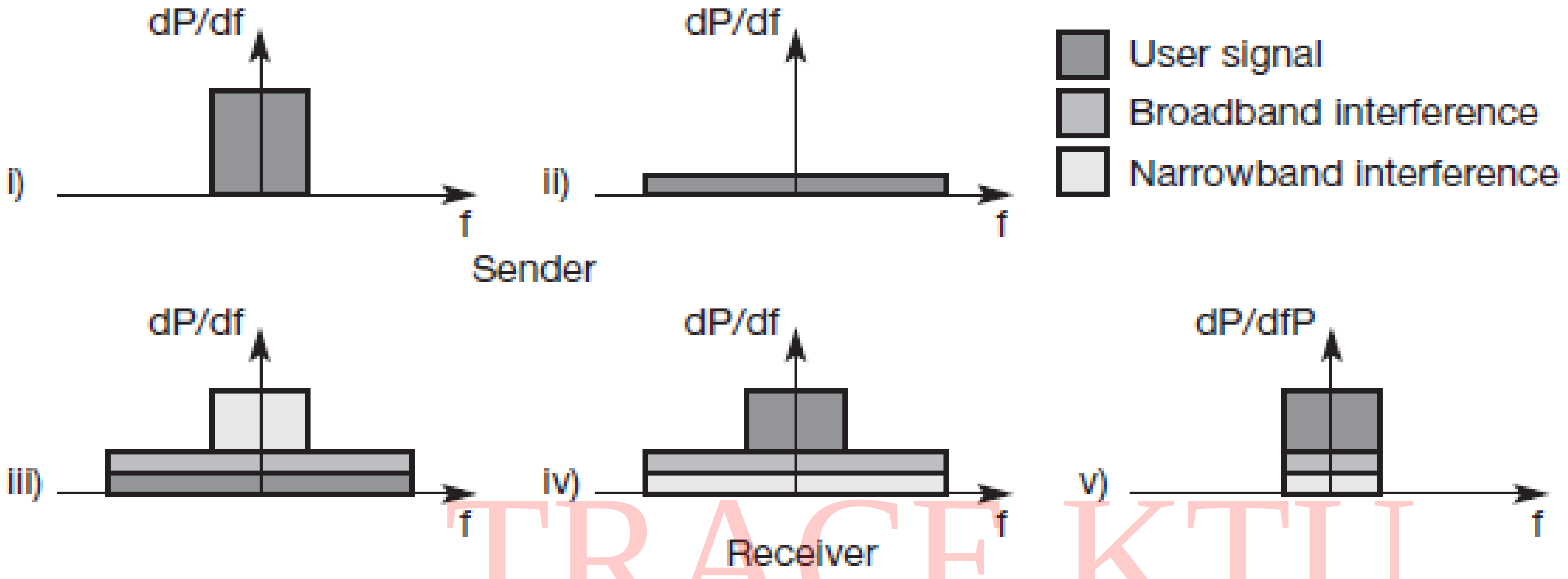
MODULE-2

(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

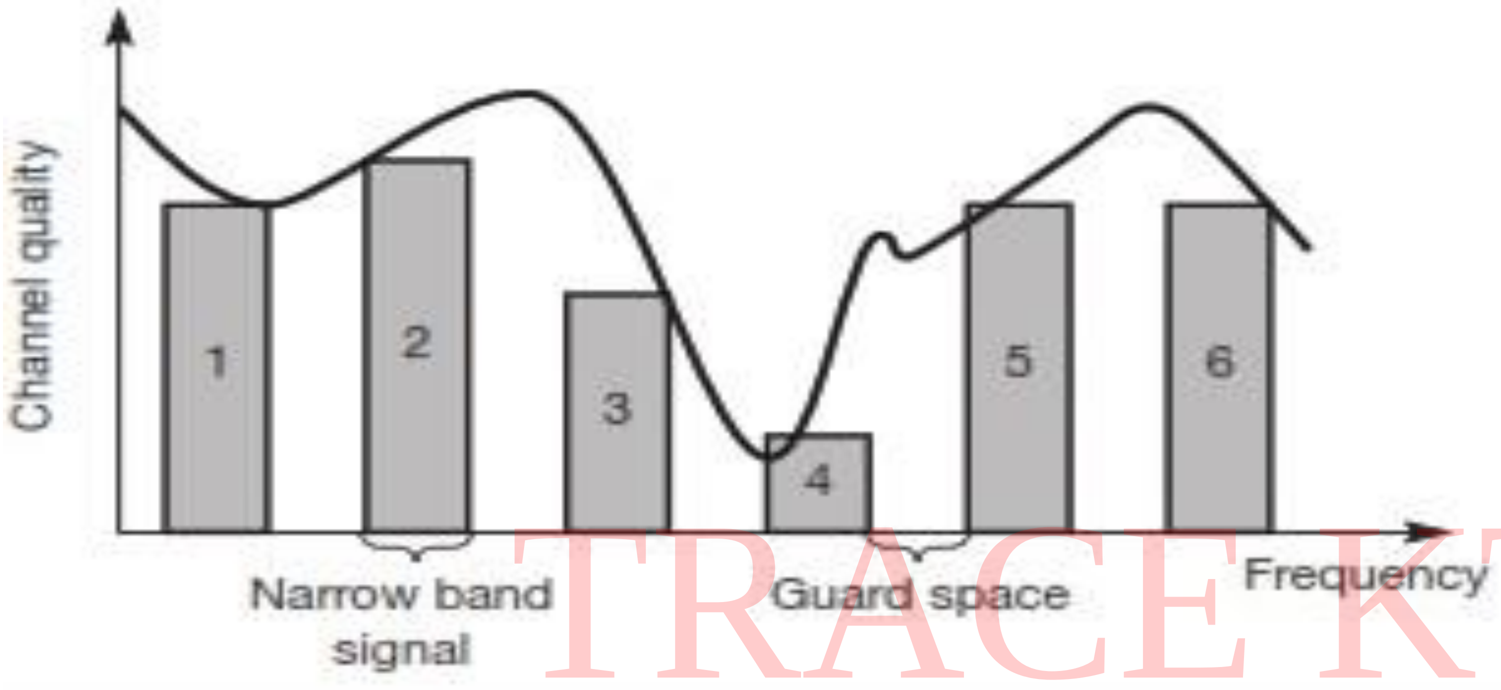
- Spread-spectrum techniques are methods by which a signal (e.g., an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.



i) Idealized narrowband signal from a sender (power density dP/df versus frequency f)
ii) Converts the narrowband signal into a broadband signal (The power level of the spread signal can be much lower than that of the original narrowband signal without losing data)
iii) During transmission, narrowband and broadband interference add to the signal
iv) Convert the spread user signal into a narrowband signal again
v) 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.

.

Narrowband interference without spread spectrum

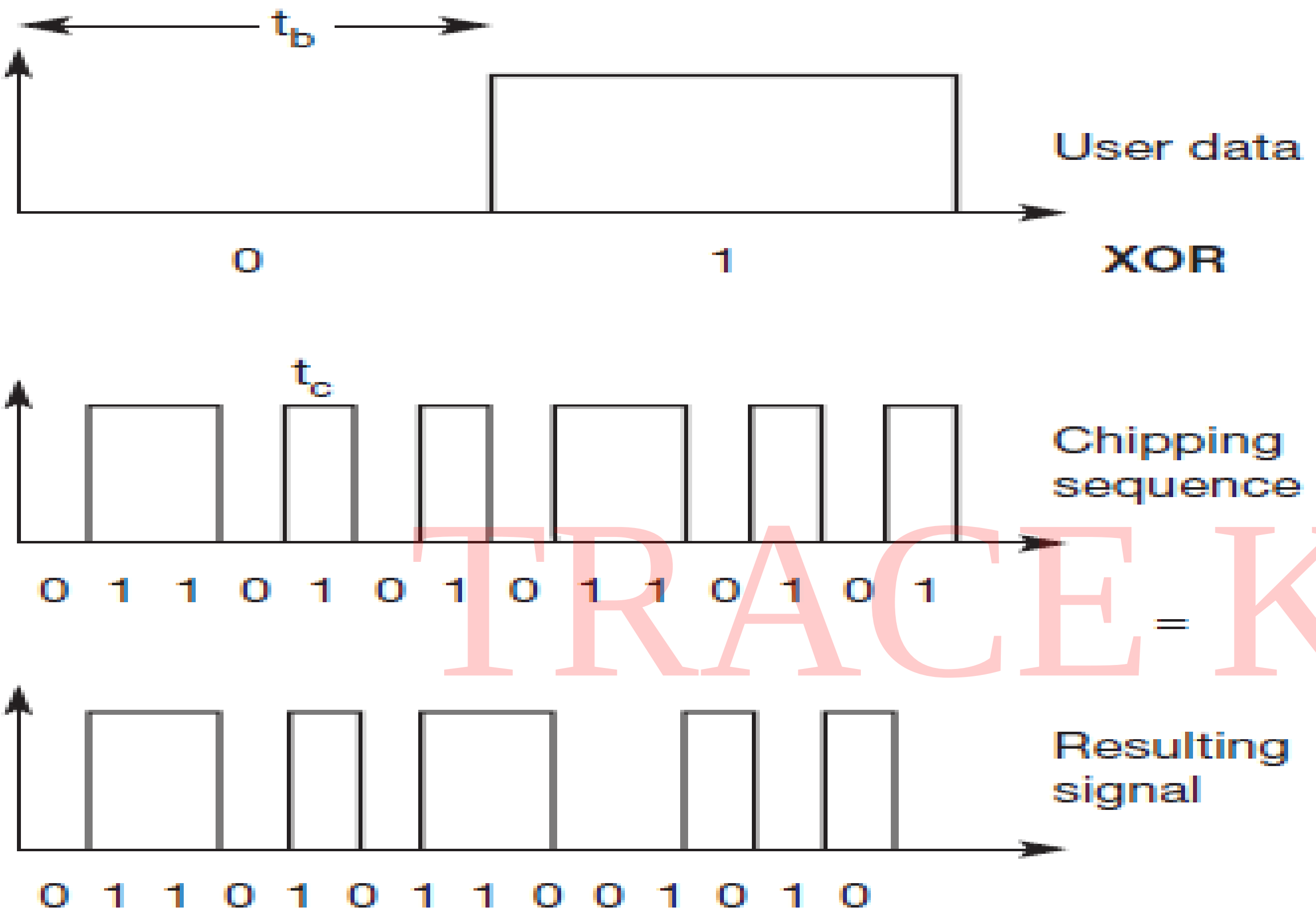


- ➢ Six different channels use FDM for multiplexing, which means that each channel has its own narrow frequency band for transmission.
- ➢ A guard space is needed to avoid adjacent channel interference.
- ➢ Channel quality also changes over time
- ➢ Depending on receiver characteristics, channels 1, 2, 5, and 6 could be received while the quality of channels 3 and 4 is too bad to reconstruct transmitted data

Drawbacks of Spread spectrum technology

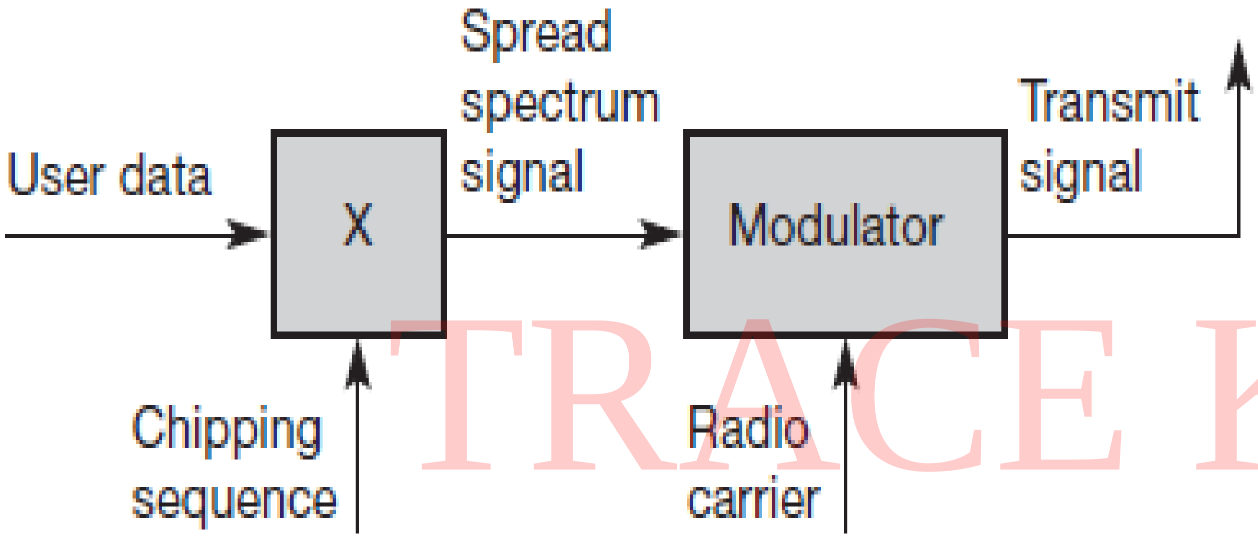
- Increased complexity of receivers that have to despread a signal
- Large frequency band that is needed due to the spreading of the signal.

