
# KTU NOTES

The learning companion.

**KTU STUDY MATERIALS | SYLLABUS | LIVE NOTIFICATIONS | SOLVED QUESTION PAPERS**

# 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

Spread-spectrum techniques are methods by which a signal (e.g., an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. Spreading the bandwidth has several advantages. The main advantage is the resistance to narrowband interference. In Figure 2.1, diagram i) shows an idealized narrowband signal from a sender of user data (here power density dP/df versus frequency f). The sender now spreads the signal in step ii), i.e., converts the narrowband signal into a broadband signal. The energy needed to transmit the signal(the area shown in the diagram) is the same, but it is now spread over a larger frequency range. The power level of the spread signal can be much lower than that of the original narrowband signal without losing data. Depending on the generation and reception of the spread signal, the power level of the user signal can even be as low as the background noise. This makes it difficultto distinguish the user signal from the background noise and thus hard to detect.



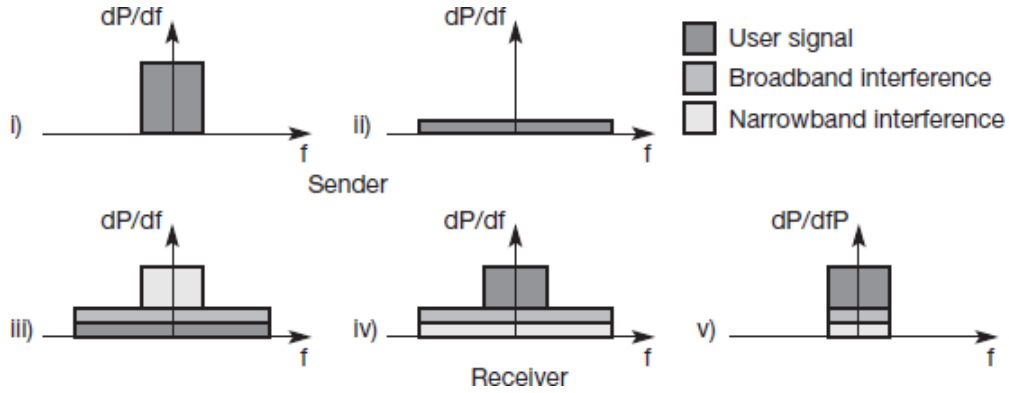



**Fig 2.1 Spread spectrum:spreading and despreading**

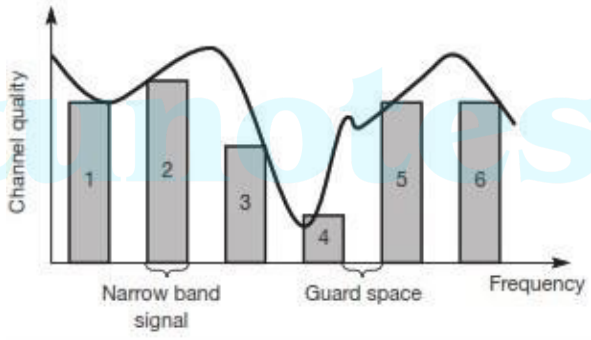
During transmission, narrowband and broadband interference add to the signal in step iii). The sum of interference and user signal is received. The receiver now knows how to despread the signal, converting the spread user signal into a narrowband signal again, while spreading the narrowband interference and leaving the broadband interference. In step v) the receiver applies a bandpass filter to cut off frequencies left and right of the narrowband signal. Finally, the receiver

can reconstruct the original data because the power level of the user signal is high enough, i.e., the signal is much stronger than the remaining interference. The following sections show how spreading can be performed.

Just as spread spectrum helps to deal with narrowband interference for a single channel, it can be used for several channels. Consider the situation shown in Figure 2.2. Six different channels use FDM for multiplexing, which means that each channel has its own narrow frequency band for transmission. Between each frequency band a guard space is needed to avoid adjacent channel interference. Additionally, Figure 2.2 depicts a certain channel quality. This is frequency dependent and is a measure for interference at this frequency. Channel quality also changes over time – the diagram only shows a snapshot at one moment. Depending on receiver characteristics, channels 1, 2, 5, and 6 could be received while the quality of channels 3 and 4 is too bad to reconstruct transmitted data. Narrowband interference destroys the transmission of channels 3 and

4. This illustration only represents a snapshot and the situation could be completely differentat the next moment. All in all, communication may be very difficult using such narrowband signals.

**Fig:-2.2Narrowband interference without spread spectrum**






Spread spectrum technologies also exhibit drawbacks. One disadvantage is the increased complexity of receivers that have to despread a signal. Today despreading can be performed up to high data rates thanks to digital signal processing. Another problem is the large frequency band that is needed due to the spreading of the signal. Although spread signals appear more like noise, they still raise the background noise level and may interfere with other transmissions if no special precautions are taken.

Spreading the spectrum can be achieved in two different ways as shown in the following two sections.

## Direct sequence spread spectrum

Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence as shown in Figure 2.2. The example shows that the result is either the sequence 0110101 (if the user bit equals 0) or its complement 1001010 (if the

user bit equals 1). While each user bit has a duration tb, the chipping sequence consists of smaller pulses, called chips, with a duration tc. If the chipping sequence is generated properly it appears as random noise: this sequence is also sometimes called pseudo-noise sequence. The spreading factor s = tb/tc determines the bandwidth of the resulting signal. If the original signal needs a bandwidth w, the resulting signal needs s·w after spreading. While the spreading factor of the very simple example is only 7 (and the chipping sequence 0110101 is not very random), civil applications use spreading factors between 10 and 100, military applications use factors of up to 10,000. For example, the sequence 10110111000, a so-called Barker code, if implemented using DSSS.

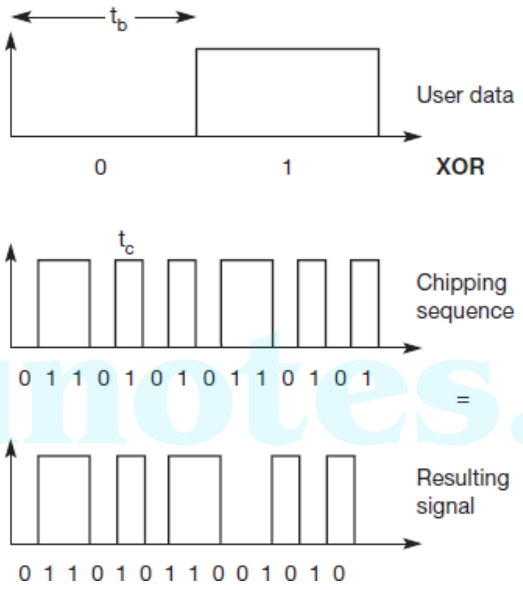



**Fig:2.2 Spreading with DSSS**

Barker codes exhibit a good robustness against interference and insensitivity tomulti-path propagation. Other known Barker codes are 11, 110, 1110, 11101, 1110010, and 1111100110101.

However, transmitters and receivers using DSSS need additional components as shown in the simplified block diagrams in Figure 2.3 and Figure 2.4. The first step in a DSSS transmitter, Figure 2.3 is the spreading of the user data with the chipping sequence (digital modulation). The spread signal is then modulated with a radio carrier (radio 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.

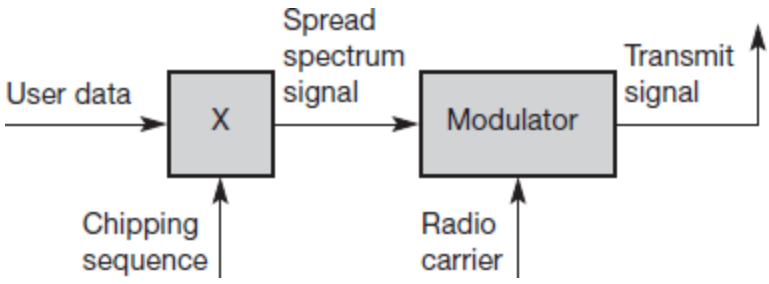



**Fig:2.3 DSSS transmitter**

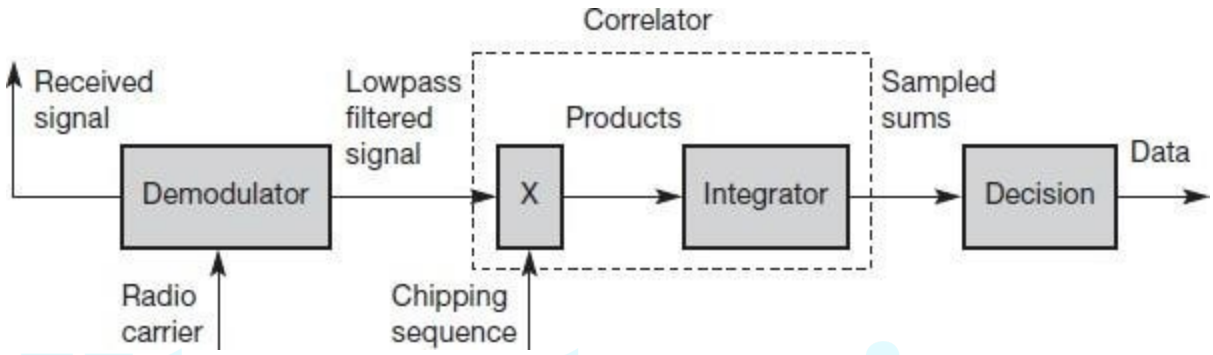



**Fig:2.4 DSSS receiver**



The DSSS receiver is more complex than the transmitter. The receiver only has to perform the inverse functions of the two transmitter modulation steps. However, noise and multi-path propagation require additional mechanisms to reconstruct the original data. 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. Additional filtering can be applied to generate this signal.

