Module – 2 (Wireless Transmission and Communication Systems)

Spread spectrum – Direct sequence, Frequency hopping. Medium Access Control – Space Division Multiple Access (SDMA), Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA). Satellite Systems – Basics, Applications, Geostationary Earth Orbit (GEO), Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Routing, Localization, Handover. Telecommunication Systems - Global System for Mobile Communication (GSM) services, Architecture, Handover, Security.

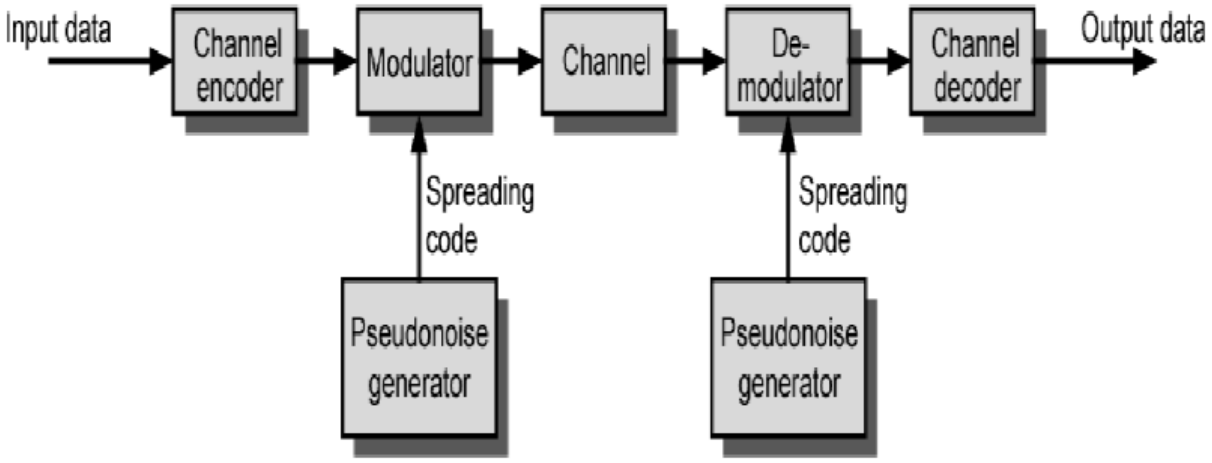
Spread spectrum

In the spread spectrum technique, **the frequency of the signal to be transmitted is varied by injecting pseudo-random noises into it**. This injection increases the bandwidth of signal transmission, and thereby reduces the effects of interference, noise, and signal fading.

Spread Spectrum refers to a system originally developed for military applications, to provide secure communications by spreading the signal over a large frequency band.

The increasing demand for wireless communications has problems due to limited spectrum efficiency and multipath propagation. The use of spread spectrum communication has simplified these problems. In the spread spectrum, signals from different sources are combined to fit into **larger bandwidth**. **spread spectrum** techniques involve spreading the bandwidth needed to transmit data – which does not make sense at first sight. Spreading the bandwidth has several advantages. The main advantage is the resistance to **narrowband interference**.

Spread Spectrum Spread spectrum is an important form of encoding for wireless communications. The use of spread spectrum makes jamming and interception more difficult and provides improved reception. The basic idea of spread spectrum is to modulate the signal so as to increase significantly the bandwidth (spread the spectrum) of the signal to be transmitted. Input is fed into a channel encoder that produces an analog signal with a relatively narrow bandwidth around some center frequency. This signal is further modulated using a sequence of digits known as a spreading code or spreading sequence. Typically, but not always, the spreading code is generated by a pseudo noise, or pseudorandom number, generator. The effect of this modulation is to increase significantly the bandwidth (spread the spectrum) of the signal to be transmitted. On the receiving end, the same digit sequence is used to demodulate the spread spectrum signal. Finally, the signal is fed into a channel decoder to recover the data



Spread spectrum is designed to be used in wireless applications (LANs and WANs). In wireless applications, all stations use air (or a vacuum) as the medium for communication. Stations must be able to share this medium without interception by an eavesdropper and without being subject to jamming from a malicious intruder. To achieve these goals, spread spectrum techniques add redundancy; they spread the original spectrum needed for each station. If the required bandwidth for each station is B, spread spectrum expands it to Bss, such that Bss >> B. The expanded bandwidth allows the source to wrap its message in a protective envelope for a more secure transmission.

There are two techniques to spread the bandwidth: frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS).

DIRECT SEQUENCE SPREAD SPECTRUM

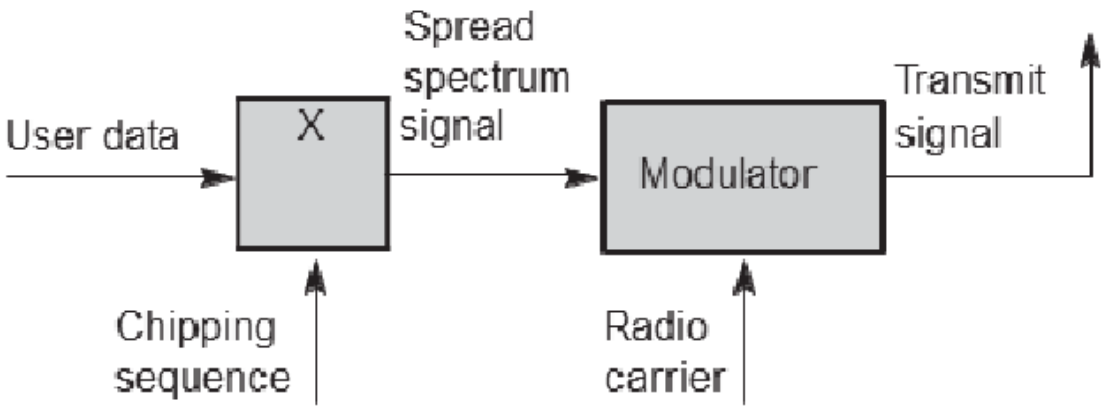
Direct sequence spread spectrum (DSSS) is **a transmission technology used in local area wireless network transmissions**. In this technology, a data signal at the sending station is combined with a high data rate bit sequence, which divides user data based on a spreading ratio.

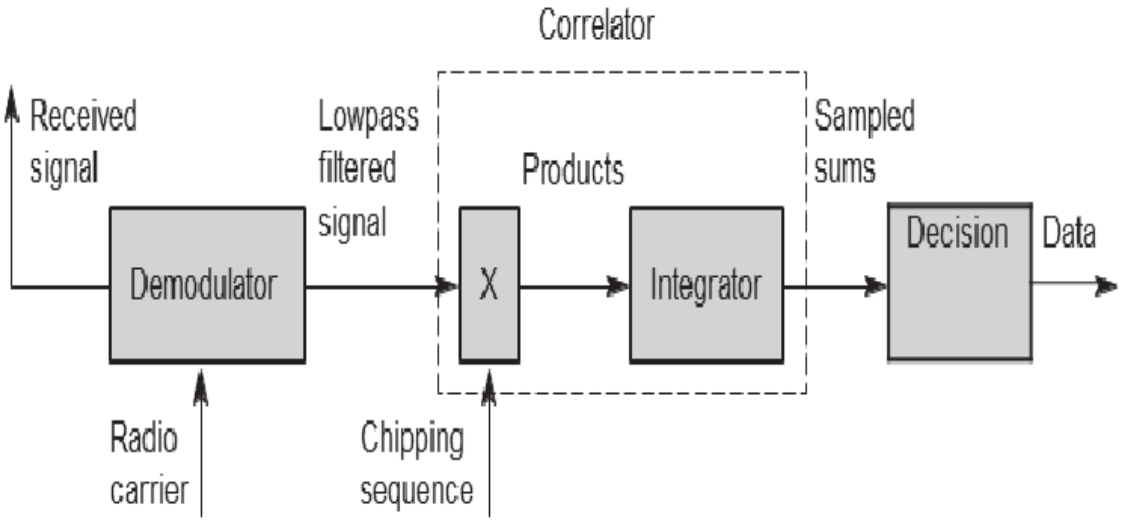
With direct sequence spread spectrum (DSSS), each bit in the original signal is represented by multiple bits in the transmitted signal, using a spreading code. The spreading code spreads the signal across a wider frequency band in direct proportion to the number of bits used.

