Mobile computing

UNIT I

(1) Introduction to Mobile computing:

*) Mobile computing is a technology that allows transmission of data, voice & video via a computer or any other wireless device without connected to fixed physical link.

*) There are two types of mobility:

a) User Mobility:

In this case, the user moves ie, the user access the same or similar telecommunication services at different places, ie, the user is mobile and the service follows him.

Example:
i) Call forwarding solution
ii) The user can login to this mail from any desktop both in home & in college.

b) Device portability:

In this case the communication device moves with or without a user

Example:
i) Mobile phone system
ii) Mobile phone moves from one base station to another base station

i) A communication device exhibit the following characteristics:

i) Fixed and wired:

→ These devices uses fixed networks.

→ Example: desktop computers in office.

ii) Mobile and wired:

→ eg: Laptop

→ users carry the laptop from one place to another.

iii) Fixed and wireless:

→ This mode is used for installing networks in historical buildings to avoid damage by installing wires. eg: Modem

iv) Mobile and wireless:

→ No wires between users.

→ eg: Mobile phone.

(2) Applications of Mobile computing:

The following are some of the applications of mobile computing:

i) Vehicles:

The cars that are introduced in the market are expected to have a number of wireless devices. They receive digital data through digital audio broadcasting (DAB) for receiving music, news, road conditions, weather reports and other important information.

*) The data rate is expected to be @ 1.5 Mb/s. (@ 1.5 MB/)

*) Additionally, GSM phones are available in the vehicle for voice & data communication at a data rate of 384 kb/s.

*) In case of accident an automatic call to the service provider may be initiated resulting in faster ambulance service & police information. Similar type of information exchange is also possible in case of buses, trucks, trains, etc.

2) Emergencies

*) Timely communication is needed in case of emergency situation such as accident, natural calamities or medical emergencies.

*) When an accident victim is being transported to a hospital in an ambulance, it will be a great help if the victims information (ie, victim's health) is monitored and relayed to the hospital so that the medical team at the hospital may be ready with required material.

*) Just on arrive at the hospital the victim can be given necessary emergency support without any further delay thus avoiding wastage of golden-hour.

3) Buisness:

*) communication is the backbone of any buisness. There is a need for all stack holders of an organisation to keep in touch with vital information of the company so that they will be able to take considerable decision.

*) Another example is sales person can know the availability of various goods, the purchase functionality.

4) Replacement of wired networks:

*) In specific circumstances, the wired network has to be replaced by wireless network. In situation such as weather forecast or earthquake, it is impractical to have wired network, in these situations we need sensors ie, ad-hoc network with a satellite as the backbone.

*) Many tradefairs use wireless network as it is fast to implement.

5) Information Entertainment and more:
(Infotaiment and more)

*) Internet access is everywhere.

*) The wireless internet is used in the areas of information & entertainment.

*) wireless internet is used in the development of games. It is used as travel guide to tell somethiny about the history of building (via Gps).

6) Location dependent service:

*) Wireless n/w has 2 major drawbacks. They are:

→ Mobile device network access is constantly changing.

→ wireless link is more prone to errors.

*) Some of the services that are location dependent are:

i) Follow-on- services:

*) For successful implementation of the service, the information about the current location of the subscriber is needed. when using mobile computing network, it is possible to redirect all emails to one's current location where ever in the world.

ii) Location aware services:

Sometimes it may be required to access a service (printing), that may not be available in one's laptop. In such cases, it is required for the laptop to know the environment and services that are available in the environment. If a laser printer is available in the environment then laptop can access the network and take the print out.

iii) Privacy:

*) In many situation, the user prefer to access in privacy with the fear that the information might be misused.

iv) Information services:

While walking around in a city, you can use your wireless travel guide to "pull" the information like "where is the nearest . restaurant". You can also "push" information on your travel guide.

7) Mobile and wireless devices:

The types of devices that are used in mobile networks are increasing. The following are some of the devices

i) Sensor:

*) It is a simple wireless device that can transmit the data indicating the state of the variable and it is measured by using sensor.

*) Example, if the door is closed, the switch transmits this state to the mobile phone inside the office and the mobile phone will not accept the incoming call.

ii) Embedded Controller:

*) Many electronic appliances already contains a simple or sometimes more complex controllers eg. Keyboard, headsets, washing machines, TV, Coffee m/c's etc. Some of them can be made wireless operative.

iii) Pager:

*) It is a very simple receiver.

*) A pager can only display short messages & it has a tiny display and cannot send any message.

iv) Mobile phones:

*) Traditional mobile phone had only a simple black and white text display and could send/receive voice or SMS.

*) Nowadays mobile phones are with full colour graphic display, touch screen and internet brower.

V) Personal Digital Assistant (PDA):

*) PDA is easily carriable and run simple softwares such as calendar, note pad & mail.

*) PDA use pen as i/p device and character recognition software to convert handwritten information into characters.

vi) Palmtop / pocket computer:

*) Palmtop have a small keyboard as an input device and have colour display.

vii) Laptop / Note books

*) Laptop are fully flat edged computers that are lesser in size & weight. Laptop performance are the same as desk top computers.

*) If laptop's are operated via touch sensitive display then it is called as notepad or tablet PCs.

(3) Generation of Mobile communication Technologies:

*) In 1794, Claude Chappe invented optical telegraph.

*) In 1831, Michael Faraday, demonstrated electromagnetic induction.

*) In 1843, Alexander Graham bell invented first commercial telegraph line.

*) In 1864, James C. Maxwell, Lay theoritical foundation for electromagnetic fields.

*) In 1886, Hertz demonstrate the electical transmission through space.

*) In 1895, Marconi demostrated first wireless telegraphy.

*) In 1906, first radio broadcast.

*) In 1915, first wireless voice transmission was set up.

*) In 1920, Marconi demonstrated the discovery of Short waves.

*) In 1911, First mobile transmitter

*) In 1926, first telephone in a trains.

*) In 1932, John. L. Baird transmitted TV & demonstrated color TV, TV news

*) In 1933, Armstrong invented frequency Modulation

a) *) In 1980s, Nordic Mobile Telephone system (NMT):
Northern European countries Denmark, Finland, Norway & Sweden invented nordic mobile Telephone (NMT) system

→ NMT uses 450 MHz

*) NMT-900

→ use a new spectrum at 900MHz
→ allow roaming throughout Europe
→ fully digital
→ offer voice & data service

b) Cordless phones:

*) Telephones at home were wireless with standard CTO (cordless telephone) in 1980. Followed by CT1 in 1984. Followed by CT2 in 1987. (data rate 32 Kb/s).

*) In early 1990's is the beginning of Fully digital system. In 1991, came digital European cordless telephone (DECT) (freq → 1880 – 1900 MHz), (data rate → 1.2 M bits/s).

*) DECT is renamed as digital enhanced cordless telecommunication.

c) GSM:

*) The first version of GSM is called global system for Mobile communication.
→ (900 MHz, 124 full-duplex channels)
→ offer full roaming, Authentication & encryption.

*) In 1983, US discovered Advanced Mobile phone System (AMPS). It is an analog mobile phone sys. (850 MHz)

*) US's → AMPS & Europe's → GSM is not sufficient for high user densities. So, arise 3 systems
i) analog narrow band AMPS
ii) 2 digital → TDMA
→ CDMA

*) In 1994, (By Europe) GSM-1800 was developed (also known as DCS 1800 – digital cellular System [1800 MHz freq)

*) By US, GSM-1900 (also known as PCS 1900) was developed (1900 MHz freq)

d) Mobile communication using Satellite:

*) 1998, was the beginning of mobile comm. using satellite, with Iridium system

*) Iridium consists of → 66 satellite in low earth orbit
→ uses 1.6 GHz freq for mobile phones.

*) In 1998, Europeans agreed on Universal mobile Telecommunication System (UMTS), as a proposal for International Telecommunication Union (ITU).

e) Wireless LAN:

*) In 1999, IEEE published 802.11 b (11 Mb/s at 2.4 GHz)

*) Bluetooth, is a short-range technology is developed (data rate less than 1 Mb/s)

*) HIPERLAN was developed in 1996
type-1 → (5.2 GHz, at 23.5 Mb/s)
type-4 → 17 GHz, at 155 Mb/s.

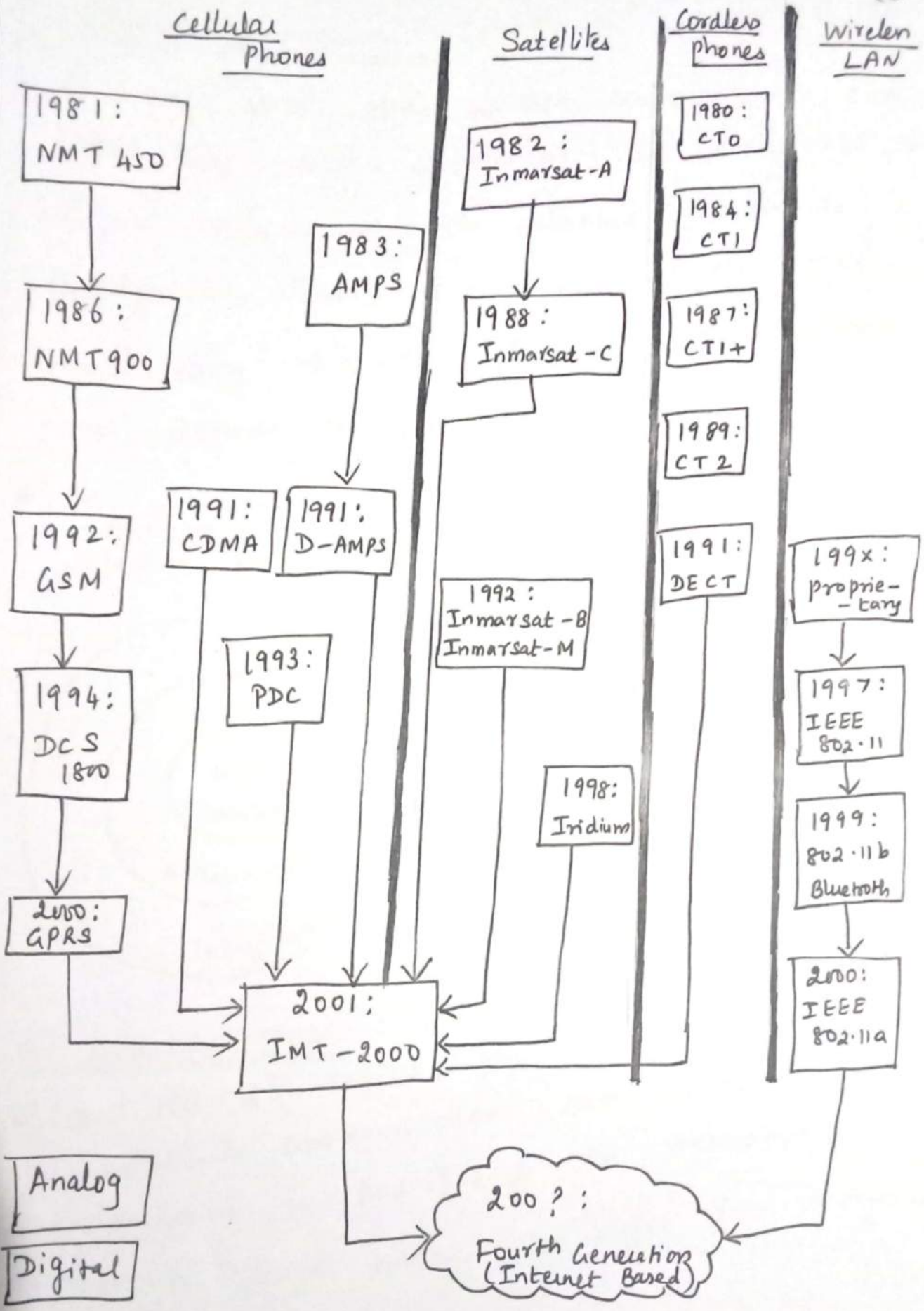


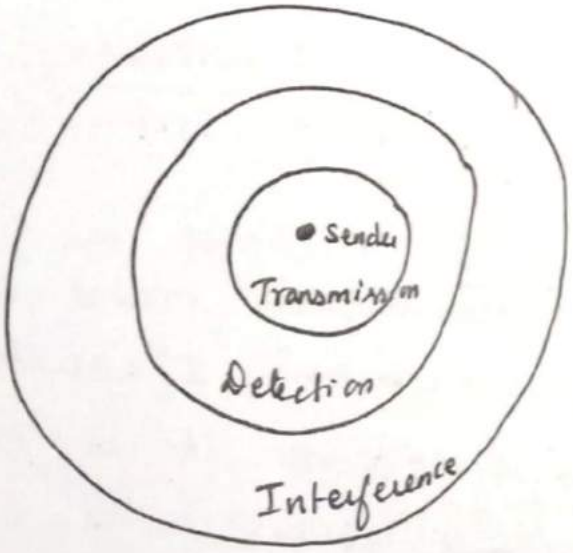
Figure: Overview of some wireless communication systems

(4) Signal Propogation:

*) Liked wired n/w, wireless communication n/w also have senders & receivers. In wireless n/w, the signal has no wire to determine the direction of propogation, whereas signals in wired n/w only travel along the wire. In wired n/w the receiver power depends on the length of travel.