## 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 (see Figure 2.5).

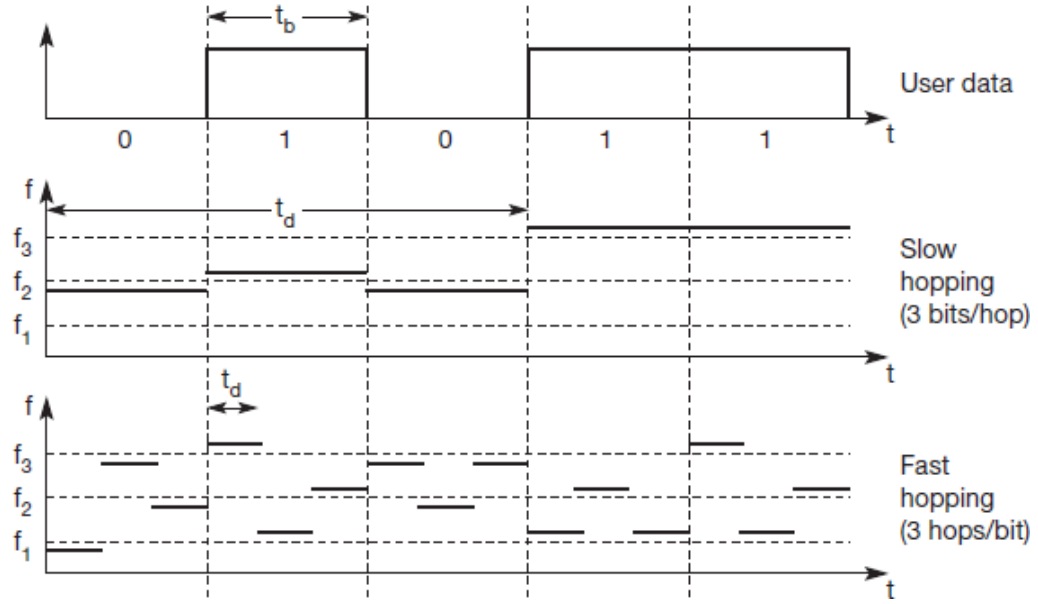



**Fig 2.5 Slow and fast frequency hopping**

In slow hopping, the transmitter uses one frequency for several bit periods.3 Figure 2.38 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, but they are not as immune to narrowband interference as fast hopping systems. 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 Figure 2.5, 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.

**Another example of an FHSS system is Bluetooth. Bluetooth performs 1,600 hops per second and uses 79 hop carriers equally spaced with 1 MHz in the 2.4 GHz ISM band.**

Figures 2.6 and 2.7 show simplified block diagrams of FHSS transmitters and receivers respectively. The first step in an FHSS transmitter is the modulation of user data according toone of the digital-to-analog modulation schemes, e.g., FSK or BPSK . This results in a narrowband signal, if FSK is used with a frequency f0 for a binary 0 and f1 for a binary 1. In BPSK represented by two different phase states in the carrier signal: $0^o$ for binary 1 and $180^o$ for binary 0. In the next step, frequency hopping is performed, based on a hopping sequence. The hopping sequence is fed into a frequency synthesizer generating the carrier frequencies fi. A second modulation uses the modulated narrowband signal and the carrier frequency to generate a new spread signal with frequency of fi+f0 for a 0 and fi+f1 for a 1 respectively.

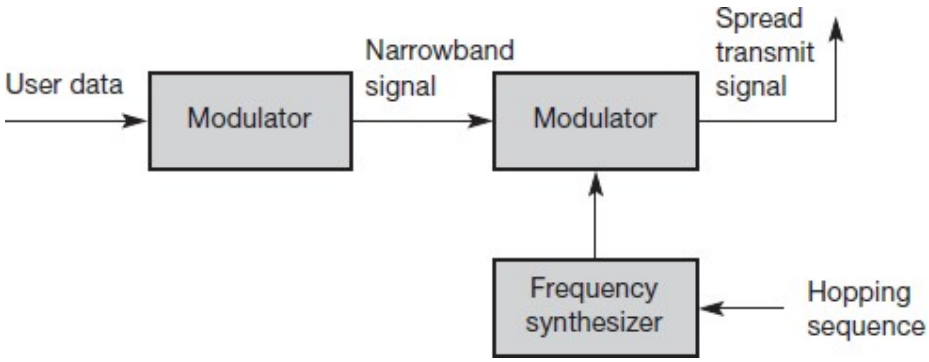



**Fig:2.6 FHSS transmitter**

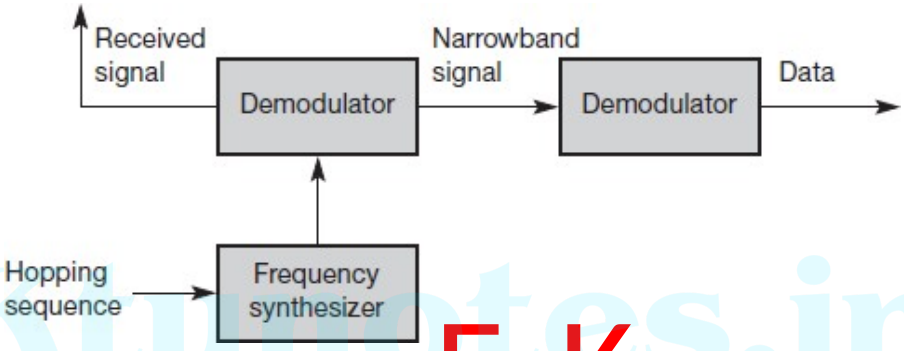



**Fig 2.7 FHSS receiver**



The receiver of an FHSS system has to know the hopping sequence and must stay synchronized. It then performs the inverse operations of the modulation to reconstruct user data.

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 (MAC) algorithms are specifically adapted to the wireless domain.Medium access control comprises all mechanisms that regulate user access to a medium using SDM, TDM, FDM, or CDM. MAC is thus similar to traffic regulations in the highway.MAC belongs to layer 2 of ISO/OSI, the data link control layer (DLC). Layer 2 is subdivided into the logical link control (LLC), layer b, and the MAC, layer 2a.

**Motivation for a specialized MAC**

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( carrier sense multiple access with collision detection).

Why does this scheme fail in wireless networks? CSMA/CD is not really interested in collisions at the sender, but rather in those at the receiver. The signal should reach the receiver without collisions. But the sender is the one detecting collisions. The following sections show some more scenarios where schemes known from fixed networks fail in wireless networks.

**1. Hidden and exposed terminals**

Consider the scenario with three mobile phones as shown in Figure 2.8. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission rangeof C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa.

A starts sending to B, C does not receive this transmission. C also wants to send something to B and senses the medium. The medium appears to be free, the carrier sense fails. C also starts sending causing a collision at B. But A cannot detect this collision at B and continues with its transmission. **A is hidden for C and vice versa.**



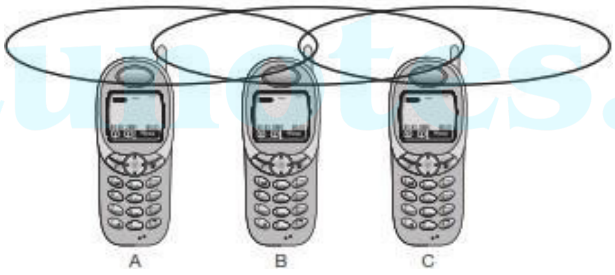



**Fig:2.8 Hidden and exposed terminals**

While hidden terminals may cause collisions, the exposed terminals only causes unnecessary delay. Now consider the situation that B sends something to A and C wants to transmit data to some other mobile phone outside the interference ranges of A and B. C senses the carrier and detects that the carrier is busy (B'signal). C postpones its transmission until it detects the medium as being idle again. But as A is outside the interference range of C, waiting is not necessary. Causing a 'collision' at B does not matter because the collision is too weak to propagate to A. In this situation, **C is exposed to B.**

**2. Near and far terminals**

Consider the situation as shown in Figure 2.9. A and B are both sending with the same transmission power. As the signal strength decreases proportionally to the square of the distance, B's signal drowns out A's signal. As a result, C cannot receive A's transmission.

The near/far effect is a severe problem of wireless networks using CDM. All signals should arrive at the receiver with more or less the same strength.

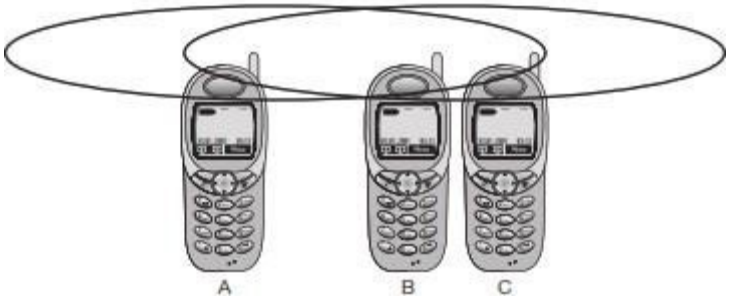



**Fig:2.8 Near and far terminals**

**MAC mechanisms**

**1. SDMA(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).



**2. FDMA(Frequency division multiple access)**

FDMA comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM). Allocation can either be **fixed or dynamic** (i.e., demanddriven). 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.

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)**. Again, both partners have to know the frequencies in advance; they cannot just listen into the medium. 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.

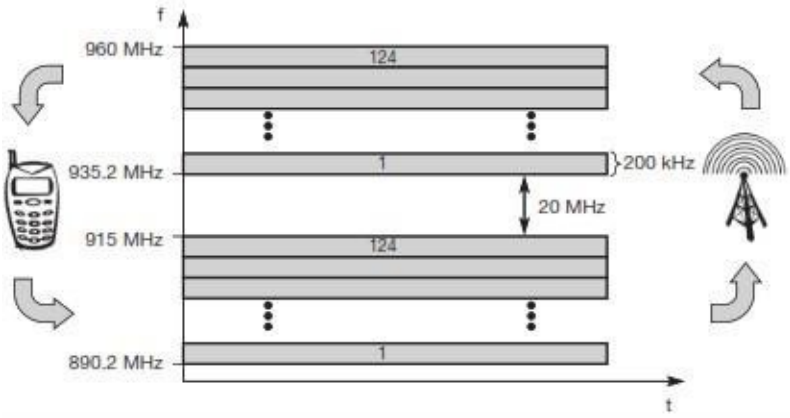



**Fig:2.9 Frequency division multiplexing for multiple access and duplex**

As for example FDM and FDD, Figure 2.9 shows the situation in a mobile phone network based on the GSM standard for 900 MHz . 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 = 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.