Direct sequence spread spectrum



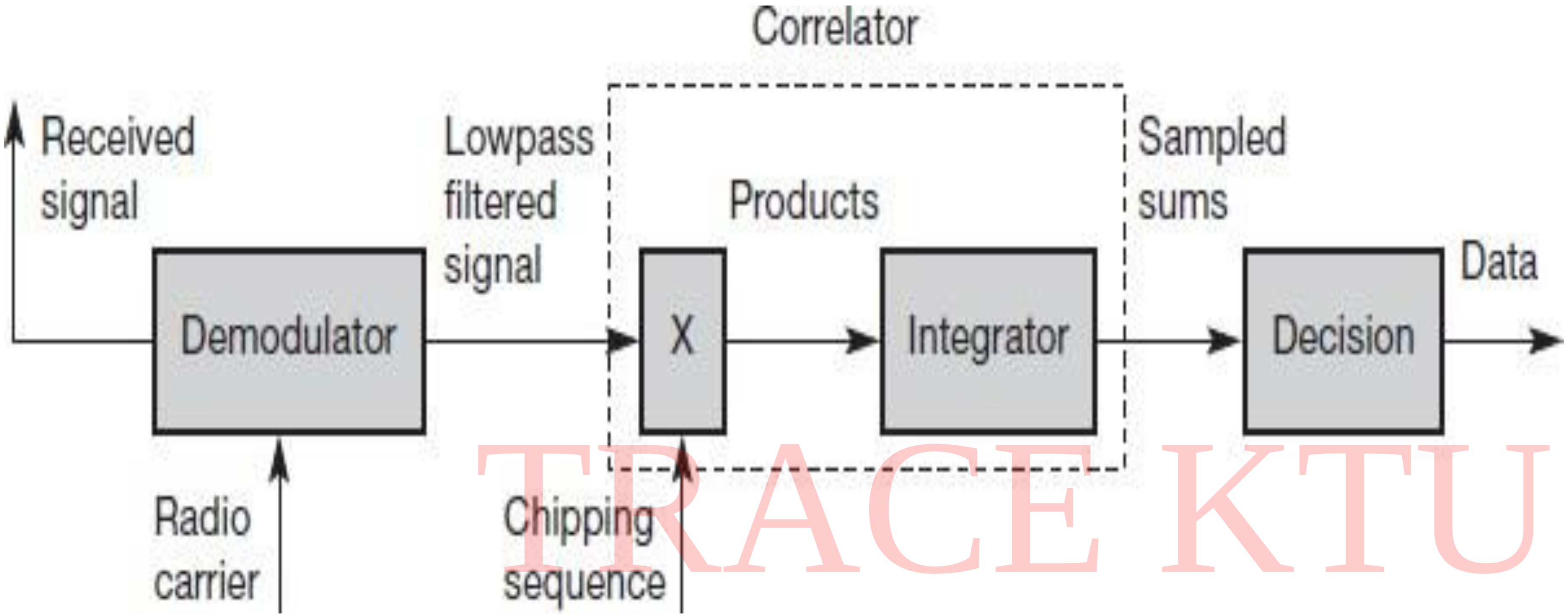
- Direct sequence spread spectrum (DSSS) systems take a user bit stream and perform an (XOR) with a so-called chipping sequence
- 0110101 (Bit=0) or 1001010 (Bit=1)
- Each user bit has a duration tb,
- The chipping sequence consists of smaller pulses, called chips, with a duration tc.
- If the chipping sequence is generated properly it appears as random noise also called pseudo-noise sequence.

DSSS transmitter



- Spreading of the user data with the chipping sequence (digital modulation)
- The spread signal is then modulated with a radio carrier (radio modulation)
- 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

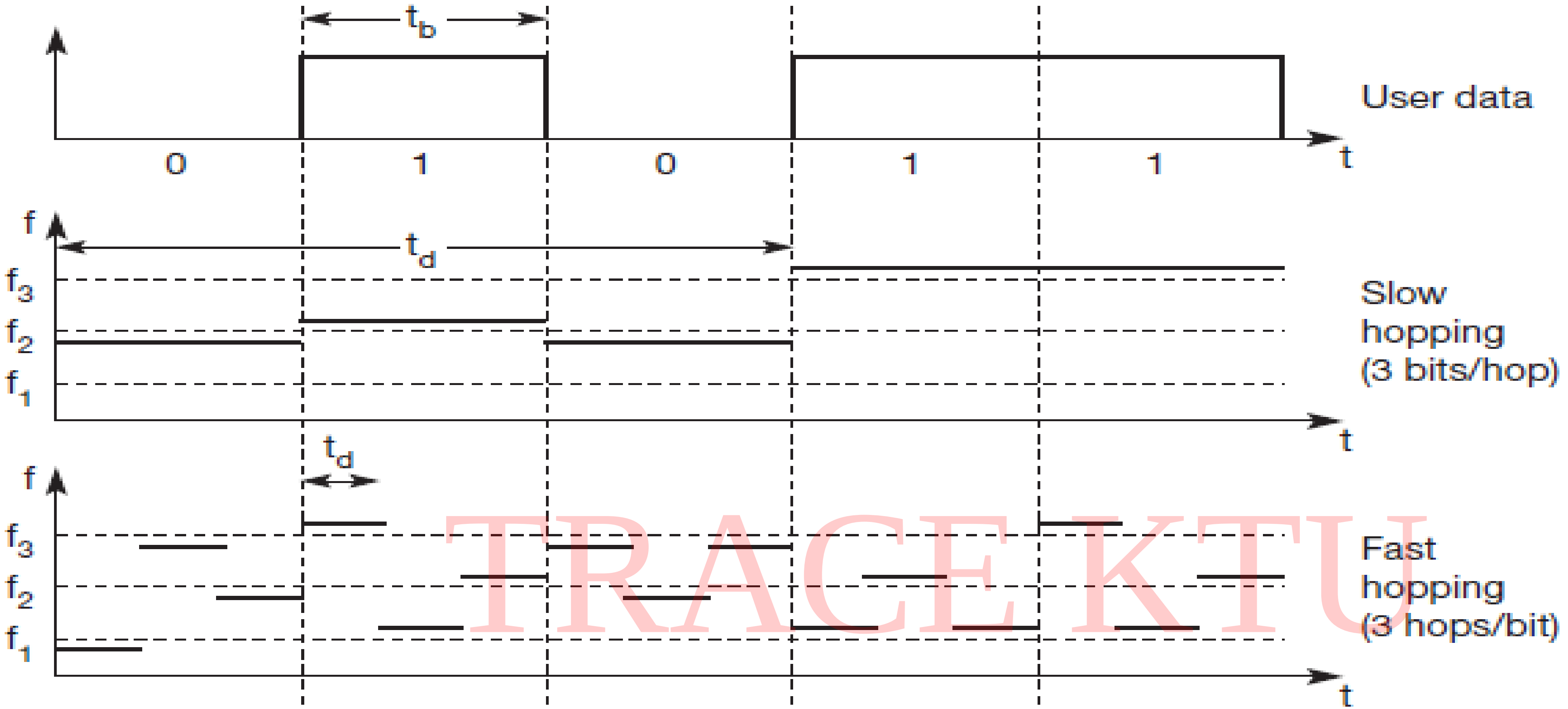
DSSS receiver



- The DSSS receiver is more complex than the transmitter.
- The receiver only has to perform the inverse functions of the transmitter.
- 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

- **FHSS 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**
- **FHSS comes in two variants, slow and fast hopping**

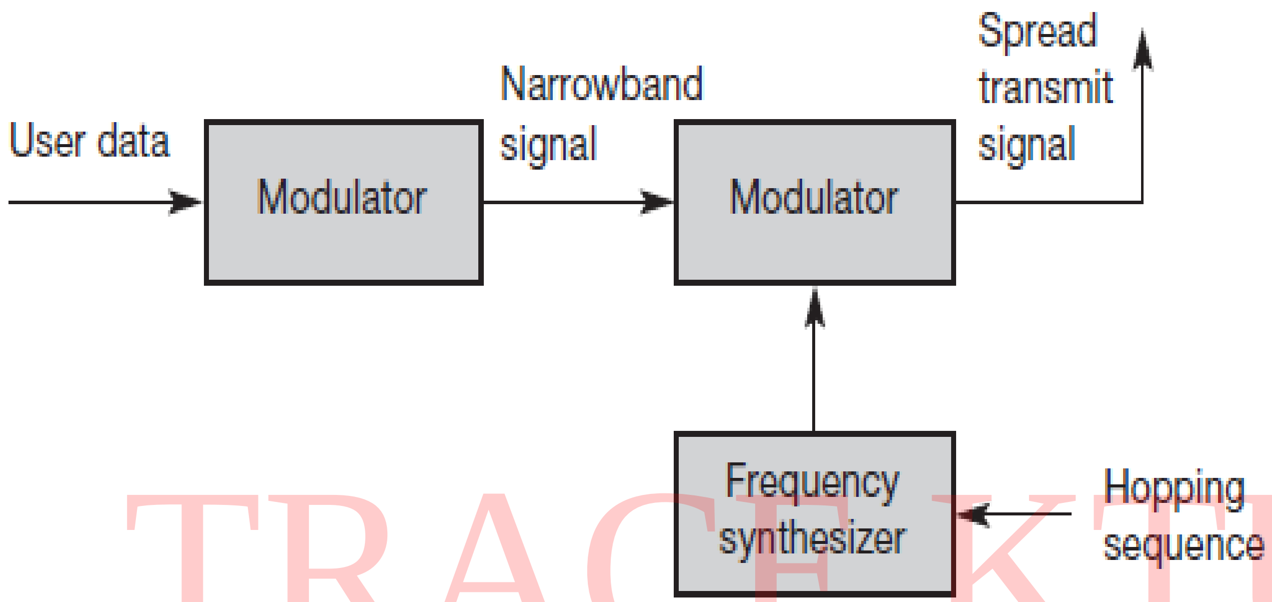


- In slow hopping, the transmitter uses one frequency for several bit periods
- 5 User Bits (f2=3bits & f3=2bits)
- Slow hopping systems are cheaper and have relaxed tolerances, but they are not as immune to narrowband interference as fast hopping systems.
- Slow frequency hopping is an option for GSM

Fast hopping systems

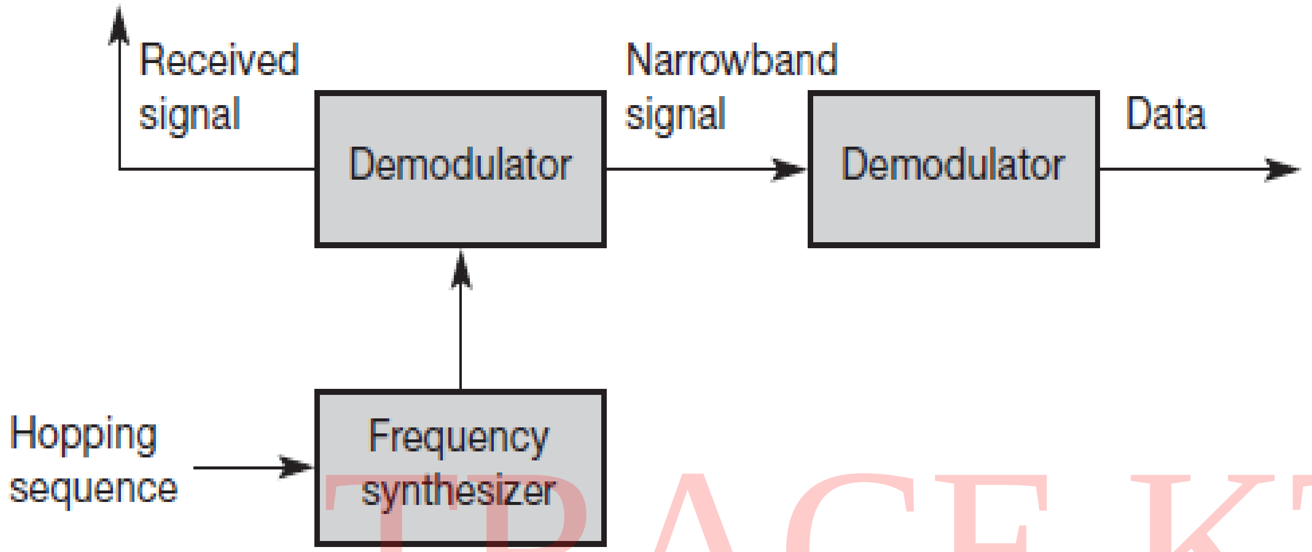
- Transmitter changes the frequency several times during the transmission of a single bit.
- The transmitter changes three times during a bit period
- Fast hopping systems are more complex to implement because the transmitter and receiver have to stay synchronized within smaller tolerances
- Better for overcoming the effects of narrowband interference and frequency selective fading

FHSS transmitter



- First step is modulation of user data by any one of the digital-to-analog modulation schemes such as FSK or BPSK (Binary Phase shift key).
- In FSK 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.
- 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.