*) In wireless, the distance of travel is well explained by 3 types of ranges:

i) Transmission range
ii) Detection range
iii) Interference range



i) Transmission range:

*) within a certain radius around the sender, transmission is possible. A receiver receives the signal with low error rate.

ii) Detection range:

*) In the 2nd radius, the error rate is too high to establish communication. Here detection of transmission is possible & the transmitted power is large enough to differ from background noise.

iii) Interference range:

*) In the 3rd radius, the sender may interfere with other transmission by adding to the background noise.

*) For wireless communication, the above said behaviour is possible only if the transmission takes place in vaccum, ie, nothing exists b/w sender & receiver.

*) However in real life this does not happen, because the radio signals has to cross atmosphere, mountains, buildings, moving sender & receiver etc.

The difference between wired & wireless transmission is explained below:

i) Path loss of radio signals:

*) In free space, the radio signals travel in a st. line similar to light waves. If such st. line exists between a sender & receiver it is called as line-of-sight (LOS).

*) Even if no matter exists between sender & receiver (in vaccum), the signal still experience the free space loss.

*) The received power is inversely Proportional to the distance $P \propto \frac{1}{d^2}$ between the sender & receiver.

*) The signal send from the sender moves with a spherical shape. If there is no obstacle. the sphere grows continuously.

*) If the distance between the sender and receiver increases, the received power decreases.

*) The received power also depends on
i) Distance
ii) wavelength
iii) gain of the receiver & transmitter antenna.

*) Depending on freq, the radio waves can penetrate through objects

→ Lower the frequency → Long wave

Low frequency
i) wavelength longer
ii) called as Infrared light
iii) has Less energy
iv) FM
v) Has better penetration
vi) can penetrate thro' ocean.

→ Higher the frequency → Short wave

High frequency
i) shorter wavelength
ii) called as visible light
iii) has lot of energy
iv) AM
v) Even blocked by tree.

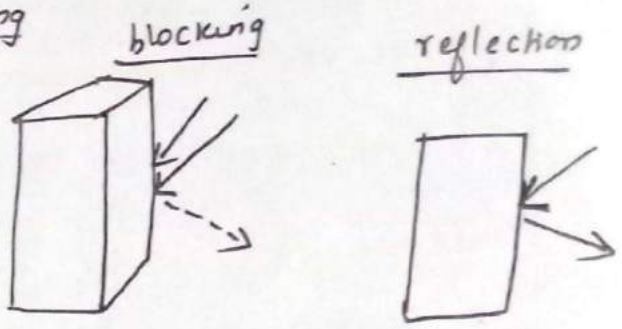
*) At high frequency, the radio signal resemble more that of light wave.

ii) Additional signal propagation effects:

*) In real life, rarely we have LOS b'w the sender & receiver b'z of mountains, buildings, etc between sender & receiver.

*) There are 4 forms of attenuation (destroying)

i) blocking or shadowing
ii) reflection
iii) Scattering
iv) Diffraction



a) Blocking / shadowing:

*) This is the extreme form of attenuation of radio signals due to large obstacle.

*) If the frequency of the signal is higher, it behaves like an light and even small obstacle like tree, wall may block the signal.

b) Reflection: (obj > wavelength)

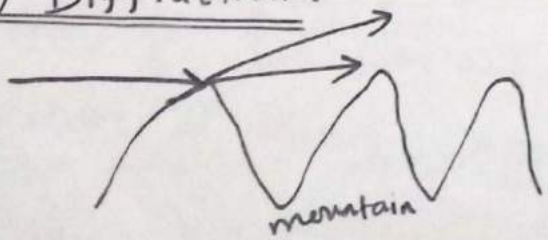
*) If an object is large compared to the wavelength of the signal eg, large buildings, mountain, etc, the signal is reflected. The reflected signal is not as strong as the original, because the objects absorb some of the signal's power.

*) Shadowing & reflection are caused by objects much larger than the wavelength of the signal.

c) Scattered: (obj < wavelength)

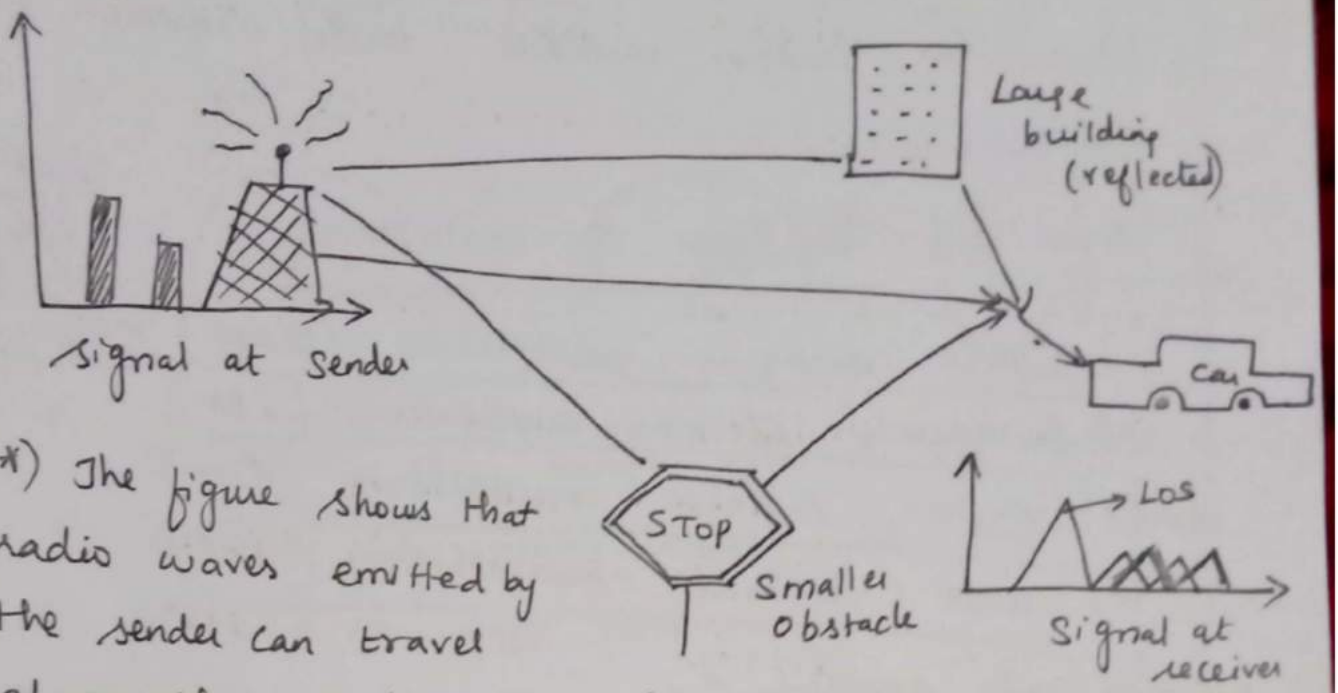
*) If the size of an obstacle is less than the wavelength, then the incoming signal gets scattered. The incoming signal is scattered into several weaker outgoing signals

d) Diffraction:



*) Diffraction is similar to scatter Radio waves will be deflected at the edges are propagated in different direction.

iii) Multipath Propagation



*) The figure shows that radio waves emitted by the sender can travel along the st. line or they may be reflected at a large building or scattered by small obstacle. This propagation effect is called Multi-path propagat

*) In reality, many more paths are possible. Hence signal travelling along different path with different lengths arrive the receiver at different times. This effect caused by multi path propagation is called delay spread.

*) The delay spread are up to 3μs in cities

(5) Multiplexing: (Many to one)

Multiplexing explains how many users share a single medium with minimum or no interference.

There are 4 types of multiplexing

i) Space division multiplexing (SDM)
ii) Frequency division multiplexing (FDM)
iii) Time division multiplexing (TDM)
iv) code division multiplexing (CDM)

*) One example is,

If many users (car drivers) want to use the same medium (highways) without any interference (accident). This is possible by

→ providing several lanes (space division multiplexing)
→ using same lane but in diff time (Time division multiplexing)

i) Space division Multiplexing (SDM):

*) The task of multiplexing is to assign space, time, frequency & code to each communication channel with a minimum of interference and a maximum of medium utilization.

*) Consider 6 channels $K_1, K_2 \cdots K_6$ and 3-D coordinate system (Code C, time t & freq f)

Channel K_i

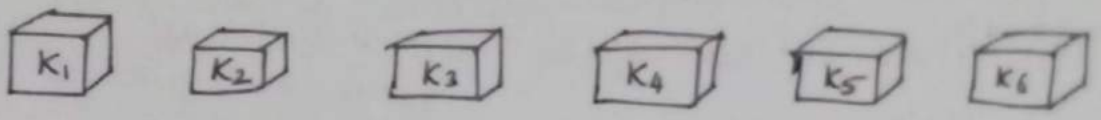
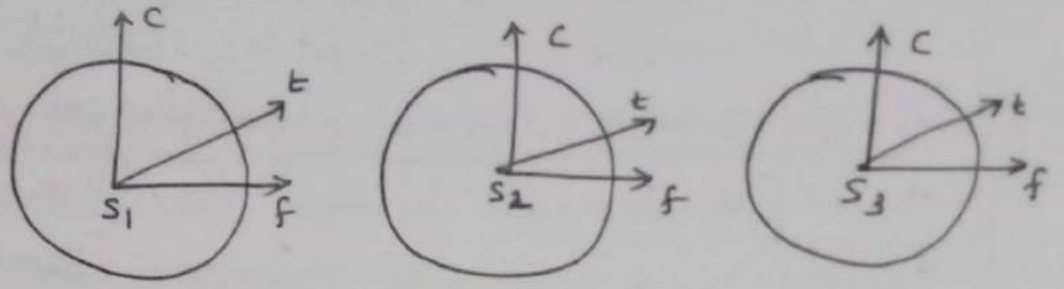


Figure: Space division multiplexing



*) In SDM, the entire system eg, mobile comm. is divided into many states and each state is allocated to each user.

*) In this diagram, K_1, K_2 & K_3 are mapped to 3 spaces S_1, S_2 & S_3.

*) In all the 4 multiplexing guard space is used to reduce the interference. It is between 2 states (interference range)

*) For K_4, K_5 & K_6 three additional spaces are needed.

*) The example for SDM is old analog telephone system, ie, each subscriber is given a seperate pair of copper wires to the local exchange.

*) Even though the transmission range (space) is limited to a certain range but any one of different space can use the same frequency.

Disadvantage:

*) If there is additional channels added and there is no space for them, they have to be added within the previous space.

ii) Frequency division Multiplexing (FDM):

*) FDM scheme divides the frequency into many non-overlapping frequency bands.

*) Each channel ($K_1 \cdots K_6$) are allotted different frequencies. Guard space are needed to avoid frequence overlapping (also called as adjacent channel interference)

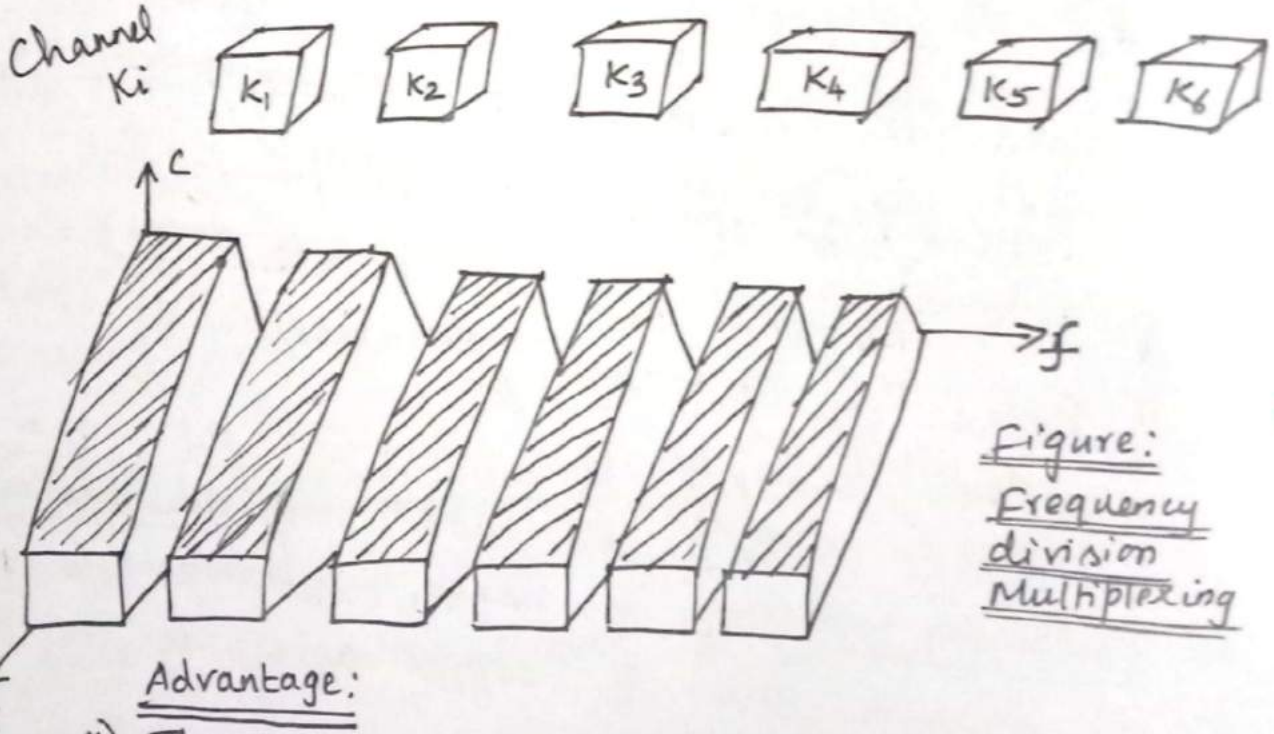


Figure: Frequency division Multiplexing

Advantage:

*) This is a very simple multiplexing scheme, it does not need a complex coordination b/w sender & receiver, the receiver only has to tune to the specific sender.