### 3. TDMA( Time division multiple access)

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.

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

### 3.1 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.

Figure 2.10 shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station. Assigning different slots for uplink and downlink using the same frequency is called **time division duplex (TDD)**. As shown in the figure, the base station

uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink. Uplink and downlink are separated in time. Up to 12 different mobile stations can use the same frequency without interference using this scheme. Each connection is allotted its own up- and downlink pair.

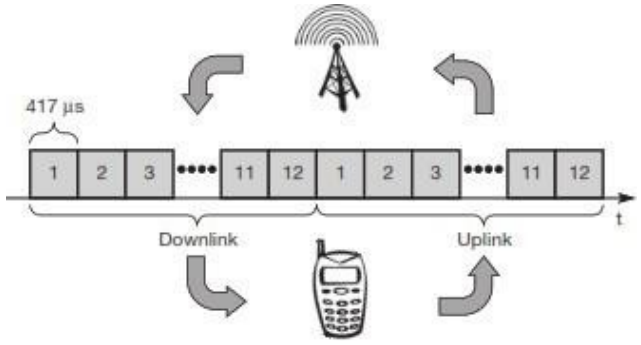



**Fig:2.10 Time division multiplexing for multiple access and duplex**

The fixed access patterns are perfectly apt for connections with a constant data rate (e.g., classical voice transmission with 32 or 64 kbit/s duplex), they are very inefficient for bursty data or asymmetric connections. If temporary bursts in data are sent from the base station to the mobile station often or vice versa (as in the case of web browsing, where no data transmission occurs while reading a page, whereas clicking on a hyperlink triggers a data transfer from the mobile station, often to the base station, often followed by huge amounts of data returned from the web server).



### 3.2 Classical Aloha

Aloha neither coordinates medium access nor does it resolve contention on the MAC layer. Instead, each station can access the medium at any time as shown in Figure 2.11. This is a random access scheme, without a central arbiter controlling access and without coordination among the stations. If two or more stations access the medium at the same time, a collision occurs and the transmitted data is destroyed. Resolving this problem is left to higher layers (e.g., retransmission of data).

The simple Aloha works fine for a light load and does not require any complicated access mechanisms.

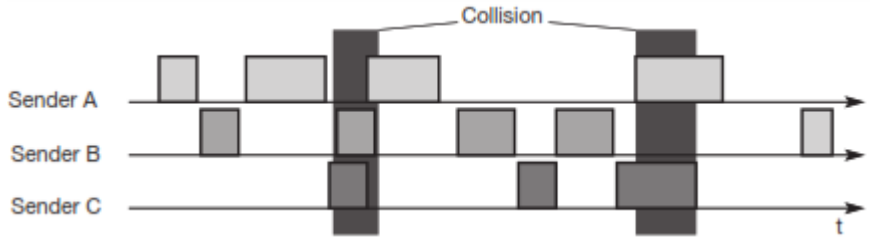



**Fig:2.11 Classical Aloha multiple access**

### 3.3 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 2.12. Still, access is not coordinated.

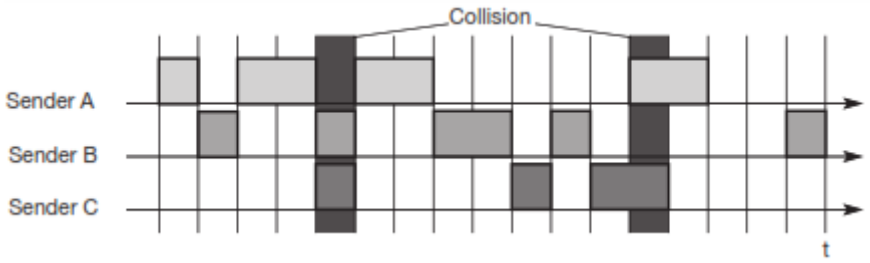



**Fig:2.12 Slotted Aloha multiple access**

Aloha systems work perfectly well under a light load (as most schemes do), but they cannot give any hard transmission guarantees, such as maximum delay before accessing the medium, or minimum throughput. Here one needs additional mechanisms.

### 3.4 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 . 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.

Several variants of CSMA strategy are:

**a)1-persistent CSMA**:- The terminal listens to the channel and waits for transmission until it finds the channel idle.As soon as the channel is idle,the terminal transmits its message with probability one.

**b)non-persistent CSMA:-**After receiving a negative acknowledgement the terminal waits a random time before retransmission of the packet.

**c)p-persistent CSMA:-**It is applied to slotted channels.When a channel is found to be idle, the packet is transmitted in the first available slot with probability p or in the next slot with probability 1-p.

**d)CSMA/CA (carrier sense multiple access with collision avoidance) :-** Here a user monitors its transmission for collisions.If two or more terminals start a transmission at the same time,collision is detected ,and the transmission is immediately aborted in midstream.

### 3.5 Demand assigned multiple access (explicit reservation protocol)

This scheme typically have a **reservation period followed by a transmission period.** During the reservation period, stations can reserve future slots in the transmission period. While, depending on the scheme, collisions may occur during the reservation period, the transmission period can then be accessed without collision.

One basic scheme is **demand assigned multiple access (DAMA)** also called **reservation Aloha,** a scheme typical for satellite systems. DAMA, as shown in Figure 2.13 has two modes. Duringa 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. To maintain the fixed TDM pattern of reservation and transmission, the stations have to be synchronized from time to time. **DAMA is an explicit reservation scheme.**

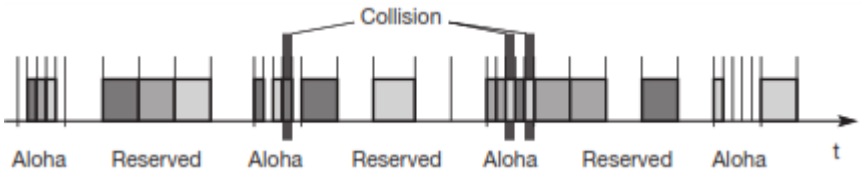



**Fig:2.13 Demand assignment multiple access with explicit reservation**

**3.6 PRMA( packet reservation multiple access)** (implicit reservation protocol)

An example for an implicit reservation scheme is packet reservation multiple access (PRMA). Here, slots can be reserved implicitly according to the following scheme. A certain number of slots forms a frame (Figure 2.14 shows eight slots in a frame). The frame is repeated in time (forming frames one to five in the example), i.e., a fixed TDM pattern is applied.



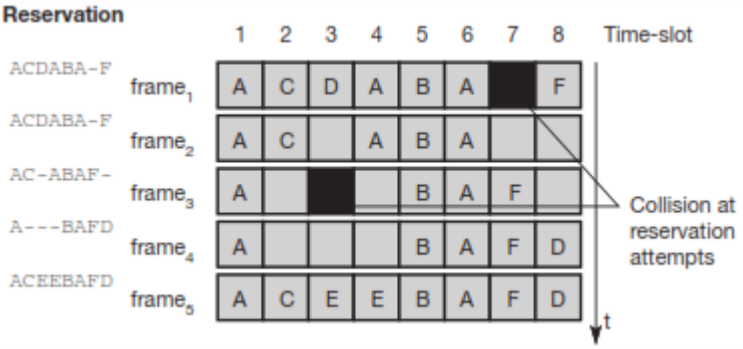



**Fig:2.14 Demand assignment multiple access with implicit reservation**

A base station, which could be a satellite, now broadcasts the status of each slot (as shown on the left side of the figure) to all mobile stations. All stations receiving this vector will then know which slot is occupied and which slot is currently free. In the illustration, a successful transmission of data isindicated by the station's name (A to F). In the example, the base station broadcasts the reservation status 'ACDABA-F' to all stations, here A to F. This means that slots one to six and eight are occupied, but slot seven is free in the following transmission. All stations wishing to transmit can now compete forthis free slot in Aloha fashion. The already occupied slots are not touched. In the example shown, more than one station wants to access this slot, so a collision occurs. The base station returns the reservation

status ‘ACDABA-F’, indicating that the reservation of slot seven failed (still indicated as free) and that nothing has changed for the other slots. Again, stations can compete for this slot. Additionally, station D has stopped sending in slot three and station F in slot eight. This is noticed by the base station after the second frame.

### 3.7 Reservation TDMA

An even more fixed pattern that still allows some random access is exhibited by reservation TDMA (see Figure 2.15). In a fixed TDM scheme N mini-slots followed by N·k data-slots form a frame that is repeated. Each station is allotted its own mini-slot and can use it to reserve up to k data-slots. This guarantees each station a certain bandwidth and a fixed delay. Other stations can now send data in unused data-slots as shown. Using these free slots can be based on a simple round-robin scheme or can be uncoordinated using an Aloha scheme.

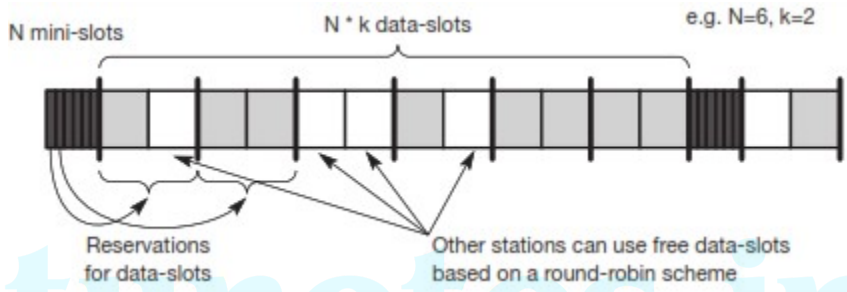



**Fig:2.15 Reservation TDMA access scheme**

**3.8 Multiple access with collision avoidance(**solution to hidden and exposed terminal problem) Multiple access with collision avoidance (MACA) presents a simple scheme that solves the hiddenterminal problem. Figure 2.16 shows a scenario where A and C both want to send to B. A has alreadystarted the transmission, but is hidden for C, C also starts with its transmission, thereby causing acollision at B.

