Point-to-Point messages as well as Location Updates that we will look at later.

The Slow Associated Channel (SACCH) is used to pass routine system information (power level changes) during a call. It is synchronized to occur at known breaks in the mobile's reception on the traffic channel.

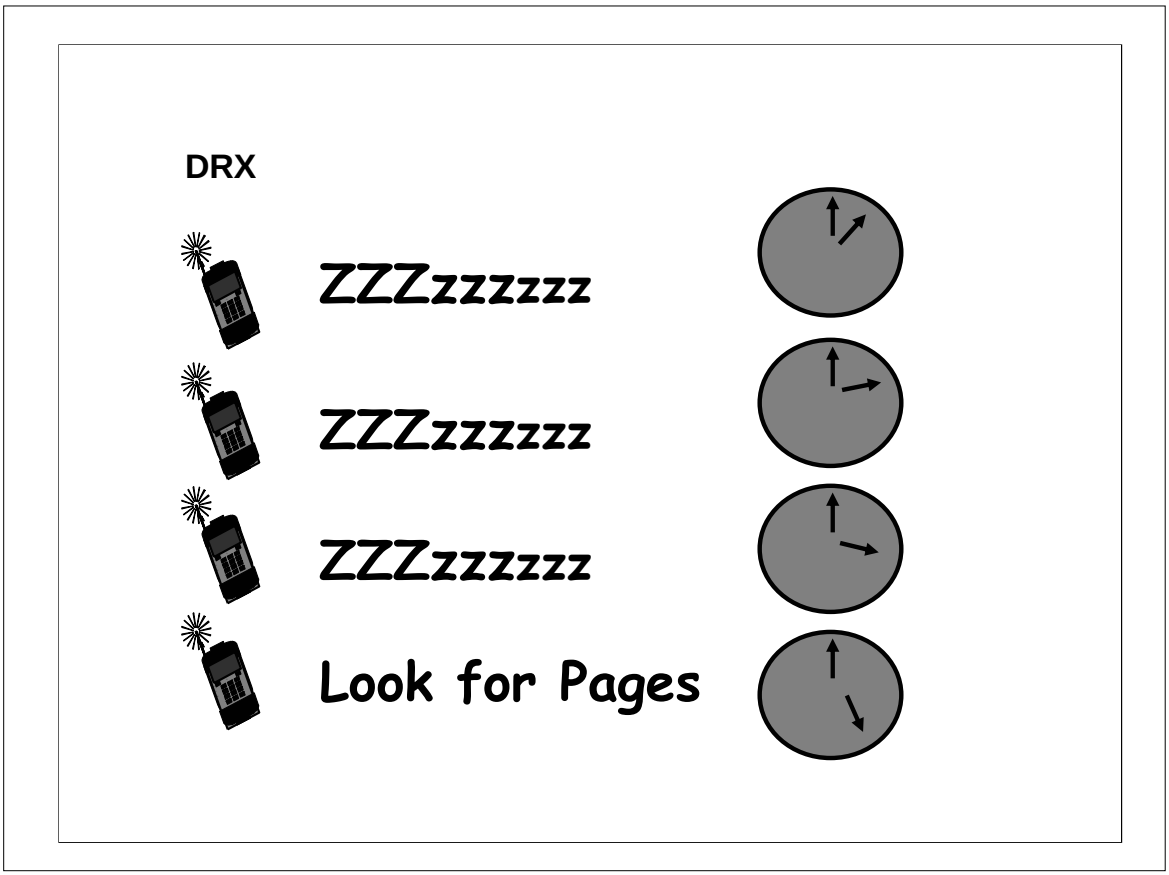
The Fast Associated Control Channel is used to pass critical information to the mobile during a call, by taking over the TCH from the callers. More later.

During the call set-up process, there can be a lot of time between the mobile getting service and the start of conversation. Time is taken up while the phone is ringing and waiting to be answered. During this period, there's a need to exchange control information between the mobile and base station. Alerting messages are sent, and authentication takes place, but there's no need to send speech information.

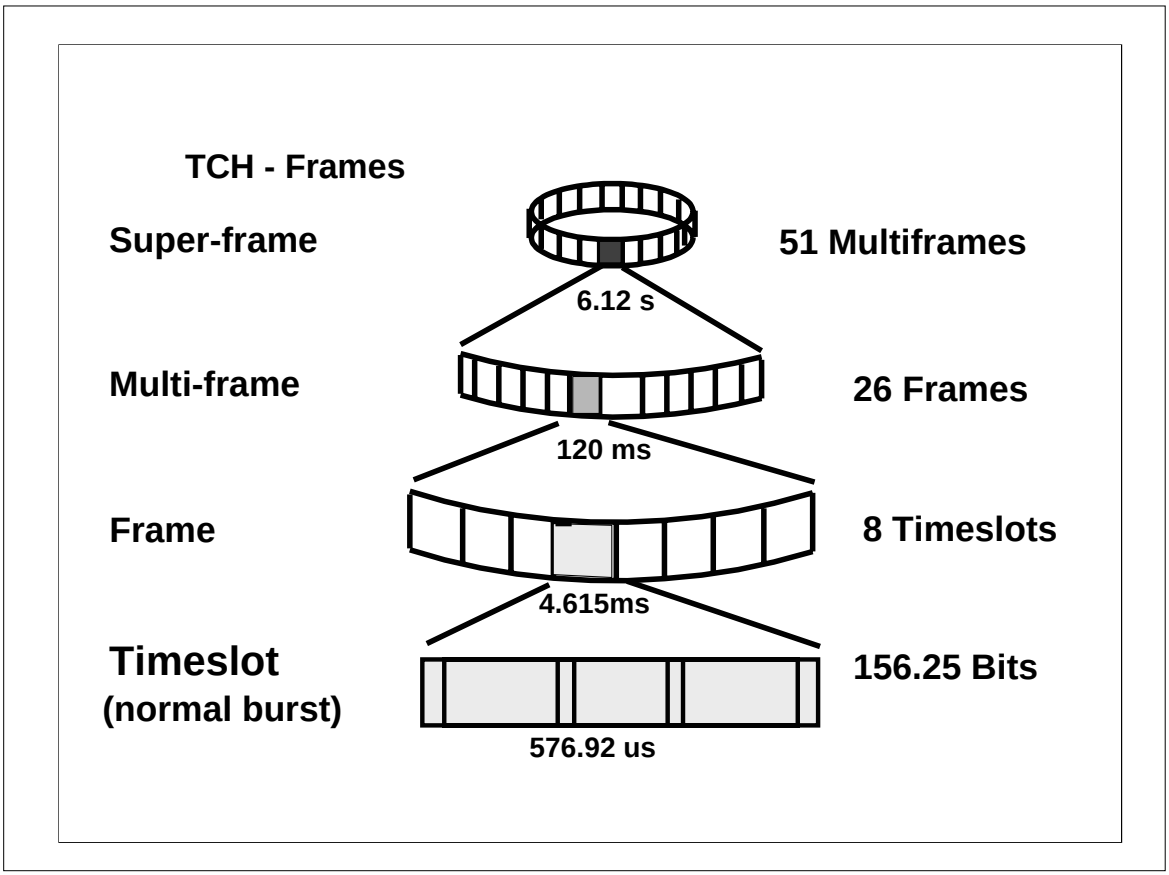
The SDCCH, by using less of the cell resource of physical channels, improves efficiency, and provides a useful holding channel for the mobile until speech or data needs to be exchanged.

When the mobile has become synchronized to the frequency and frame timing of the cell, and looked at the other information on the BCH, it is ready to make and receive calls. Once the mobile is in this state it is 'camped' to the base station.

If the mobile is near the base station, their timing will be closely aligned. If the mobile is on the edge of the cell, maybe 30 km from the base station, the mobile's timing could be 100us in error. This would cause it to overlap another timeslot. When the mobile sends out a RACH, to start a call, to avoid collisions with bursts in adjacent TS, RACH bursts, that are shorter than normal are sent. Until the mobile gets its timing advance information (that we talked about earlier) from the cell it sends short bursts.