*) This scheme is used for radio stations within the same region, where each radio station has its own frequency.

Disadvantage:

a) By assigning seperate frequency for each channel there is a tremendous waste of frequency resources.

b) Need careful frequency planning.

c) Makes the scheme very inflexible.

iii) Time division multiplexing (TDM)

*) More flexible multiplexing scheme is TDM, here all the senders can use the same freq but at different point of time.

*) Guard space are used, which represents the time gap, i.e, it seperates the time period.

[Guard space → space b/w 2 cars in highways]

*) If 2 channels overlap in time, this is called as co-channel interference. To avoid this type of interference, synchronization b/w different senders is necessary.

*) In highways, interference between two cars results in an accident.

Disadvantage:

i) The sender has to wait until his time slot arrives.

ii) All senders need precise clocks, to distribute synchronization signal to all senders.

Advantage:

i) This scheme is flexible.

ii) This scheme allots more time to senders with heavy load & less son time to senders with light load.

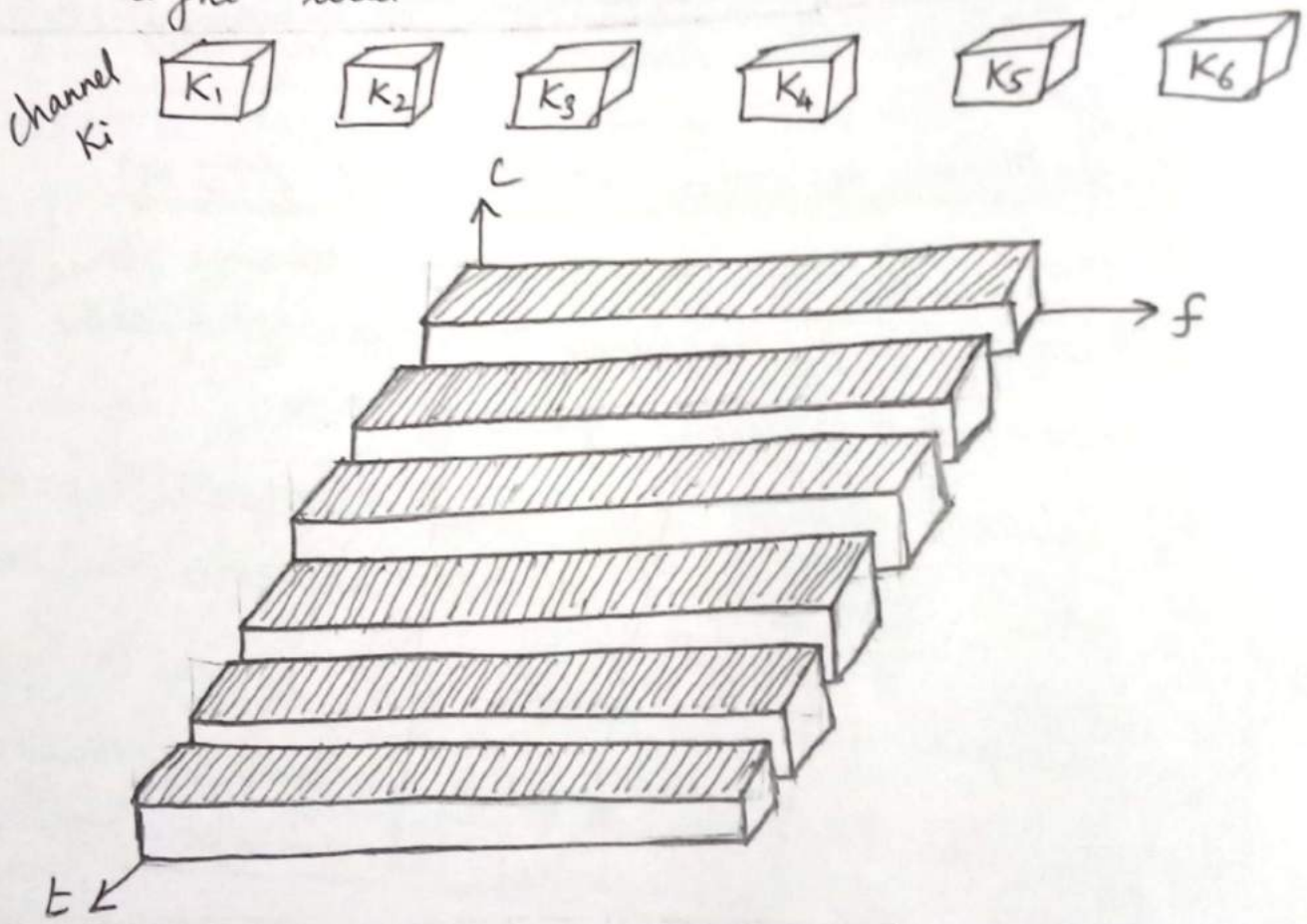


Figure: Time division multiplexing

FDM ↓

[All senders → same freq → same time]

FDM + TDM Combined:

*) Frequency division and Time division multiplexing can be combined.

*) Here each channel K_i can use certain frequency in certain amount of time.

*) Guard space are needed both in time & in freq. dimension.

*) A channel can use a certain frequency only for a short period of time.

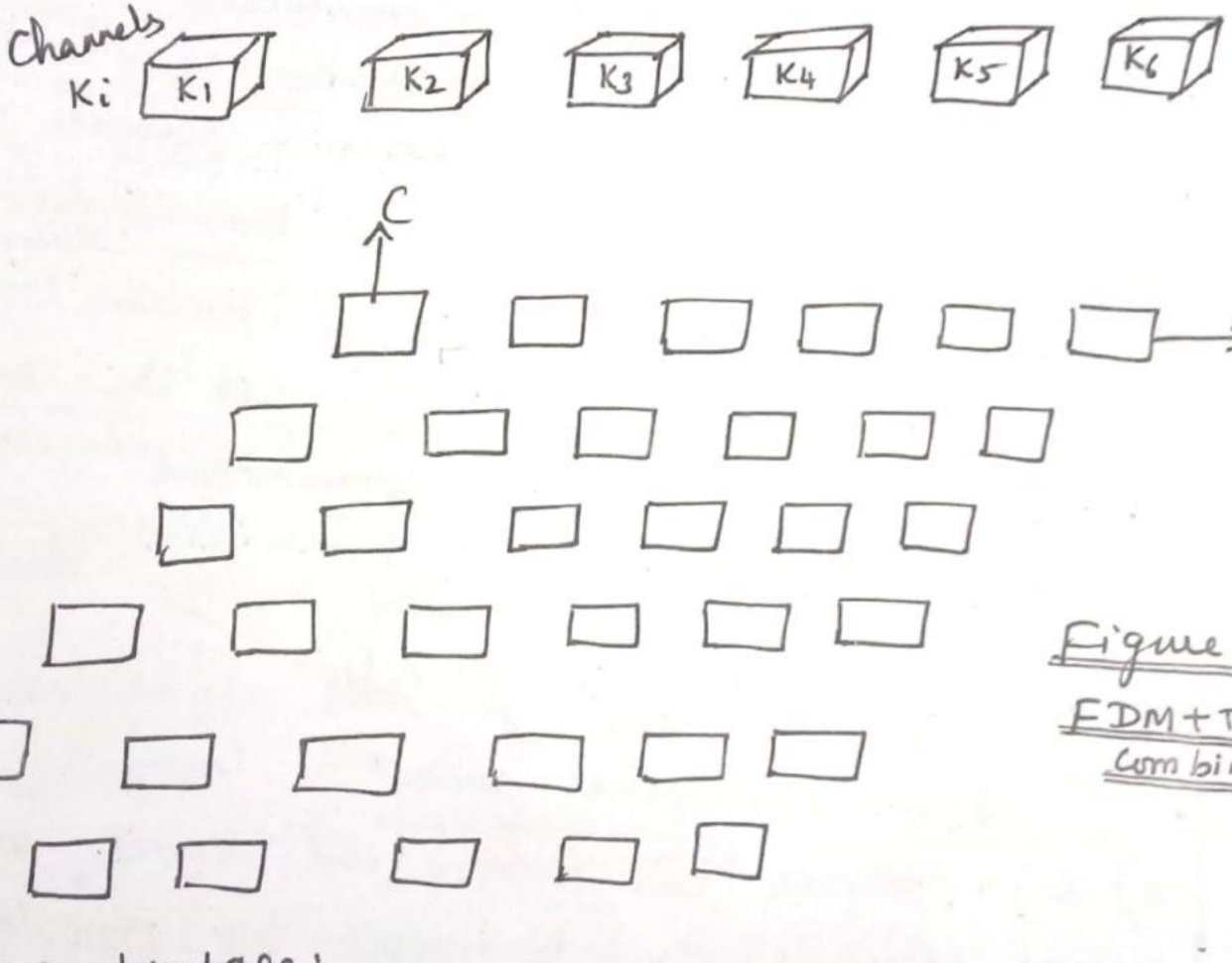


Figure: FDM+TDM Combined

Disadvantage:

i) Necesary coordination b'w diff. senders is needed. ie, one has to control the sequence of freq & time.

ii) Two senders will interfere if both select the same freq. at same time.

If freq. change (freq. hopping) is fast, the period [illegible] (collision) will be small.

iv) Code division Multiplexing (CDM):

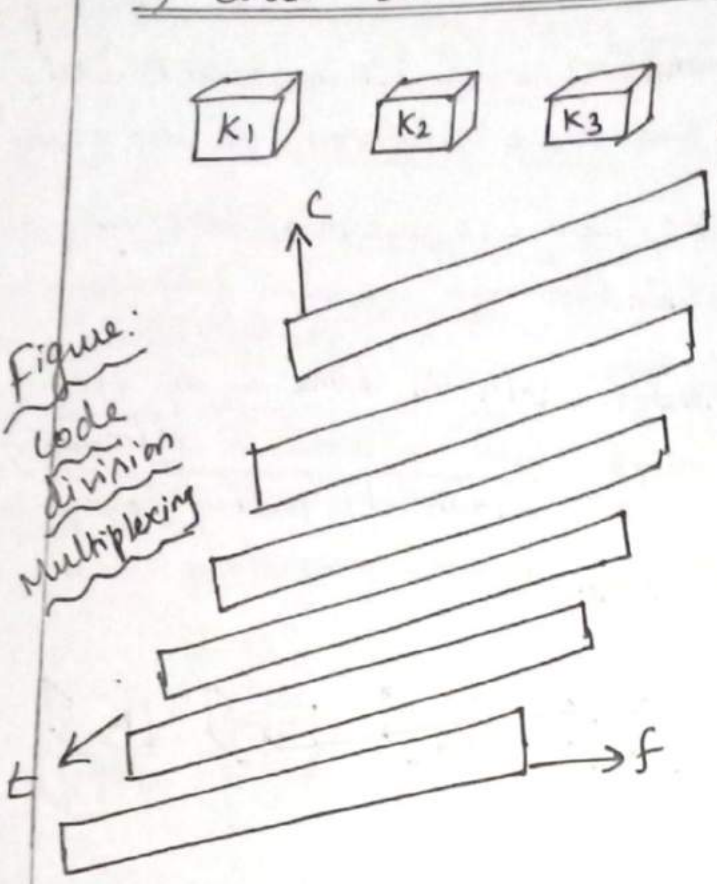


Figure: code division Multiplexing

*) SDM & FDM are well known from the early days of radio transmission.

*) TDM is used in many application.

*) CDM is the new scheme in commertial comm. system

*) Mainly used in military application due to its security features.

*) It is also used in civil wireless transmission because of cheap processing power.

*) In CDM, all channels (K_i) use the same freq. at the same time for transmission.

*) A seperate code is alloted to each channel.

*) Guard space is used for code space
eg. orthogonal codes.

*) If receiver can receive the signal, only if he knows the code sent by the sender. Each & every channel possess seperate code hence there is high security.

Advantage:

i) Main adv. of CDM in wireless transmission is the good protection against interference & tapping.

ii) High security.

iii) Assigning individual to each sender does not cause any problems.

Disadvantage:

i) High complexity

ii) Receiver has to know the code & must seperate the channel data from background noise & environmental noise.

iii) Receiver must be synchronized with the transmitter to apply decoding correctly.

iv) code space is huge compared to frequency space.

v) For CDM, precise power control is required

---

6) Spread Spectrum

Spread spectrum involves spreading the bandwidth (BW). Spreading the BW has several advantage. The main adv. of these technology is the resistance of narrow band interference.

steps for spreading & despreading:

Step 1:

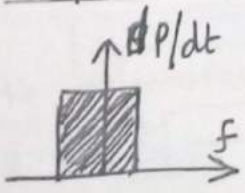
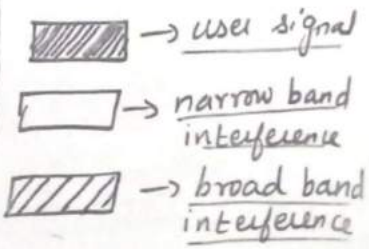
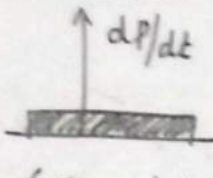


Figure shows the
*) Narrow band signal from a sender of user data
*) power density (dP/dt) verses freq. f



Step (ii)

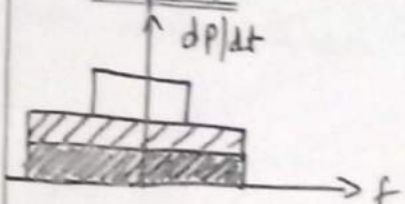


(spreading takes place)

*) During step (ii), narrow band signal is converted into broad band signal.
i.e, same signal is spread over large frequency range.