FHSS receiver

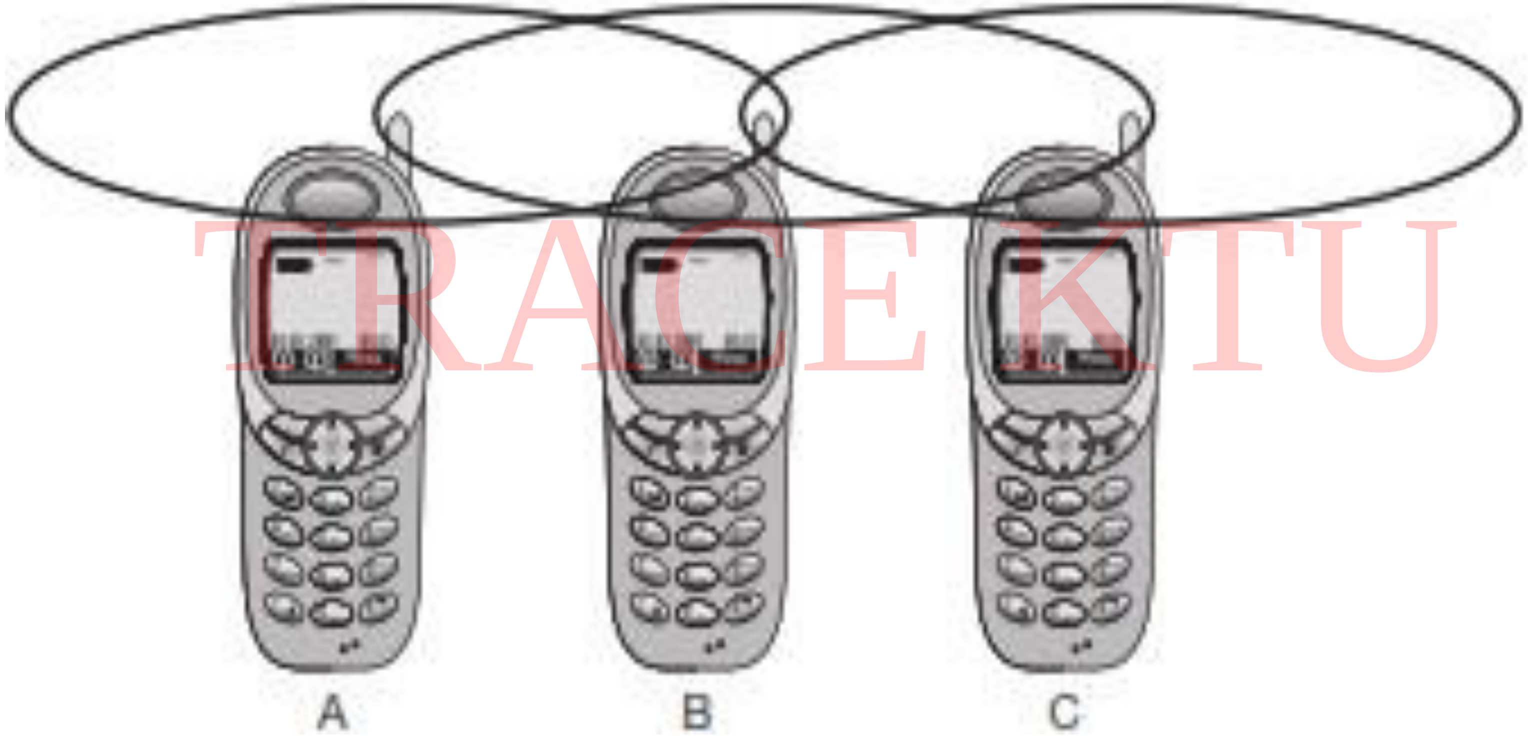


- It performs the inverse operations of the modulation to reconstruct user data.
- FHSS systems only use a portion of the total band at any time, while DSSS systems always use the total bandwidth available.
- DSSS systems are more resistant to fading and multi-path effects
- DSSS signals are much harder to detect without knowing the spreading code, detection is virtually impossible.

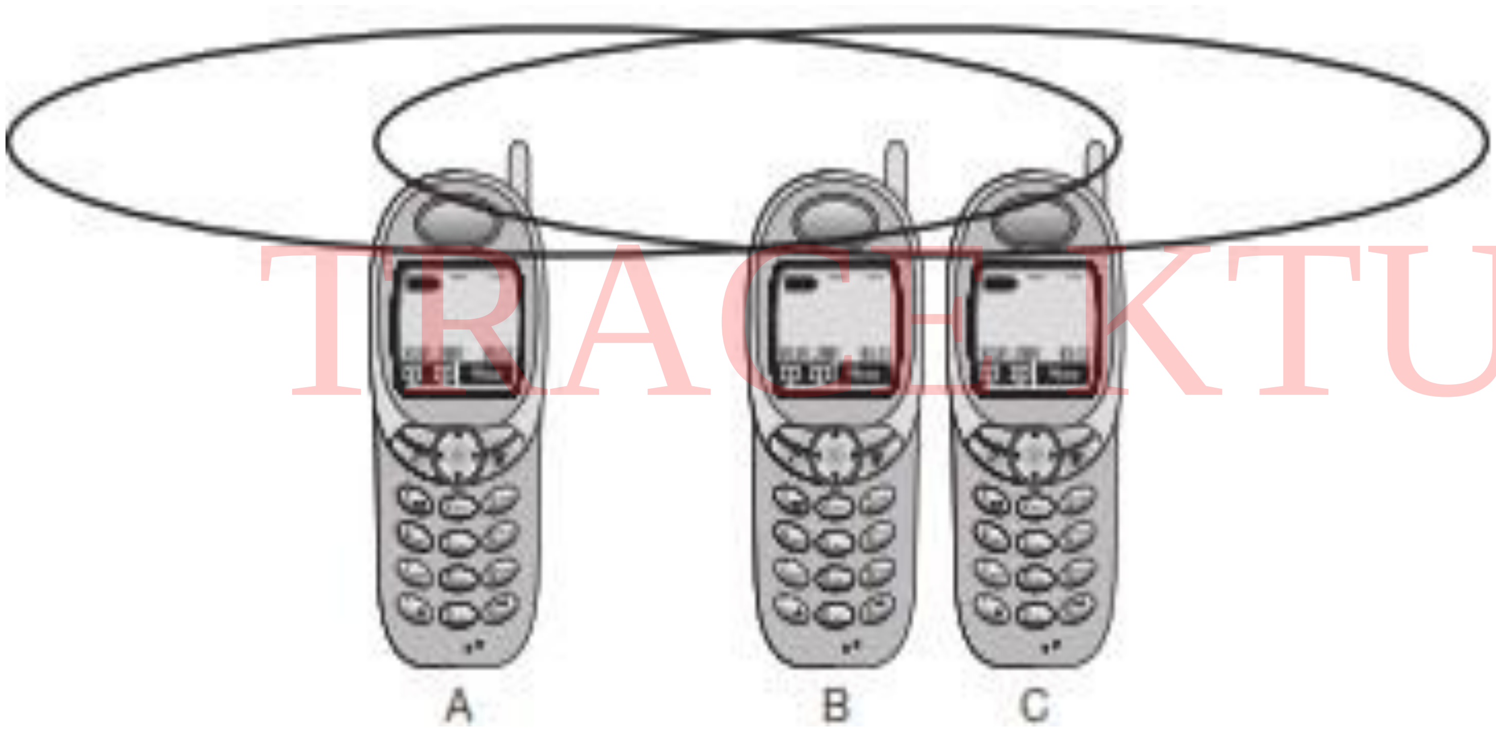
MEDIUM ACCESS CONTROL

- **Medium access control (MAC) algorithms are specifically adapted to the wireless domain**
- **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.**
- **Why does this scheme fail in wireless networks? CSMA/CD**
- **Hidden and exposed terminals**
- **Near and far terminals**

Hidden and exposed terminals



Near and far terminals

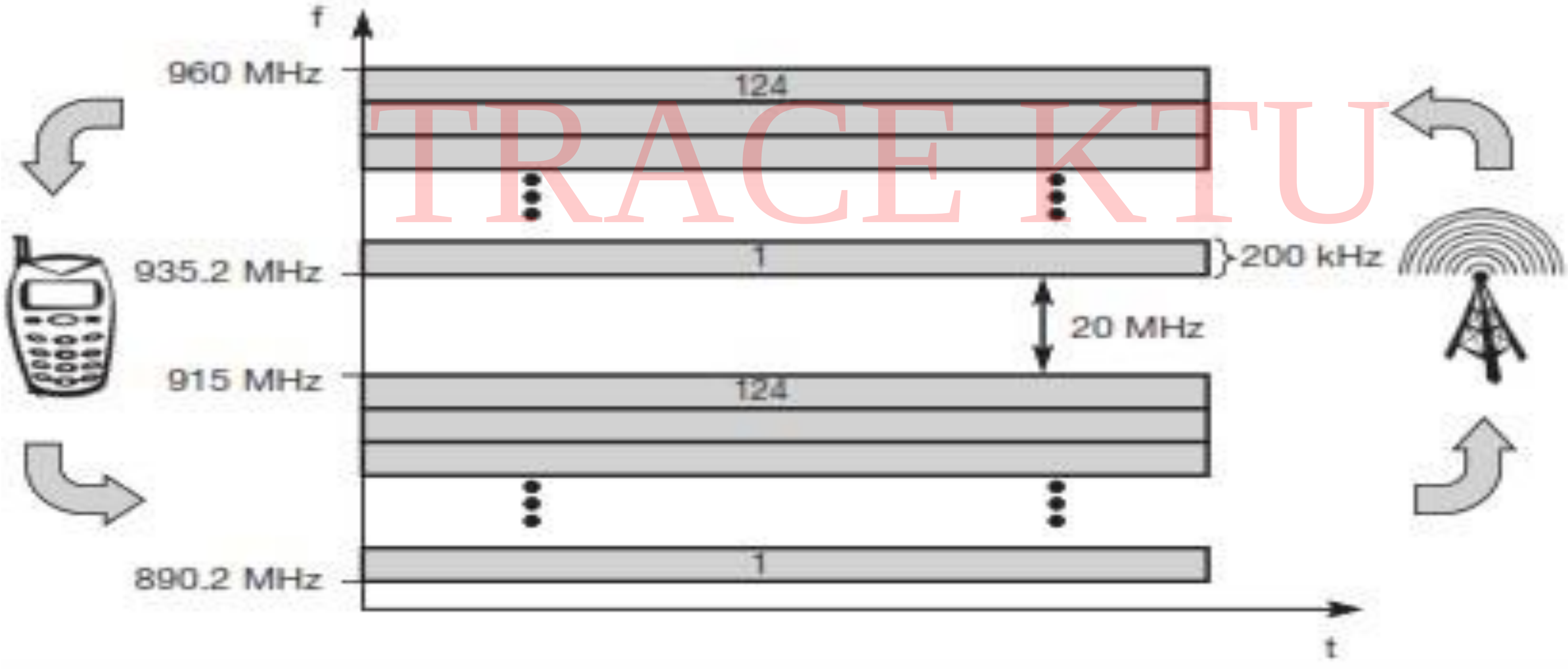


MAC mechanisms

SDMA(Space Division Multiple Access)

- **SDMA is used for allocating a separated space to users in wireless networks.**
- **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.**
- **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).**

FDMA(Frequency division multiple access)

- Allocating frequencies to transmission channels according to the frequency division multiplexing
- Allocation can either be **fixed or dynamic** (i.e., demand driven).
- 

Uplink

- Mobile station to base station or from ground control to satellite
- All uplinks use the band between 890.2 and 915 MHz
- $f_u = 890 \text{ MHz} + n \cdot 0.2 \text{ MHz}$