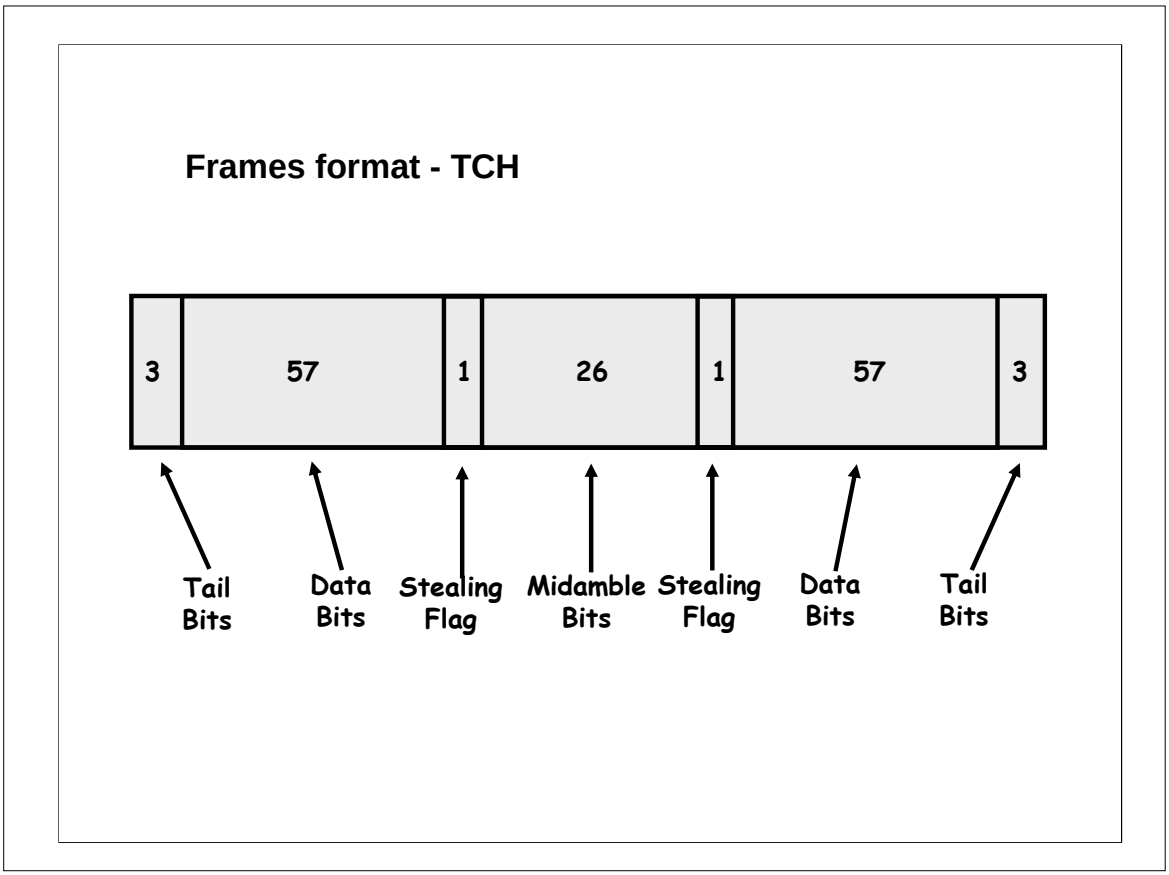


It is worth mentioning at this point that although mobiles all look at the Paging Channel (PCH) in order to find if the base station is calling them, they do not need to look all the time. There is a method called Discontinuous Reception that allows mobiles to turn off their receivers when they know that they will not be paged, and only turn them on when they know they might be paged.



So far we have only talked about what happens when a mobile is looking for a network and wants to camp and set up a call. What happens when it has achieved all this and been granted a Traffic Channel? Lets look at this now.

This diagram may look familiar. It is similar to the BCH frames that we looked at in the previous section. There is one fundamental difference: The multiframe is now 26 frames and the superframe is now 51 frames. This is the opposite of the BCH implementation. It will become clear why this is different as we move on.



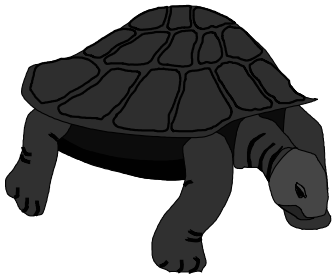
Lets look at the frame format that the TCH uses. This is what is carried on the full sized bursts that we looked at, at the beginning of this lesson.

There are 148 bits of which 147 are 'useful.' Again, we can have half bits if we think of the tail bits as bit periods, rather than data. There are four main areas to the burst:

- The leading and trailing 3 bit blocks are called tail bits and are fixed data.
- The center 26 bits are called the Midamble or Color Code
- The single bits on either side of the midamble are known as Stealing Flags
- The two remaining 57 bit blocks carry the user data.

GSM SACCH

Slow Associated Control Channel



DOWNLINK

- **Mobile Tx Power Commands**
- **Mobile Timing Advance**
- **Cell's Channel Configuration**

UPLINK

- **RXQual report**
- **RXLev report**
- **Adjacent BCH powers**

The Downlink Slow Associated Control Channel (SACCH) is used to send slowly but regularly changing control information to the mobile. Examples are instructing the mobile to change its transmitter power (MS_Tx_Lev) and burst timing advance (to compensate for RF transit time) as it moves around the cell.

The Uplink SACCH carries information about received signal strength (RxLev) and quality (RxQual) of the TCH and the adjacent cell BCH measurement results (also RxLev).

There is another role that the SACCH plays. It is the way that a mobile and base station know if a call is still in progress. When the SACCH is sent, it will start/reset a timer called the Radio_Link_Timeout timer. If the timer value exceeds a set value, the call is deemed dropped.

SACCH

DOWNLINK	*UPLINK*
* Timing	* Adjacent BCH
* Power Ctrl.	* Channel Power
* Call configuration	* Rx Level
* Hopping frequency	* Rx Qual.

Here is a table that summarizes the roles that the Uplink and Downlink SACCH's play in the communication models. Note that the Uplink is usually reports where the downlink is instructions.

GSM FACCH

Fast Associated Control Channel

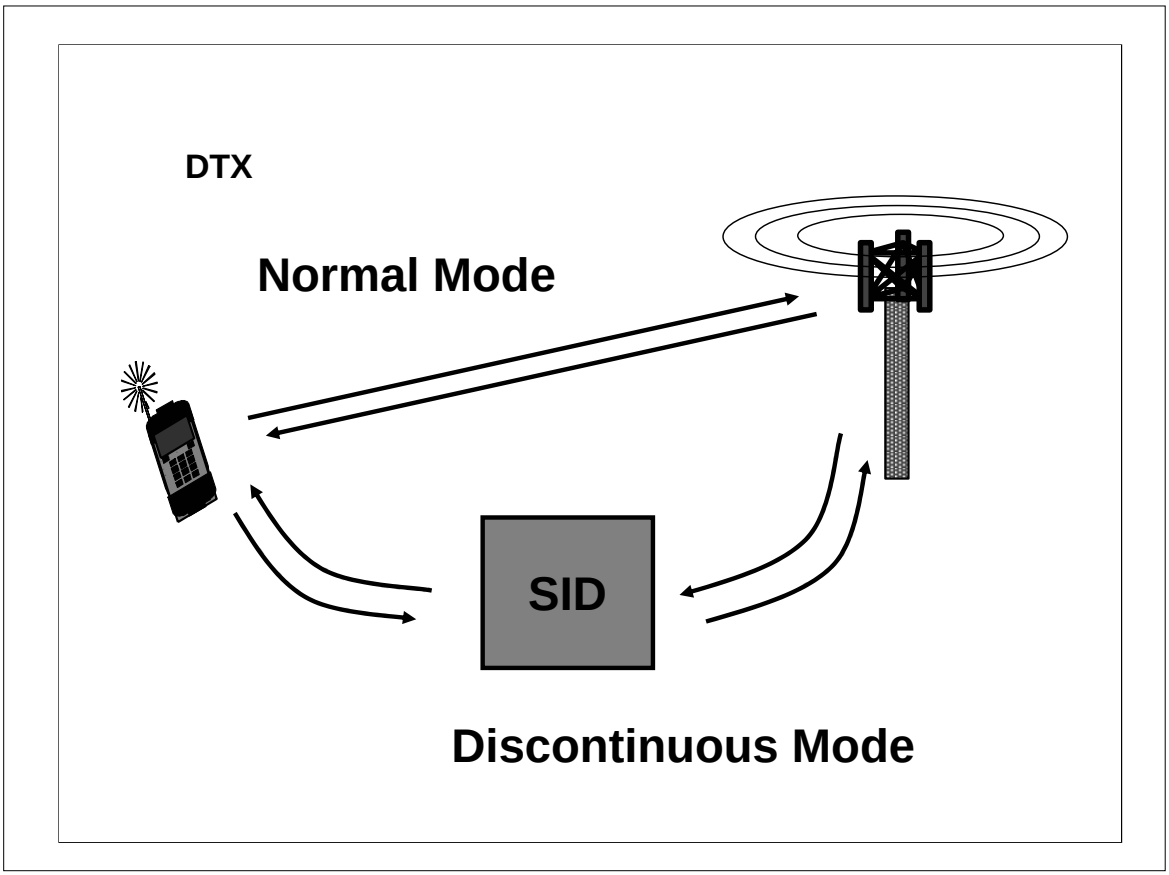
Used by BS and MS to send large amounts of data FAST

Hand-offs

Set Stealing Flags

When the SACCH reports coming back to the base station indicate that another cell would offer the mobile better signal quality, a hand-off may be necessary.