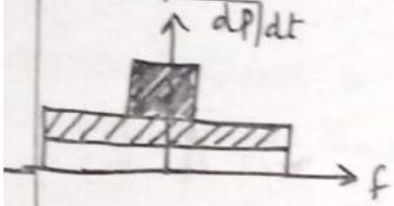
*) Power level is lower than the original narrow band signal.

Step (iii)



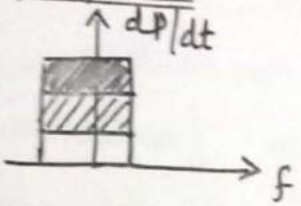
*) During step (iii), narrow band and broad band interference adds to the user signal.

Step (iv):



In step iv,
*) Despreading takes place ie, converting user signal into narrow band signal again

Step (v):

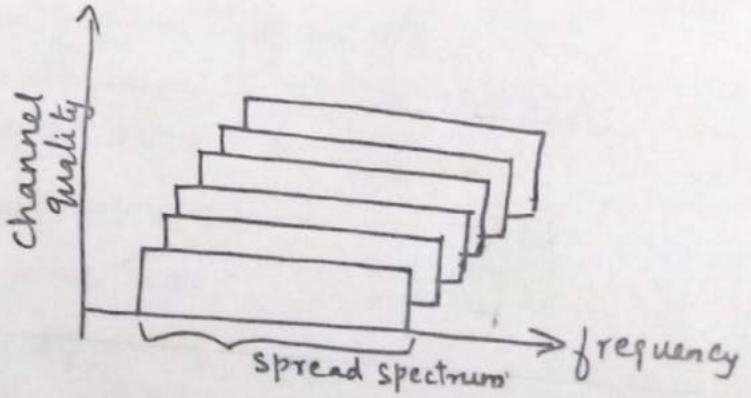


*) In step v, the receiver applies band pass filter to cut off frequencies left and right of the narrow band signal. Finally the original data is reconstructed because the power level is high.

*) Till now we have seen that spread spectrum is used for single channel. Now let us consider 6 different channels. To seperate diff channel, CDM is used instead of FDM.

*) Spreading of narrow band is achieved by using a special code. ~~Each~~

Figure:
Spread spectrum to avoid narrow band interference



*) Each channel is alloted its own code, and the receiver should also known its code. without knowing the code, the receiver cannot receive the signal and the signal behaves like a background noise.

*) Combination of CDM + Spread spectrum is used in military applications.

Disadvantage:

i) Increased complexity of receivers
ii) Large freq. band is needed [due to spreading of signal].
iii) Spread signal interfere with other transmission if no special precaution is taken.

*) Spreading can be achieved in 2 ways

i) Direct sequence spread spectrum (DSSS)
ii) Frequency Hopping Spread spectrum (FHSS)

i) Direct Sequence Spread spectrum (DSSS):

*) DSSS system performs an XOR operation with user data and chipping sequence. The example shows that result is either 0 1 1 0 1 0 1 → if user bit = 0

(or)

1 0 0 1 0 1 0 → if user bit = 1.

user data ⊕ chipping sequence = Resulting signal

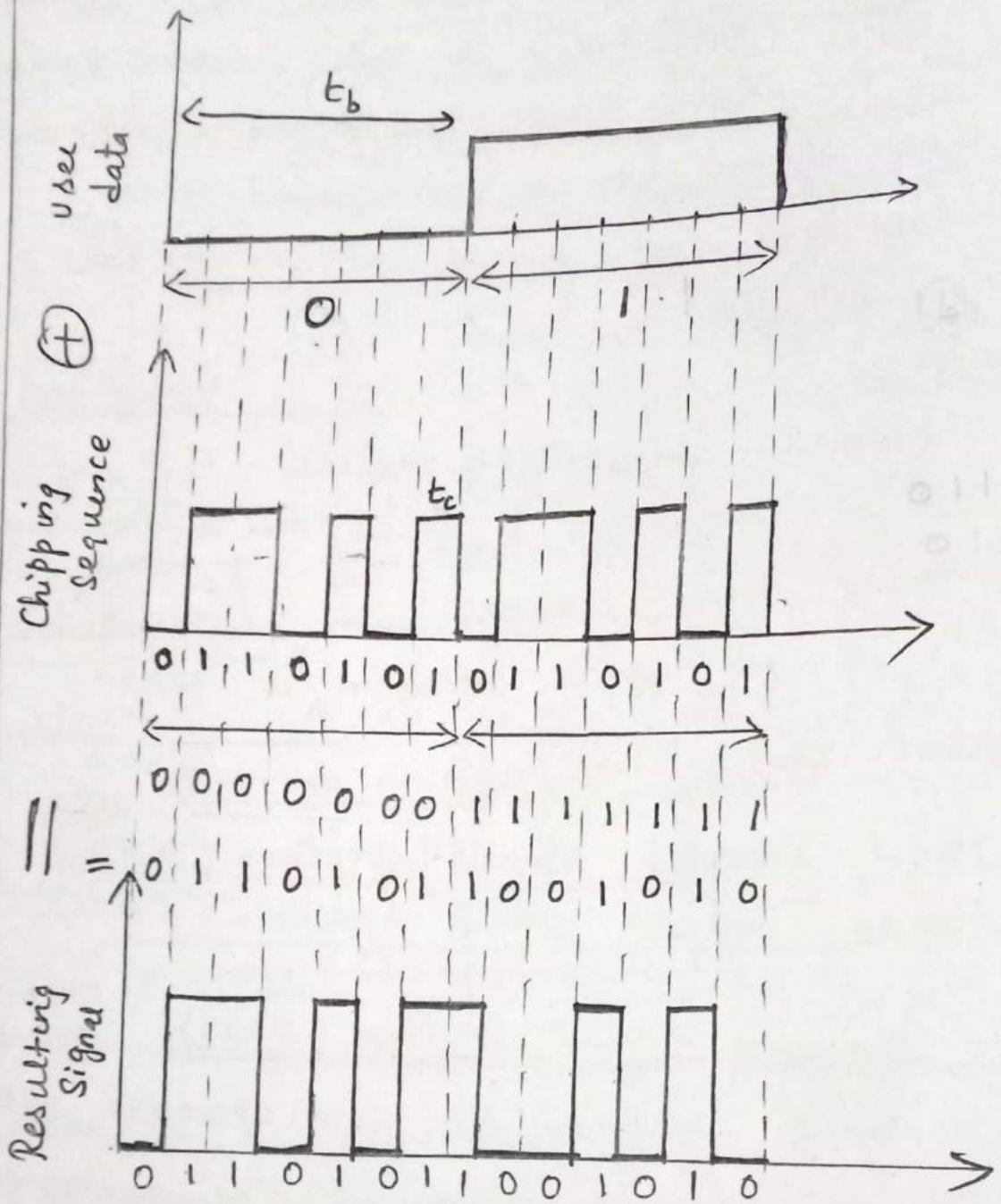
XOR

0 0 → 0
0 1 → 1
1 0 → 1
1 1 → 0

t_b → user bit duration

The chipping sequence consists of smaller pulses called chip

t_c → chip duration.



X-OR

0 0 → 0
0 1 → 1
1 0 → 1
1 1 → 0

User data ⊕ Chipping sequence = Resulting Signal

Figure : Spreading with DSSS

*) If chipping sequence is generated properly it appears as noise, this sequence is also known as Pseudo - noise sequence.

*) Spreading factor

$$S = \frac{t_b}{t_c}$$

determines the BW of resulting signal

Pseudo Noise Sequence

Pseudo Noise sequence.

$S = \frac{t_b}{t_c}$

a) DSSS Transmitter:

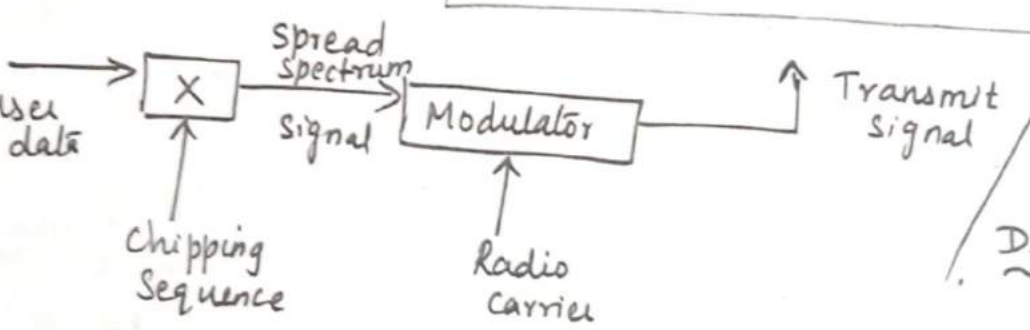


Figure: DSSS Transmitter

*) Step 1: Spreading of the user data with the chipping sequence (Digital Modulation).

*) Step 2: The spread spectrum is then modulated with a radio carrier (radio Modulation).

*) Assume the BW of user data to be 1 MHz, by spreading with barker code the BW of the user data will be 11 MHz. This signal is transmitted.

b) **DSSS Receiver:**

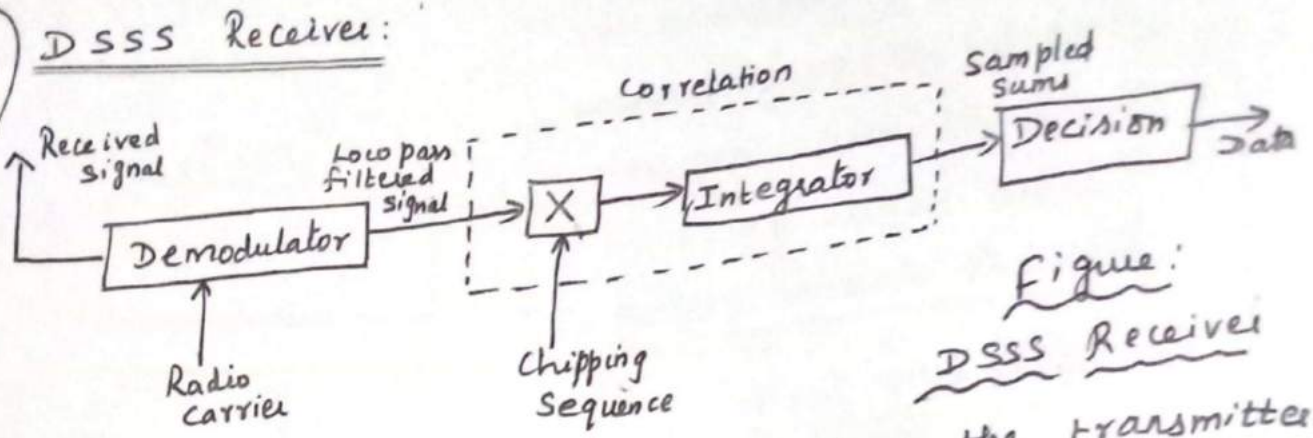


Figure: DSSS Receiver

*) DSSS receiver is more complex than the transmitter. Receiver performs inverse fn. of a transmitter steps:

Step 1: Demodulating the received signal by using the same carrier as the transmitter. Additional filtering can be applied to generate this signal.

Step 2: The signal obtained after passing through low pass filter is X-ORed with the same chipping sequence used by the transmitter. The chipping sequences at the sender & receiver have to be synchronized.

Step 3: The integrator adds all the products of each chip. Calculating the products of chip & signal and adding the products in an integrator is called correlation and the device is correlator.

Step 4: During each bit period, the decision unit checks the sum generated by the integrator & decide whether the sum represent a binary 1 or 0.

*) Sender

user data → 01 and applying barker code and the resulting spread signal is

10110111000100100011 1.

Receiver

Spread signal is X-ored bitwise after demodulation with Barker code as the chipping sequence.

ii) Frequency Hopping Spread Spectrum (FHSS):

*) In FHSS, total BW is split into many channel of smaller BW and guard space is between the channels. Transmitter & receiver stay in one of these channels for certain time and then hop (jump) to another channel. It uses FDM + TDM. This pattern is known as hopping sequence. The time spend on a channel with certain frequency is called dwell time.

*) Hopping are of 2 types i) slow hopping & ii) fast hopping.

a) Slow hopping:

The transmitter uses one freq. for several bit periods. The figure shows 5 bit period. (5 user bit)

*) In slow hopping the transmitter uses the freq. f_2 for transmitting the first 3 bits in the dwell time t_d. Then the transmitter hops to the next frequency f_3.

*) Slow hopping is cheaper & have relaxed synchronization.