With MACA, A does not start its transmission at once, but sends a **request to send (RTS)** first. B receives the **RTS that contains the name of sender and receiver, as well as the length of the future transmission**. This RTS is not heard by C, but triggers an acknowledgement from B, called **clear to send (CTS).** The CTS again contains the names of sender (A) and receiver (B) of the user data, and the length of the future transmission. This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission. After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS toward B. A collision cannot occur at B during data transmission, and the hidden terminal problem is solved.

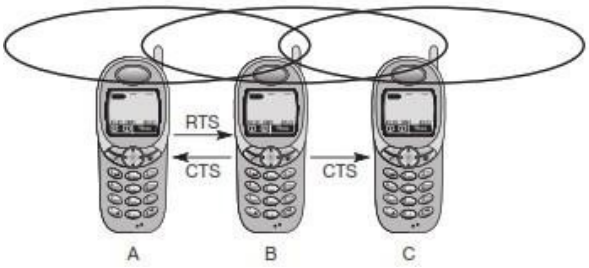



**Fig:2.16 MACA can avoid hidden terminals**

Can MACA also help to solve the 'exposed terminal' problem? With MACA, B has to transmit an RTS first (as shown in Figure 2.17) containing the name of the receiver (A) and the sender (B). C does not react to this message as it is not the receiver, but A acknowledges using a CTS which identifies B as the sender and A as the receiver of the following data transmission. C does not receive this CTS and concludes that A is outside the detection range. C can start its transmission assuming it will not cause a collision at A. The problem with exposed terminals is solved without fixed access patterns or a base station. **One problem of MACA is clearly the overheads associated with the RTS and CTS transmissions.**



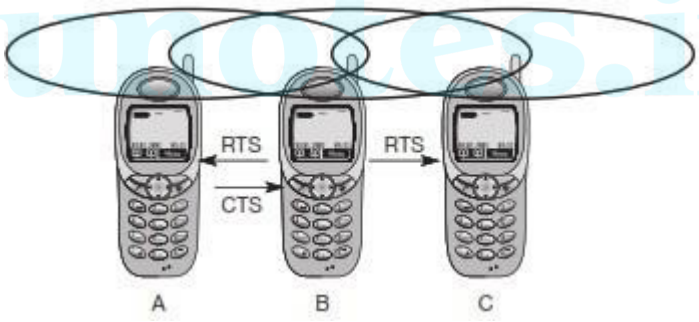



**Fig:2.17 MACA can avoid exposed terminals**

Figure 2.18 shows simplified state machines for a sender and receiver. The sender is idle until a user requests the transmission of a data packet. The sender then issues an RTS and waits for the right to send. If the receiver gets an RTS and is in an idle state, it sends back a CTS and waits for data. The sender receives the CTS and sends the data. Otherwise, the sender would send an RTS again after a time-out (e.g., the RTS could be lost or collided). After transmission of the data, the sender waits for a positive acknowledgement to return into an idle state. The receiver sends back a positive acknowledgement if the received data was correct. If not, or if the waiting time for data is too long, the receiver returns into idle state. If the sender does not receive any acknowledgement or a negative acknowledgement, it sends an RTS and again waits for the right to send. Alternatively, a receiver could indicate that it is currently busy via a separate Rx Busy.

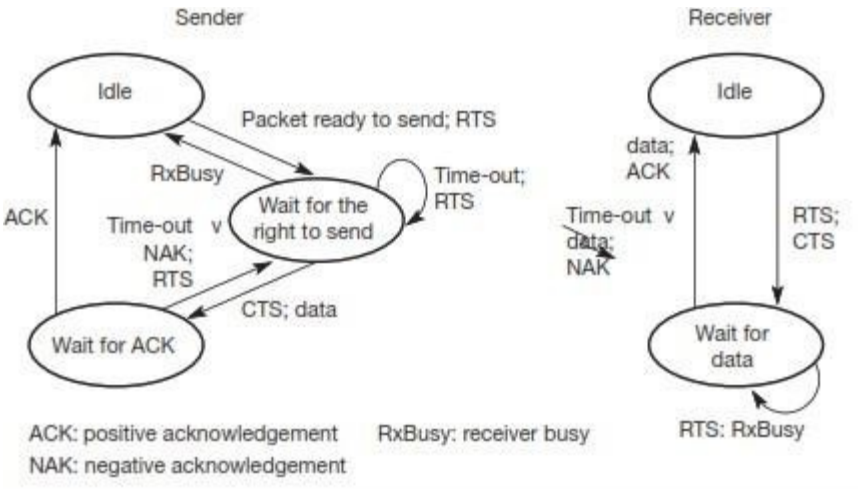



**Fig:2.18 Protocol machines for multiple access with collision avoidance**

### 3.9 Polling

Where one station is to be heard by all others (e.g., the base station of a mobile phone network or any other dedicated station), polling schemes (known from the mainframe/terminal world) can be applied. **Polling is a strictly centralized scheme with one master station and several slave stations.** The master can poll the slaves according to many schemes: round robin , randomly, according to reservationsetc. The master could also establish a list of stations wishing to transmit during a contention phase. Afterthis phase, the station polls each station on the list. Similar schemes are used, e.g., in the Bluetooth wireless LAN.



### 3.10 Inhibit sense multiple access[digital sense multiple access (DSMA)]

Another combination of different schemes is represented by **inhibit sense multiple access (ISMA)**. This scheme, which is used for the packet data transmission service is also known as digital sense multiple access (DSMA). Here, the base station only signals a busy medium via a busy tone (called BUSY/IDLE indicator) on the downlink . After the busy tone stops, accessing the uplink is not coordinated any further. The base station acknowledges successful transmissions, a mobile station detects a collision onlyvia the missing Positive acknowledgement. In case of collisions, additional back-off and retransmission mechanisms are implemented.

## CELLULAR SYSTEMS

Cellular systems for mobile communications implement SDM. Each transmitter, typically called a base station, covers a certain area, a cell. Cell radii can vary from tens of meters in buildings, and hundreds of meters in cities, up to tens of kilometers in the countryside. Each cellular base station is allocated a group of radio channels to be used within a small geographic area called a **cell.** Base stations in adjacent cells are assigned channel groups which contain completely different channels than neighboring cells. The base station antennas are designed to achieve the desired coverage within the particular cell. By limiting the coverage area to within

the boundaries of a cell, the same group of channels may be used to cover different cells that are separated from one another by distances large enough to keep interference levels within tolerable limits. The design process of selecting and allocating channel groups for all of the cellular base stations within a system is called **frequency reuse or frequency planning**.

Figure 2.19 illustrates the concept of cellular frequency reuse, where cells labeled with the same letter use the same group of channels. The frequency reuse plan is overlaid upon a map to indicate where different frequency channels are used. The hexagonal cell shape shown in .Figure 2.19 is conceptual and is a simplistic model of the radio coverage for each base station. The actual radio coverage of a cell is known as the **footprint.**

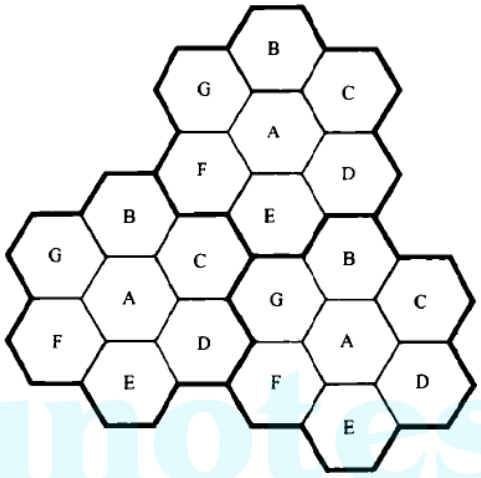





**Fig:2.19 Illustration of the cellular frequency reuse concept. Cells with the sameFig:2.19 Illustration of the cellular frequency reuse concept. Cells with the same set of frequencies. A cell cluster is outlined in bold and replicated over the coverage**

**area. In this example, the cluster size, N, is equal to seven, and the frequency reuse factor is 1/7 since each cell contains one-seventh of the total number of available channels.**

A cell must be designed to serve the weakest mobiles within the footprint, and these are typically located at the edge of the cell. When using hexagons to model coverage areas, base station transmitters are depicted as either being in the center of the cell (center-excited cells) or on three of the six cell vertices (edge-excited cells).

'To understand the frequency reuse concept, consider a cellular system which has a total of S duplex channels available for use. If each cell is allocated a group of k channels (k < S), and if the S channels are divided among N cells into unique and disjoint channel groups which each have the same number of

channels, the total number of available radio channels can be expressed as, **S = kN**

The N cells which collectively use the complete set of available frequencies is called a cluster. If a cluster is replicated M times within the system, the total number of duplex channels, C, can be used as a measure of capacity and is given **C = MkN = MS.**

**Handoff Strategies**

When a mobile moves into a different cell while a conversation is in progress, the MSC automatically transfers the call to a new channel belonging to the new base station. This handoff operation not only involves a new base station, but also requires that the voice and control signals be allocated to channels associated with the new base station. Handoffs must be performed successfully and as infrequently as possible, and be imperceptible to the users. In orderto meet these requirements, system designers must specify an optimum signal level at which to initiate a handoff. Once a particular signal level is specified as the minimum usable signal for acceptable voice quality at the base station receiver (normally taken as between —90 dBm and—100 dBm), a slightly stronger signal level is used as a threshold at which a handoff is made. This margin, given by $\Delta = P_{r\ handoff} - P_{r\ minimum\ usable}$ cannot be too large or too small. If $\Delta$ is too large, unnecessary handoffs which burden the MSC may occur, and if $\Delta$ is too small, there may be insufficient time to complete a handoff before a call is lost due to weak signal conditions. Therefore, $\Delta$ is chosen carefully to meet these conflicting requirements.

Figure 2.21 illustrates a handoff situation. Figure 2.21(a) demonstrates the case where a handoff is not made and the signal drops below the minimum acceptable level to keep the channel active. This dropped call event can happen when there is an excessive delay by the MSC in assigning a handoff, or when the threshold $\Delta$ is set too small for the handoff time in the system. Excessive delays may occur during high traffic conditions due to computational loading at the MSC or due to the fact that no channels are available on any of the nearby base stations (thus forcing the MSC to wait until a channel in
a nearby cell becomes free).