Therefore, a 10-bit spreading code spreads the signal across a frequency band that is 10 times greater than a 1-bit spreading code. One technique with direct sequence spread spectrum is to combine the digital information stream with the spreading code bit stream using an exclusive OR (XOR)

An information bit of one inverts the spreading code bits in the combination, while information bit of zero causes the spreading code bits to be transmitted without inversion. The combination bit stream has the data rate of the original spreading code sequence, so it has a wider bandwidth than the information stream.

However, transmitters and receivers using DSSS need additional components as shown in the simplified block diagrams in the following figure 2 and 3 The first step in a DSSS transmitter, Figure 2 is the spreading of the user data with the chipping sequence (**digital modulation**). Assuming for example a user signal with a bandwidth of 1 MHz. Spreading with the above 11-chip Barker code would result in a signal with 11 MHz bandwidth. The radio carrier then shifts this signal to the carrier frequency (e.g., 2.4 GHz in the ISM band). This signal is then transmitted.





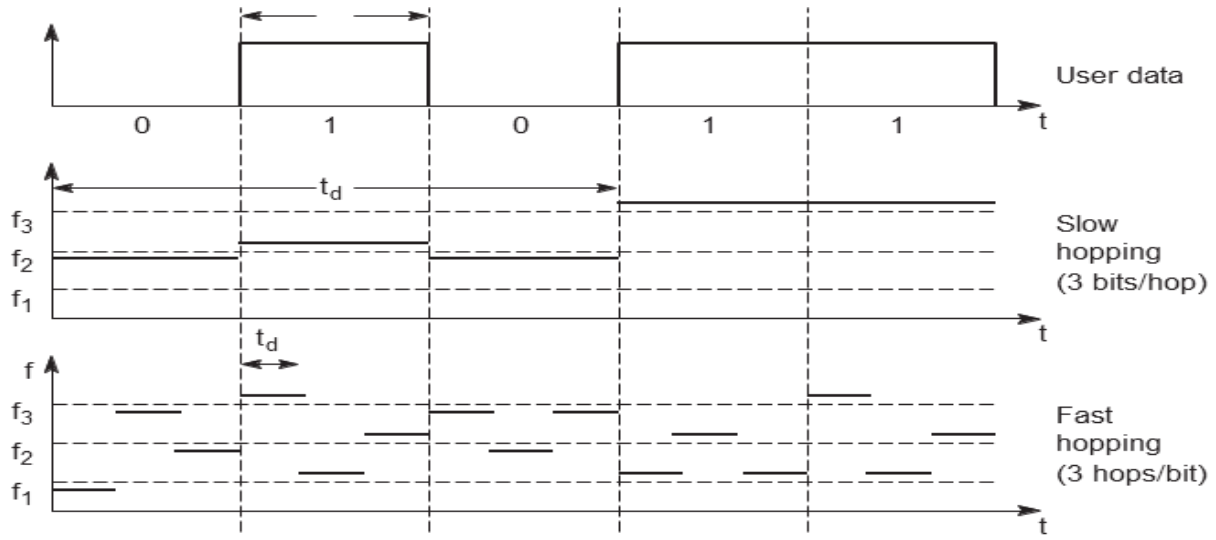
The DSSS receiver is more complex than the transmitter. The receiver only has to perform the inverse functions of the two transmitter modulation steps. The first step in the receiver involves demodulating the received signal. This is achieved using the same carrier as the transmitter reversing the modulation and results in a signal with approximately the same bandwidth as the original spread spectrum signal. The receiver has to know the original chipping sequence, i.e., the receiver basically generates the same pseudo random sequence as the transmitter. During a bit period, which also has to be derived via synchronization, an **integrator** adds all these products. Calculating the products of chips and signal, and adding the products in an integrator is also called correlation, the device a **correlator**. Finally, in each bit period a **decision unit** samples the sums generated by the integrator and decides if this sum represents a binary 1 or a 0.

If transmitter and receiver are perfectly synchronized and the signal is not too distorted by noise or multi-path propagation, DSSS works perfectly well according to the simple scheme shown

Frequency hopping spread spectrum

For **frequency hopping spread spectrum (FHSS)** systems, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels. Transmitter and receiver stay on one of these channels for a certain time and then hop to another channel. This system implements FDM and TDM. The pattern of channel usage

is called the **hopping sequence**, the time spend on a channel with a certain frequency is called the **dwell time**. FHSS comes in two variants, slow and fast hopping



In **slow hopping**, the transmitter uses one frequency for several bit periods.3 Above figure shows five user bits with a bit period tb. Performing slow hopping, the transmitter uses the frequency f2 for transmitting the first three bits during the dwell time td. Then, the transmitter hops to the next frequency f3. Slow hopping systems are typically cheaper and have relaxed tolerances. Slow frequency hopping is an option for GSM

For **fast hopping** systems, the transmitter changes the frequency several times during the transmission of a single bit. In the example of above figure , the transmitter hops three times during a bit period. Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances to perform hopping at more or less the same points in time. However, these systems are much better at overcoming the effects of narrowband interference and frequency selective fading as they only stick to one frequency for a very short time.

Compared to DSSS, spreading is simpler using FHSS systems. FHSS systems only use a portion of the total band at any time, while DSSS systems always use the total bandwidth available. DSSS systems on the other hand are more resistant to fading and multi-path effects. DSSS signals are much harder to detect – without knowing the spreading code, detection is virtually impossible. If each sender has its own pseudo-random number sequence for spreading the signal (DSSS or FHSS), the system implements CDM.

Medium Access Control

Medium access control protocols are mechanisms that allow several users or transmitters to access a common medium or channel. They play an important role in the development of both wired and wireless networks.

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels.

Media access control (MAC) protocols enforce a methodology to allow multiple devices access to a shared media network. Before LANs, communication between computing devices had been point-to-point. That is, two devices were connected by a dedicated channel.

Medium Access Control (MAC) address is a hardware address use to uniquely identify each node of a network. It provides addressing and channel access control mechanisms to enable the several terminals or network nodes to communicate in a specified network. Medium Access Control of data communication protocol is also named as Media Access Control. In IEEE 802 OSI Reference model of computer networking, the Data Link Control (DLC) layer is subdivided into two sub-layers:

- The Logical Link Control (LLC) layer and
- The Medium Access Control (MAC) layer

The main question in connection with MAC in the wireless is whether it is possible to use elaborated MAC schemes from wired networks, for example, CSMA/CD as used in the original specification of IEEE 802.3 networks (aka Ethernet).

Space Division Multiple Access (SDMA)

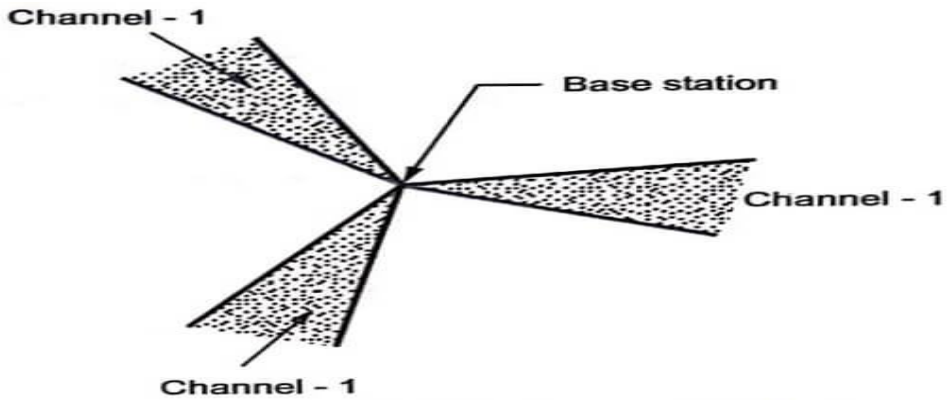
Advanced multiple antenna technique that increases the spectral efficiency, range and bandwidth available to moving wireless devices. Traditional cellular base stations radiate power in all directions, because they have no information about where the mobile device is located.

All users can communicate at the same time using the same channel. SDMA is completely free from interference. A single satellite can communicate with more satellites receivers of the same frequency.

Spatial division multiple access (SDMA) is a channel access method used in mobile communication systems which reuses the same set of cell phone frequencies in a given service area. Two cells or two small regions can make use of the same set of frequencies if they are separated by an allowable distance (called the reuse distance).