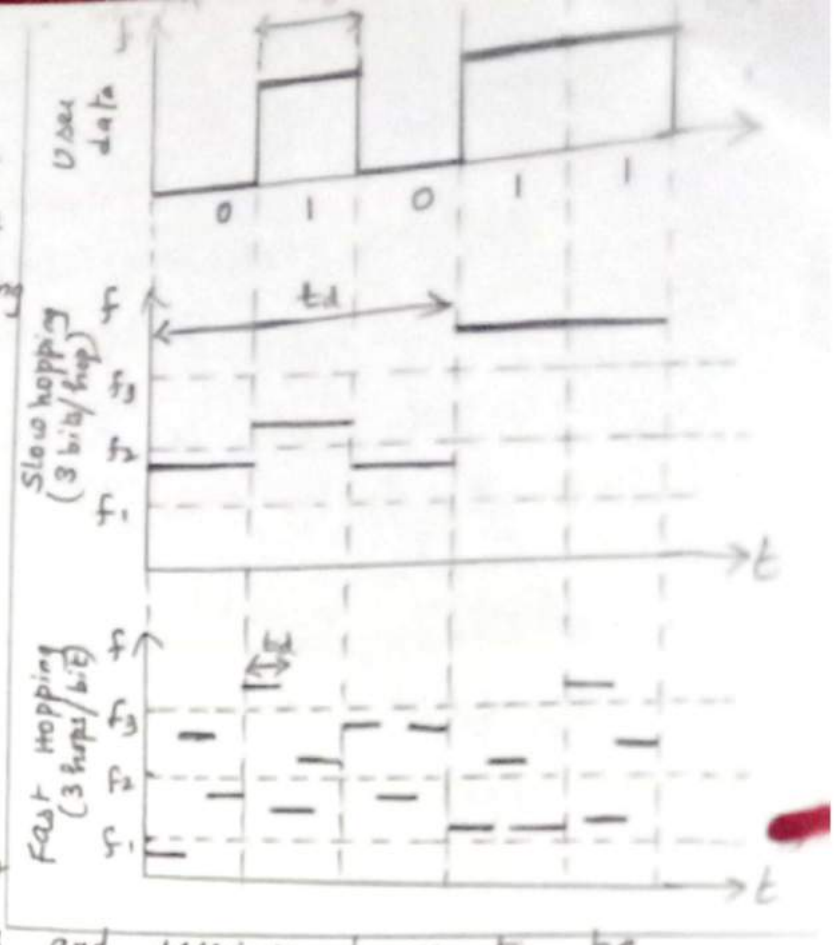
t_b → bit period
t_d → dwell period.

b) Fast Hopping :

*) In fast hopping, the transmitter changes the freq. several times during the transmission of single bit.

*) In this eg, the transmitter hops 3 times during a bit period.

*) Fast hopping is more complex to implement because the transmitter and receiver have to be synchronized.



1) FHSS Transmitter :

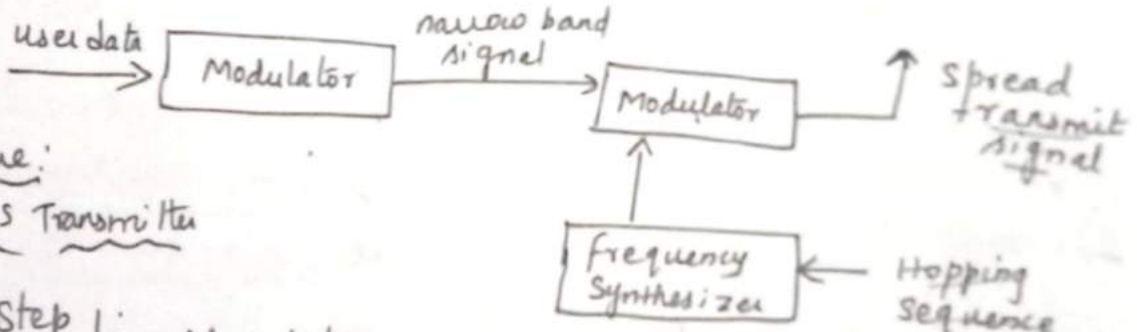


Figure: FHSS Transmitter

Step 1: Modulating the user data. The result is a narrow band signal. If FSK (frequency shift keying) is used, freq f_0 is for binary 0 & f_1 is for binary 1.

Step 2: Frequency hopping is performed based on the hopping sequence. The hopping sequence is fed into a frequency synthesizer which generates the carrier frequencies f_i.

Step 3: Second Modulation takes place.

*) It modulates the narrow band signal generated by the 1st modulator with the carrier freq (f_i) generated by the frequency synthesizer.

*) After the 2nd modulation, the spread signal is transmitted.

ii) FHSS Receiver:

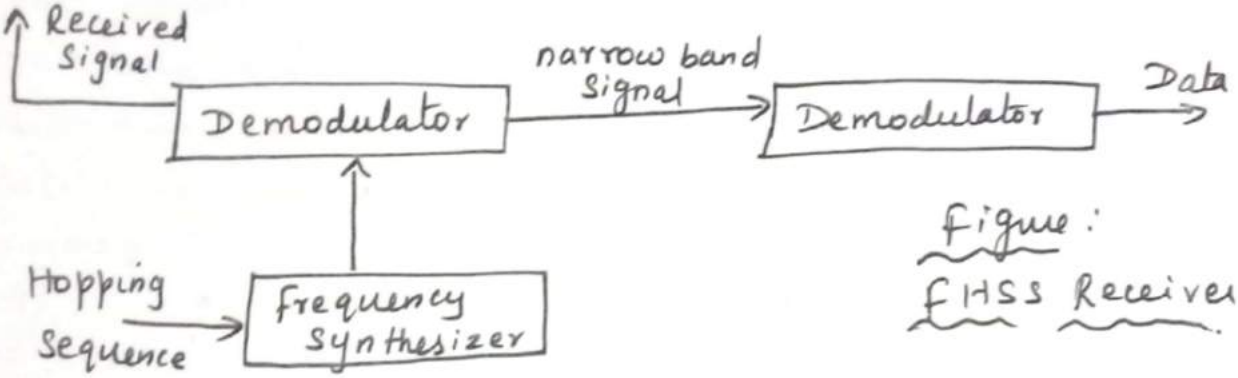


Figure: FHSS Receiver.

*) Demodulation performs the inverse operation of modulation, to reconstruct the original data. Several filters are needed (but not shown in fig.).

Comparision b'w FHSS & DSSS

DSSS	FHSS
1. Complex when compared to FHSS	1) Simpler than DSSS.
2. Always use total BW	2) Use only portion of total BW at any time.
3. More resistable to fading & multi path effects.	3) Less resistable.
4. DSSS signals are much harder to detect.	4) comparitevly less harder to detect FHSS signal.

(7) Multiple Access control (MAC) Protocols

In ISO/OSI reference model, MAC below to layer 2 (data link layer). Layer 2 is subdivided into i) logical link control (LLC)
ii) Multiple access control (MAC)

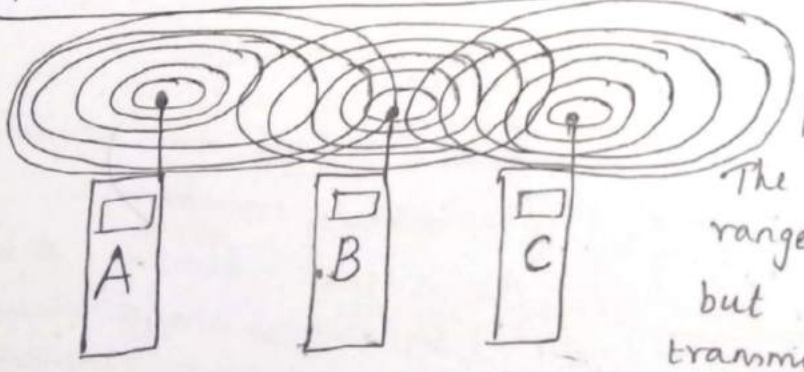
*) Now let us consider carrier sense Multiple access with collision detection (CSMA/CD).

It works as follows: The sender senses whether the tr. medium is free, if it is busy the sender waits until it is free. If it is free, the sender starts transmitting data. If the sender detects a collision while sending the data, it stops at once and sends the jamming signal. (damaged signal)

*) CSMA/CD really is not bothered about the collision at sender, but cares about the receiver side (ie the signal should reach the receiver without collision)

*) Where as in wireless media strength of signal decreases as the distance increases by $P \propto \frac{1}{d^2}$

i) Hidden & exposed terminals:

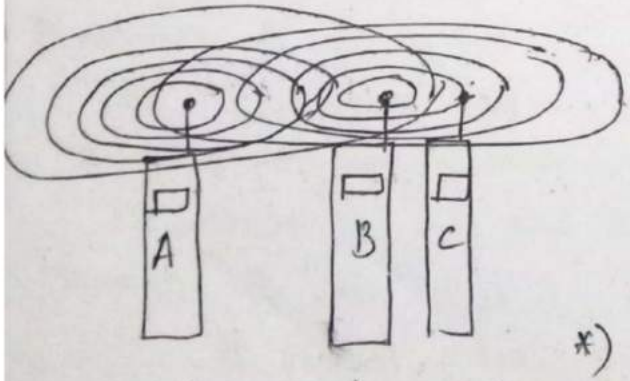


Consider 3 mobile phones A, B, C. The transmission range of A reaches B, but not C.. The transmission range of C reaches B, but not not A. Hence tr. range of B reaches A & C ie, A cannot detect C, Similarly C cannot detect A.

*) A starts sending to B, but C does not receive it. C also wants to send to B and checks the medium and found it to be free, thus C also starts sending hence causing a collision at B. But now A cannot detect this collision & continues with its transmission. Thus A is <u>hidden for C</u> & C is hidden for A

*) Now consider the situation that B sends something to A and now C wants to send to some other mobiles other than A & B. C detects that tr. medium is busy and postpones its transmission now if A wants to transmit data it can transmit and the waiting is not necessary b'z A is outside the intifeence range of C. collision at B is not a matter b'z the collision is too weak to propagate to A. In this situation, C is <u>exposed</u> to B.

ii) <u>Near & far terminals:</u>



*) Both A & B are sending with the same transmission power. B's signal diwon's A's signal [b'z A signal streyth decreases as distance increases) as a result C cannot receive A's transmission

*) Near / far is a severe pblm in wireless nlw using CDM. Near & far signal arrive at the receiver with more or less the same strength.

(8) Space Division Multiple Access (SDMA) :-

SDMA is used for allocating a seperate space to users in wireless n/w. A mobile phone may receive several base stations with different quality. A MAC algorithm decide which base station is best based on freq, time slot, & code. Thus SDMA assign an optimal base station to the Mobile phone user.

(9) Frequency Division Multiple Access (FDMA) :

*) FDMA uses FDM technology. Allocation can be either fixed or dynamic

*) In pure FDMA freq is divided into slots & each channel is assigned a different frequency slot, the channel should use only its freq. at all times.

*) To change from one freq. to another FDMA is combined with TDMA . In wireless system to change from one freq. to another is know as frequency hopping. The sender & receiver should agree for the freq. hopping & it should be fixed for a longer period.

*) FDM uses duplex channel ie both Mobile Station & base station communicate using diff freq. This is called as frequency division duplex(FDD) Both partners should know the freq. in advance The two freq. are i) up link

Uplink (fu) → from mobile station to base station (or) ground control to satellite

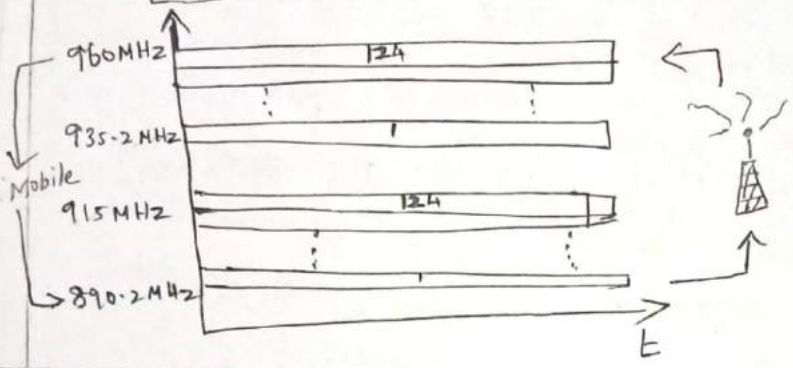
(fd) downlink → from base station to Mobile station (or) Satelite to ground control

(fu) uplink → uses freq b/w 890.2 & 915 MHz

(fd) downlink → 935.2 to 960 MHz

if fu → 890 MHz + n·0.2 MHz then

fd = fu + 45 MHz i.e fd = 935 MHz + n·0.2 MHz



---

(10) TDMA (Time Division Multiple access)

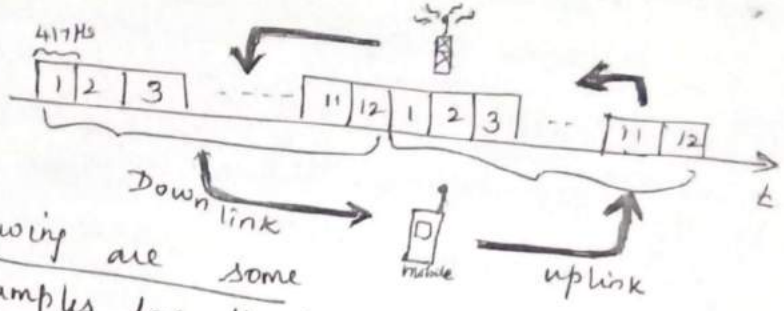
*) compared to FDMA, more flexible scheme is TDMA

*) It uses TDM technology, where the channels are seperated by different time slots and also the channels can use diff freq. in their time slots.

*) Synchonigation is established b/w sender & receiver. Time slot allocation can be done by fixed or dynamic scheme.

→ Dynamic allocation scheme require an identification for each transmision

→ fixed allocation scheme do not require an identification



The following are some several examples for fixed & dynamic allocations used for wireless transmission

(i) Fixed TDM:

*) This is the simplest and it has fixed BW and it has fixed delay

*) Assigning diff time slots for uplink & downlink using same frequency is called time division duplex (TDD)

From the above fig. base station use 12 slots for down link, where as a mobile station use one of the 12 slots for uplink. Hence 12 diff mobile station use the 12 slots with same freq. without interference using this scheme.