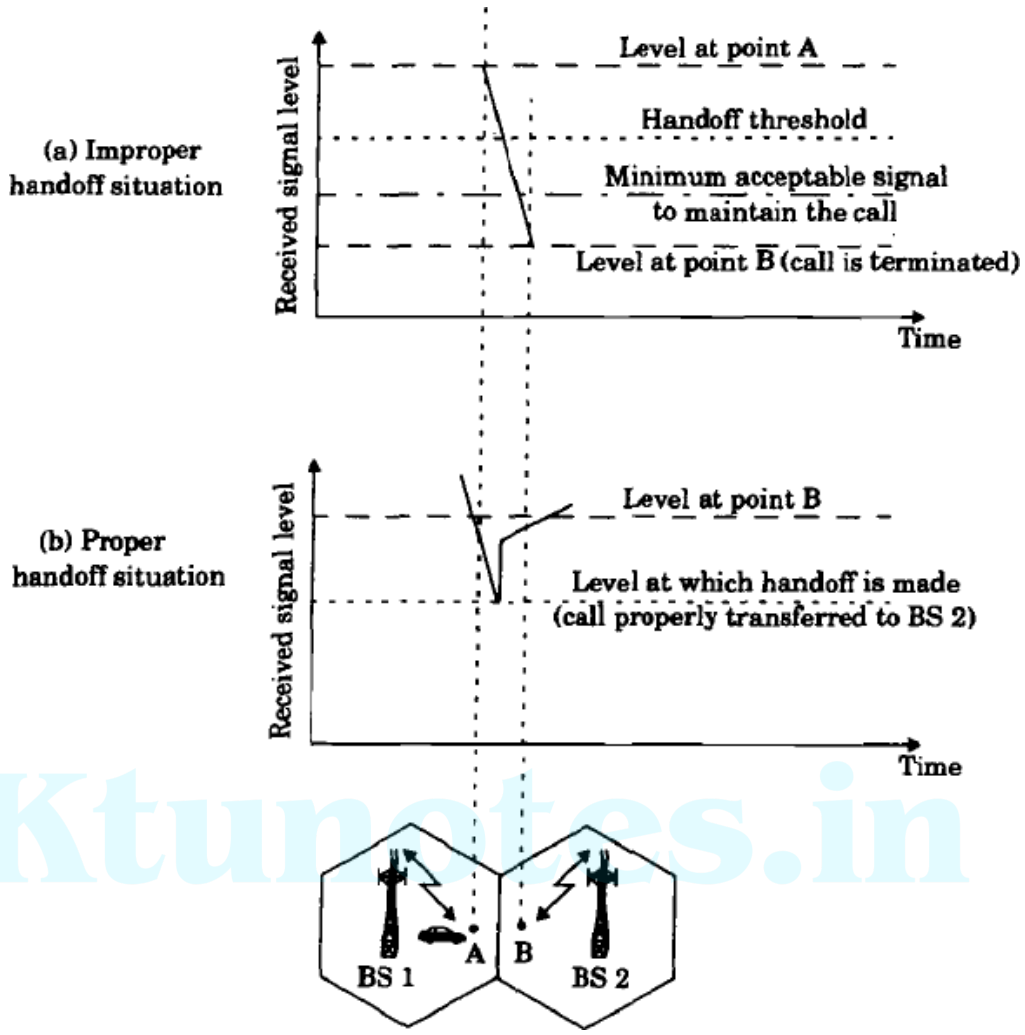



**Fig:2.21 Illustration of a handoff scenario at cell boundary.**

**Dwell time**: The time over which a call may be maintained within a cell, without handoff, is called the dwell time. The dwell time of a particular user is governed by a number of factors, which include propagation, interference, distance between the subscriber and the base station, and other time varying effects.

In first generation analog cellular systems, signal strength measurements are made by the base stations and supervised by the MSC. Each base station constantly monitors the signal strengths of all of its reverse voice channels to determine the relative location of each mobile user with respect to the base station tower. In addition to measuring the RSSI of calls in progress within thecell, a spare receiver in each base station, called the **locator receiver**, is used to determine signal strengths of mobile users which are in neighboring cells. The locator receiver is controlled by the MSC and is used to monitor the signal strength of users in neighboring cells which appear to be in need of handoff and reports all RSSI values to the MSC. Based on the locator receiver signal strength information from each base station, the MSC decides if a handoff is necessary or not.

In second generation systems that use digital TDMA technology, handoff decisions are mobile assisted. In **mobile assisted handoff(MAHO)**, every mobile station measures the receivedpower from surrounding base stations and continually reports the results of these measurements to the serving base station. A handoff is initiated when the power received from the base station of a neighboring cell begins to exceed the power received from the current base station by a certain level or for a certain period of time. The MAHO method enables the call to be handed over between base stations at a much faster rate than in first generation analog systems since the handoff measurements are made by each mobile, and the MSC no longer constantly monitors signal strengths.

During the course of a call, if a mobile moves from one cellular system to a different cellular system controlled by a different MSC, an intersystem handoff becomes necessary An MSC engages in an **intersystem handoff(roaming)** when a mobile signal becomes weak in a given cell and the MSC cannot find another cell within its system to which it can transfer the call in progress. **Prioritizing Handoffs**

One method for giving priority to handoffs is called the **guard channel** concept, whereby a fraction of the total available channels in a cell is reserved exclusively for handoff requests from ongoing calls which may be handed off into the cell. This method has the disadvantage of reducing the total carried traffic, as

fewer channels are allocated to originating calls. **Queuing of handoff requests** is another method to decrease the probability of forced termination of a call due to lack of available channels.

**Practical Handoff Considerations**

**a)The umbrella cell approach**

High speed vehicles pass through the coverage region of a cell within a matter of seconds, whereas pedestrian users may never need a handoff during a call. By using different antenna heights (often on the same building or tower) and different power levels, it is possible to provide "large" and "small" cells which are co-located at a single location. This technique is called the **umbrella cell approach** and is used to provide large area coverage to high speed users while providing small area coverage to users traveling at low speeds. The umbrella cell approach ensures that the number of handoffs is minimized for high speed users and provides additional microcell channels for pedestrian users.

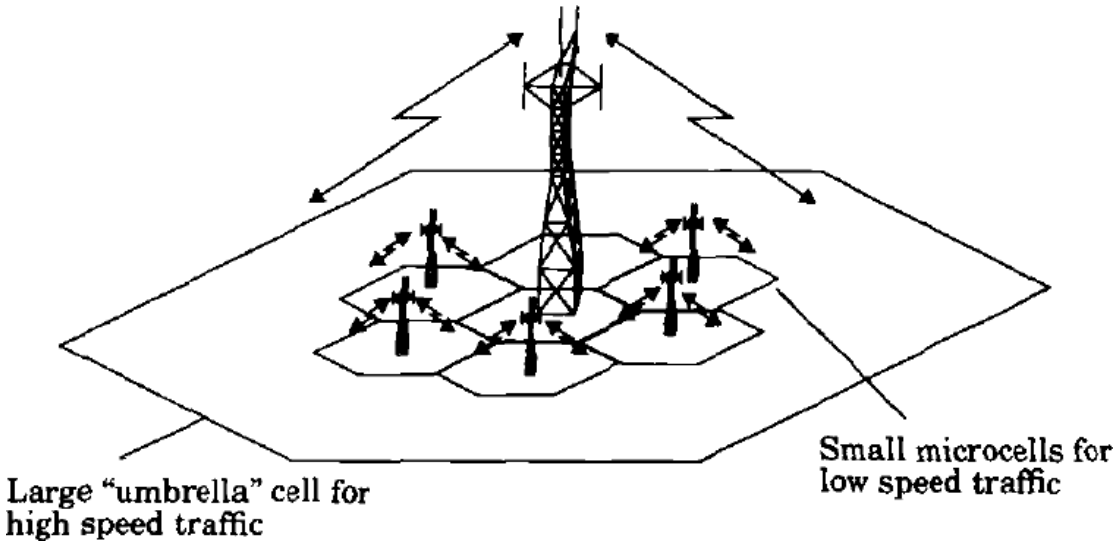



**Fig:2.22 The Umbrella cell approach**

**b)Cell dragging**

Another practical handoff problem in microcell systems is known as cell dragging. Cell dragging results from pedestrian users that provide a very strong signal to the base station. Such a situation occurs in an urban environment when there is a line-of-sight (LOS) radio path between the subscriber and the base station. As the user travels away from the base station at a very slow speed, the average signal strength does not decay rapidly. Even when the user has traveled well beyond the designed range of the cell, the received signal at the base station may be above the handoff threshold, thus a handoff may not be made. This creates a potential interference and traffic management problem, since the user has meanwhile traveled deep within a neighboring cell.

## SATELLITE SYSTEMS

Satellites offer global coverage without wiring costs for base stations and are almost independent of varying population densities. The high speed of satellites with a low altitude raises new problems for routing, localization of mobile users, and handover of communication links. The first commercial geostationary communication satellite INTELSAT 1 (also known as 'Early Bird') went into operation in 1965. It was in service for one-and-a-half years, weighed 68 kg and offered 240 duplex telephone channels or, alternatively, a single TV channel.

Applications

Traditionally, satellites have been used in the following areas:

● Weather forecasting: Several satellites deliver pictures of the earth using, e.g., infrared 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.

● Military satellites: 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.
● Global telephone backbones: One of the first applications of satellites for communication was the establishment of international telephone backbones. Instead of using cables it was sometimes faster to launch a new satellite (aka 'big cable in the sky').
● 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.

Figure 2.27 shows a classical scenario for satellite systems supporting global mobile communication. Depending on its type, each satellite can cover a certain area on the earth with its beam (the so-called 'footprint' ). Within the footprint, communication with the satellite is possible for 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.