The SACCH doesn't have the bandwidth to transfer all the information associated with a hand-off, such as the new ARFCN and timeslot. For a short period of time, the TCH is replaced by an FACCH. The frame stealing flags (the control bits on either side of the midamble) are set to indicate that the data being sent is an FACCH, not the TCH. When the FACCH steals bursts from the TCH, speech data is lost. It's often possible to hear a small speech dropout when hand-off takes place. The FACCH can also carry the SMS Point-to-Point and Cell Broadcast data.



Earlier we mentioned Discontinuous Reception (DRX). There is also something called Discontinuous Transmission. The only similarity is that they both save the mobile's battery.

The mobile can be empowered by the base station (that usually makes all the decisions) to not transmit all the time. It can notice when a mobile user is listening and only send samples of the background noise to give the other party comfort.

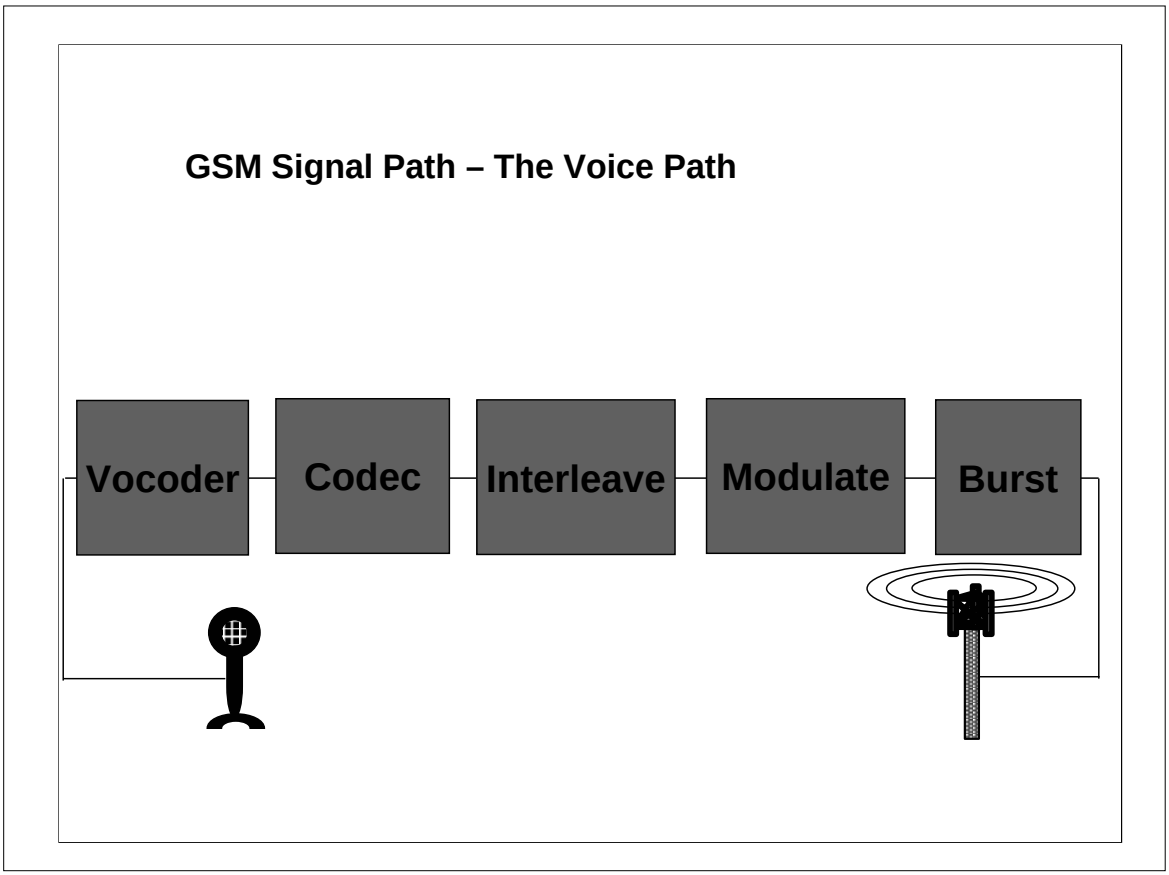
The mobile transmits samples called SID frames. These are Silence Descriptor Frames. These are updated periodically to give the 'lifelike' sound to the caller.

There are two advantages to using DTX:

The power consumption of the mobile drops

The amount of energy put into the spectrum is reduced

The first point is obvious, but the second less so. All radio systems must try to overcome the noise of the environment. This means that the more mobiles that a network has, the more noise. So by adding more users, it gets harder to run the network. If the operator can get the mobile to reduce its power output, it will reduce the background noise and hence the problems for other users.

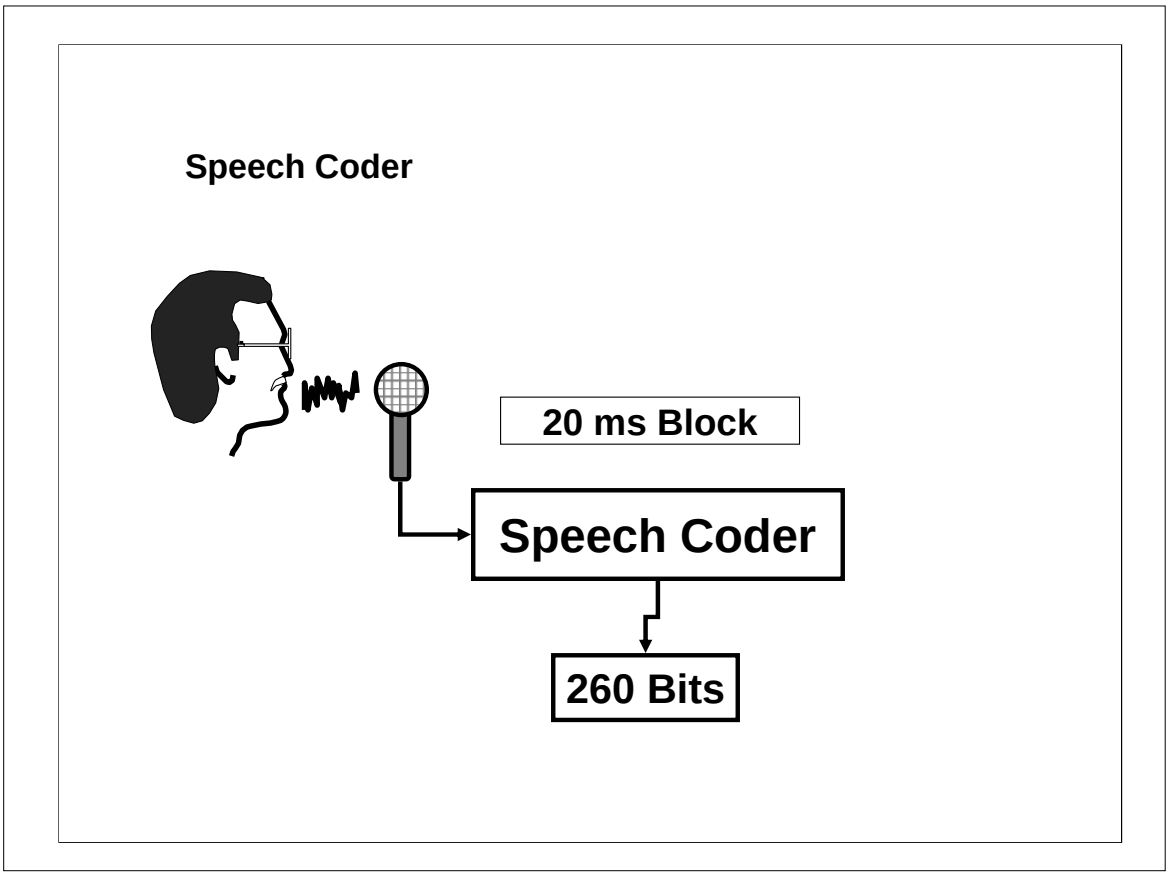


Now that we know how all the information is passed over the air-interface, we need to understand how the mobile and base station take a voice signal and get the data onto the bursts. This is the GSM Signal Path.