Space Division Multiple Access (SDMA) is used for allocating a separated space to users in wireless networks. A typical application involves assigning an optimal base station to a mobile phone user. The mobile phone may receive several base stations with different quality. A MAC algorithm could now decide which base station is best, taking into account which frequencies (FDM), time slots (TDM) or code (CDM) are still available (depending on the technology). Typically, SDMA is never used in isolation but always in combination with one or more other schemes. The basis for the SDMA algorithm is formed by cells and sectorized antennas which constitute the infrastructure implementing space division multiplexing (SDM)**.** Single users are separated in space by individual beams. This can improve the overall capacity of a cell (e.g., measured in bit/s/m2 or voice calls/m2) tremendously.

Principle : The narrow beam of radio waves is aimed at particular part of space. The same channel is reused over the another narrow beam aimed at another part of the space. This division of space in different directions of base station through highly directional beams is called Space Division Multiple Access (SDMA)



Space Division Multple Access (SDMA)

As shown above the space is divided and three channels are transmitted on same frequency.

Frequency Division Multiple Access (FDMA)

Frequency Division Multiple Access (FDMA) is **a channel access technique found in multiple-access protocols as a channelization protocol**. FDMA permits individual allocation of single or multiple frequency bands, or channels to the users.

Frequency Division Multiple Access (FDMA) is one of the most common analogue multiple access methods. The frequency band is divided into channels of equal bandwidth so that each conversation is carried on a different frequency .

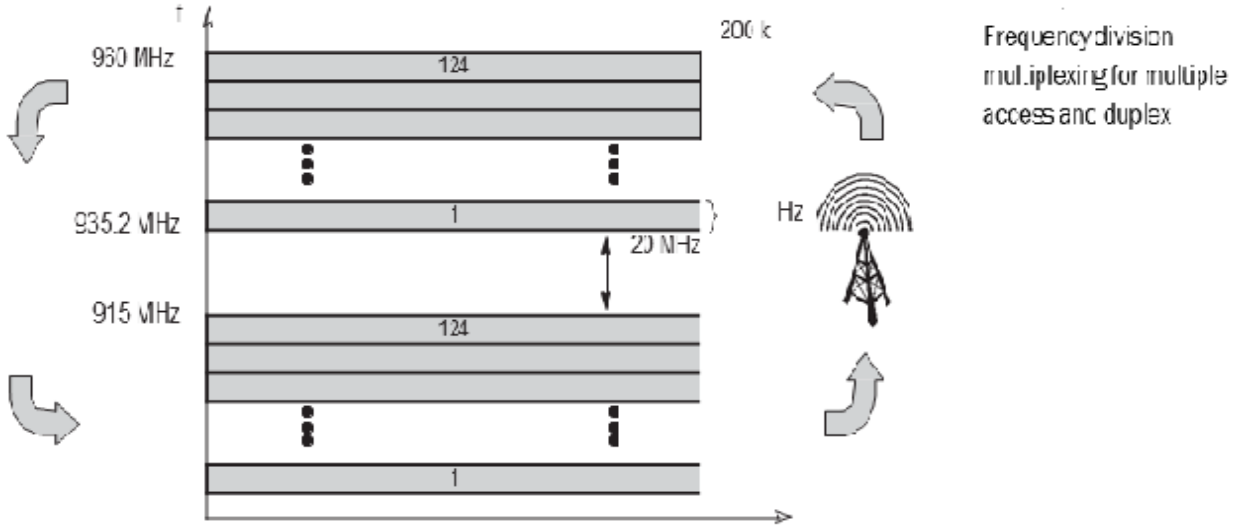
In FDMA method, guard bands are used between the adjacent signal spectra to minimize crosstalk between the channels. A specific frequency band is given to one person, and it will received by identifying each of the frequency on the receiving end. It is often used in the first generation of analog mobile phone.

Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM) scheme as presented. Allocation can either be fixed (as for radio stations or the general planning and regulation of frequencies) or dynamic (i.e., demand driven).

Channels can be assigned to the same frequency at all times, i.e., pure FDMA, or change frequencies according to a certain pattern, i.e., FDMA combined with TDMA. The latter example is the common practice for many wireless systems to circumvent narrowband interference at certain frequencies, known as frequency hopping. Sender and receiver have to agree on a hopping pattern, otherwise the receiver could not tune to the right frequency. Hopping patterns are typically fixed, at least for a longer period. The fact that it is not possible to arbitrarily jump in the frequency space (i.e., the receiver must be able to tune to the right frequency) is one of the main differences between FDM schemes and TDM schemes.

Furthermore, FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks. Here the two partners typically establish a duplex channel, i.e., a channel that allows for simultaneous transmission in both directions. The two directions, mobile station to base station and vice versa are now separated using different frequencies. This scheme is then called **frequency division duplex (FDD)**.

The two frequencies are also known as **uplink**, i.e., from mobile station to base station or from ground control to satellite, and as **downlink**, i.e., from base station to mobile station or from satellite to ground control.



As for example FDM and FDD, Figure 3.3 shows the situation in a mobile phone network based on the GSM standard for 900 MHz (see chapter 4). The basic frequency allocation scheme for GSM is fixed and regulated by national authorities. (Certain variations exist regarding the frequencies mentioned in the examples.) All uplinks use the band between 890.2 and 915 MHz, all downlinks use 935.2 to 960 MHz. According to FDMA, the base station, shown on the right side, allocates a certain frequency for up- and downlink to establish a duplex channel with a mobile phone. Up- and downlink have a fixed relation. If the uplink frequency is fu = 890 MHz + n·0.2 MHz, the downlink frequency is fd = fu + 45 MHz, i.e., fd = 935 MHz + n·0.2 MHz for a certain channel n. The base station selects the channel. Each channel (uplink and downlink) has a bandwidth of 200 kHz. This illustrates the use of FDM for multiple access (124 channels per direction are available at 900 MHz) and duplex according to a predetermined scheme.

Time Division Multiple Access (TDMA)

Time Division Multiple Access (TDMA) is **a digital modulation technique used in digital cellular telephone and mobile radio communication**. TDMA is one of two ways to divide the limited spectrum available over a radio frequency (RF) cellular channel. The other is known as frequency division multiple access (FDMA)..

Time Division Multiple Access (TDMA) is a complex technology, because it requires an accurate synchronization between the transmitter and the receiver. TDMA is used in digital mobile radio systems. The individual mobile stations cyclically assign a frequency for the exclusive use of a time interval.

In most of the cases, the entire system bandwidth for an interval of time is not assigned to a station. However, the frequency of the system is divided into sub-bands, and TDMA is used for the multiple access in each sub-band. Sub-bands are known as carrier frequencies. The mobile system that uses this technique is referred as the multi-carrier systems.

Compared to FDMA, **time division multiple access (TDMA)** offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling TDM. Now tuning in to a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time. Using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access. As already mentioned, listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple. Almost all MAC schemes for wired networks work according to this principle, e.g., Ethernet, Token Ring, ATM etc.

The following sections present several examples for fixed and dynamic schemes as used for wireless transmission.

Fixed TDM

The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. This results in a fixed bandwidth and is the typical solution for wireless phone systems. MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment. If this synchronization is assured, each mobile station knows its turn and no

interference will happen. The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.

Classical Aloha

The University of Hawaii and was used in the ALOHANET for wireless connection of several stations. Aloha neither coordinates medium access nor does it resolve contention on the MAC layer. Instead, each station can access the medium at any time. The simple Aloha works fine for a light load and does not require any complicated access mechanisms.

Slotted Aloha

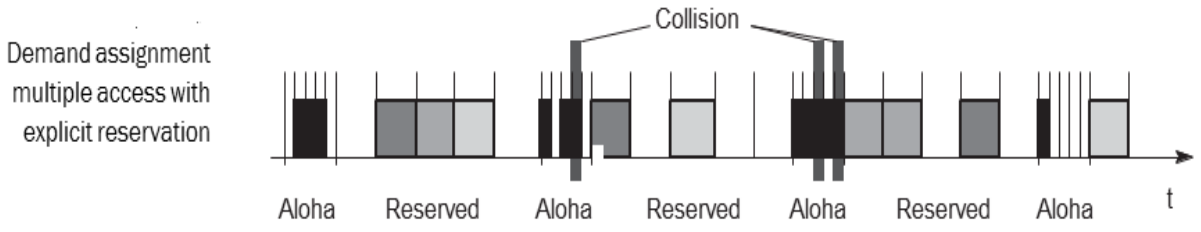
The first refinement of the classical Aloha scheme is provided by the introduction of time slots (**slotted Aloha**). In this case, all senders have to be **synchronized**, transmission can only start at the beginning of a **time slot** as shown in Figure 3.6. Still, access is not coordinated. Under the assumption stated above, the introduction of slots raises the throughput from 18 per cent to 36 per cent, i.e., slotting doubles the throughput.