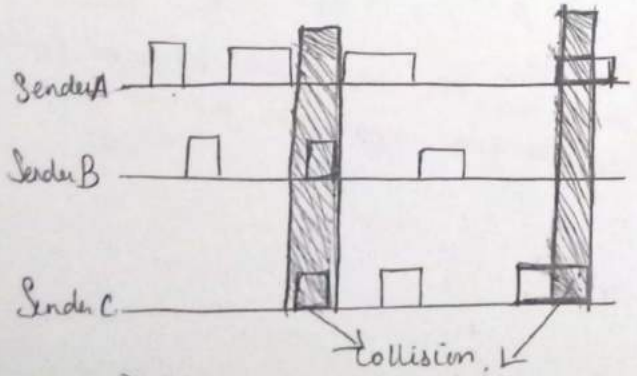
*) The duration of each time slot is 417μs.

Disadvantage

→ Fixed TDM is inefficient for bursty data or asymmetric connections

(ii) Classical Aloha:

If TDM is applied without controlling access then it is classical Aloha scheme.



*) Each station can access the medium at any time. This is a random access scheme i) without controlling access & ii) without coordination among stations

*) If 2 or more stations stations access the medium at the

same time collision occurs and the transmitted data is destroyed

Disadvantage:

i) works good only for light load.

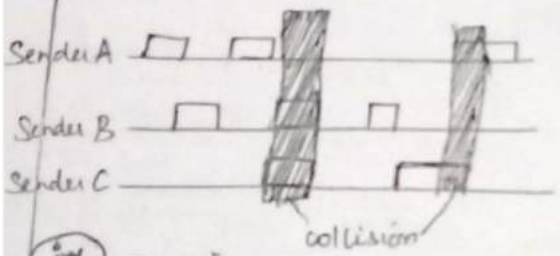
ii) Max throughput achieved is 1/e % load.

(iii) Slotted aloha:

*) If the time slots is added in classical aloha then the scheme is called as slotted aloha.

*) In this case all the senders has to be syncheonized & the transmision starts only at the beginning of the time slots. Still the accen is not co-ordinated.

*) Thruyhput raises from 18% to 36%. slotted aloha doubles the throughput



(iv) Carrier Sense Multiple Accen:

*) CSMA the carrier is sensed before accessing the medium.

*) Several version of CSMA is gn. below.

→ (a) non-persistent CSMA:

In non-persistant CSMA, station sense the carrier and check whether the transmision medium is free, if it is idle (free) the datas are send immediately

→ (b) p-persistent CSMA:

In p-persistent CSMA, node sense the medium and if it found to be free, the datas are transmitted with a probability of p.

→ (c) 1-persistent CSMA

As soon as the medium become idle, all the stations wishing to transmit accen the medium

(iv) Elimination Yield - non preemptive multiple access (EY-NMPA)

*) After sensing the medium, if it is idle, only one station can transmit and it is the 'winner' ie winner can finally access the medium for data transmission. The winner station is identified based on priority schemes.

(v) Demand assigned Multiple access (DAMA)

*) DAMA is also called as reservation aloha. It is used in satellite systems.

*) It has 2 modes i) contention phase
ii) Reservation phase.

*) In contention phase:

All ground stations will try to reserve future slots. eg diff stations on earth try to reserve access time for satellite transmission

*) In reservation phase:

Since the time slots are reserved for future, the collision do not destroy data transmission.

*) Since a time slot is reserved for future use, no other station is allowed to transmit during this slot.

*) The satellite collects the requests and sends back a reservation list indicating access rights for future slots. All ground stations has to obey this list.

*) Stations has to be synchronized from time to time

DAMA is a explicit reservation scheme.

(vi) PRMA (Packet Reservation Multiple Access):-

*) In PRMA, slots are reserved implicitly ie it is a implicit reservation scheme.

*) A certain no. of slots forms a frame. Here 8 slots form a frame.

	1	2	3	4	5	6	7	8
Frame 1	A	C	D	A	B	A		F

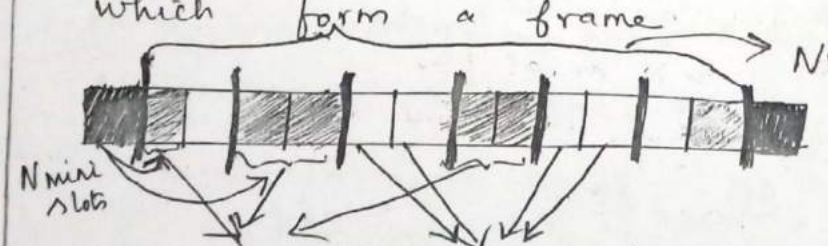
*) A base station broadcasts the status of each slot to all mobile stations

eg base station broadcasts the reservation status 'ACDABA — F' to all stations.

*) This means 1 to 6 and 8 are occupied but slot 7 is free. Base station broadcasts the above inf to all mobile stations. Therefore all stations wishing to transmit can now compete for the free slot in Aloha fashion. If more than one station wants to access this slot, collision occurs.

(vii) Reservation TDMA:

*) This is a fixed pattern. In this scheme it has N mini-slots followed by N·K data slots which form a frame.



eg N = 6 (mini-slot)
K = 2 (data slot)
totally = 6 × 2 = 12 data slot
N*K

*) 6 mini slot ∴ 6 station can use this slots

*) Each station is allotted a mini-slot and it can be used to reserve upto $K^{(2)}$ data slots.

*) The unused data slots can be used based on simple round-robin scheme.

(viii) Polling:

Polling is a centralized scheme with one master station & several slave stations. The master can poll the slaves according to many schemes: round robin, randomly.

(ix) Inhibit Sense Multiple accen (ISMA):-

ISMA is a scheme which is used for the packet data transmission service Cellular Digital Packet data (CDPD) in the AMPS mobile phone system. It is also known as digital sense multiple accen (DSMA).

(vii) Code Division Multiple Access (CDMA)

*) CSMA system we exactly the codes to seperate different users

*) Main problem in CSMA is
- How to frid 'good' code.
- How to seperate the signal from noise generated by other signal & environment

*) A code should have
- a good auto correlation
- be orthogonal to other codes

*) Consider the system coordinates & vectors starting at the origin ie (0,0,0)

*) Two vectors are called orthogonal, if their inner product is 0 eg: consider 2 vectors

(2,5,0) * (0,0,17) = 0. In this case the 2 vectors are orthogonal. bz the inner pdt is 0.
=0+0+0=0

eg2 (1,2,3) * (4,2,-3) = 4+4-9 = -1 almost orthogonal

eg3 (1,2,3) * (4,2,-6) = -10 not orthogonal

The basic function of CDMA is

Step 1

Two senders A & B want to send Data
CDMA assign key for A & B is A_k & B_k

$A_k \rightarrow$ A's key $A_d \rightarrow$ A's Data
$B_k \rightarrow$ B's key $B_d \rightarrow$ B's Data

Sender A want to send bit $A_d = 1$
Sender B want to send bit $B_d = 0$
and key A_k = 010011 & B_k = 110101

Now let us code binary 0 as -1 &
binary 1 as +1

Step 2:

Both senders spread their signals using their key. "spreading" means multiplying data bit with the key.

$A_s \rightarrow$ A's Signal
$B_s \rightarrow$ B's Signal

→ $\boxed{A_s = A_d * A_k}$
$= +1 * (-1, +1, -1, -1, +1, +1)$
$= (-1, +1, -1, -1, +1, +1)$

→ Sender B's signal is

$\boxed{B_s = B_d * B_k}$
$= -1 * (+1, +1, -1, +1, -1, +1)$
$= (-1, -1, +1, -1, +1, -1)$

Step 3

Both the A's signal (A_s) and B's signal (B_s) are transmitted at same time, using same frequency, having same strength & their is no interference.

The signal received at the receiver is C

$C = A_s + B_s$

$= (-1, +1, -1, -1, +1, +1) + (-1, -1, +1, -1, +1, -1)$

$C = (-2, 0, 0, -2, +2, 0)$

Step 4:

Now despreading takes place at the receiver side to obtain the original A's & B's data.

→ Sender A's data can be obtained by

$C * A_K = (-2, 0, 0, -2, +2, 0) * (-1, +1, -1, -1, +1, +1)$

$= 2 + 0 + 0 + 2 + 2 + 0 = 6.$

The result is +ive, hence receiver detects it as binary 1

→ Sender B's data can be obtained by

$C * B_K = (-2, 0, 0, -2, +2, 0) * (+1, +1, -1, +1, -1, +1)$

$= -2 + 0 + 0 - 2 - 2 + 0 = -6$

The result is -ive, hence the receiver detects it as binary 0.

*) In the above cases noise was neglected

*) If Sender A wants to transmit bit 101 & A's key is given as signal Sender B wants to transmit bit 100 and B's key is also given as signal.

Spreading is done by XORing

Mathematically $A_d \oplus A_K \Rightarrow A_s$

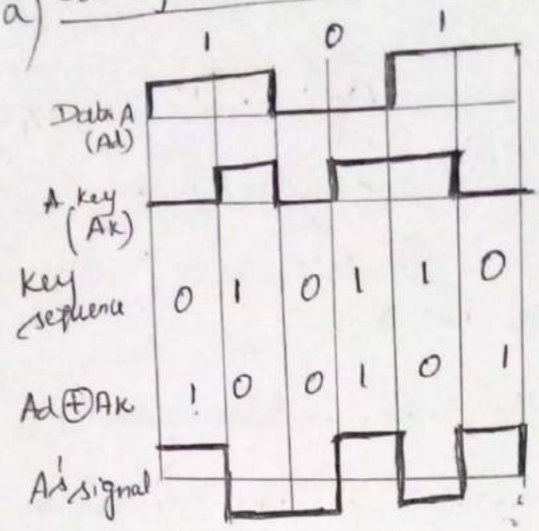
$B_s = B_d \oplus B_K$

$B_d = 100$, $A_d = 101$.

*) Finally A_s and B_s are added $C = A_s + B_s$ and transmitted via transmission line.

Sender Side:

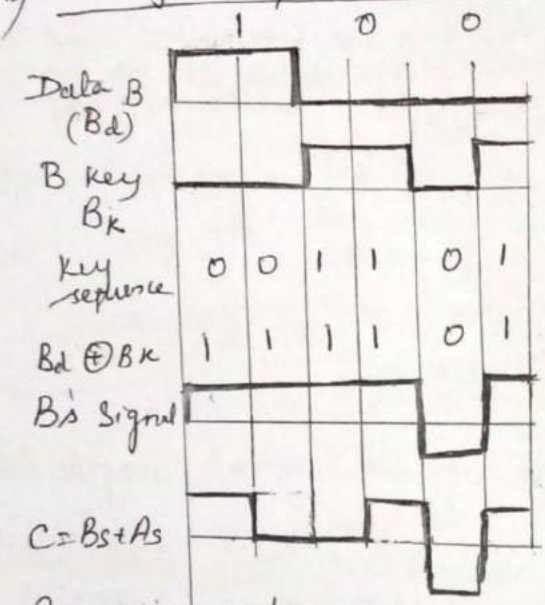
a) coding & spreading of data from Sender A



X-OR

0 0	0
0 1	1
1 0	1
1 1	0

b) coding & spreading of data from sender B

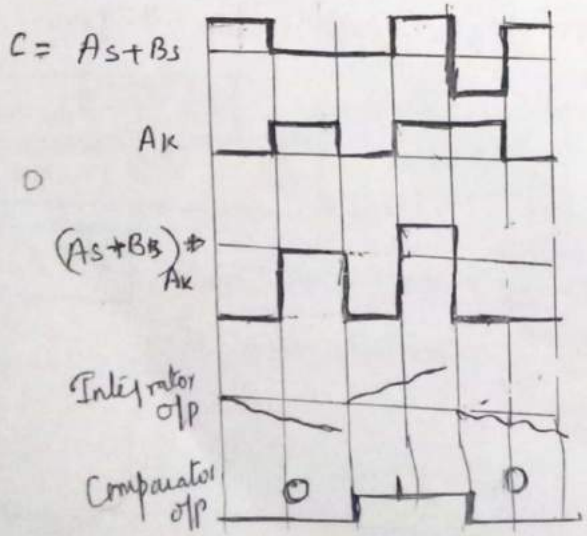


X-OR

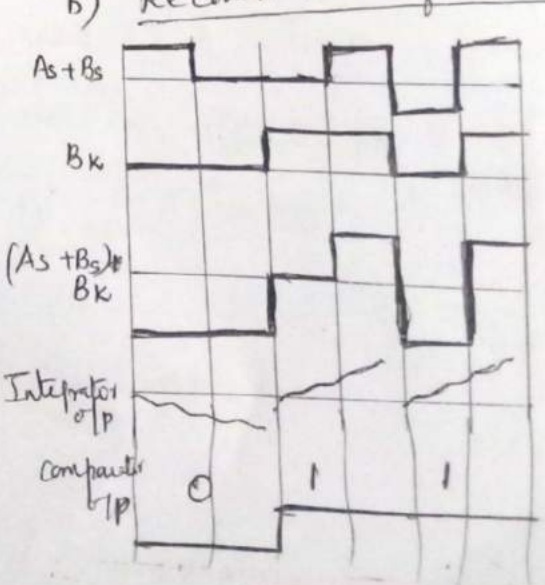
0 0	0
0 1	1
1 0	1
1 1	0

Receiver side

a) Reconstruction of A's data



b) Reconstruction of B's data



*) Invert the comparator o/p to produce the original data

*) At the receiver side the original A data can be obtained by despreading technique.