A simple view of what needs to be done to take a voice and get it onto a burst, as it were, is in the diagram above.

- There needs to be some way to encode the voice into data
- Next the data must have error protection added to it
- The Data has further error protection
- It is modulated
- It is bursted

Again, this is very simplistic and other steps will be explored during this section.



Most modern digital communications systems use some sort of voice compression. GSM is no exception. It uses a voice coder to model the tone and noise generation in the human throat and the acoustic filtering of the mouth and tongue. These characteristics are used to produce coefficients that are sent via the TCH.

The speech coder is based on a residually excited linear predictive coder (RELP); including a long term predictor (LTP) enhances this.

The voice is sampled into 20ms blocks. As you saw in the previous pages, the data rate is fixed at 13kbits per second. If we want to send the same voice with less bits, we will have to use Half Rate vocoders which will only output half the bits, in other words 6.6 kbits per second.

In Digital the rate is not necessarily related to the quality. This is all tied up in the complex coding algorithms used by the vocoders. We will see this later. At this point let us say that the 20 ms of speech becomes 260 bits of data.

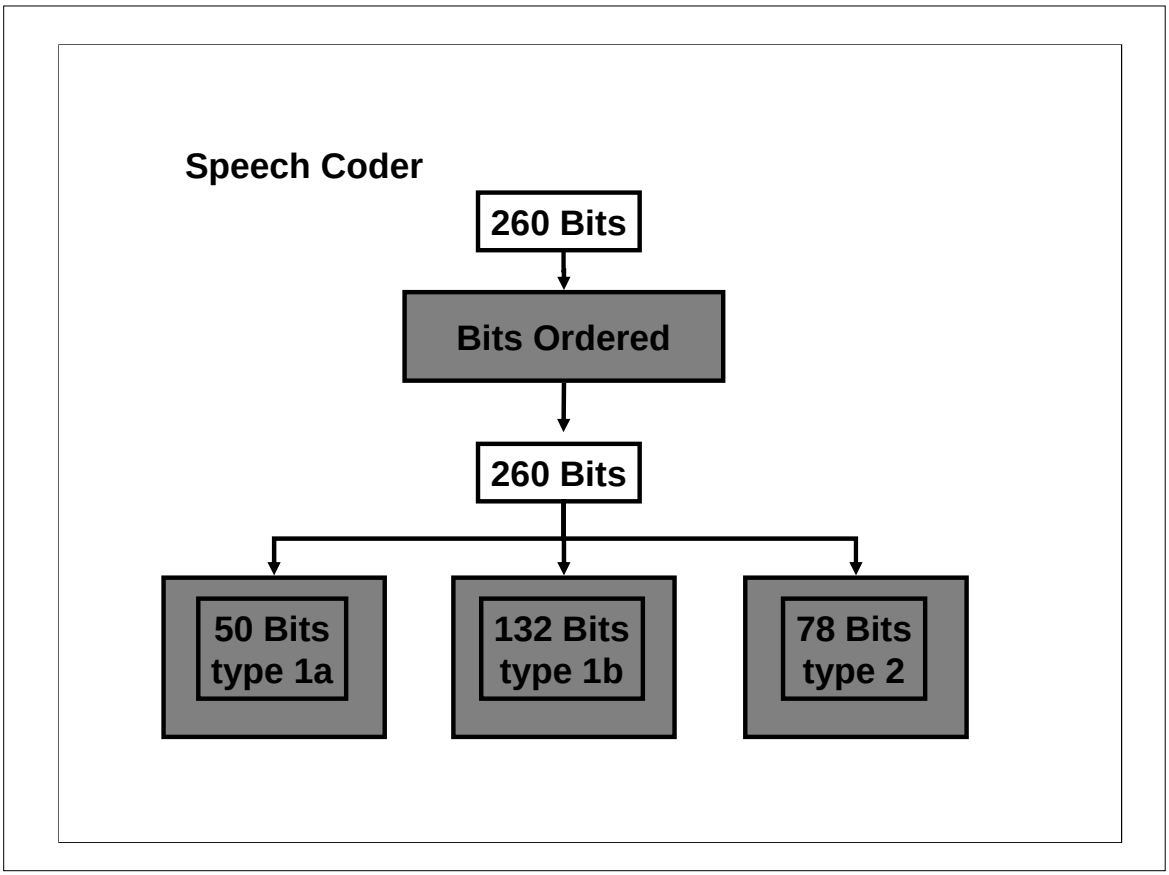
So what is the LTP and LPC used in the vocoder? These are digital filters and inverse filters that combine images of the data with itself to produce a model of the voice. What the effect of this is, is to make some sounds more important than others.

A very simple way to look at this system is:

Sounds that have long repeated components will be coded as shorter ones, as the repetition does not really convey lots of useful data. Short consonant sounds will carry lots of information so will get more merit. The OO sound in smooth, contains less information that the TZ sound in Spritzer.

ADPCM is a version of Pulse Coded Modulation that is used in communications. It allows lots of sampling where it is needed and restricts the sampling when little is needed.

MOS is the Mean Opinion Score. This is a subjective way to rate the quality of sound from a vocoder. The sounds are judged by people and scored 1 to 4. This is the only way to rate a vocoder. We mentioned before that the data rate is not the best guide, and if you are comparing equal data rates, this system is the only way. The system of sound modeling and codebooks are where the real improvements come from.