Carrier sense multiple access

One improvement to the basic Aloha is sensing the carrier before accessing the medium. This is what **carrier sense multiple access (CSMA)** schemes generally do (Kleinrock, 1975, Halsall, 1996). Sensing the carrier and accessing the medium only if the carrier is idle decreases the probability of a collision. But, as already mentioned in the introduction, hidden terminals cannot be detected, so, if a hidden terminal transmits at the same time as another sender, a collision might occur at the receiver. This basic scheme is still used in most wireless LANs.

Demand assigned multiple access

One basic scheme is **demand assigned multiple access (DAMA)** also called **reservation Aloha**, a scheme typical for satellite systems. DAMA, as shown in Figure



During a contention phase following the slotted Aloha scheme, all stations can try to reserve future slots. For example, different stations on earth try to reserve access time for satellite transmission. Collisions during the reservation phase do not destroy data transmission, but only the short requests for data transmission. If successful, a time slot in the future is reserved, and no other station is allowed to transmit during this slot. Therefore, the satellite collects all successful requests (the others are destroyed) and sends back a reservation list indicating access rights for future slots. All ground stations have to obey this list.

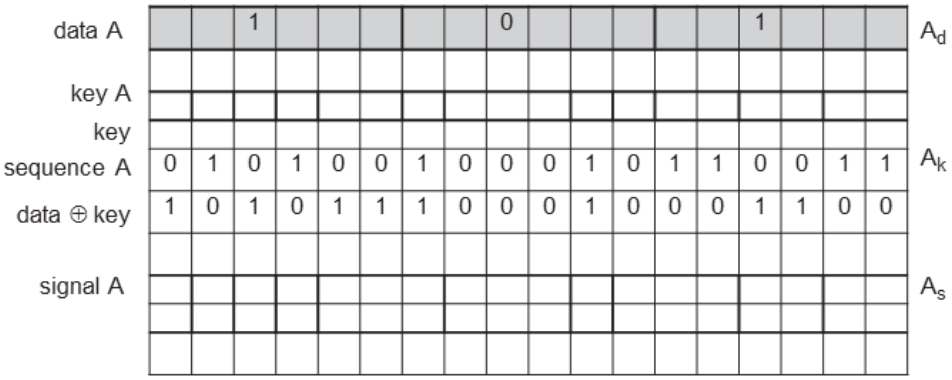
CDMA (Code-Division Multiple Access)

CDMA (Code-Division Multiple Access) refers to any of several protocols used in second-generation (2G) and third-generation (3G) wireless communications. As the term implies, CDMA is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in ultra-high-frequency (UHF) cellular phone systems in the 800 megahertz (MHz) and 1.9 gigahertz (GHz) bands.

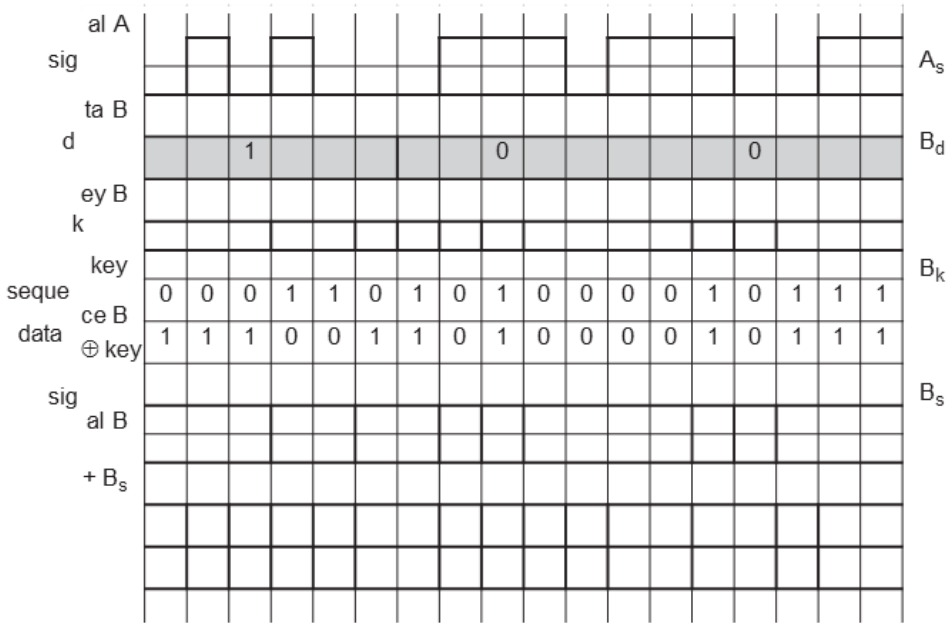
CDMA is an example of multiple access, where **several transmitters can send information simultaneously over a single communication channel**. This allows several users to share a band of frequencies.

Finally, codes with certain characteristics can be applied to the transmission to enable the use of **code division multiplexing (CDM)**. **Code division multiple access (CDMA)** systems use exactly these codes to separate different users in code space and to enable access to a shared medium without interference. The main problem is how to find “good” codes and how to separate the signal from noise generated by other signals and the environment.

Following figure shows a sender A that wants to transmit the bits 101. The key of A is shown as signal and binary key sequence Ak. In this example, the binary “0” is assigned a positive signal value, the binary “1” a negative signal value. After spreading, i.e., XORing Ad and Ak, the resulting signal is As.



Coding and spreading of data from sender A



Coding and spreading of data from sender B

The same happens with data from sender B, here the bits are 100. The result of spreading with the code is the signal Bs. As and Bs now superimpose during transmission (again without noise and both signals having the same strength).

The resulting signal is simply the sum As + Bs as shown in the above Figure .

Comparison of SDMA, TDMA, FDMA, and CDMA mechanisms

Approach	SDMA	TDMA	FDMA	CDMA
Idea	Segment space into cells/sectors	Segment sending time into disjoint time-slots, demand driven or fixed patterns	Segment the frequency band into disjoint sub-bands	Spread the spectrum using orthogonal codes
Terminals	Only one terminal can be active in one cell/one sector	All terminals are active for short periods of time on the same frequency	Every terminal has its own frequency, uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted
Signal separation	Cell structure directed antennas	Synchronization in the time domain Established, fully digital, very flexible	Filtering in the frequency domain	Code plus special receivers
Advantages	Very simple, increases capacity per km^2	Guard space needed (multi-path propagation), synchronization difficult	Simple, established, robust	Flexible, less planning needed, soft handover
Disadvantages	Inflexible, antennas typically fixed	Standard in fixed networks, together with FDMA/SDMA used in many mobile networks	Inflexible, frequencies are a scarce resource	Complex receivers, needs more complicated power control for senders
Comment	Only in combination with TDMA, FDMA or CDMA useful		Typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	Used in many 3G systems, higher complexity, lowered expectations; integrated with TDMA/FDMA

Satellite systems

Satellite communication began after the Second World War. Scientists knew that it was possible to build rockets that would carry radio transmitters into space. In 1945, Arthur C. Clarke published his essay on 'Extra Terrestrial Relays'. But it was not until 1957, in the middle of the cold war, that the sudden launching of the first satellite SPUTNIK by the Soviet Union shocked the Western world.

There are currently almost 200 geostationary satellites in commercial use which shows the impressive growth of satellite communication over the last 30 years (Miller, 1998), (Maral, 1998), (Pascall, 1997). However, satellite networks are currently facing heavy competition from terrestrial networks with nationwide coverage or at least enough coverage to support most applications and users.

Applications

Traditionally, satellites have been used in the following areas:

- **Weather forecasting:** Several satellites deliver pictures of the earth using, e.g., infra red or visible light. Without the help of satellites, the forecasting of hurricanes would be impossible.

● **Radio and TV broadcast satellites:**

Hundreds of radio and TV programs are available via satellite. This technology competes with cable in many places, as it is cheaper to install and, in most cases, no extra fees have to be paid for this service. Today's satellite dishes have diameters of 30–40 cm in central Europe, (the diameters in northern countries are slightly larger).