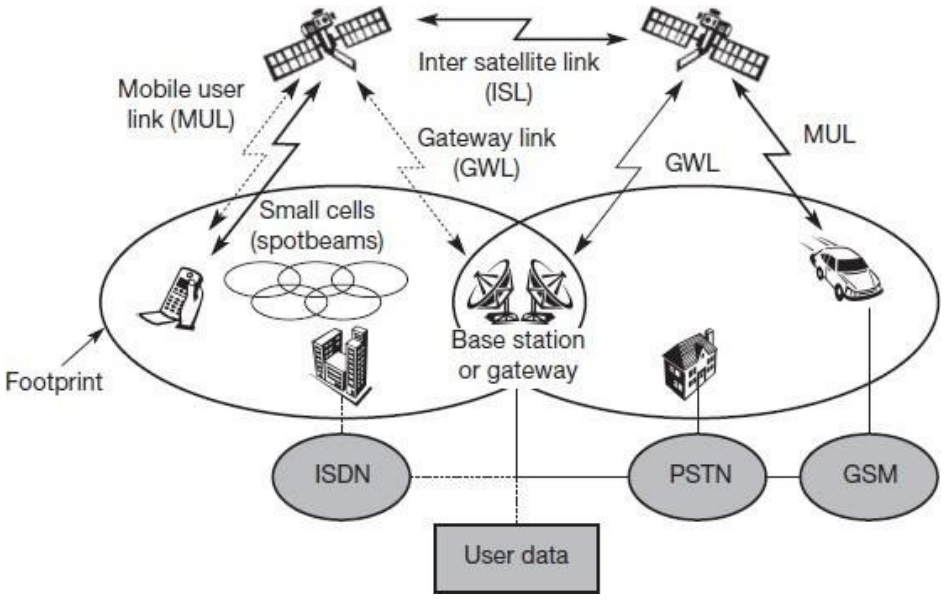



**Fig:2.27 Typical satellite system for global mobile telecommunications**

**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 surfacefollowing a simple law:

- The attractive force $F_g$ of the earth due to gravity equals $m \cdot g \cdot (R/r)2$.
- The centrifugal force $F_c$ 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 $\omega$ 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:

- $F_g = F_c$, i.e., both forces must be equal.
- 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



Important parameters in satellite communication are the **inclination and elevation angles**. The inclination angle δ (see Figure 2.28) is defined as the angle between the equatorial plane and the plane described by the satellite orbit. An inclination angle of 0 degrees means that the satellite is exactly above the equator.

If the satellite does not have a circular orbit, the closest point to the earth is called the **perigee.** The elevation angle ε (see Figure 2.29) is defined as the angle between the center of the satellite beam and the plane tangential to the earth's surface. A so called footprint can be defined as the area on earth where the signals of the satellite can be received.

**Fig:2.29**

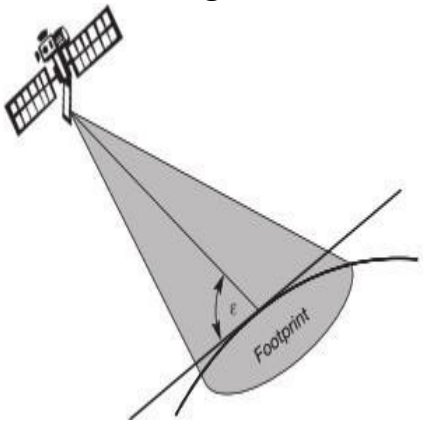
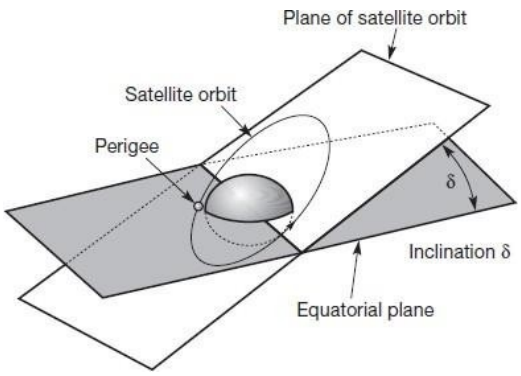



**Fig:2.28**



Four different types of orbits can be identified as shown in Figure 2.30:

● **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 reasons

● **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 communicationquality.

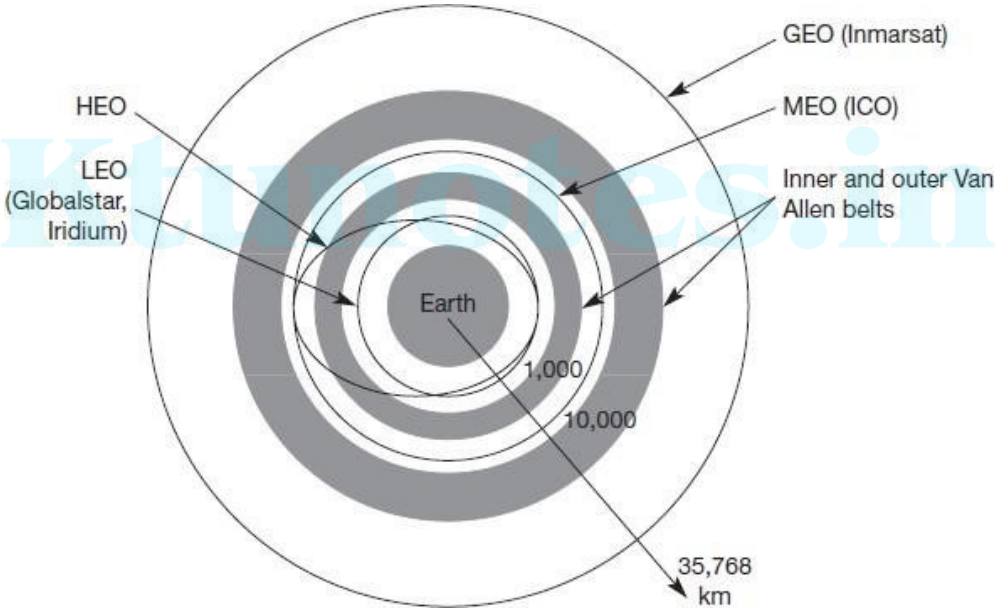



**Fig:2.30 Different types of satellite orbits**

## GEO

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·R2/(2·π·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.

● Advantages: 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.

● Disadvantages: Northern or southern regions of the earth have more problems receiving these satellites due to the low elevation above a latitude of 60°, i.e., larger antennas are needed in this case. Shading of the signals in cities due to high buildings and the low elevation further away from the equator limit transmission quality. The transmit power needed is relatively high (some 10 W) which causes problems for battery powered devices. These satellites cannot be used for small mobile phones. The biggest problem for voice and also data communication is the high latency of over 0.25 s one-way – many retransmission schemes which are known from fixed networks fail. Due to the large footprint, either frequencies cannot be reused or the GEO satellite needs special antennas focusing on a smaller footprint. Transferring a GEO into orbit is very expensive.

## 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.

● Disadvantages: The biggest problem of the LEO concept is the need for many satellites if global coverage is to be reached. Several concepts involve 50–200 or even more satellites in orbit. The short time of visibility with a high elevation requires additional mechanisms for connection handover between different satellites. (Different cases for handover are explained in section 5.4.) The high number of satellites combined with the fast movements results in a high complexity of the whole satellite system. One general problem of LEOs is the short lifetime of about five to eight years due to atmospheric drag and radiation from the inner Van Allen belt. Assuming 48 satellites and a lifetime of eight years (as expected for the system Globalstar), anew satellite would be needed every two months. The low latency via a single LEO is only halfof the story. Other factors are the need for routing of data packets from satellite to satellite (or several times from base stations to satellites and back) if a user wants to communicate around the

world. Due to the large footprint, a GEO typically does not need this type of routing, as senders and receivers are most likely in the same footprint.

## 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.

## TELECOMMUNICATION SYSTEMS- GSM

GSM is the most successful digital mobile telecommunication system in the world today. 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 group special mobile (GSM)was founded in 1982. This system was soon named the **global system for mobile communications (GSM).**



**Services offered by GSM**

**1.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 2.31 shows a reference model for GSM services. A mobile station MS is connected to the GSM public land mobile network (PLMN) via the Um interface. (GSM-PLMN is the infrastructure needed for the GSM network.) This networkis connected to transit networks, e.g., integrated services digital network (ISDN) or traditional public switched telephone network (PSTN). There might be an additional network, the source/destination network, before another terminal TE is connected. Bearer services now comprise all services that enable the transparent transmission of data between the interfaces to the network, i.e., S in case of the mobile station. Interfaces like U, S, and R in case of ISDN have not been defined for all networks, so it depends on the specific network which interface is used as a reference for the transparent transmission of data. Within the mobile station MS, the mobile termination (MT) performs all network specific tasks (TDMA, FDMA, coding etc.) and offers an interface for data transmission

(S) to the terminal TE which can then be network independent. Depending on the capabilities of TE, further interfaces may be needed, such as R, according to the

ISDN reference model . Tele services are application specific and may thus need all seven layers of the ISO/OSI reference model. These services are specified end-to-end, i.e., from one terminal TE to another.

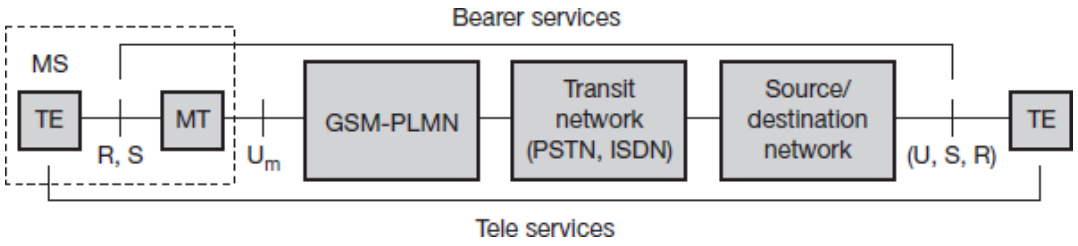



**Fig:2.31 Bearer and teleservices reference model**

**1.1 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. The only mechanism to increase transmissionquality is the use of forward error correction (FEC), which codes redundancy into the data stream and helps to reconstruct the original data in case of transmission errors. Depending on the FEC, data rates of 2.4, 4.8, or 9.6 kbit/s are possible. Transparent bearer services do not try to recover lost data in case of, for example, shadowing or interruptions due to handover. Non-transparent bearer services use protocols of layers two and three to implement error correction and flow control. These services use the transparent bearer services, adding a radio link protocol (RLP). This protocol comprises mechanisms of high-level data link control (HDLC), and special selective-reject mechanisms to trigger retransmission of erroneous data.