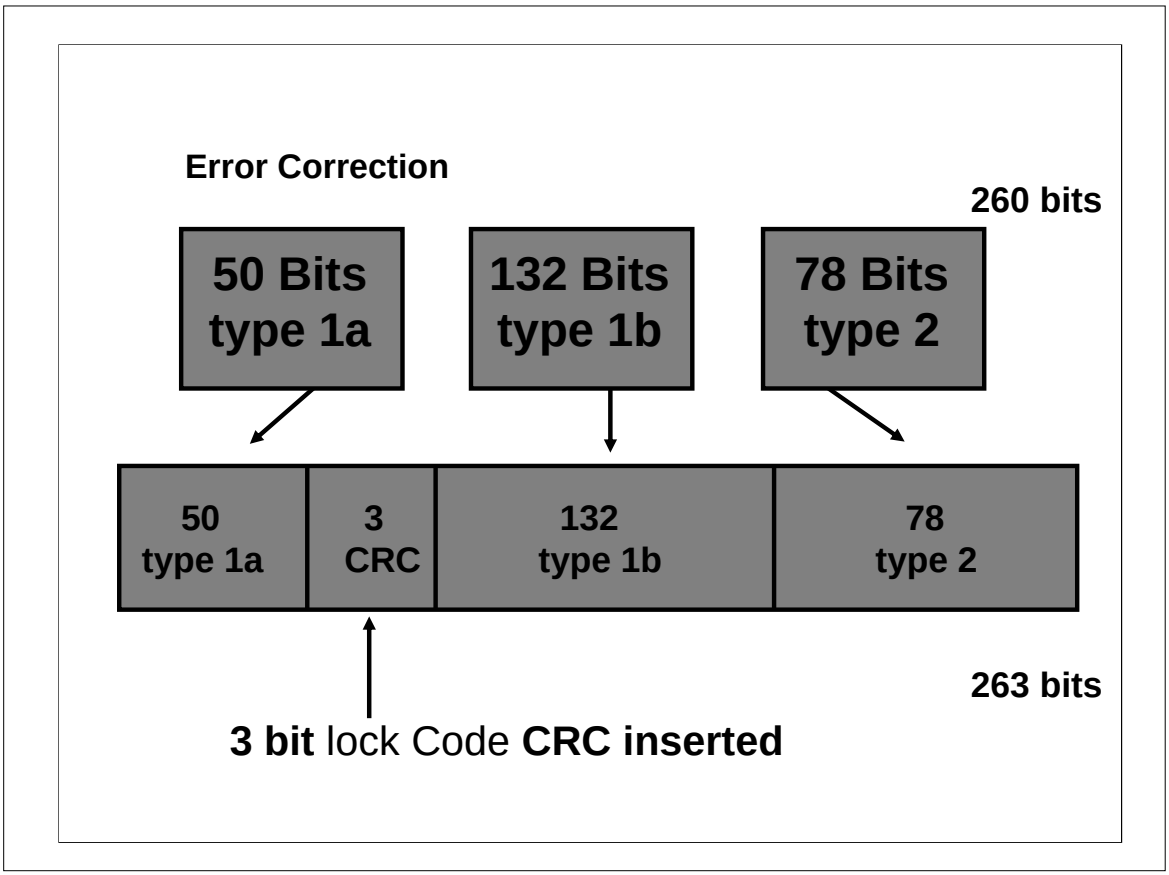


Now that the voice has been modeled, it needs to be protected on its rough journey through the hostile Rf environment. The vocoder will output 260 bits of three types or classes 1a, 1b and 2(II). These are the result of the coding schemes that give rise to important, less important and unimportant bits. The point here is that they will receive different amounts of error protection in the codec.

The least important or type II bits have no error correction or detection. The premier type Ia bits have error detection CRC bits added. Both type Ia and the medium importance type Ib have convolutional error correction bits added.

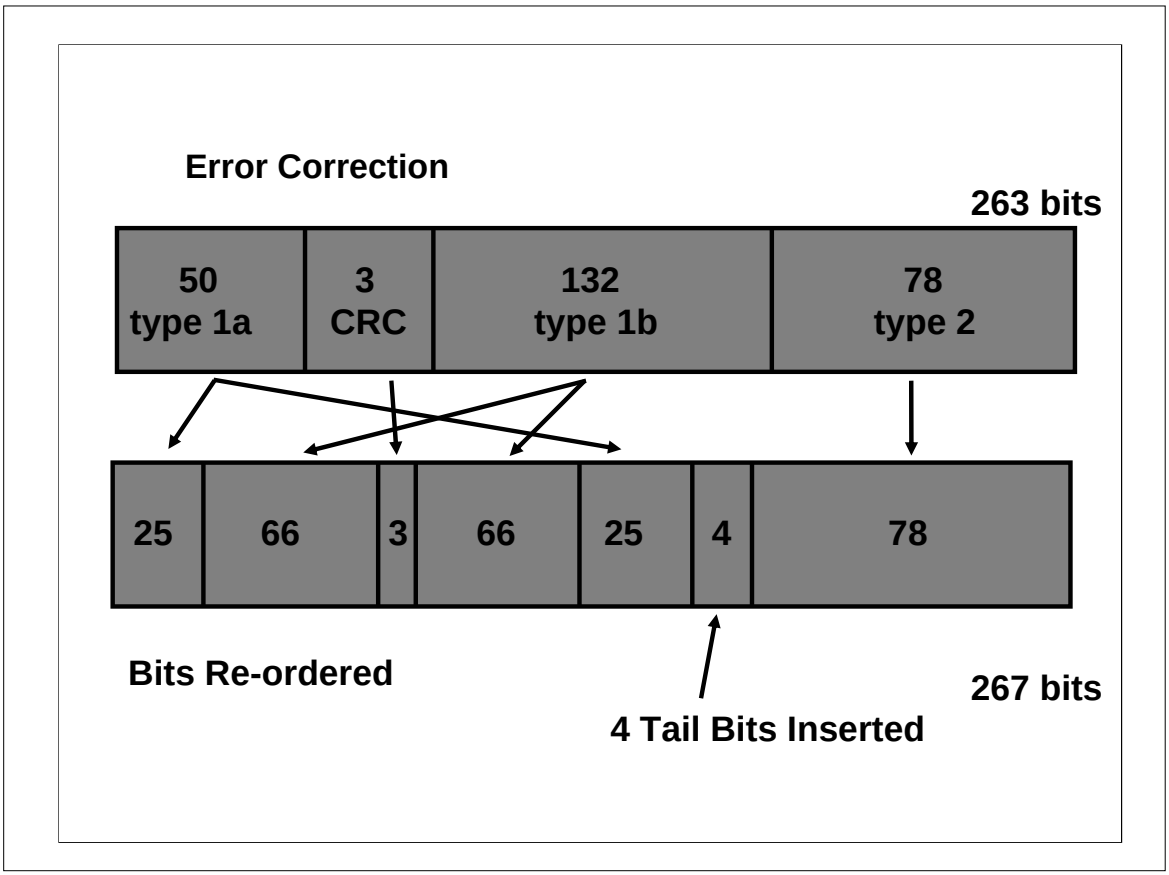
It's sometimes interesting to think of GSM bits as aircraft passengers:

There are three classes, Ia, Ib and II. The most important bits get first-class treatment; they get surrounded by lots of error correction, and in the case of Ia bits, error detection as well. These extra bits take up space in the TCH bursts. The second class, type II bits, take up the least space on the TCH, just like first and second class passengers on an airplane.



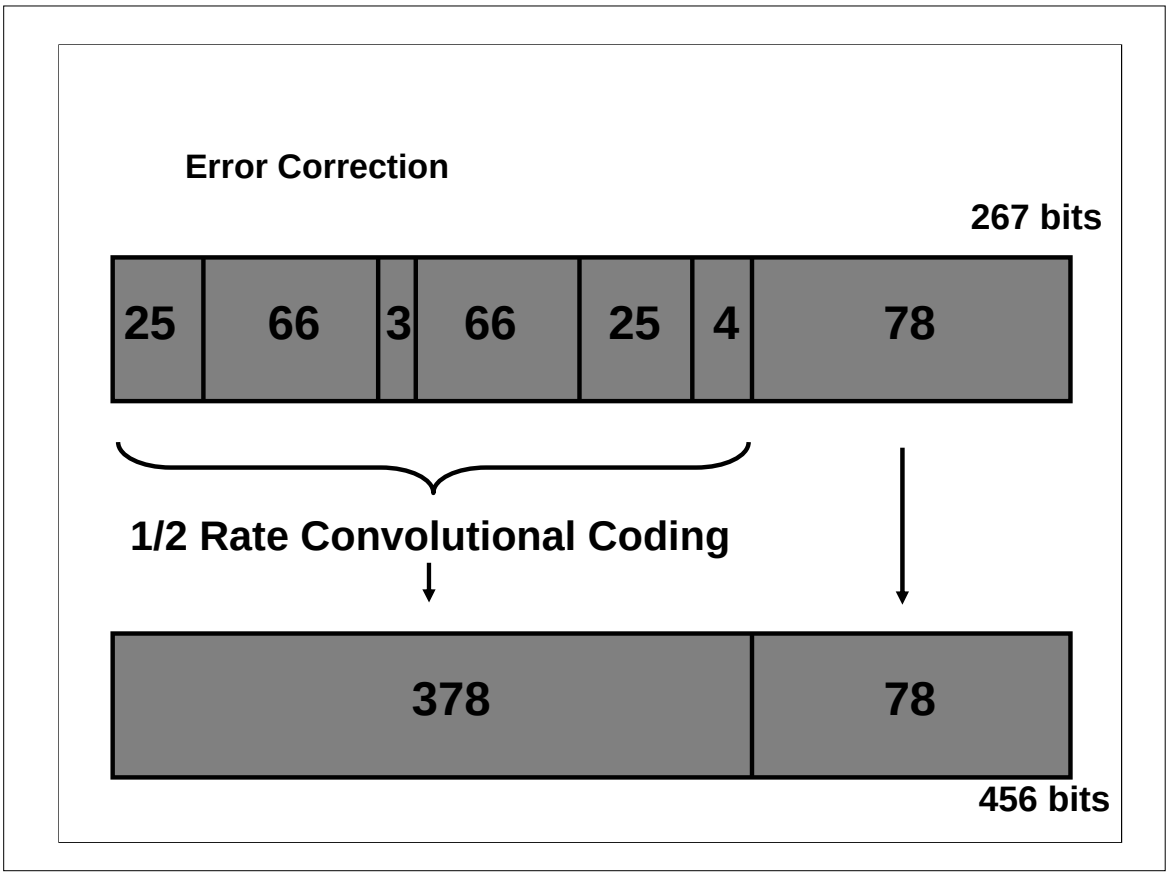
What does this error correction look like? The first step is to add the Cyclic Redundancy Check to the 50 type 1a bits. This is a three-bit parity code or checksum. At this point the 132 1b and 78 type II bits are not changed.