● **Military satellites:**

One of the earliest applications of satellites was their use for carrying out espionage. Many communication links are managed via satellite because they are much safer from attack by enemies.

Satellites for navigation:

Even though it was only used for military purposes in the beginning, the global positioning system (GPS) is nowadays well-known and available for everyone. The system allows for precise localization worldwide, and with some additional techniques, the precision is in the range of some metres. Almost all ships and aircraft rely on GPS as an addition to traditional navigation systems. Many trucks and cars come with installed GPS receivers. This system is also used, e.g., for fleet management of trucks or for vehicle localization in case of theft.

Global telephone backbones:

One of the first applications of satellites for communication was the establishment of international telephone backbones. Using satellites for telephone conversation is sometimes annoying and requires particular discipline in discussions.

Connections for remote or developing areas:

Due to their geographical location many places all over the world do not have direct wired connection to the telephone network or the internet (e.g., researchers on Antarctica) or because of the current state of the infrastructure of a country. Satellites now offer a simple and quick connection to global networks (Schwartz, 1996).

Global mobile communication:

The latest trend for satellites is the support of global mobile data communication. The basic purpose of satellites for mobile communication is not to replace the existing mobile phone networks, but to extend the area of coverage. Cellular phone systems, such as AMPS and GSM (and their successors) do not cover all parts of a country. Areas that are not covered usually have low population where it is too expensive to instal a base station. With the integration of satellite communication, however, the mobile phone can switch to satellites offering worldwide connectivity to a customer.

Following figure shows a classical scenario for satellite systems supporting global mobile communication

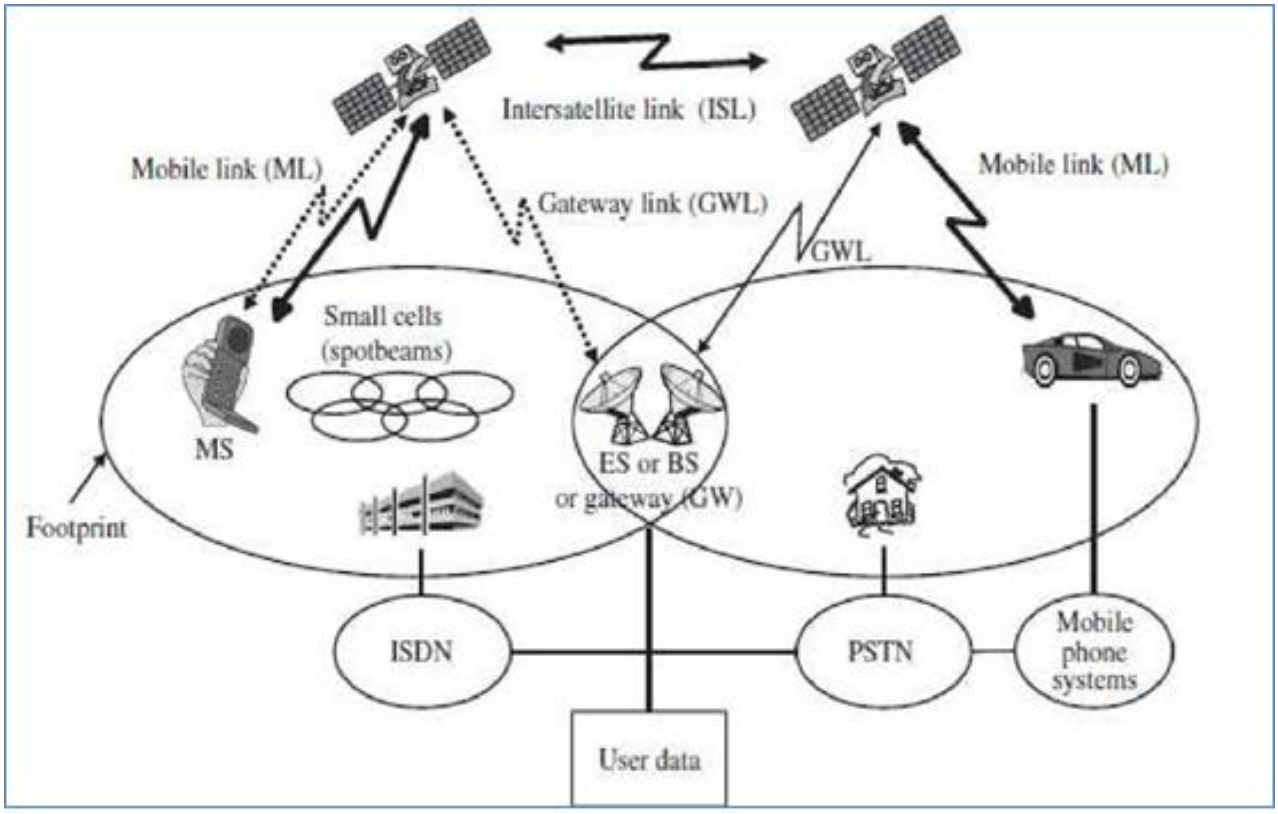


Fig: A typical satellite system

Mobile users via a **mobile user link (MUL)** and for the base station controlling the satellite and acting as gateway to other networks via the **gateway link (GWL)**. Satellites may be able to communicate directly with each other via **intersatellite links (ISL)**. This facilitates direct communication between users within different footprints without using base stations or other networks on earth. Saving extra links from satellite to earth can reduce latency for data packets and voice data. Some satellites have special antennas to create smaller cells using spot beams.

Satellite systems are, and will continue to be, a valuable addition to the many networks already in existance on earth. Users might communicate using ISDN or other PSTN, even cellular networks such as GSM and UMTS. Many gateways provide seamless communication between these different networks. A real challenge, for example, is the smooth, seamless handover between a cellular network and a satellite system (vertical handover) as it is already well known from within cellular networks (horizontal handover). Users should not notice the switching from, e.g., GSM, to a satellite network during conversation.

Basics

Satellites orbit around the earth. Depending on the application, these orbits can be circular or elliptical. Satellites in circular orbits always keep the same distance to the earth's surface following a simple law:

● The attractive force *Fg* of the earth due to gravity equals $m \cdot g \cdot (R/r)2$.

● The centrifugal force *Fc* trying to pull the satellite away equals $m \cdot r \cdot \omega 2$.

The variables have the following meaning:

● *m* is the mass of the satellite;

● *R* is the radius of earth with *R* = 6,370 km;

● *r* is the distance of the satellite to the centre of the earth;

● *g* is the acceleration of gravity with *g* = 9.81 m/s2;

● and ω is the angular velocity with $\omega = 2 \cdot \pi \cdot f$, *f* is the frequency of the rotation.

To keep the satellite in a stable circular orbit, the following equation must hold:

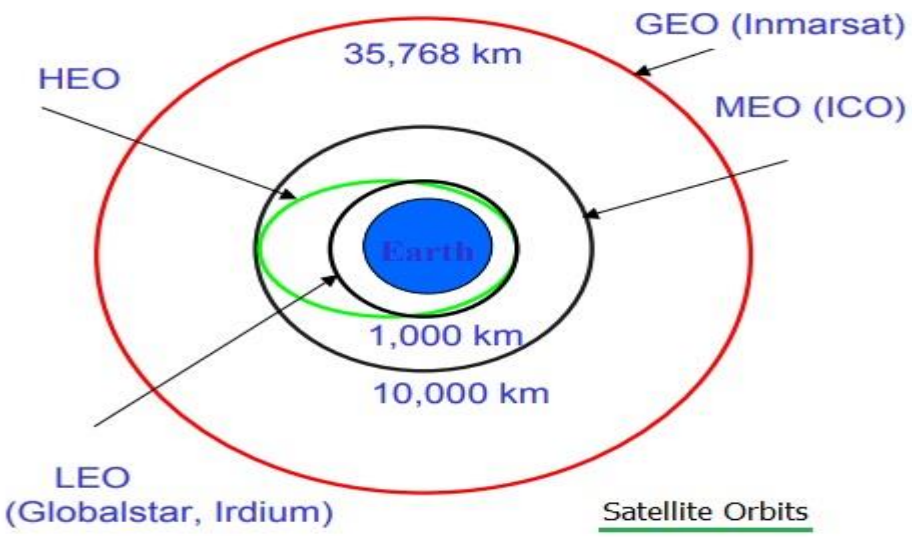
● *Fg* = *Fc*, i.e., both forces must be equal. Looking at this equation the first thing to notice is that the mass *m* of a satellite is irrelevant (it appears on both sides of the equation).