Downlink

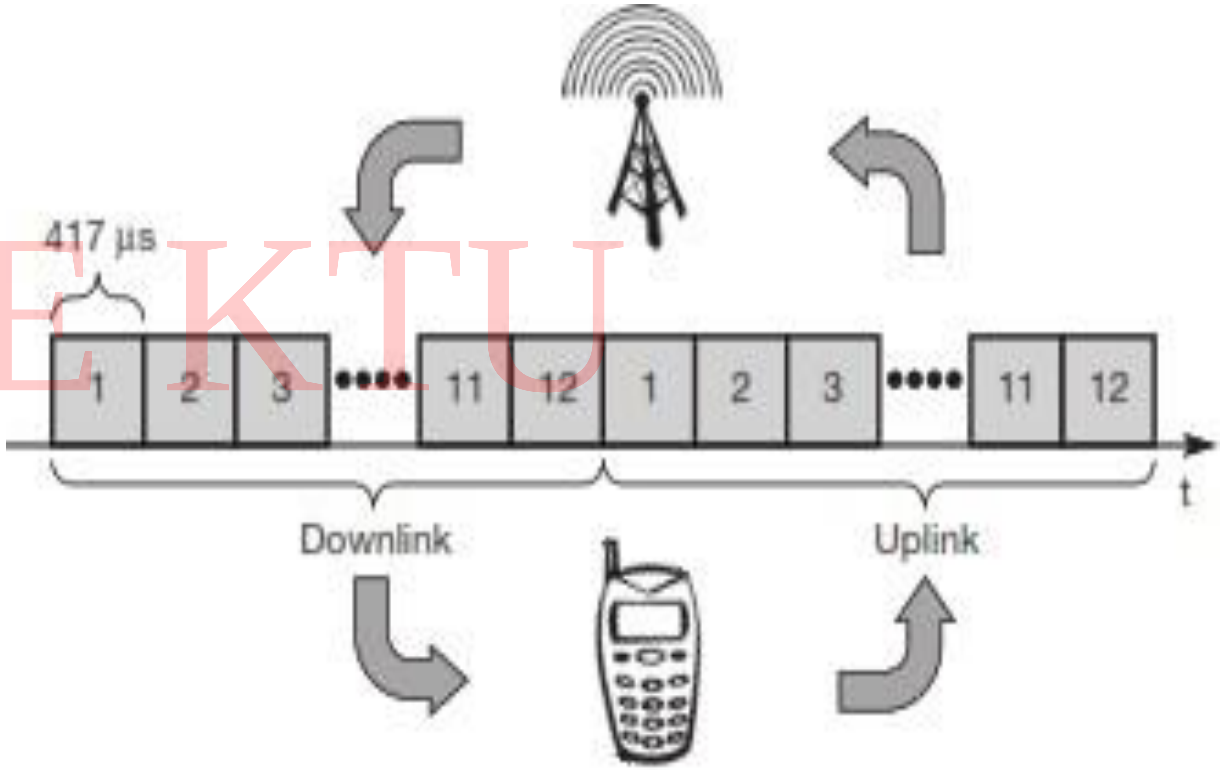
- Base station to mobile station or from satellite to ground control.
- 935.2 to 960 MHz
- $f_d = 935 \text{ MHz} + n \cdot 0.2 \text{ MHz}$

TDMA(Time division multiple access)

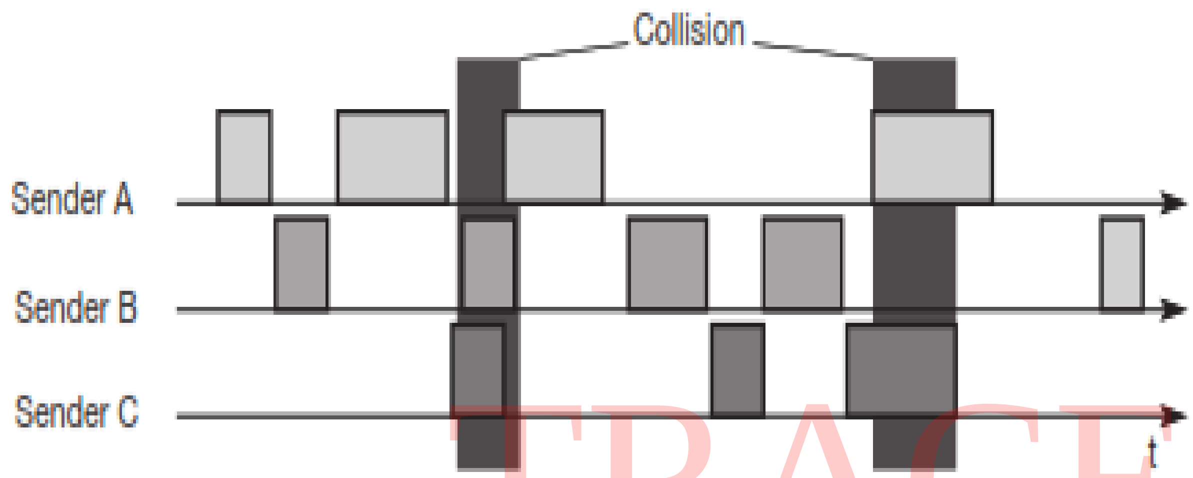
- **Much more flexible scheme, which comprises all technologies that allocate certain time slots for communication**
- **The receiver can stay at the same frequency the whole time. Using only one frequency, and thus very simple receivers and transmitters**

Fixed TDM

- **TDM is allocating time slots for channels in a fixed pattern**
- **Uplink and downlink are separated in time**
- **Each connection is allotted its own up- and downlink pair.**
- **Apt for connections with a constant data rate**
- **Inefficient for bursty data or asymmetric connections**

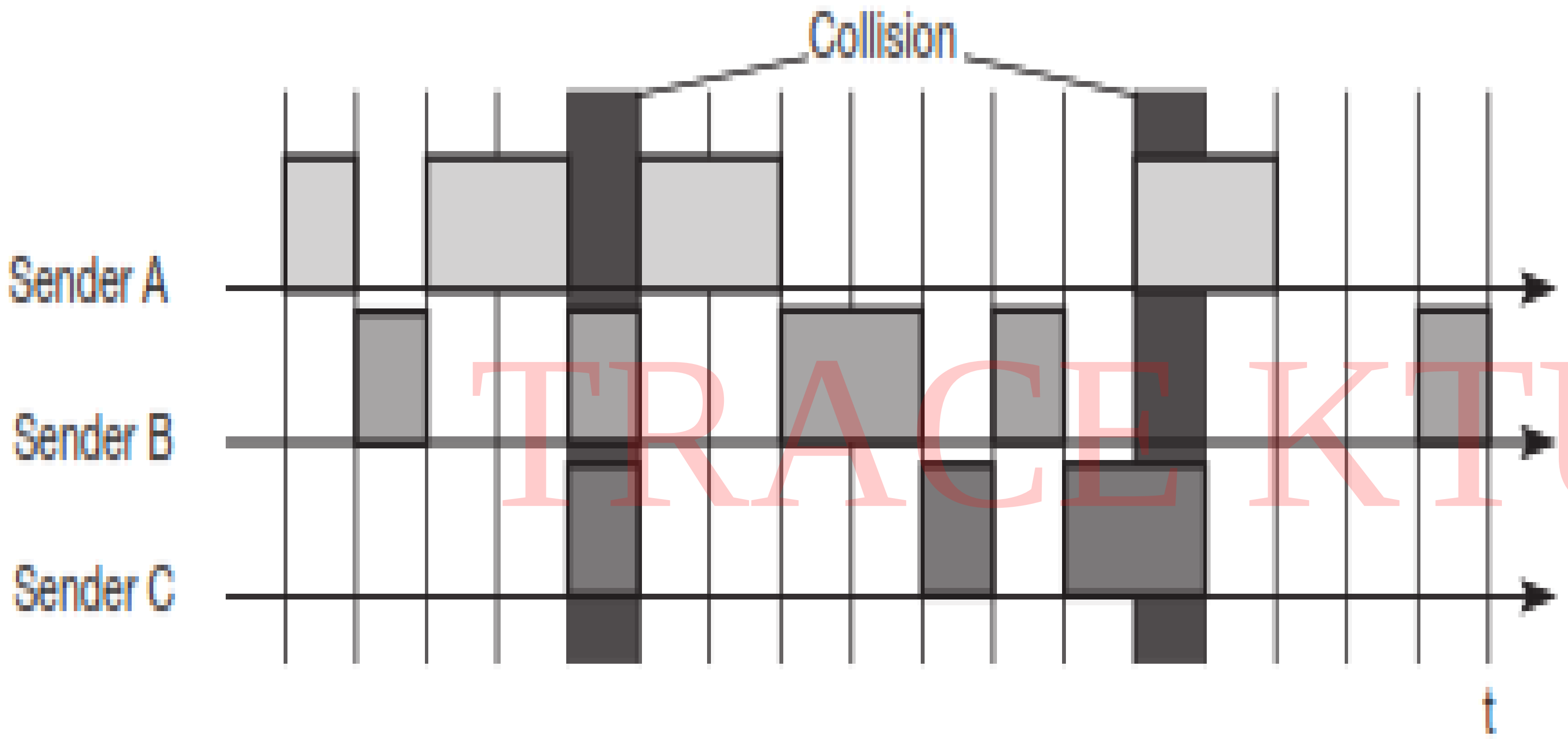


Classical Aloha



- Each station can access the medium at any time
- 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

Slotted Aloha



- The first refinement of the classical Aloha scheme
- In this case, all senders have to be synchronized, transmission can only start at the beginning of a time slot
- Still, access is not coordinated

Carrier sense multiple access

- Improvement to the basic Aloha is sensing the carrier before accessing the medium.
- Sensing the carrier and accessing the medium only if the carrier is idle decreases the probability of a collision

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

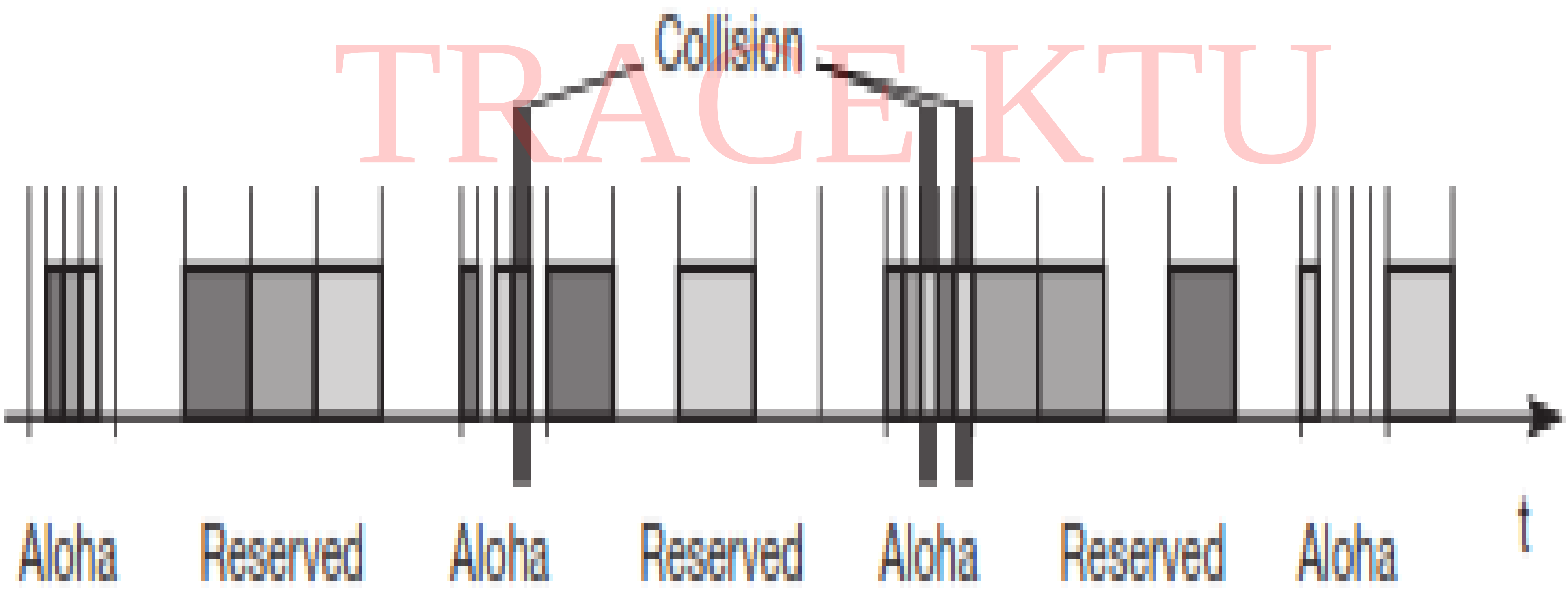
Non-persistent CSMA : After receiving a negative acknowledgement the terminal waits a random time before retransmission of the packet.