A brief comment about CRC's. The GSM CRC is really only capable of correcting a single error in the TCH frame. In the SCH and RACH there are more parity bits included, which can correct for up to 3 errors in a frame.



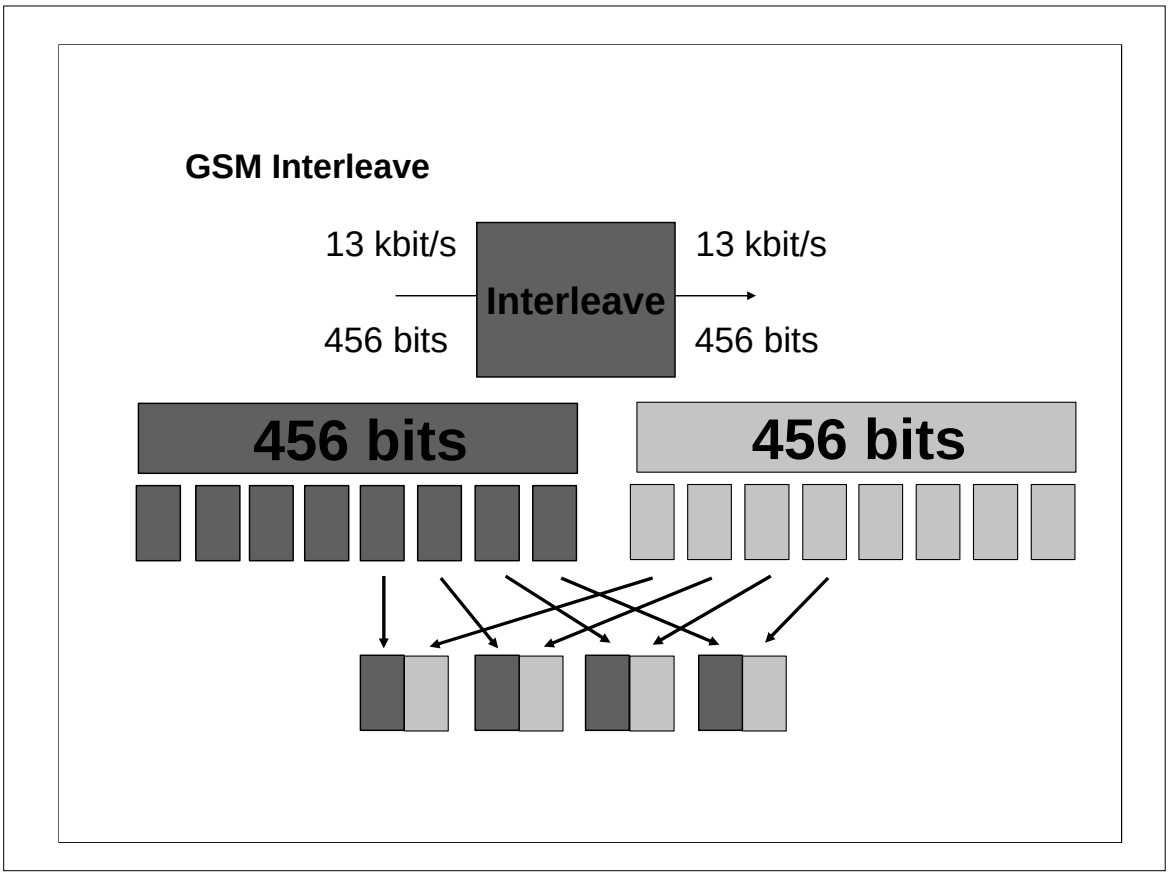
The next step is to ‘shuffle’ the bits around so that they are no longer in sequential order. This means that when they are transmitted, the loss of one section can still be rectified using the error correction schemes (described next) and the fact that not all bits have been lost.

The type 1 bits are also separated from the type II bits by 4 tail bits.

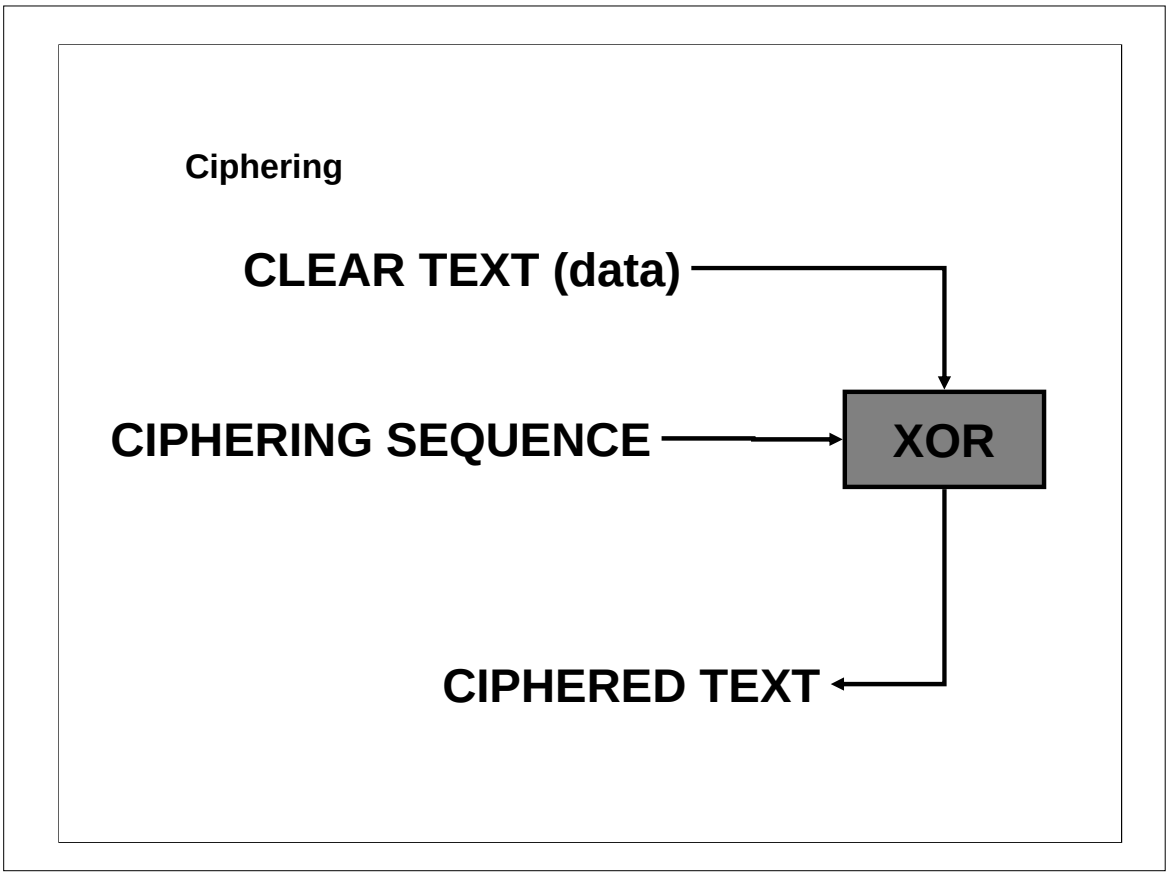


The final error correction step is to add the convolutional coding to the type 1 bits and all the other correction already added. None of this is applied to the type II bits, which have the 'make it if you can' protection applied!

We are left with an output of 456 bits.