**1.2Tele 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.

A useful service for very simple message transfer is the **short message service (SMS)**, which offers transmission of messages of up to 160 characters. SMS messages do not use the standard

data channels of GSM but exploit unused capacity in the signaling channels. Sending and receiving of SMS is possible during data or voice transmission.

The successor of SMS, the **enhanced message service (EMS)**, offers a larger message size (e.g., 760 characters, concatenating several SMs), formatted text, and the transmission of animated pictures, small images and ring tones in a standardized way (some vendors offered similar proprietary features before). EMS never really took off as the **multimedia message service(MMS)** was available. MMS offers the transmission of larger pictures (GIF, JPG, WBMP), short video clips etc.

**1.3Supplementary 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.

**System architecture**

Figure 2.32 gives a simplified overview of the GSM system. A GSM system consists of three subsystems, the **radio sub system (RSS)**, the **network and switching subsystem (NSS)**, and the **operation subsystem (OSS)**.

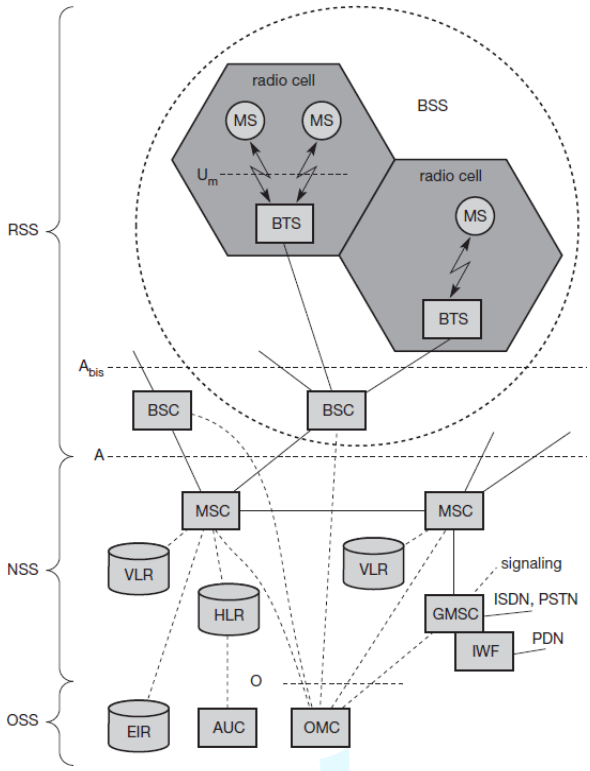



**Fig:2.32 Functional architecture of a GSM system**

**1 Radio subsystem**

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 2.32 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. A BTS can form a radio cell or, using sectorized antennas, several cells , and is connected to MS via the Um interface , and to the BSC via the Abis interface. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.) and will be discussed in more detail below. The Abis interface consists of 16 or 64 kbit/s connections. A GSM cell can measure between some 100 m and 35 km depending on the environment (buildings, open space, mountains etc.) but also expected traffic.

● **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. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.

Table below gives an overview of the tasks assigned to the BSC and BTS or of tasks in which these entities support other entities in the network.

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



- **Mobile station (MS):** The MS 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. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible.

The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key Ki, and the international mobile subscriber identity (IMSI). The PIN is used to unlock the MS. Using the wrong PIN three times will lock the SIM. In such cases, the PUK is needed to unlock the SIM.

The MS stores dynamic information while logged onto the GSM system, such as, e.g., the cipher key Kc and the location information consisting of a temporary mobile subscriber identity (TMSI) and the location area identification (LAI).

**2 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. Typically, an MSC manages several BSCs in a geographical region. A **gateway MSC (GMSC)** has additional connections to other fixed networks, such as PSTN and ISDN. 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 signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls). Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three- way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.

● **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). Dynamicinformation is also needed, e.g., the current location area (LA) of the MS, the mobile subscriber roaming

● number (MSRN), the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized databases which must fulfill certain real- time requirements to answer requests within certain time-bounds.

● **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 (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information. Some VLRs in existence, are capable of managing up to one million customers.

**3. Operation subsystem**

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. The following entities have been defined:

● **Operation and maintenance center (OMC):** The OMC monitors and controls all other network entities via the O interface. Typical OMC management functions are traffic monitoring,

status reports of network entities, subscriber and security management, or accounting and billing.
**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. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible (the reader may speculate as to why this is the case). The EIR also contains a list of valid IMEIs **(white list),** and a list of malfunctioning devices **(gray list).**

**Radio interface**

The most interesting interface in a GSM system is Um , the radio interface, as it comprises many mechanisms for multiplexing and media access. GSM implements SDMA using cells with BTS and assigns an MS to a BTS. Furthermore, FDD is used to separate downlink and uplink. Media access combines TDMA and FDMA. In GSM 900, 124 channels, each 200 kHz wide, are used for
FDMA.



Figure 2.33 also shows the TDM used. Each of the 248 channels is additionally separated in time via a GSM TDMA frame, i.e., each 200 kHz carrier is subdivided into frames that are repeated continuously. The duration of a frame is 4.615 ms. A frame is again subdivided into 8 GSM time slots, where each slot represents a physical TDM channel and lasts for 577 µs. Each TDM channel occupies the 200 kHz carrier for 577 µs every 4.615 ms. Data is transmitted in small portions, called bursts. Figure 2.33 shows a so called **normal burst** as used for data transmissioninside a time slot (user and signaling data). In the diagram, the burst is only 546.5 µs long and contains 148 bits. The remaining 30.5 µs are used as guard space to avoid overlapping with otherbursts due to different path delays and to give the transmitter time to turn on and off. Filling the whole slot with data allows for the transmission of 156.25 bit within 577 µs.
The first and last three bits of a normal burst (tail) are all set to 0 and can be used to enhance the receiver performance. The **training sequence** in the middle of a slot is used to adapt theparameters of the receiver to the current path propagation characteristics and to select thestrongest signal in case of multi-path propagation. A flag **S** indicates whether the data field contains user or network control data. Apart from the normal burst, ETSI defines four morebursts for data transmission: a **frequency correction burst** allows the MS to correct the local oscillator to avoid interference with neighboring channels, a **synchronization burst** with an extended training sequence synchronizes the MS with the BTS in time, an **access burst** is

used

for the initial connection setup between MS and BTS, and finally a **dummy burst** is used if no data is available for a slot.

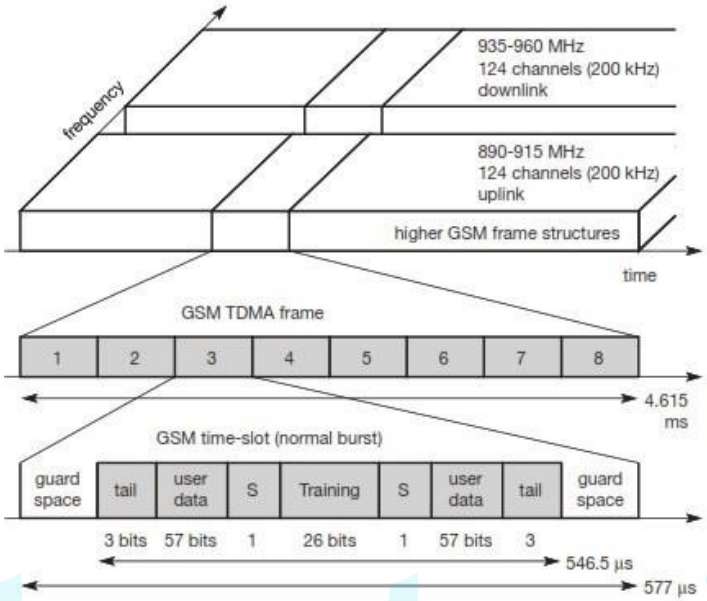



**Fig:2.33GSM TDMA frame, slots, and**



**bursts Logical channels and frame hierarchy**

GSM specifies two basic groups of logical channels, i.e., traffic channels and control channels:

**a)Traffic channels (TCH):** GSM uses a TCH to transmit user data (e.g., voice, fax). Two basic categories of TCHs have been defined, i.e., (TCH/F) and half-rate TCH (TCH/H). A TCH/F has a data rate of 22.8 kbit/s, whereas TCH/H only has 11.4 kbit/s.

**b)Control channels (CCH):** Many different CCHs are used in a GSM system to control medium access, allocation of traffic channels or mobility management. Three groups of control channels have been defined, each again with subchannels

● **Broadcast control channel (BCCH)**: A BTS uses this channel to signal information to all MSs within a cell. Information transmitted in this channel is, e.g., the cell identifier, options available within this cell (frequency hopping), and frequencies available inside the cell and in Neighboring cells. The BTS sends information for frequency correction via the **frequencycorrection channel (FCCH)** and information about time synchronization via the **synchronization channel (SCH)**, where both channels are subchannels of the BCCH.

● **Common control channel (CCCH):** All information regarding connection setup between MS and BS is exchanged via the CCCH. For calls toward an MS, the BTS uses the **paging channel (PCH)** for paging the appropriate MS. If an MS wants to set up a call, it uses the **random access**

**channel (RACH)** to send data to the BTS. The BTS uses the **access grant channel (AGCH)** to signal an MS that it can use a TCH or SDCCH for further connection setup.

- **Dedicated control channel (DCCH):** While the previous channels have all been unidirectional, the following channels are bidirectional. As long as an MS has not established a TCH with the BTS, it uses the **stand-alone dedicated control channel (SDCCH)** with a low data rate (782 bit/s) for signaling. This can comprise authentication, registration or other data needed for setting up a TCH. Each TCH and SDCCH has a **slow associated dedicated control channel (SACCH)** associated with it, which is used to exchange system information, such as thechannel quality and signal power level. Finally, if more signaling information needs to betransmitted and a TCH already exists, GSM uses a **fast associated dedicated control channel (FACCH).** The FACCH uses the time slots which are otherwise used by the TCH. This is necessary in the case of handovers where BTS and MS have to exchange larger amounts of data in less time.