P-persistent CSMA : 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.

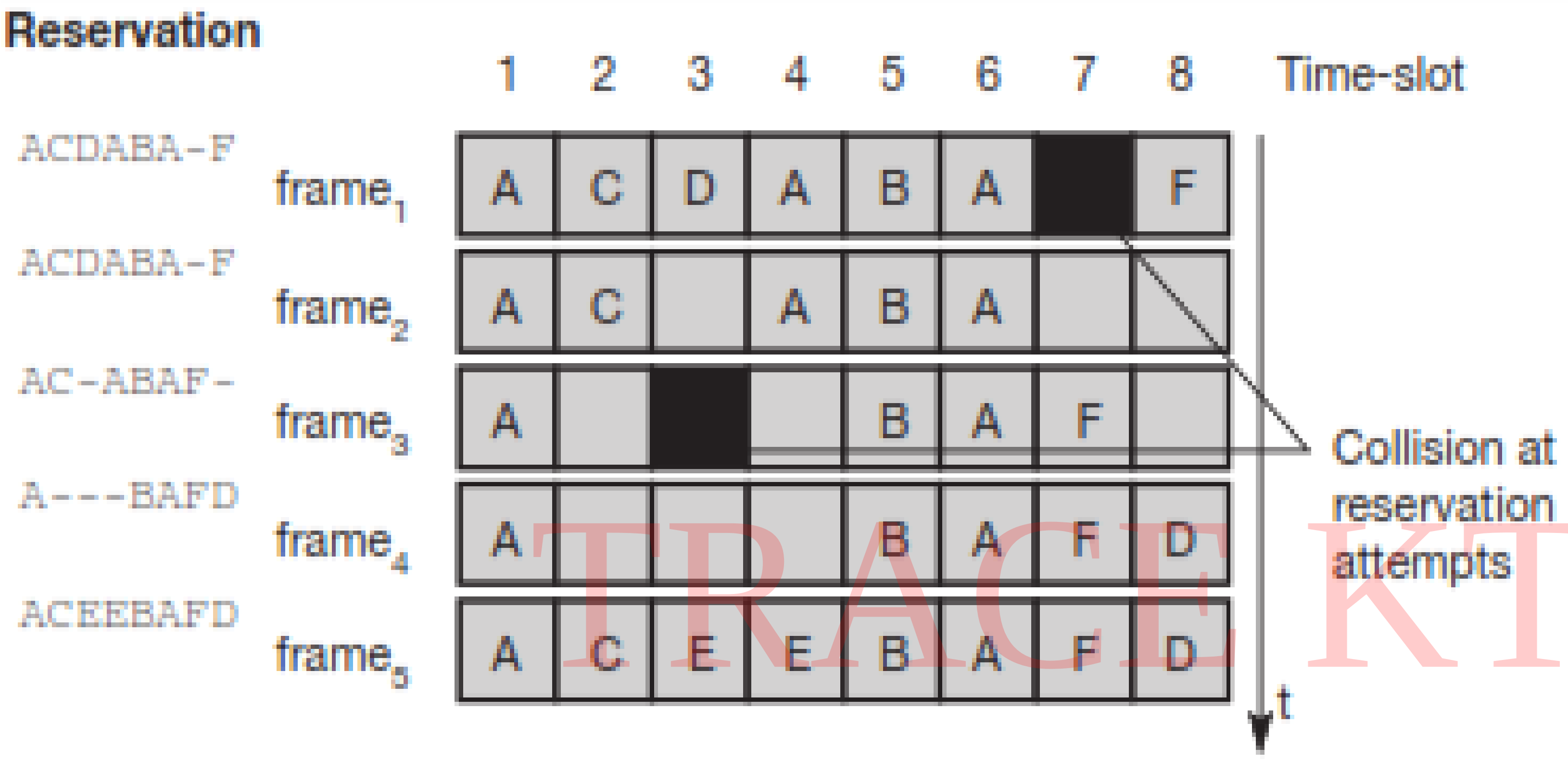
CSMA/CA : If two or more terminals start a transmission at the same time, collision is detected and the transmission is immediately aborted in midstream.

Demand assigned multiple access

- Have a **reservation period followed by a transmission period**
- During the reservation period, stations can reserve future slots in the transmission period
- Collisions may occur during the reservation period and not in the transmission period

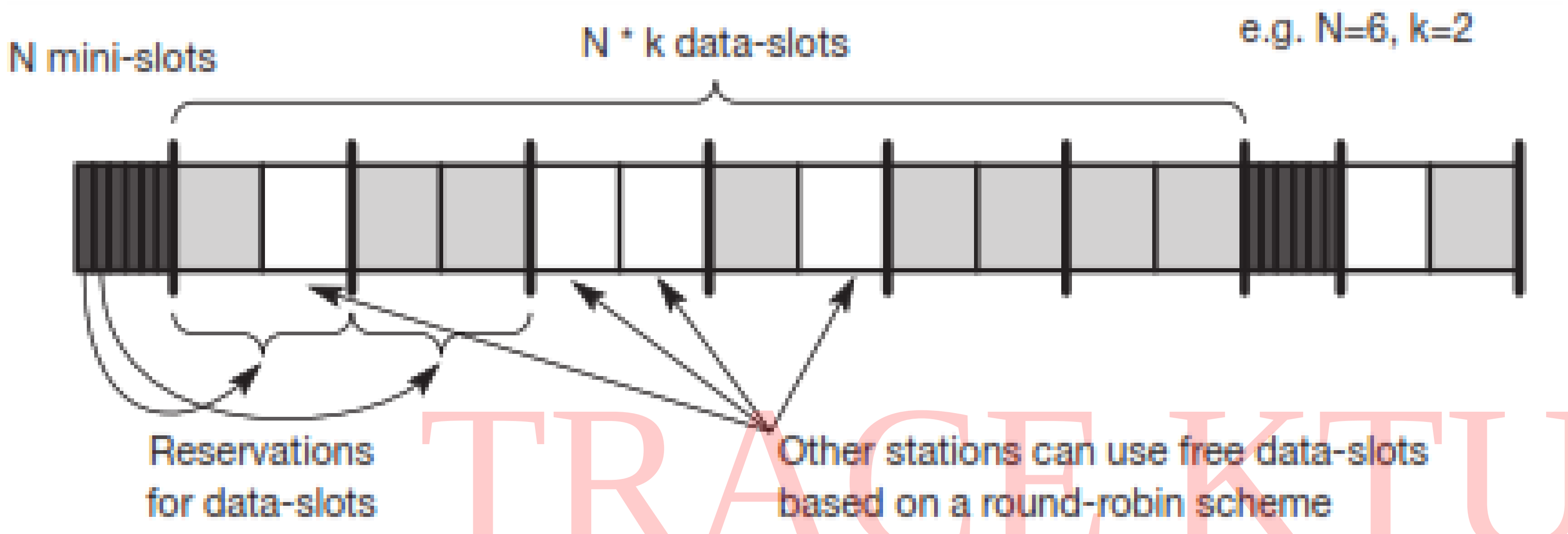


PRMA(packet reservation multiple access) (implicit reservation protocol)



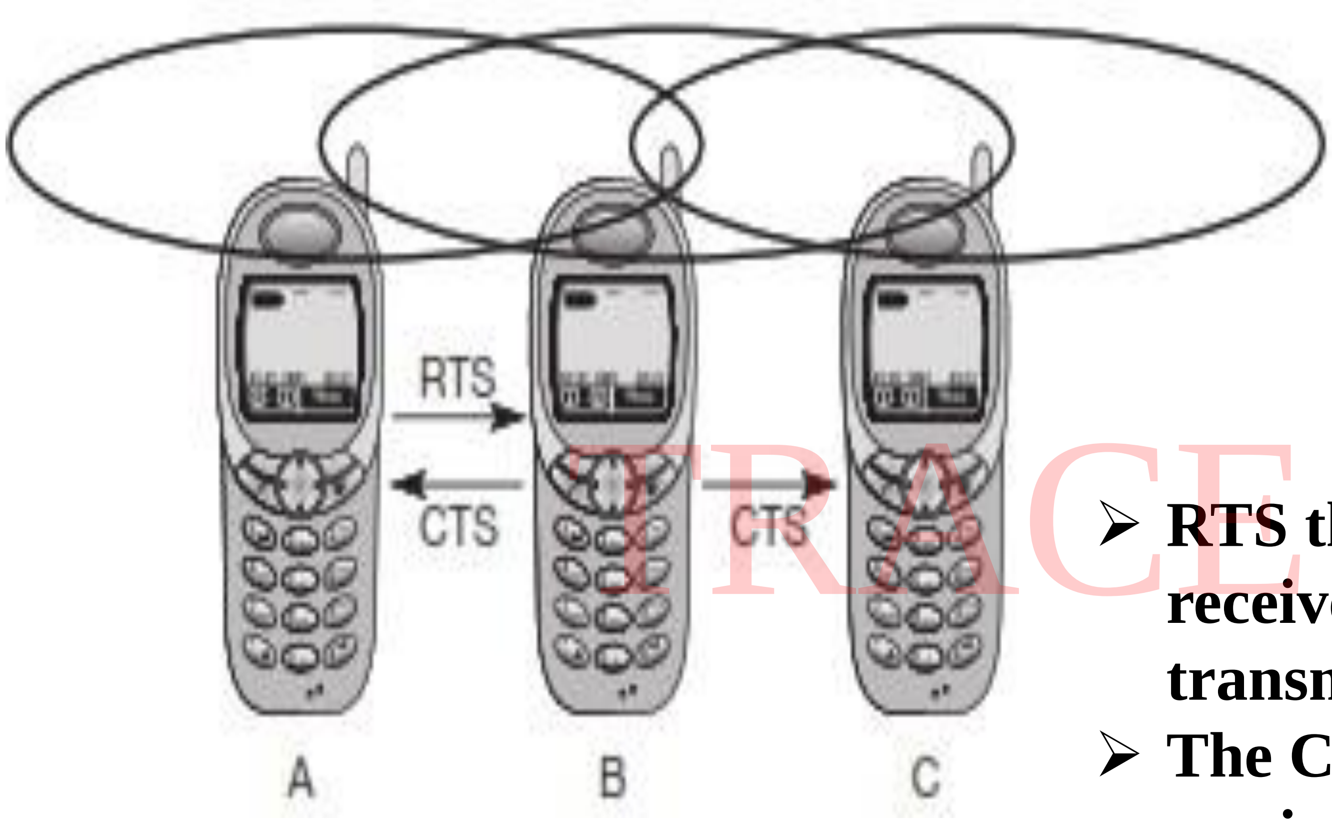
- A to F- Base station
- The base station broadcasts the reservation status ‘ACDABA-F’ to all stations
- Slots one to six and eight are occupied, but slot seven is free in the following transmission
- More than one station wants to access this slot, so a collision occurs