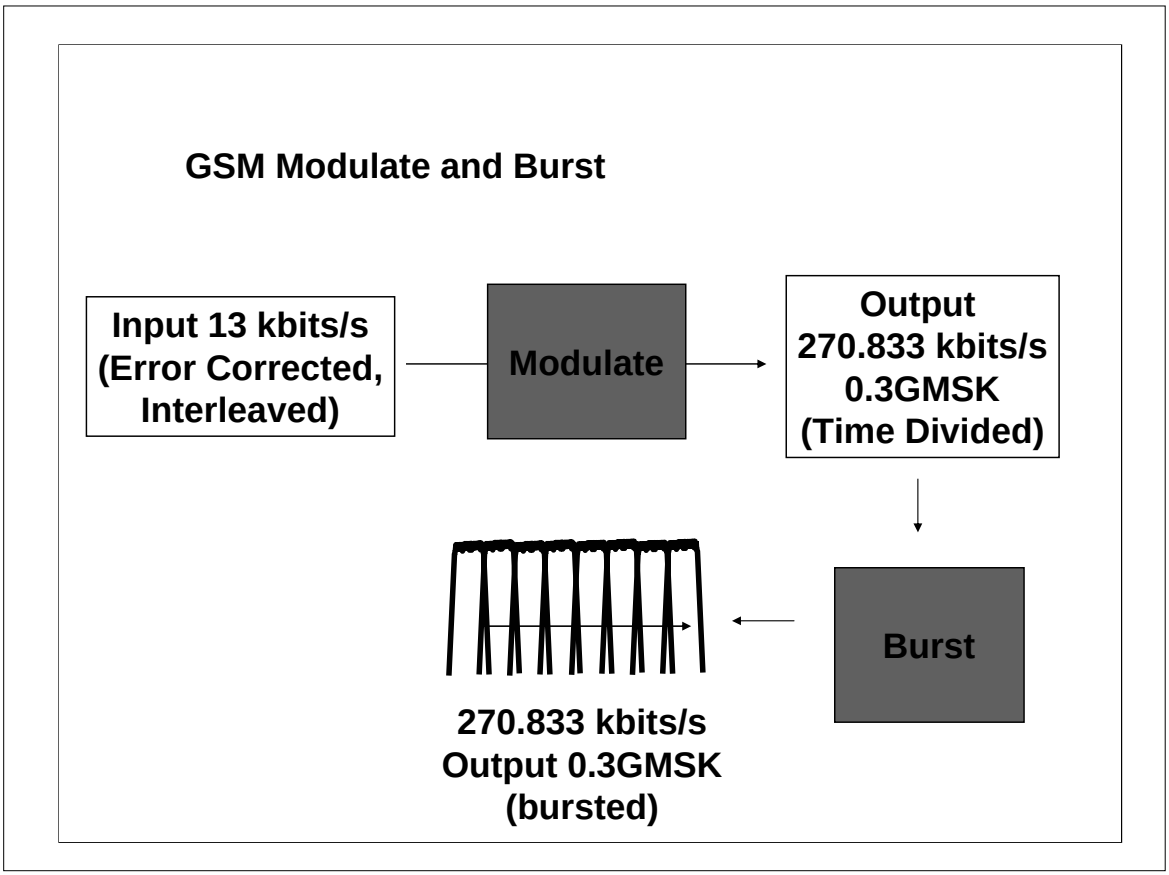
Just as important groups of individuals, like a company board of directors, generally don't travel together (in case the plane crashes and wipes out the whole management team); GSM bits spread themselves over several TCH bursts. If a burst is lost due to interference, enough bits will still get through to allow the error correction algorithms to work, maintaining reasonable speech quality. The 456 bits of speech data are sliced up into 8 blocks of 57. Each TCH frame carries two 57-bit blocks of data from two different 20ms 456-bit speech segments.



There is also a way of further scrambling the data known as ciphering. The cipher is a code that requires an intimate piece of information to be known by both sending and receiving parties. In this case it is the cipher key Ki.

This held in only two places, the SIM card and the Home Location Register.

The coding scheme works by XORing the data with a ciphering sequence derived from the cipher key.



Just before modulation, one more step has to be performed. This is burst building. This is where the data blocks are added to the tail bits, stealing flags and midamble to make up the burst structure that we saw earlier. Some call this channel coding.

Now the signal can be modulated with a 0.3GMSK modulation scheme.

All that remains is to add enough power at the right time to get the signal into the air from the transmission antenna.

Mobile Turn-On

Mobile Searches for Broadcast Channels (BCH)

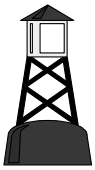
Synchronizes Frequency and Timing

Decodes BCH sub-channels (BCCH)

Checks if Network Allowed by SIM

Location Update

Authentication

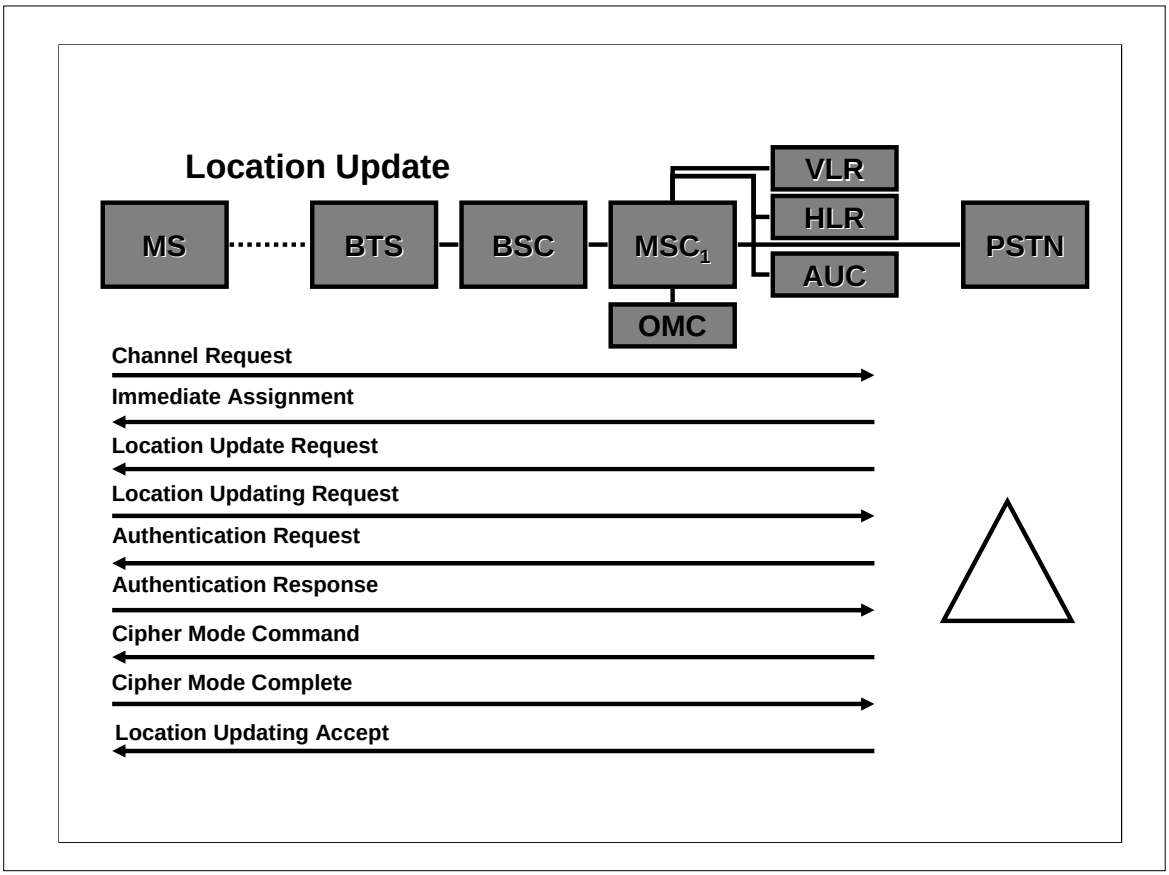


When a mobile first turns on, it searches all 124 channels in the downlink for signals. It will then order the channels by received signal strengths and check to determine if the channel was a BCH (Broadcast CHannel).

Once the MS finds a BCH, it adjusts internal frequency and timing from the FCH and SCH, then checks to determine if the BCH is from its PLMN (Public Land Mobile Network). This involves comparing the allowed network and country codes stored on the SIM card with the information encoded on the BCCH. The mobile repeats this cycle until a good broadcast channel is found.

If the mobile recognizes that it's in a different cell from the last time it was used, it needs to tell the network where it is. The network has to keep track of where every mobile is so that it can route calls to the correct cell for any particular mobile. This process of telling the network "here I am" is called a location update.