**Localization and calling**

**a) Mobile terminated call (MTC)**

It is a situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station). Figure 2.34 shows the basic steps needed to connect the calling station with the mobile user. In step 1, a user dials the phone number of a GSM subscriber. The fixed network (PSTN) notices (looking at the destination code) that the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC (2). The GMSC identifies the HLR for the subscriber (which is coded in the phone number) and signals the call setup to the HLR (3). The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and requests an MSRN from the current VLR (4). After receiving the MSRN (5), the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC (6). The GMSC can now forward the call setup requestto the MSC indicated (7).

From this point on, the MSC is responsible for all further steps. First, it requests the current status of the MS from the VLR (8). If the MS is available, the MSC initiates paging in all cells it is responsible for (i.e. the location area, LA, 10), as searching for the right cell would be too time consuming (but this approach puts some load on the signaling channels so optimizations exist). The BTSs of all BSSs transmit this paging signal to the MS (11). If the MS answers (12 and 13), the VLR has to perform security checks (set up encryption etc.). The VLR then signals to the MSC to set up a connection to the MS (steps 15 to 17). It is much simpler to perform a mobile originated call (MOC) compared to a MTC (see Figure 2.34).

The MS transmits a request for a new connection (1), the BSS forwards this request to the MSC (2). The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

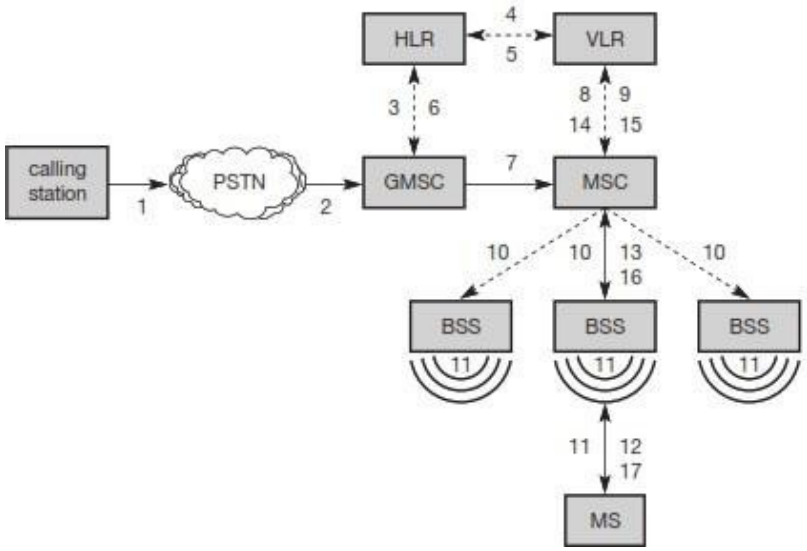



**Fig:2.34 Mobile terminated call (MTC)**

**b)Mobile originated call (MOC)**

It is much simpler to perform a mobile originated call (MOC) compared to a MTC (see Figure 2.35). The MS transmits a request for a new connection (1), the BSS forwards this request to the MSC (2). The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

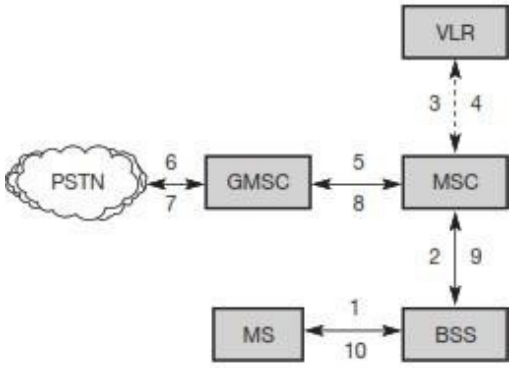



**Fig:2.35 Mobile originated call (MOC)**

**Handover**

Cellular systems require handover procedures, as single cells do not cover the whole service area, but, e.g., only up to 35 km around each antenna on the countryside and some hundred meters in cities. The smaller the cell size and the faster the movement of a mobile station throughthe cells (up to 250 km/h for GSM), the more handovers of ongoing calls are required. However, a handover should not cause a cut-off, also called call drop.

Figure 2.36 shows four possible handover scenarios in GSM:

1. **Intra-cell handover:** Within a cell, narrow-band interference could make transmission at a certain frequency impossible. The BSC could then decide to change the carrier frequency (scenario 1).
2. **Inter-cell, intra-BSC handover:** This is a typical handover scenario. The mobile station moves from one cell to another, but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one (scenario 2).
3. **Inter-BSC, intra-MSC handover:** As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC (scenario 3).
4. **Inter MSC handover:** A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together (scenario 4).

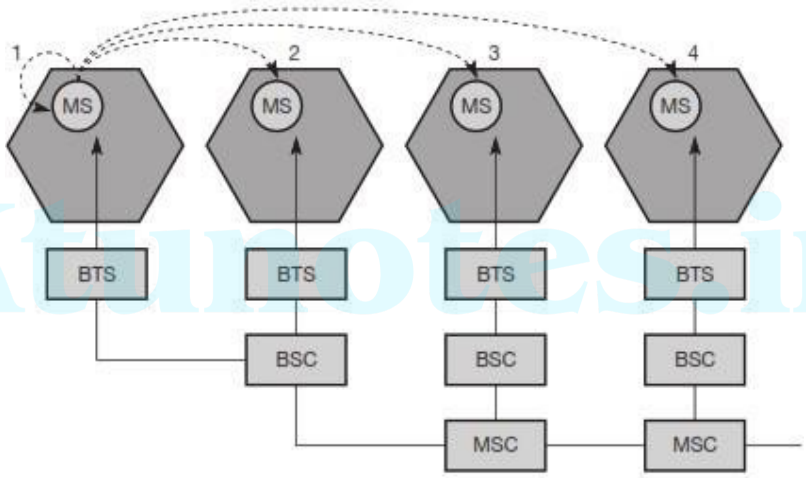



**Fig:2.36 Types of handover in GSM**

## Security

Security in GSM is important to protect the privacy of communication between mobile devices and the network. The security mechanisms in GSM are based on a shared secret key called the "Subscriber Identity Module" (SIM) that is stored on the user's SIM card. The SIM card is a smart card that contains the user's identity and authentication information, including a secret key used to encrypt and decrypt communication. GSM uses several security mechanisms to protect the communication between mobile devices and the network such as,

1. Authentication: The mobile device and the network authenticate each other using the SIM

card's secret key. This prevents unauthorized access to the network.

2. Encryption: GSM uses encryption to protect the privacy of communication between mobile devices and the network. The encryption algorithm used in GSM is called A5, which is used to encrypt voice and data communication.

3. Integrity Protection: GSM also provides integrity protection to ensure that the communication between the mobile device and the network is not tampered with. The integrity protection mechanism uses a Message Authentication Code (MAC) to verify the authenticity of the message.

4. Key management: GSM uses key management to manage the secret keys used for authentication, encryption, and integrity protection. The keys are securely stored on the SIM card and are never transmitted over the air.

**CDMA**

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. But what is a good code for CDMA? A code for a certain user should have a good autocorrelation and should be orthogonal to other codes. Orthogonal in code space has the same meaning as in standard space (i.e., the three dimensional space). Think of a system of coordinates and vectors starting at the origin, i.e., in (0, 0, 0).3 Two vectors are called orthogonal if their inner product is 0, as is the case for the two vectors (2, 5, 0) and (0, 0, 17): (2, 5, 0)*(0, 0, 17) = 0 + 0 + 0 = 0. But also vectors like (3, –2, 4) and (–2, 3, 3) are orthogonal: (3, –2, 4)*(–2, 3, 3) = –6 – 6 + 12 = 0. By contrast, the vectors (1,2,3) and (4,2, –6) are not orthogonal (the inner product is –10), and (1, 2, 3) and (4, 2, –3) are “almost” orthogonal, with their inner product being –1 (which is “close” to zero). Orthogonality cannot be guaranteed for initially orthogonal code

Two senders, A and B, want to send data. CDMA assigns the following unique and

orthogonal key sequences: key Ak = 010011 for sender A, key BK = 110101 for sender B. Sender A wants to send the bit Ad = 1, sender B sends Bd = 0. To illustrate this example, let us assume that we code a binary 0 as –1, a binary 1 as +1. We can then apply the standard addition and multiplication rules.

- Both senders spread their signal using their key as chipping sequence (the term 'spreading' here refers to the simple multiplication of the data bit with the whole chipping sequence). In reality, parts of a much longer chipping sequence are applied to single bits for spreading. Sender A then sends the signal As = Ad*Ak = +1*(–1, +1, –1, –1, +1, +1) = (–1, +1, –1, –1, +1, +1). Sender B does the same with its data to spread the signal with the code: Bs = Bd*Bk = –1*(+1, +1, –1, +1, –1, +1) = (–1, –1, +1, –1, +1, –1).

Both signals are then transmitted at the same time using the same frequency, so, the signals superimpose in space (analog modulation is neglected in this example). Discounting interference from other senders and environmental noise from this simple example, and assuming that the signals have the same strength at the receiver, the following signal C is received at a receiver: C = As + Bs = (–2, 0, 0, –2, +2, 0).



- The receiver now wants to receive data from sender A and, therefore, tunes in to the code of A, i.e., applies A's code for despreading: C*Ak = (–2, 0, 0, –2, +2, 0)*(–1, +1, –1, –1, +1, +1)

= 2 + 0 + 0 + 2 + 2 + 0 = 6. As the result is much larger than 0, the receiver detects a binary 1. Tuning in to sender B, i.e., applying B's code gives C*Bk = (–2, 0, 0, –2, +2, 0)* (+1, +1, –1, +1, –1, +1) = –2 + 0 + 0 – 2 – 2 + 0 = –6. The result is negative, so a 0 has been detected.