Reservation TDMA

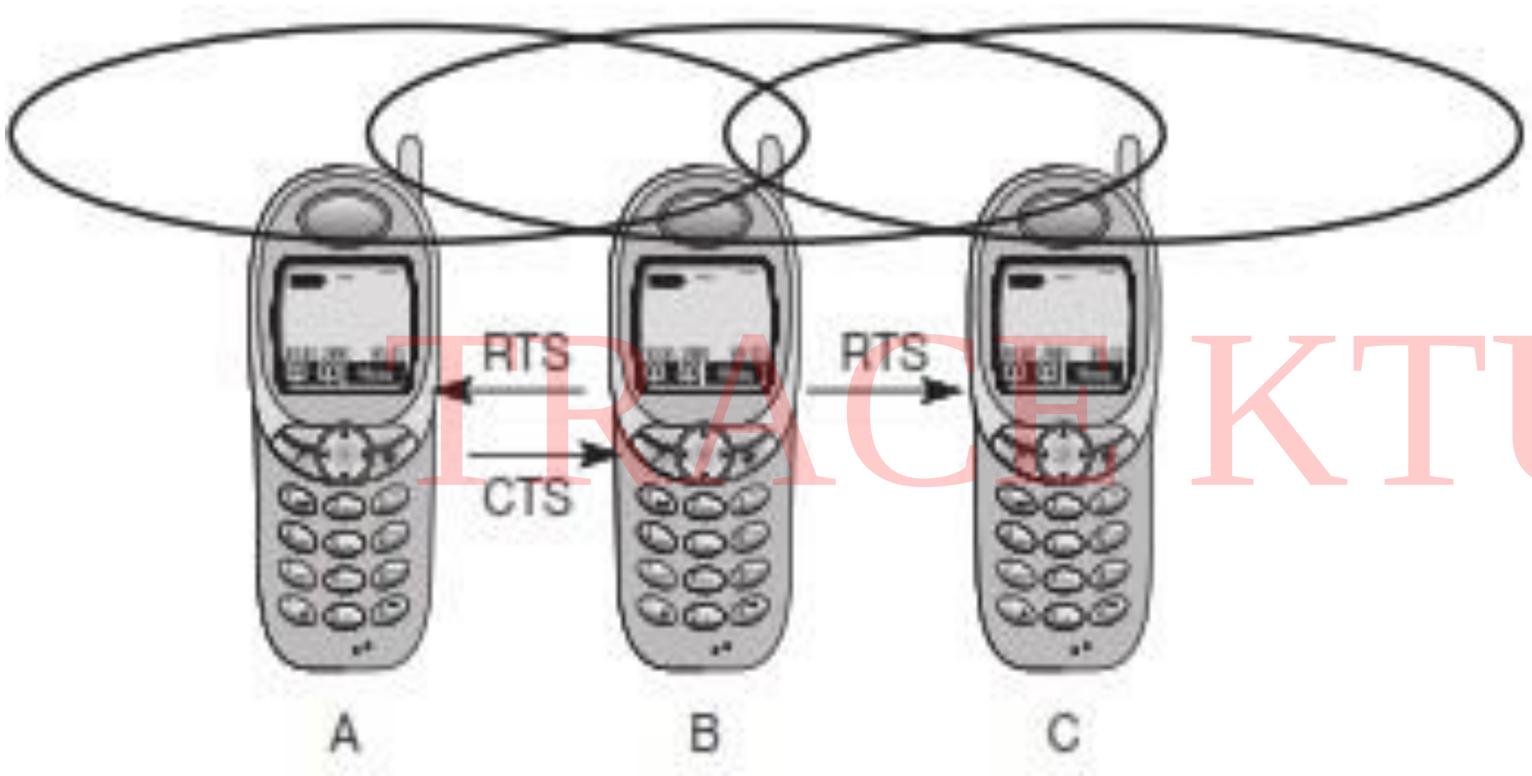


N mini-slots followed by N·k data-slots form a frame that is repeated

Multiple access with collision avoidance



- RTS that contains the name of sender and receiver, as well as the length of the future transmission.
- The CTS contains the names of sender and receiver and the length of the future transmission
- Received CTS- Not able to send data
- Can avoid hidden terminal problem



- Received RTS but not CTS can send and receive the data
- Can avoid exposed terminal problem

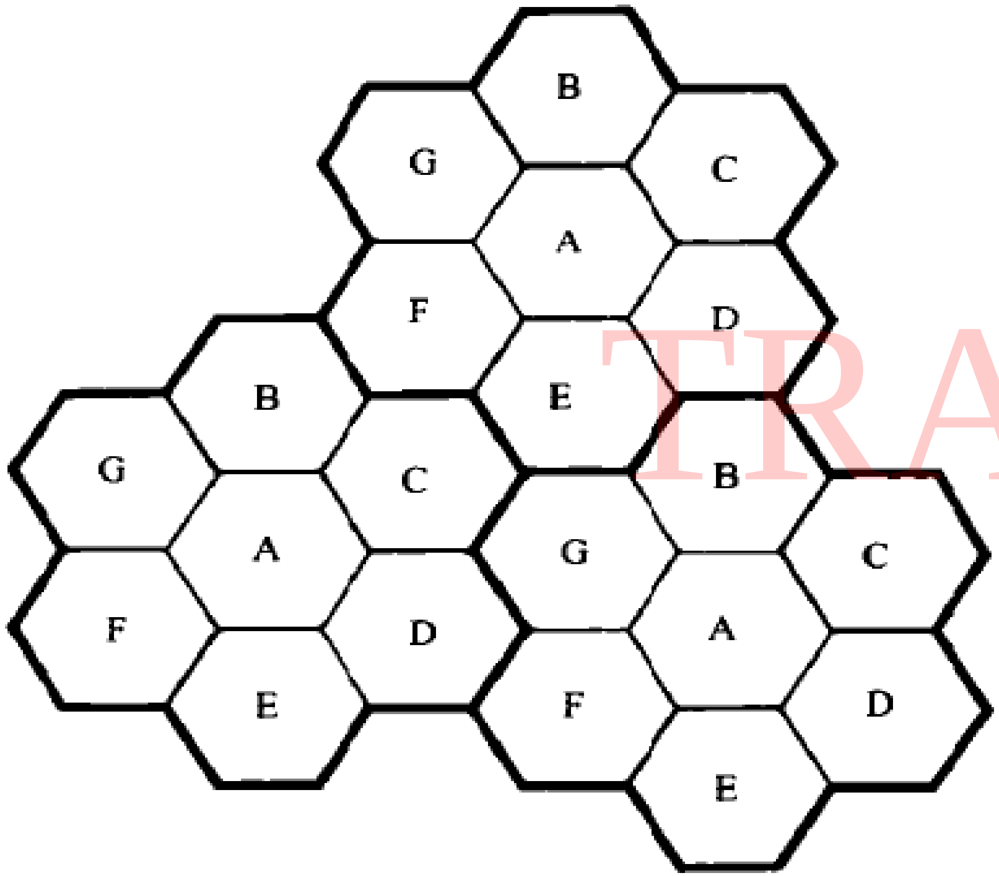
Polling

- 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 reservations etc.
- The master could also establish a list of stations wishing to transmit during a contention phase. After this phase, the station polls each station on the list.

Inhibit sense multiple access (ISMA/DSMA) (digital)

- The base station only signals a busy medium via a busy tone (called BUSY/IDLE indicator) on the downlink .
- After the busy tone stops, can access the uplink.
- The base station acknowledges successful transmissions
- A mobile station detects a collision only via the missing Positive acknowledgement.

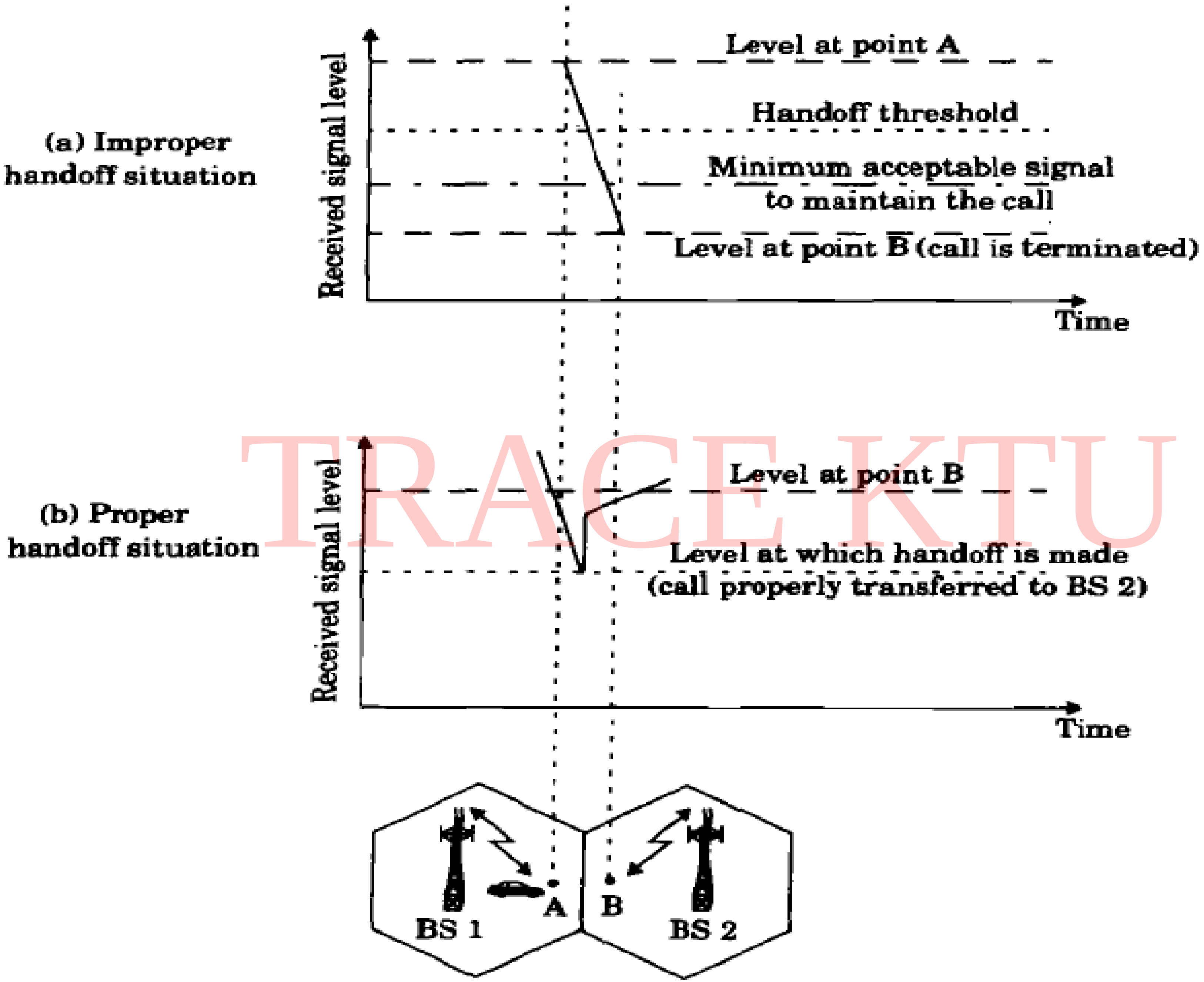
CELLULAR SYSTEMS



- **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.**
- **Frequency reuse or frequency planning**
- **The actual radio coverage of a cell is known as the footprint.**

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.**
- **Minimum usable signal for acceptable voice quality at the base station receiver (normally taken as between —90 dBm and—100 dBm)**
- **When a mobile moves from one cellular system to a different cellular system controlled by a different MSC, an intersystem handoff becomes necessary**


(a) Improper
handoff situation
Received signal level
Level at point A
Handoff threshold
Minimum acceptable signal
to maintain the call
Level at point B (call is terminated)
Time
(b) Proper
handoff situation
Received signal level
Level at point B
Level at which handoff is made
(call properly transferred to BS 2)
Time
BS 1
A
B
BS 2

Dwell time:

- The time over which a call may be maintained within a cell, without handoff, is called the dwell time.

Prioritizing Handoffs

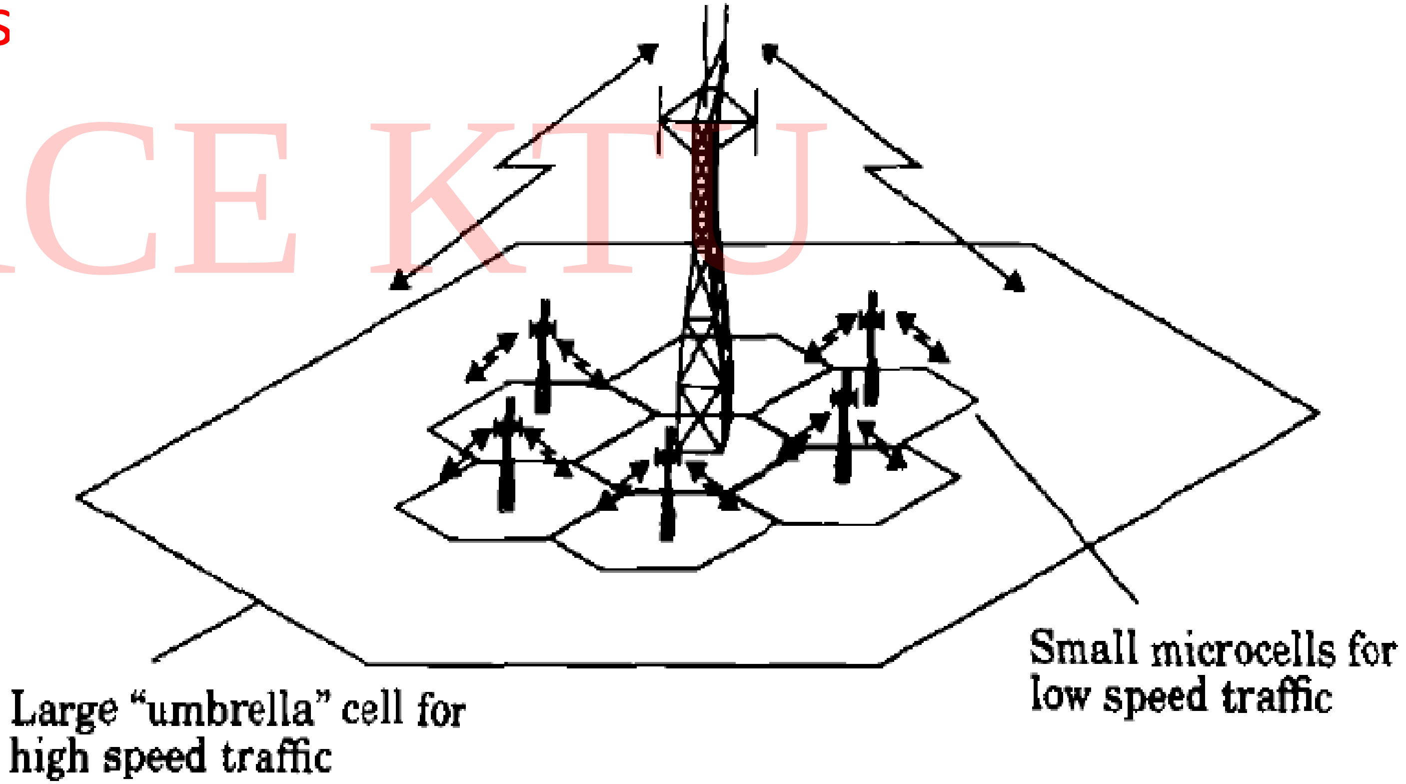
- Channels in a cell is reserved exclusively for handoff requests from ongoing calls which may be handed off into the cell