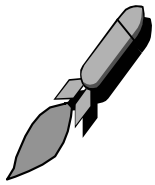
The mobile sends a RACH, gets assigned to an SDCCH, exchanges control information, then ends the call. The user will typically not be aware that this process is taking place.

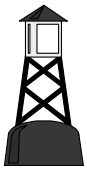


This is a step by step process for Location Updates; this time showing which part of the network is involved in transactions.

The IMSI attach/detach process is a way of forcing all mobiles to inform the network when they have camped and when they have turned off (or just before they turn off!). The SIM stores the last location Area Code (LAC) when it is powered down and it compares this to the camping LAC on Power up and if they are different it will perform an IMSI attach.

Mobile Originated Call



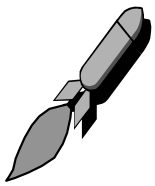


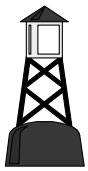
Mobile Sends RACH
Channel Assignment Posted on BCH (AGCH)
Mobile and Base Station communicate on SDCCH
Authentication
Mobile Assigned to Traffic Channel (TCH)
Speech Data sent and received

Once camped, the mobile is ready to send or receive calls.

When a user dials a number, and presses the send button on the mobile, call origination takes place. The mobile transmits a short RACH burst on the uplink, using the same ARFCN as the BCH is using on the downlink. The base station responds to the RACH by posting an AGCH (Access Grant CHannel) on the CCCH. These are logical channels on the BCH physical channel. The mobile listens on the BCH for the AGCH, when it receives it and decodes the instructions, it re-tunes to another ARFCN and/or timeslot and begins a two-way dialogue with the base station on an SDCCH. One of the first things that the mobile will receive is the SACCH associated with the SDCCH. Once it receives the SACCH, it will get timing advance and transmitter power information from the base station. The base station will have calculated the correct timing advance from the arrival time of the RACH. Once the mobile gets timing advance information, it can send normal length bursts. The SDCCH is used to send messages back and forth, taking care of alerting (making the mobile ring) and authentication (verifying that this mobile is allowed to use the network). After a short period of time (1 to 2 seconds), the mobile is commanded over the SDCCH to re-tune to a TCH. Once on the TCH, speech data is transferred on the uplink and downlink.

Mobile Terminated Call





Mobile Sees Page

Mobile Sends RACH

Channel Assignment Posted on BCH (AGCH)

Mobile and Base Station communicate on SDCCH

Authentication

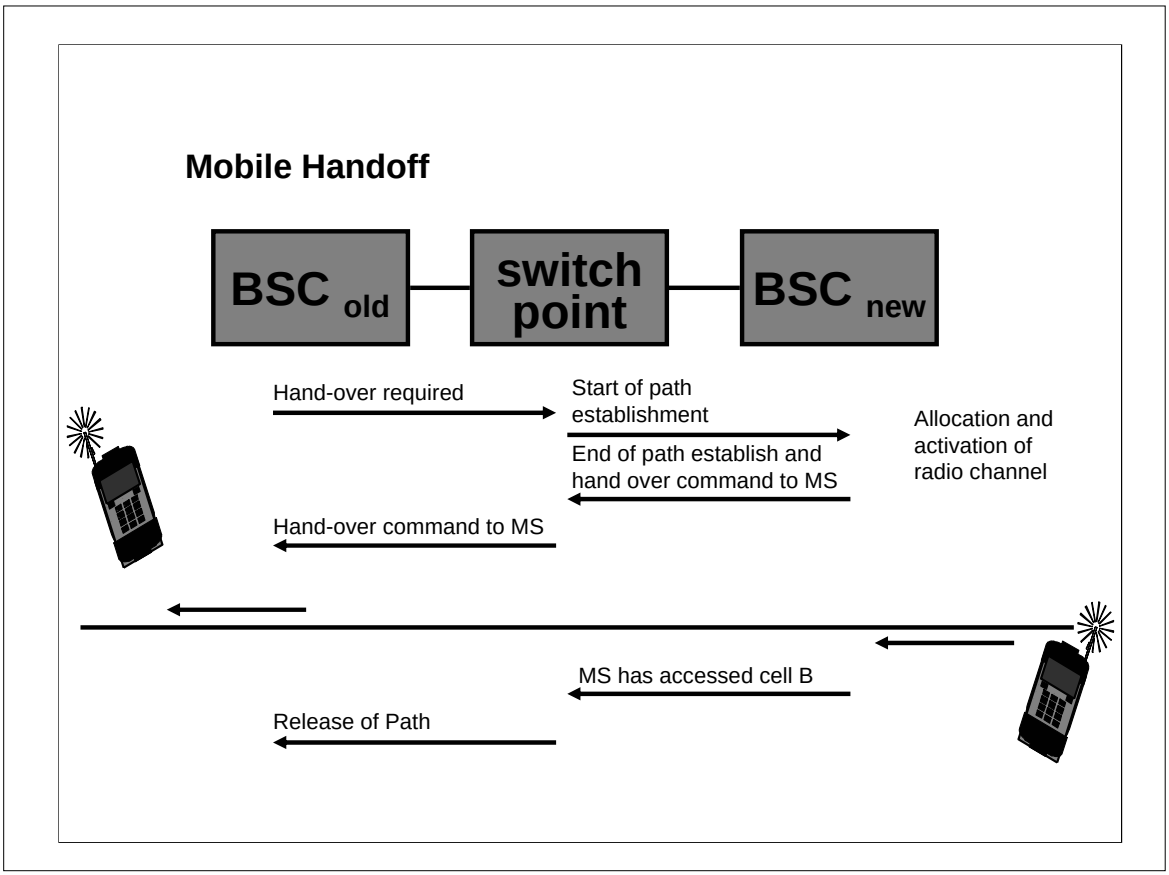
Mobile Assigned to Traffic Channel (TCH)

Speech Data sent and received

The process for base station originated calls is very similar. The base-station posts a PCH (paging CHannel) on the CCCH part of the BCH. When the mobile receives the PCH, it responds by sending a RACH. The remainder of the process is identical to the mobile originated case.

If you can find a way to translate the GSM bursts into audio tones (AM demodulate), it's interesting to hear the difference between the channel types as a call is set up. A good way to do this is to use a GSM phone near an old TV set or a conventional wired phone. The interference created in these devices amounts to AM demodulation.

The RACH burst can be heard as a single 'Tick' sound. It's quickly followed by the SDCCH 'Tat, Tat-tat-tat, tat-tat-tat ...'. After a few seconds, the TCH is connected 'Buzzzzzzzzz'



We have covered mobile power on and call establishment, but there is one other important area. During a call the mobile may have to change base stations. If the call is between faces of the same base station, this is performed locally. The case shown here is that where the base station is not the same.

The mobile reports its measurements and the serving BSC determines that it is time to perform a handoff. It will contact the new base station and get the information on the new channel and timeslot (along with midamble and timing information) and send this to the mobile. It then commends the mobile to switch base stations and then once the new call is established, close down the old link and reallocate it to another user if necessary.

Summary

GSM is a second generation cellular format

It is the most prevalent cellular system in the world.

It is a TDMA system

That brings us close to the end of this module. We have seen a brief history of GSM evolution. GSM is a TDMA system where RF channels are divided into time-slots for more capacity. We have also seen the various kinds of channels, the type of voice coding and data protection in the system.

GSM is the most popular cellular technology in the world today. It offers data, messaging and voice services.

RF & Microwave e-Academy Program

Powerful tools that keep you on top of your game

End of Module.
Thank you for attending.

Questions? Need assistance? Learn in greater detail?

Please email us at tm_ap@agilent.com if you have further questions. If you'd like to know more about our education courses, please visit www.agilent.com/find/training

And please check back at the Agilent eAcademy for updates and new modules.

Agilent Technologies

Printed on Jan, 2004 5988-8498ENA

This brings us to the conclusion of this module on GSM basics. Thank you for your time and interest. We hope that it was useful.

For more information, please send us an email to the address listed above. If you'd like to learn about GSM, GSM test or other Agilent products in more detail, please have a look at our training curriculum at the URL above. These are charged training conducted by our experts and give you the opportunity to learn in greater detail, as well as hands-on experience with the instruments.

Finally, please do visit us again at the eAcademy. You will may find new modules, materials, and may be even a special offer!