● Solving the equation for the distance *r* of the satellite to the center of the earth results in the following equation:

The distance $r = (g \cdot R2/(2 \cdot \pi \cdot f)2)1/3$

From the last equation it can be concluded that the distance of a satellite to the earth's surface depends on its rotation frequency

Four different types of orbits can be identified as shown in Figure:



Geostationary (or geosynchronous) earth orbit (GEO):

GEO satellites have a distance of almost 36,000 km to the earth. Examples are almost all TV and radio broadcast satellites, many weather satellites and satellites operating as backbones for the telephone network

Medium earth orbit (MEO):

MEOs operate at a distance of about 5,000–12,000 km. Up to now there have not been many satellites in this class, but some upcoming systems (e.g., ICO) use this class for various reason

Low earth orbit (LEO):

While some time ago LEO satellites were mainly used for espionage, several of the new satellite systems now rely on this class using altitudes of 500–1,500 km.

Highly elliptical orbit (HEO):

This class comprises all satellites with noncircular orbits. Currently, only a few commercial communication systems using satellites with elliptical orbits are planned. These systems have their perigee over large cities to improve communication quality

<u>Geostationary (or geosynchronous) earth orbit GEO</u>

If a satellite should appear fixed in the sky, it requires a period of 24 hours. Using the equation for the distance between earth and satellite

$r = (g \cdot R2/(2 \cdot \pi \cdot f)2)1/3$ and the period of 24 hours f = 1/24h, the resulting distance is 35,786 km. The orbit must have an inclination of 0 degrees.

<u>Advantages</u>:

Three GEO satellites are enough for a complete coverage of almost any spot on earth. Senders and receivers can use fixed antenna positions, no adjusting is needed. GEOs are ideal for TV and radio broadcasting.

Lifetime expectations for GEOs are rather high, at about 15 years. GEOs typically do not need a handover due to the large footprint. GEOs do not exhibit any Doppler shift because the relative movement is zero.

Low earth orbit LEO

As LEOs circulate on a lower orbit, it is obvious that they exhibit a much shorter period (the typical duration of LEO periods are 95 to 120 minutes). Additionally, LEO systems try to ensure a high elevation for every spot on earth to provide a high quality communication link. Each LEO satellite will only be visible from the earth for around ten minutes. A further classification of LEOs into little LEOs with low bandwidth services (some 100 bit/s), big LEOs (some 1,000 bit/s) and broadband LEOs with plans reaching into the Mbit/s range can be found in Comparetto (1997).

Advantages: Using advanced compression schemes, transmission rates of about 2,400 bit/s can be enough for voice communication. LEOs even provide this bandwidth for mobile terminals with omni-directional antennas using low transmit power in the range of 1W. The delay for packets delivered via a LEO is relatively low (approx 10 ms). The delay is comparable to long-distance wired connections (about 5–10 ms). Smaller footprints of LEOs allow for better frequency reuse, similar to the concepts used for cellular networks (Gavish, 1998). LEOs can provide a much higher elevation in polar regions and so better global coverage.

Medium earth orbit MEO

MEOs can be positioned somewhere between LEOs and GEOs, both in terms of their orbit and due to their advantages and disadvantages.

Advantages: Using orbits around 10,000 km, the system only requires a dozen satellites which is more than a GEO system, but much less than a LEO system. These satellites move more slowly relative to the earth's rotation allowing a simpler system design (satellite periods are about six hours). Depending on the inclination, a MEO can cover larger populations, so requiring fewer handovers.

Disadvantages: Again, due to the larger distance to the earth, delay increases to about 70–80 ms. The satellites need higher transmit power and
special antennas for smaller footprints.

Routing

A satellite system together with gateways and fixed terrestrial networks as shown in the following figure has to route data transmissions from one user to another as any other network does. Routing in the fixed segment (on earth) is achieved as usual, while two different solutions exist for the satellite network in space. If satellites offer ISLs, traffic can be routed between the satellites. If not, all traffic is relayed to earth, routed there, and relayed back to a satellite.

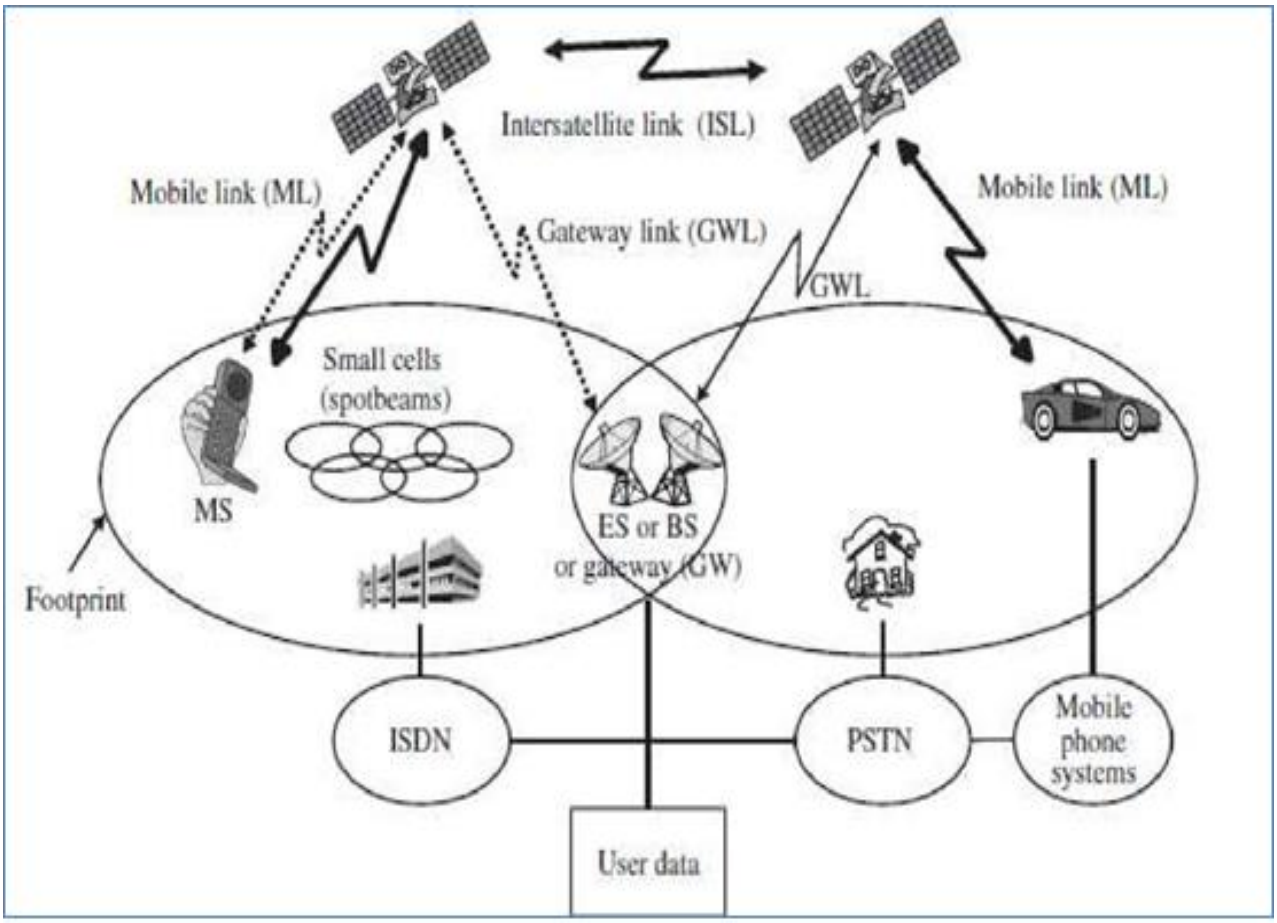


Fig: A typical satellite system

Assume two users of a satellite network exchange data. If the satellite system supports ISLs, one user sends data up to a satellite and the satellite forwards it to the one responsible for the receiver via other satellites. This last satellite now sends the data down to the earth. This means that only one uplink and one downlink per direction is needed. The ability of routing within the satellite network reduces the number of gateways needed on earth.