Practical Handoff Considerations

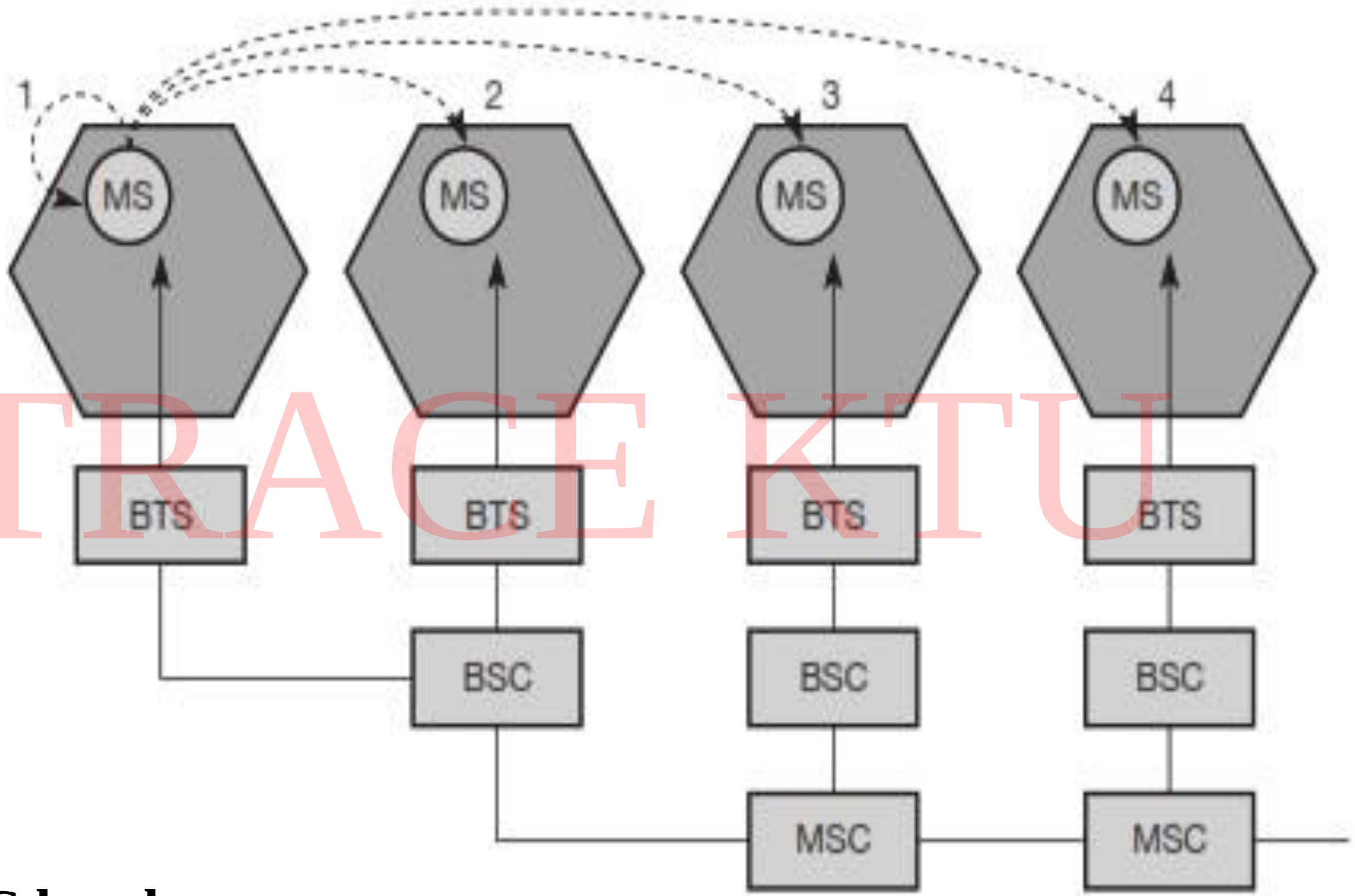
- Umbrella Cell approach
- Cell dragging

  Cell dragging results from pedestrian users that provide a very strong signal to the base station.

  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



Types of handover in GSM



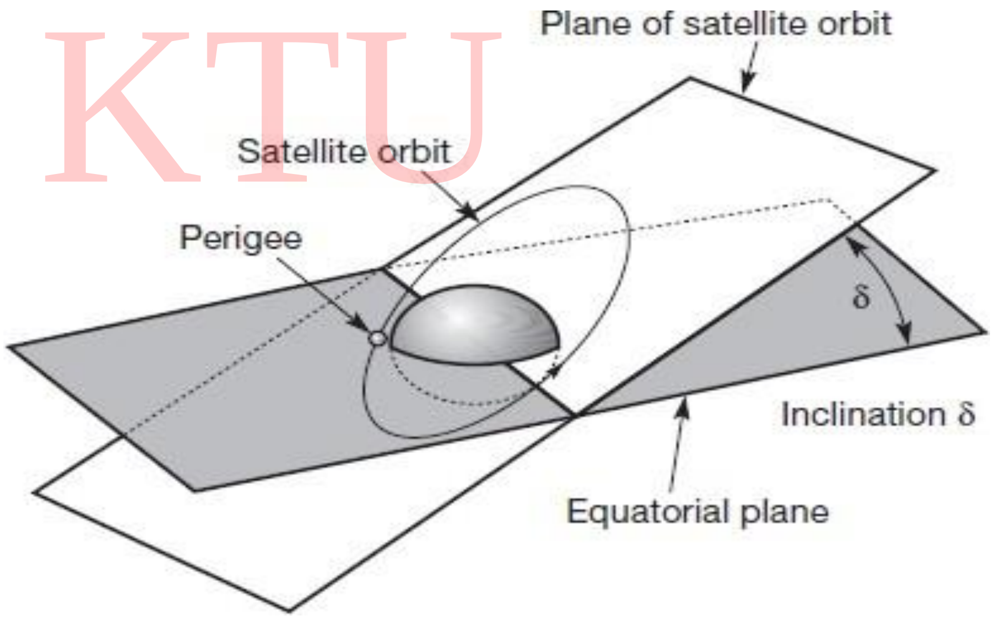
1. **Intra-cell handover**
2. **Inter-cell, intra-BSC handover**
3. **Inter-BSC, intra-MSC handover**
4. **Inter MSC handover**

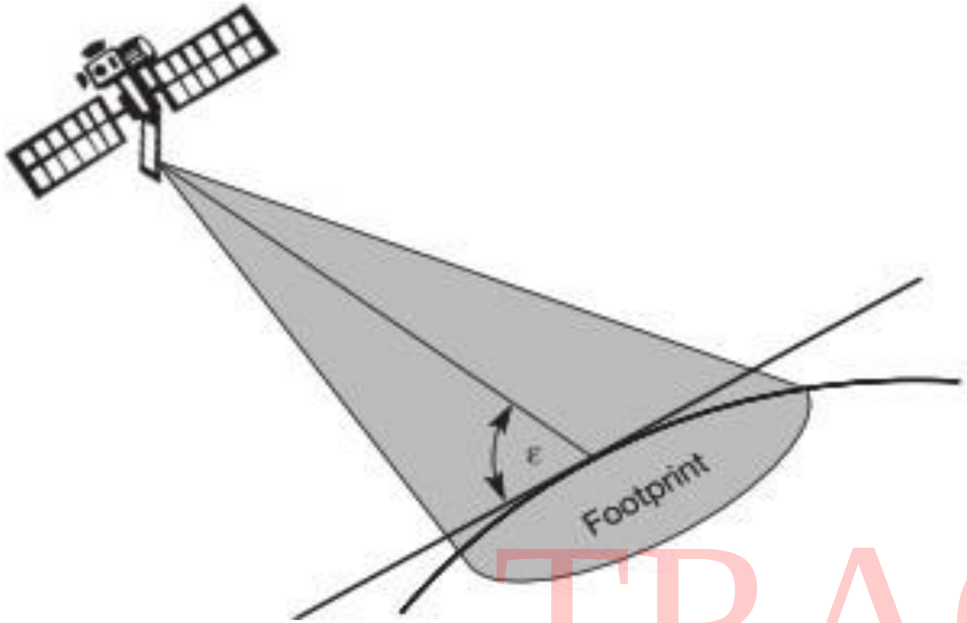
SATELLITE SYSTEMS

- Satellites offer global coverage without wiring costs for base stations and are almost independent of varying population densities.
- Satellites orbit around the earth. Depending on the application, these orbits can be circular or elliptical
- Important parameters in satellite communication are the **inclination and elevation angles**

The inclination angle δ is defined as the angle between the equatorial plane and the plane of satellite orbit.

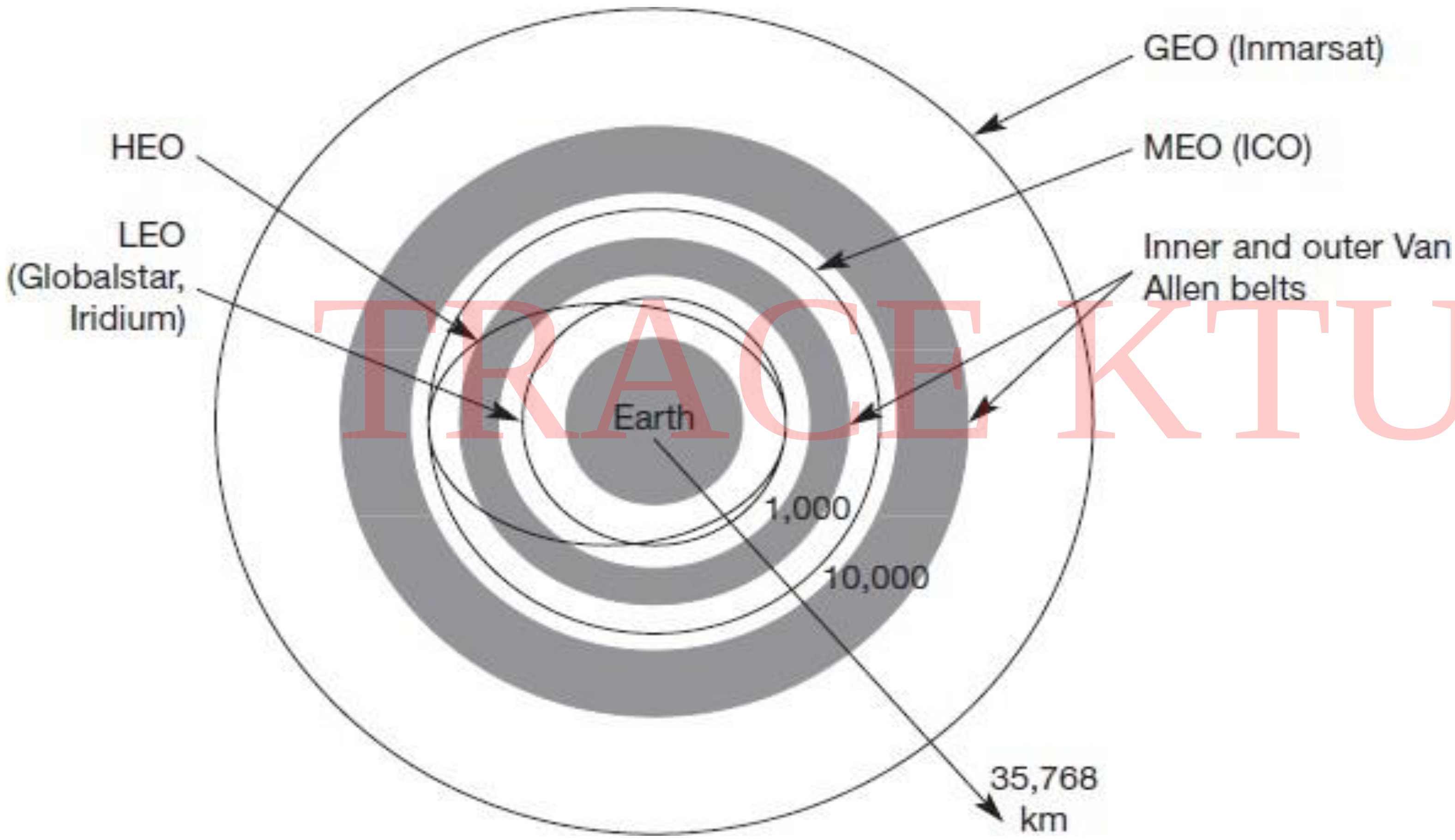
An inclination angle of 0 degrees means that the satellite is exactly above the equator.