A's data	=	$(A_s + B_s) * A_k$
B's data	=	$(A_s + B_s) * B_k$

Spread Aloha Multiple Accen (SAMA).

*) CDMA senders & receivers are not simple devices To communicate with n devices we have to decode n different codes. The CDMA scheme, is good for connection-oriented services.

*) In case of connection-less services it is too complicated.

*) Aloha is a simple, connection-less scheme with low BW due to Collision.

*) If we combine the medium accen of aloha and spreading of CDMA. The resulting scheme is spread Aloha multiple accen (SAMA)

SAMA = MA of aloha + spreading of CDMA
&
It is a combination of CDMA & TDMA

	Approach	SDMA	TDMA	FDMA	CDMA
1.	Idea	Segment space into cells / sectors	Segment sending time into disjoint time-slots	Segment freq band into disjoint sub-bands	Spread the spectrum using orthogonal codes
2.	Terminals	Only one terminal can be active in one cell / one sector	All terminals are active for short time period on same freq.	Every terminal has its own freq, uninterrupted	All terminals can be active at the same place at the same moment, uninterrupted.
3.	Signal seperation	cell structure / directed antennas	Synchronization in the time domain	Filtering in the frequency domain	code plus special receivers
4.	Advantage	very simple, increases capacity / km^2	Established, fully digital, very flexible	simple, established, robust	Flexible, less planning needed, soft hand over
5.	Disadv.	Inflexible, antennas typically fixed	Guard space needed, synchronization difficult	Inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
6.	comment	Only in combination with TDMA, FDMA or CDMA	Std - in fixed n/w's together with FDMA / SDMA	Typically combined with TDMA & SDMA	Still faces some pblms, higher complexity, lowered expectations, Integrated with TDMA / FDMA

COMPARISION OF SDMA, FDMA, TDMA, CDMA

UNIT - II Mobile computing

1) GSM (Global System for Mobile communication)

*) GSM was initially developed in Europe using 890-915 MHz for the uplinks and 935-960 MHz for downlinks. This is called as GSM-900

*) There are 3 versions of GSM

i) GSM-900 with 890-915 MHz for uplink & 935-960 MHz for downlink

ii) GSM-1800 with 1710-1785 MHz for uplink & 1805-1880 MHz for downlink

It is also called as Digital cellular system (DCS) 1800

iii) GSM-1900 with 1850-1910 MHz for uplink & 1930-1990 MHz for downlink.

It is also called as personal communication service PCS 1900

*) Transparent bearer service use only the func of physical layer to transmit data. Therefore the data transmission has a constant delay

Non-Transparent bearer services uses protocols of layer 2 and 3 to implement error correction & flow control

1.1) GSM System architecture

GSM consists of 3 subsystems

i) radio subsystem (RSS)

ii) Network & switching subsystem (NSS) &

iii) Operation subsystem (OSS)

1.1.1) Radio Subsystem (RSS)

*) Radio subsystem consists of mobile station (MS) & base station subsystem (BSS)

*) RSS & NSS are connected via A-interface

NSS & OSS are connected via O-interface

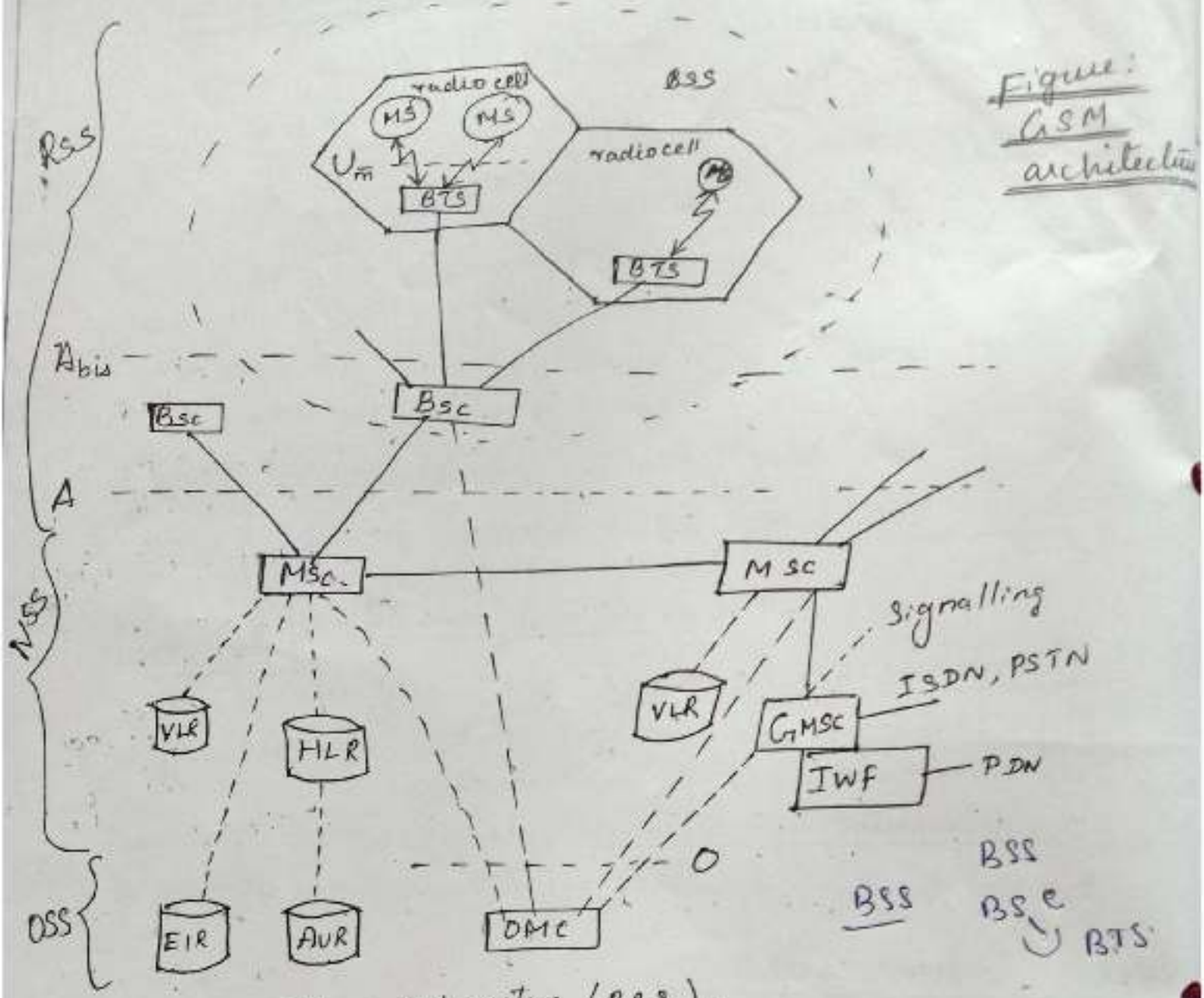


Figure: GSM architecture

a) Base station Subsystem (BSS):

A GSM n/w comprises many BSS, each controlled by a base station controller (BSC). The BSS contain many BTS's (Base transceiver station)

b) Base Transceiver station (BTS):

BTS contains all radio equipments ie, antennas, signal processing, amplifier necessary for radio transmission. A BTS form a radio cell using sectorized antennas and is connected to the MS via the Um interface and BTS is connected to Bsc via the Abis interface. Abis

c) Base station controller (BSC) :-
BSC controls all BTS's. It handles the hand over of freq. from one BTS to another BTS within the BSS.

d) Mobile Station (MS) :
MS contains all user equipments and s/w needed for communication with a GSM n/w.
MS contains H/w & s/w & SIM (subscriber Identity Module) which stores all user-specific data.

e) Network & switching Subsystem (NSS) :
NSS is the heart of GSM System
NSS contains the following switches & databases

a) Mobile Service switching centre (MSC) :
* MSCs are high-performance digital ISDN switches
MSC's are the backbone n/w of a GSM
* MSCs are connected to other MSC's via A interface.
* A gateway MSC (GMSC) is used to connect to other n/w's PSTN (public switching Telephone n/w) & ISDN (Integrated Service for digital n/w).

b) Home Location Register (HLR) :-
'HLR is the most imp. data base in the GSM system and it stores all users relevant information. It contains static + information such as Mobile subscriber ISDN no. (MSISDN) and it contains the current location area (LA) of the MS.

c) Visitor Location register (VLR):

VLR contains the dynamic information of the user (dynamic database).
If any new MS comes into the location area (LA) for which VLR is responsible, then the VLR copies the relevant information about the user from the HLR.

(iii) Operation Subsystem (OSS) :-

The 3rd part of the GSM system is the OSS, which contains all the functions necessary for n/w operation & maintenance. The OSS contains the following entities

a) Operation and Maintenance centre (OMC):

The OMC monitors and controls all other network entities via the O interface. OMC manages functions such as → traffic monitoring
→ Status reports of n/w entities
→ Subscriber & security management

b) Authentication centre (AUC) :-

*) The AUC contains the algorithms for authentication as well as the key for encryption
*) AUC is situated in a special protected part of the HLR

c) Equipment identity register (EIR) :- EIR

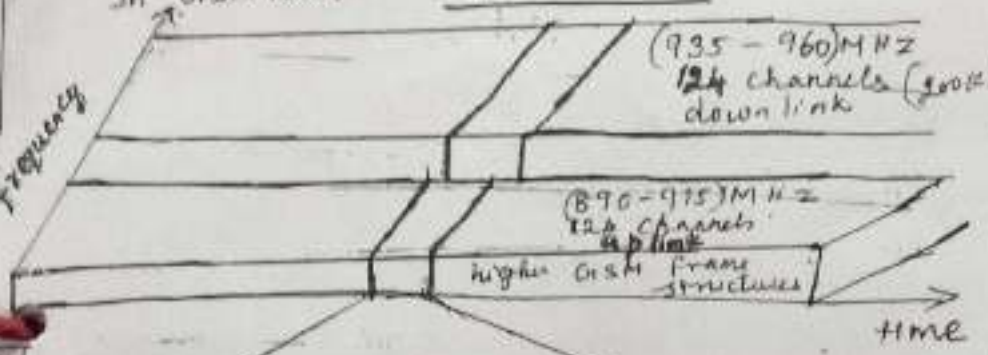
EIR is a database, it stores all device identifications registered for this n/w. If any mobile is stolen, & if the user register this SIM no. in the n/w, the EIR has a list of stolen devices. If the SIM no. is found to be roaming in the n/w, by the list in the EIR the mobile can be detected.

(2) GSM Radio Interface / Frequency allocation in GSM:

*) The most interesting interface in a GSM system is Um, the radio interface

*) GSM implements SDMA using cells
FDD is used to seperate downlink & uplink.

In GSM900, 124 channels are used for uplink & 124 channels for downlink
In GSM 1800, 374 channels are used



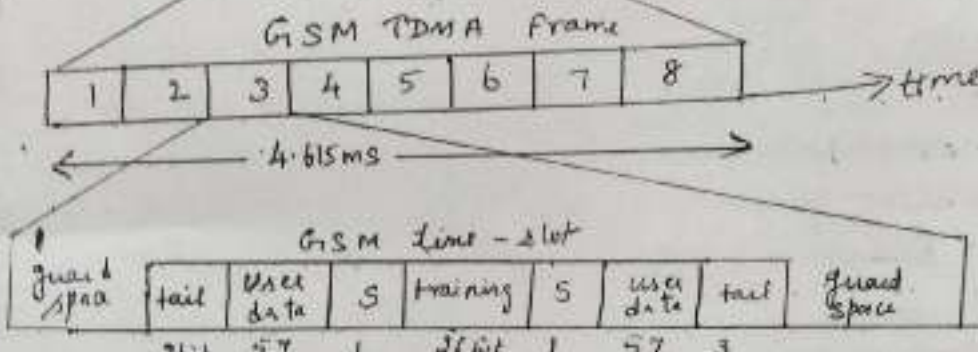


Fig: GSM TDMA frame, slots & bursts

Type	Channel	uplink (MHz)	downlink (MHz)
GSM 850	128-251	824-849	869-894
GSM 900	0-124	876-915	921-960
GSM 1800	512-885	1710-1785	1805-1880
GSM 1900	512-810	1850-1910	1930-1990
GSM-R	955-1024	876-915	921-960

Fig: GSM frequency bands

124 channels are divided into time frames

*) The figure shows 248 channels,
124 channels for uplink in freq. range (890-915) MHz
124 channels for downlink in freq range (935-960) MHz

*) Each channels are seperated in time via GSM TDMA frame and the channel freq is 200 KHz.
The duration of the GSM TDMA frame is 4.615ms.

*) The frame is again subdivided into 8 time-slots
∴ The time slots lasts for 577μs.

*) Datas are transmitted in small portion called burst.
(i.e normal burst)

*) In the diagram, the burst is only 546.5 μs long and contains 148 bits. The remaining 30.5 μs is used as guard space to avoid overlapping with other bursts.

*) The first & last three bits of a normal burst (tail) are all set to 0.

*) The flag (S) indicates whether the data field contains user data or n/w control data.

*) Training sequence in the middle of the slot is used to select the strongest signal in case of multipath propogation.