If a satellite system does not offer ISLs, the user also sends data up to a satellite, but now this satellite forwards the data to a gateway on earth. Routing takes place in fixed networks as usual

until another gateway is reached which is responsible for the satellite above the receiver. Again data is sent up to the satellite which forwards it down to the receiver. This solution requires two uplinks and two downlinks. Depending on the orbit and the speed of routing in the satellite network compared to the terrestrial network, the solution with ISLs might offer lower latency.

Localization

Localization of users in satellite networks is similar to that of terrestrial cellular networks. One additional problem arises from the fact that now the 'base stations',i.e., the satellites, move as well. The gateways of a satellite network maintain several registers. A **home location register (HLR)** stores all static information about a user as well as his or her current location. The last known location of a mobile user is stored in the **visitor location register (VLR)**. Functions of the VLR and HLR are similar to those of the registers. A particularly important register in satellite networks is the **satellite user mapping register (SUMR)**. This stores the current position of satellites and a mapping of each user to the current satellite through which communication with a user is possible.

Registration of a mobile station is achieved as follows. The mobile station initially sends a signal which one or several satellites can receive. Satellites receiving such a signal report this event to a gateway. The gateway can now determine the location of the user via the location of the satellites. User data is requested from the user's HLR, VLR and SUMR are updated.

Calling a mobile station is again similar to GSM. The call is forwarded to a gateway which localizes the mobile station using HLR and VLR. With the help of the SUMR, the appropriate satellite for communication can be found and the connection can be set up.

Handover

An important topic in satellite systems using MEOs and in particular LEOs is handover. Imagine a cellular mobile phone network with fast moving base stations. This is exactly what such satellite systems are – each satellite represents a base station for a mobile phone. Compared to terrestrial mobile phone networks, additional instances of handover can be necessary due to the movement of the satellites.

● **Intra-satellite handover:** A user might move from one spot beam of a satellite to another spot beam of the same satellite. Using special antennas, a satellite can create several spot beams within its footprint. The same effect might be caused by the movement of the satellite.

● **Inter-satellite handover:** If a user leaves the footprint of a satellite or if the satellite moves away, a handover to the next satellite takes place. This might be a hard handover switching at one moment or a soft handover using both satellites (or even more) at the same time (as this is possible with CDMA systems). Inter-satellite handover can also take place between satellites if they support ISLs. The satellite system can trade high transmission quality for handover frequency. The higher the transmission quality should be, the higher the elevation angles that are needed. High elevation angles imply frequent handovers which in turn, make the system more complex.

● **Gateway handover:** While the mobile user and satellite might still have good contact, the satellite might move away from the current gateway. The satellite has to connect to another gateway.

● **Inter-system handover:** While the three types of handover mentioned above take place within the satellite-based communication system, this type of handover concerns different systems. Typically, satellite systems are used in remote areas if no other network is available. As soon as traditional cellular networks are available, users might switch to this type usually because it is cheaper and offers lower latency. Current systems allow for the use of dual-mode (or even more) mobile phones but unfortunately, seamless handover between satellite systems and terrestrial systems or vice versa has not been possible up to now.

Telecommunication systems

Digital cellular networks are the segment of the market for mobile and wireless devices which are growing most rapidly. They are the wireless extensions of traditional PSTN or ISDN networks and allow for seamless roaming with the same mobile phone nation or even worldwide.

The electronic transmission of information over distances, called telecommunications, has become nearly inseparable from computers: Computers and telecommunications create value together. Components of a Telecommunications Network Telecommunications are the means of electronic transmission of information over distances. Telecommunication is the

exchange of signs, signals, messages, words, writings, images and sounds or information of any nature by wire, radio, optical or other electromagnetic systems. A complete, single telecommunications circuit consists of two stations, each equipped with a transmitter and a receiver. The transmitter and receiver at any station may be combined into a single device called a transceiver. The medium of signal transmission can be via electrical wire or cable ("copper"), optical fiber, electromagnetic fields or light. The free space transmission and reception of data by means of electromagnetic fields is called wireless communications.

GSM

GSM stands for **G**lobal **S**ystem for **M**obile Communication. It is a digital cellular technology used for transmitting mobile voice and data services. Important facts about the GSM are given below −

- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- GSM is the most widely accepted standard in telecommunications and it is implemented globally.
- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.
- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.

- GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network.

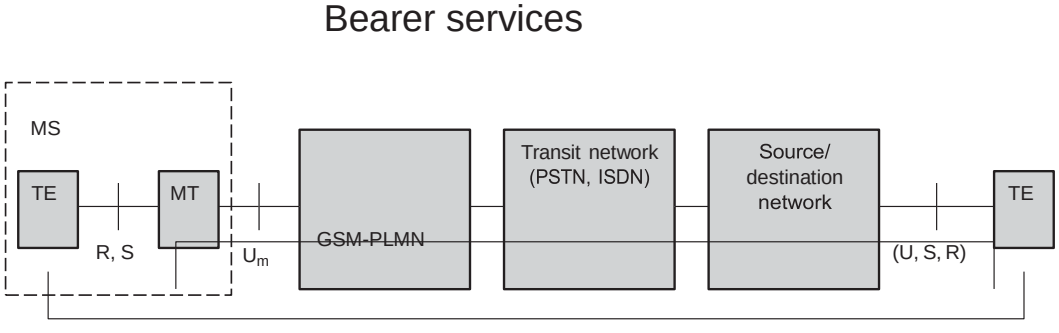
GSM is the most successful digital mobile telecommunication system in the world today. It is used by over 800 million people in more than 190 countries. In the early 1980s, Europe had numerous coexisting analog mobile phone systems, which were often based on similar standards (e.g., NMT 450), but ran on slightly different carrier frequencies. To avoid this situation for a second generation fully digital system, the **groupe spéciale mobile (GSM)** was founded in 1982. This system was soon named the **global system for mobile communications.**

(GSM), with the specification process lying in the hands of ETSI (ETSI, 2002), (GSM Association, 2002).

The primary goal of GSM was to provide a mobile phone system that allows users to roam throughout Europe and provides voice services compatible to ISDN and other PSTN systems. The specification for the initial system already covers more than 5,000 pages; new services, in particular data services, now add even more specification details. Readers familiar with the ISDN reference model will recognize many similar acronyms, reference points, and interfaces. GSM standardization aims at adopting as much as possible.

Mobile services

GSM permits the integration of different voice and data services and the interworking with existing networks. Services make a network interesting for customers. GSM has defined three different categories of services: bearer, tele, and supplementary services. These are described in the following subsections. Figure 4.3 shows a reference model for GSM services



Bearer and tele services reference model

Bearer services

GSM specifies different mechanisms for data transmission, the original GSM allowing for data rates of up to 9600 bit/s for non-voice services. Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission. **Transparent bearer services** only use the functions of the physical layer (layer 1) to transmit data. Data transmission has a constant delay and throughput if no transmission errors occur.

Using transparent and non-transparent services, GSM specifies several bearer services for interworking with PSTN, ISDN, and packet switched public data networks (PSPDN) like X.25, which is available worldwide.

Tele services

GSM mainly focuses on voice-oriented tele services. These comprise 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 the provision of high-quality digital voice transmission, offering at least the typical bandwidth of 3.1 kHz of analog phone systems. Special codecs (coder/decoder) are used for voice transmission, while other codecs are used for the transmission of analog data for communication with traditional computer modems used in, e.g., fax machines.

Another service offered by GSM is the **emergency number**. The same number can be used throughout Europe. This service is mandatory for all providers and free of charge. This connection also has the highest priority, possibly pre-empting other connections, and will automatically be set up with the closest emergency center.

Supplementary services

In addition to tele and bearer services, GSM providers can offer **supplementary services**. Similar to ISDN networks, these services offer various enhancements for the standard telephony service, and may vary from provider to provider. Typical services are user **identification**, call **redirection**, or **forwarding** of ongoing calls. Standard ISDN features such as **closed user groups** and **multiparty** communication may be available. Closed user groups are of special interest to companies because they allow, for example, a company-specific GSM sub-network, to which only members of the group have access.

System architecture

As with all systems in the telecommunication area, GSM comes with a hierarchical, complex system architecture comprising many entities, interfaces, and acronyms. Figure 4.4 gives a simplified overview of the GSM system as specified in ETSI (1991b). A GSM system consists of three subsystems, the **Radio Sub System (RSS)**, the **Network and Switching Subsystem (NSS)**, and the **Operation Subsystem (OSS)**. Generally, a GSM customer only notices a very small fraction of the whole network – the mobile stations (MS) and some antenna masts of the base transceiver stations (BTS).