The elevation angle ε is defined as the angle between the center of the satellite beam and the plane tangential to the earth’s surface

Different types of satellite orbits



Geostationary (or geosynchronous) earth orbit (GEO)

- GEO satellites have a distance of almost 36,000 km to the earth.
- Examples: TV and radio broadcast satellites, many weather satellites and satellites operating as backbones for the telephone network.
- To fix in the sky, it requires a period of 24 hours
- The orbit must have an inclination of 0 degrees
- Distance between earth and satellite $r = (g\cdot R2/(2\cdot\pi\cdot f)2)1/3$
    - g is the acceleration of gravity
    - R is the radius of earth
    - f is the frequency of the rotation

Advantages:

- Three GEO satellites are enough for a complete coverage of earth.
- Senders and receivers can use fixed antenna positions, no adjusting is needed.
- Lifetime expectations for GEOs are rather high, at about 15 years.
- GEOs typically do not need a handover due to the large footprint.

Disadvantages:

- Northern or southern regions of the earth have more problems receiving these satellites, hence larger antennas are needed in this case.
- Shading of the signals in cities due to high buildings.
- 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.
- Due to the large footprint, either frequencies cannot be reused Transferring a GEO into orbit is very expensive.

Medium earth orbit (MEO)

- **MEOs operate at a distance of about 5,000–12,000 km.**
- **At present only few satellites are in this class.**
- **Can be positioned somewhere between HEOs and GEOs**

Advantages

- **These satellites move more slowly relative to the earth's rotation**
- **Can cover larger populations, so requiring fewer handovers.**

Disadvantages

- **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.**

Highly elliptical orbit (HEO)

- It 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.

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
- ➢ Each LEO satellite will only be visible from the earth for around ten minutes
- ➢ Little LEOs with low bandwidth services (some 100 bit/s), big LEOs (some 1,000 bit/s) and broadband LEOs with Mbit/s range

Advantages:

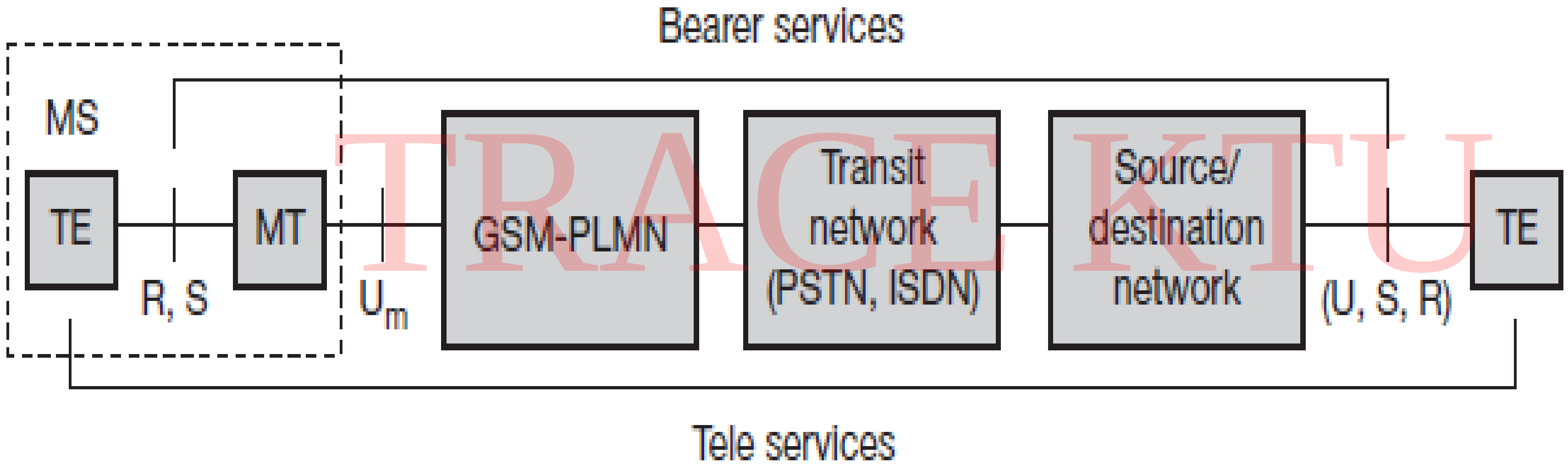
- Support for voice communication with omni-directional antennas using low transmit power in the range of 1W.
- The delay for packets delivery is relatively low (approx 10 ms).
- Smaller footprints of LEOs allow for better frequency reuse.

Disadvantages:

- Need for many satellites if global coverage is to be reached.
- The short time of visibility requires additional mechanisms for connection handover between different satellites.
- 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.

GSM

- **GSM is the most successful digital mobile telecommunication system in the world today**
- **GSM has defined three different categories of services: bearer, tele, and supplementary services.**



Bearer services

- ➢ Bearer services permit transparent and non-transparent, synchronous or asynchronous data transmission
- ➢ Bearer services only use the functions of the physical layer (layer 1) to transmit data
- ➢ Transparent bearer services do not try to recover lost data

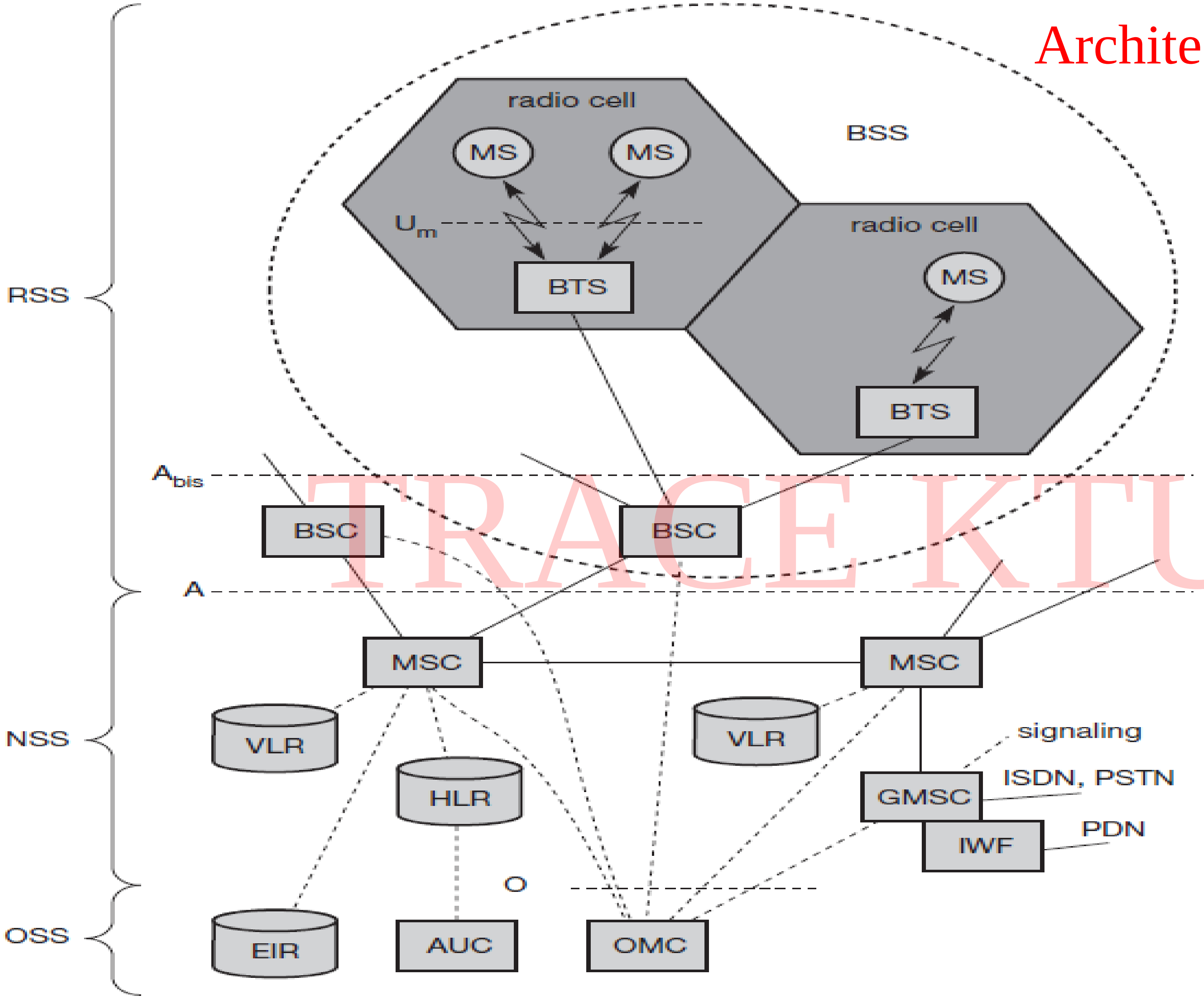
Tele services

- **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 (fax)**
- **Another service offered by GSM is the emergency number, short message service (SMS), enhanced message service (EMS-760), multimedia message service**

Supplementary services

- **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.**

Architecture of a GSM system



Radio subsystem

- The radio subsystem (RSS) comprises all radio specific entities such as, MS, BTS, BSC

Base station subsystem (BSS)

- 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.
- BSSs, are controlled by a base station controller (BSC)

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 using sectorized antennas and connected to MS via the Um interface
- The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.)

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

Mobile station

- 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
- While an MS can be identified via the international mobile equipment identity (IMEI)
- A user can personalize any MS using SIM
- 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

Network and switching subsystem

- **The "heart" of the GSM system is the network and switching subsystem**
- **Comprises functions for worldwide localization of users and supports charging, accounting and roaming of users between different providers in different countries**
- **The NSS connects the wireless network with standard public networks, performs handovers between different BSSs.**

Mobile services switching center

- **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**
- **MSC manages several BSCs in a geographical region.**
- **A gateway MSC (GMSC) has additional connections to other fixed networks, such as PSTN and ISDN**
- **An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.**

Home location register (HLR)

- It stores all user-relevant information
- It 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).
- Dynamic information such as the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC.

Visitor location register (VLR)

- If a new MS comes into an LA the VLR is responsible to copy all relevant information for the user from the HLR.
- The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA.

Operation subsystem

- Contains the necessary functions for network operation and maintenance

Operation and maintenance center (OMC)

- The OMC monitors and controls all other network entities via the O interface.
- OMC functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing

Authentication centre (AuC)

- The radio interface and mobile stations are particularly vulnerable, hence authentication is very essential.
- 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.

Equipment identity register

- It stores all device identifications(IMEI) registered for this network.
- The EIR has a blacklist of stolen (or locked) devices.
- The EIR also contains a list of valid IMEIs (white list) and a list of malfunctioning devices (gray list).

Security

- **Important to protect the privacy of communication between mobile devices and the network.**
- **The security is based on a shared secret key stored on the SIM**
- **The SIM card 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,**

Authentication: **The mobile device and the network authenticate each other using the SIM card's secret key. It prevents unauthorized access to the network.**

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.**

Integrity Protection: **Integrity protection is to ensure that the communication between the mobile device and the network. The integrity protection mechanism uses a Message Authentication Code (MAC) to verify the authenticity of the message.**

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

- **Code division multiple access (CDMA) systems use codes to separate different users and enable access to a shared medium without interference**
- **A good code should have a good autocorrelation and should be orthogonal to other codes.**
- **Two senders, A and B, want to send data**
- **CDMA assigns the following unique and orthogonal key sequences**
- **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.**
- **Assume that binary 0 as –1, a binary 1 as +1**
- **Both senders spread their signal using their key as chipping sequence**

- **As = Ad*Ak = +1*(–1, +1, –1, –1, +1, +1) = (–1, +1, –1, –1, +1, +1)**
- **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**
- **Signal C is received at a receiver: C = As + Bs = (–2, 0, 0, –2, +2, 0).**
- **Despreading A's code 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.**
- **Despreading B's code**
- **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.**