Radio subsystem (RSS)

As the name implies, the **radio subsystem (RSS)** comprises all radio specific entities, i.e., the **mobile stations (MS)** and the **base station subsystem (BSS)**. Figure 4.4 shows the connection between the RSS and the NSS via the **A interface** (solid lines) and the connection to the OSS via the **O interface** (dashed lines).

Base station subsystem (BSS): A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.

Base transceiver station (BTS): A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission

Base station controller (BSC): The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS.

Mobile station (MS): The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the **subscriber identity module (SIM)**, which stores all user-specific data that is

relevant to GSM.3 While an MS can be identified via the **international mobile equipment identity (IMEI)**, a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. MS can also offer other types of interfaces to users with display, loudspeaker, microphone, and programmable soft keys Network and switching subsystem

Network and switching subsystem

The "heart" of the GSM system is formed by the **network and switching subsystem (NSS)**. The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:

Mobile services switching center (MSC): MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Using additional **interworking functions (IWF)**, an MSC can also connect to **public data networks (PDN)** such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs. The **standard signaling system No. 7 (SS7)** is used for this purpose. SS7 covers all aspects of control signalling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls).

Home location register (HLR): The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the **mobile subscriber ISDN number (MSISDN)**, subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the **international mobile subscriber identity (IMSI).**

Visitor location register (VLR): The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC.

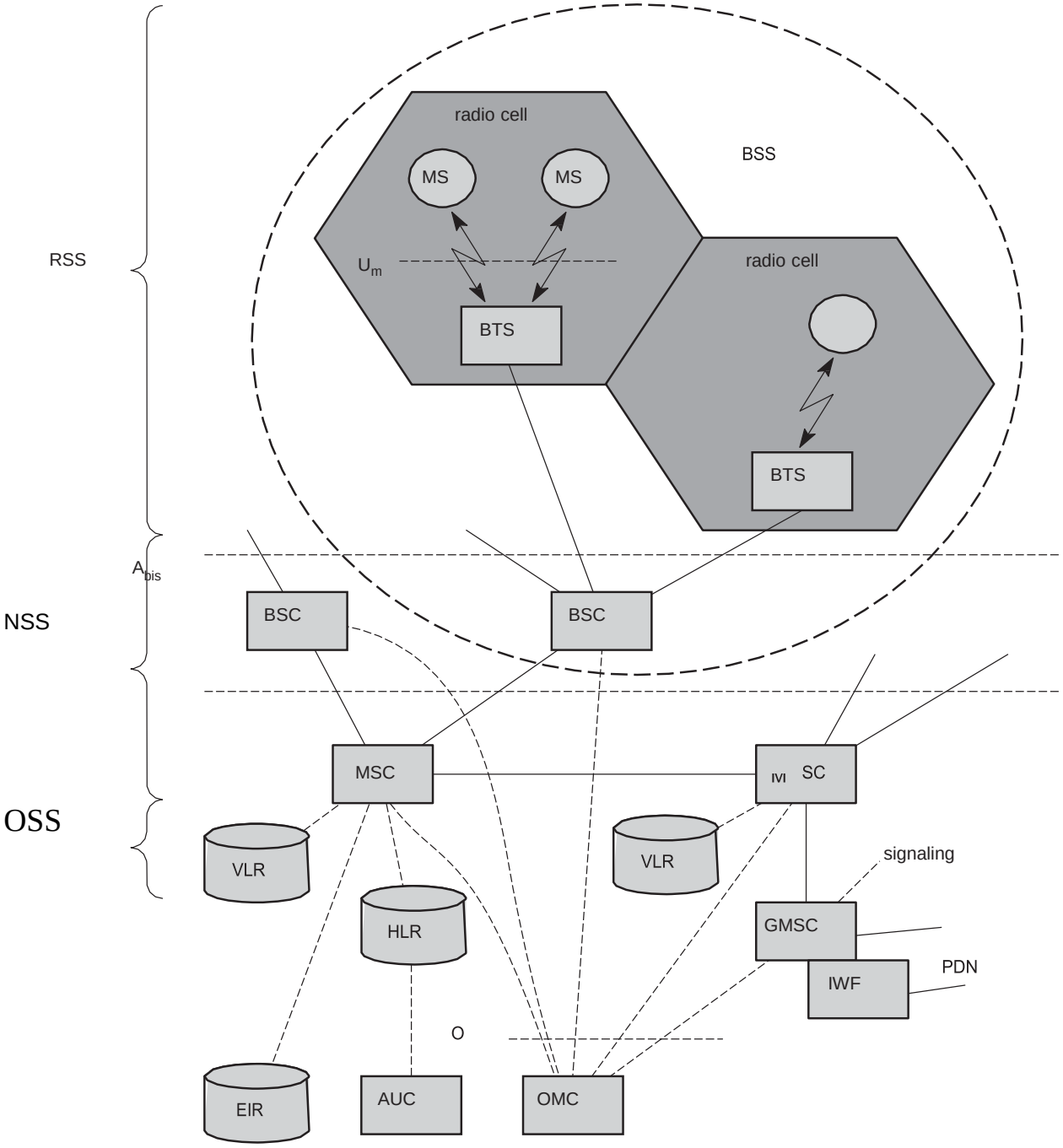
Operation Subsystem (OSS)

The third part of a GSM system, the **operation subsystem (OSS)**, contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signaling

Operation and maintenance center (OMC): The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing. OMCs use the concept of **telecommunication management network (TMN)** as standardized by the ITU-T.

Authentication centre (AuC): As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.

Equipment identity register (EIR): The EIR is a database for all IMEIs, i.e.,
it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices.



Functional architecture of a GSM system

Security in GSM

GSM allows three-band phones to be used seamlessly in more than 160 countries. In GSM, security is implemented in three entities:

1) Subscriber identity module (SIM) contains authentication key Ki (64-bit), ciphering key (Kc) generating algorithm, and authentication algorithm. SIM is a single chip computer containing the operating system (OS), the file system, and applications. SIM is protected by a PIN and owned by an operator. SIM applications can be written with a SIM tool kit.

2) GSM handset contains ciphering algorithm.

3) Network uses algorithms and IDs that are stored in the authentication center.

GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

GSM uses three different security algorithms called A3, A5, and A8. Algorithm **A3 is used for authentication, A5 is used for encryption, and A8 is used for the generation of a cipher key.**

Mobile Station Authentication A3

During the authentication process the MSC challenges the MS with a random number (RAND). The SIM card uses this RAND received from the MSC and a secret key Ki stored within the SIM as input. Both the RAND and the Ki secret are 128 bits long. Using the A3 algorithm with RAND and Ki as input a 32-bit output called signature response (SRES) is generated in the MS. This SRES is then sent back to the MSC as the response to the challenge. Using the same set of algorithms, the AUC also generates a SRES. The SRES from MS (SIM) and the SRES generated by the AUC are compared. If they are the same, the MS is authenticated. The idea is that no keys will be transacted over the air. However, if the SRES values calculated independently by the SIM and the AUC are the same, the Ki has to be same. If Ki is same, the SIM card is genuine.

The Voice-Privacy Key Generation Algorithm A8

For any type of cipher, we need a key. If the key is random and difficult to guess, the cipher is relatively secured. In the GSM security model, A8 algorithm is the key generation algorithm (A8 generates a session key), Kc, from the random challenge, RAND, received from the MSC and from the secret key Ki. The inputs for A8 are the same set of 128-bit Ki and RAND as used in A3. The A8 algorithm takes these inputs and generates a 64-bit output. The keys are generated at both the MS (SIM) and the network end. The BTS received the Kc from the MSC. The session key Kc, is used for ciphering, till the time the MSC decides to authenticate the MS once again. This might sometimes take days

The Strong Over-the-Air Voice-Privacy Algorithm A5/1

In the GSM security model, A5 is the stream cipher algorithm used to encrypt over-the-air transmissions . The stream cipher is initialized all over again for every frame sent. The stream cipher is initialized with the session key, Kc, and the number of the frame being encrypted or decrypted. The same Kc is used throughout the call, but the 22-bit frame number (Fn) changes during the call, thus generating a unique keystream for every frame.