*) Apart from normal burst, there are 4 burst
i) frequency correction burst
ii) synchronization burst
iii) access burst
iv) dummy burst

1.2.1) Logical channels:

GSM specifies 2 groups of logical channel
i) Traffic channel (TCH)
ii) Control channel (CCH)

i) Traffic channel (TCH) :-

*) GSM uses TCH to transmit user data (eg. voice, fax).
Two categories of TCH's are a) full rate TCH (TCH/F)
b) Half-rate TCH (TCH/H)

TCH/F has a data rate of 22.8 kbits/s
TCH/H → 11½ kb/s.

TCH/F

13 kb/s are used for voice code and the remaining capacity of TCH/F are used for error correction

ii) Control channel (CCH)

Many different CCH's are used in GSM system, to control medium access, allocation of traffic channels, mobility management. Three groups of control channels are defined below

1) Broad Cast Control Channel (BCCH)
2) common control channel (CCCH)
3) Dedicated control Channel (DCCH)

i) BCCH:

BTS uses this channel to signal inf to all MS's within a cell. BCCH is unidirectional

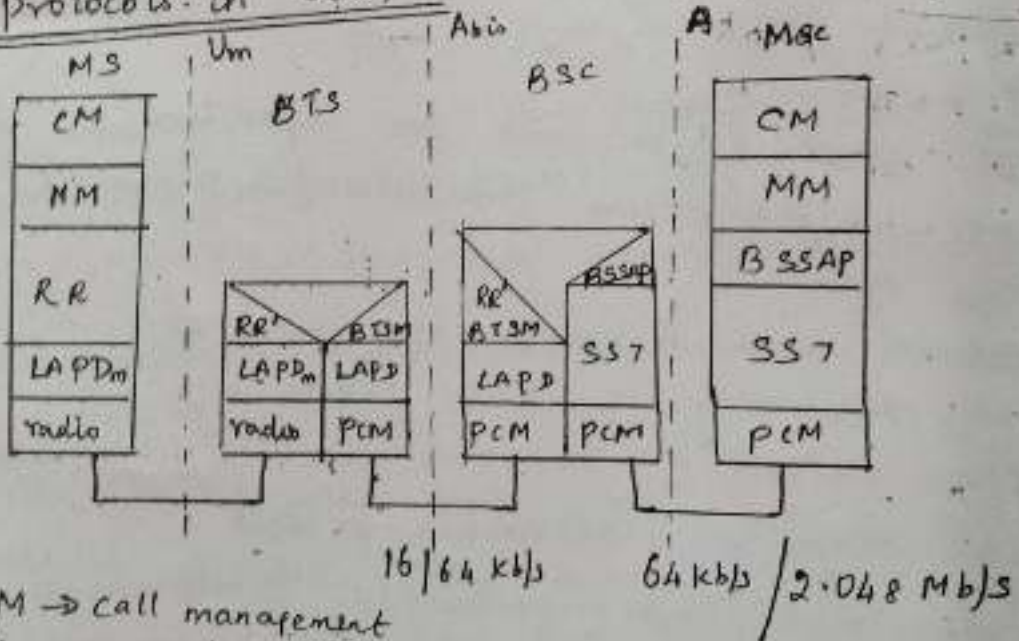
ii) CCCH: via, CCCH all the inf. regarding connection setup b/w MS & BS is exchanged, CCCH is unidirectional.

iii) DCCH:

It is bidirectional

3 types
- Stand-alone dedicated control channel (SDCCH)
- Slow associated dedicated control channel (SACCH)
- Fast associated dedicated Control channel (FACCH)

(3) Protocols in GSM



CM → Call management
MM → Mobility Management
RR → radio resource management
PCM → pulse code modulation
SS7 → Signalling System No. 7
BSSAP → BSS application part
LAPD → Link access procedure for the D-channel
BTSM → BTS management

Figure: GSM protocol Stack

*) GSM has 3 layers

(a) Layer 1 : (Physical Layer)

The fns handled by physical layer are

i) Handles all radio-specific fns &
ii) Multiplexing of bursts into TDMA frame
iii) Synchronization with BTS
iv) Detection of idle channels
v) Measurement of channel quality on the downlink.
vi) Channel coding & error detection/correction
vii) Special fn. is Voice activity detection (VAD) which transmits voice data only when there is a voice signal. During the period of silence (eg when needs time to think before talking), the physical layer generates a Comfort noise to take ~~a~~ connection

(b) Layer 2 : LAPDm

*) LAPDm protocol is used for layer two
LAPD → link access procedure for D-channel.
*) LAPDm offers
i) reliable data transfer over connection
ii) re-sequencing of data frames &
iii) flow control.
iv) segmentation & reassembly of data
v) acknowledged/unacknowledged data transfer.

(c) Layer 3 : Network Layer

Layer 3 has several sub layers

i) Lowest sublayer : Radio Resource management (RR)
ii) Next Sublayer : Mobility Management (MM)
iii) final Sublayer : Call Management (CM)

i) RR (Radio Resource Management) :-
*) only a part of this layer ie RR' is implemented in BTS remainder is situated in BSC.

i) The main task of RR are
   i) setup
   ii) maintainance &
   iii) release of radio channels.

ii) MM (Mobility Management) :-

MM contains fns for
   i) registration
   ii) authentication
   iii) Identification
   iv) location updating &
   v) provision of temporary mobile subscriber identity (TMSI)
   vi) reliable connection to next higher layer.

iii) Call Management (CM) :

It contains 3 entities
   i) Call control (CC)
   ii) Short Message Service (SMS)
   iii) Supplementary Service (SS)

CC provides - point-to-point connection b/w 2 terminals

*) Data transmission at phy. layer is done using pulse code modulation (PCM).

*) For signalling b/w MSC & BSC, signalling system No. 7 (SS7) is used.

---

(4) Hand over in GSM

*) The smaller is the cell size, the faster is the movement of MS from one cell to another. Therefore more hand over (Moving from one cell to another) is needed but the hand over should not cause a cut-off called as call drop.

*) There are 2 reasons for hand over.
   i) the MS moves out of range of BTS
   ii) Traffic in one cell is too high and so shift some MS to other cell with lower load. (Load balancing)

There are 4 possible hand over

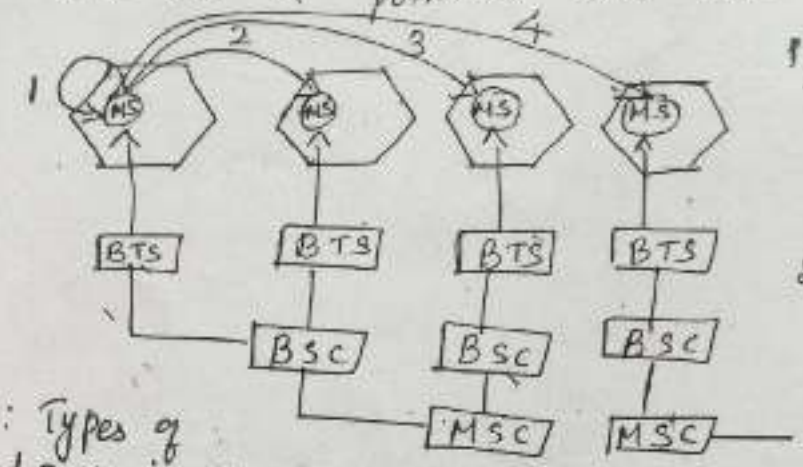


Fig: Types of handover in GSM

1) Intra - cell handover:-

Here handover takes place within a cell.

2) Inter - cell, Intra BSC handover:-

Here MS moves from one cell to another but both the cells are under the same BSC.

3) Inter BSC, Intra MSC handover:-

Here MS moves from one cell to another controlled by different BSC's.

4) Inter MSC handover:-

Here MS moves from one cell to another controlled by different MSC's [Handover b/w 2 cells belonging to diff MSC's].

Handover procedures

(1) Intra cell handover

(2) Intra cell Intra BSC handover

(3) Inter BSC Intra MSC handover

(4) Inter MSC handover

*) To provide all the necessary information for handover, both MS and BTS perform periodic measurement of downlink & uplink quality.

*) downlink & uplink quality include — signal level & bit error rate.

Figure (a): Handover decision depending on received level:

*) The below figure shows the typical behavior of the received signal level, while the MS moves away from one BTS (BTS_{old}) to another BTS (BTS_{new}).

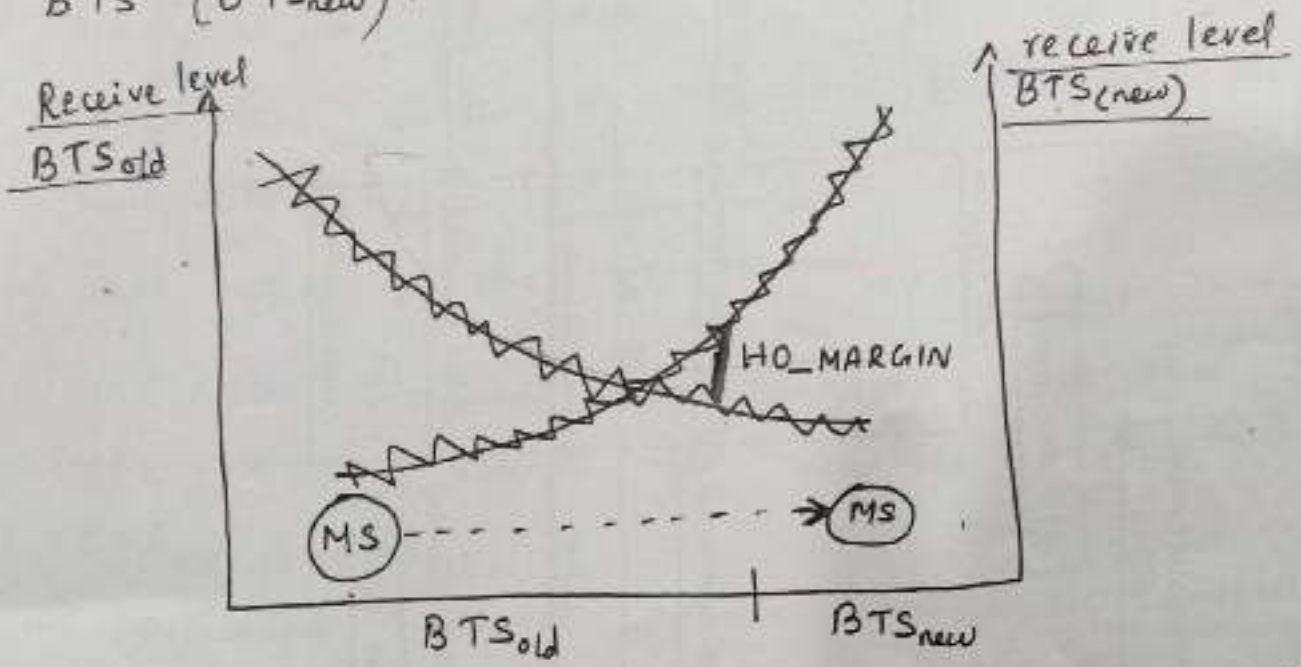


Fig (a): Handover decision depending on received level

*) BSC collects the (signal level & error rate from uplink and downlink) value from BTS and MS and calculate the average value. These values are then compared to threshold ie, the handover margin (HO_MARGIN)

*) If HO_MARGIN value is
too high → cut off occurs
too low → cause too many handovers.

Signal flow during Inter-BSC, Intra-MSC handover:

*) Figure (b): The figure shows the signal flow during inter-BSC, intra-MSC handover.

1) MS sends its periodic measurement report
2) BTS_{old} forwards these report to BSC_{old} together with its own measurement.

Fig (b). Intra MSC handover

Signal flow during Intra BSC

3) Based on these report, BSC_{old} decide to perform handover & sends the message HO_required to MSC.

4) MSC send HO_request (request for resources for handover) to BSC_{new}.

5) BSC_{new} checks whether enough resources are available and allocates resources (Resource allocation) and then activates the channel (ch. activation).

6) BTS_{new} acknowledges the succesful channel activation (ch. activation ack)

7) BSC_{new} acknowledges the handover request to MSC. (HO request ack).

8) MSC then issues a handover command (HO command) and that is forwarded to MS.

9) MS now breaks its old link and accesn the new BTS (BTS_{new}) (HO accesn).

10) Next step is the establishment of link (link establishment)

11) MS has finished the handover, but it is important the release the resources at the BSC_{old} & BTS_{old}.

12) Succesful handover occurs using HO complete and clear command & clear complete.

---

5) GSM SECURITY:

Security in GSM

(1) confidentiality
(2) Anonymity
(3) Accesn contol & Authentication

*) GSM offers security using confidential information stored in AUC and individual SIM.

*) The security services offered by GSM are

1) confidentiality:

*) All user-data's are enonypted.

*) After authentication, BTS and MS apply encryption to voice, data & signaling.

*) Confidentiality exists only b/w MS and BTS, but does not exists b/w end-to-end.

2) Access control and Authentication:

*) The 1st step of security is the → authentication of valid user for SIM. The user needs secret PIN to access SIM.

*) The 2nd step is → Subscriber authentication.

3) Anonymity:

*) To provide user anonymity, all data is encrypted before transmission.

*) GSM transmits a temporary Identifier (TMSI), which is newly assigned by VLR after each location update. VLR can change the TMSI at any time.

*) Three algorithms has be specified to provide security services in GSM

→ Algorithm A3 is used for Authentication
→ Algorithm A5 " " " encryption
→ Algorithm A8 " " " generation of cipher key.

*) A5 is publicly available.
A3 & A8 were secret

*) A3 & A8 are located in SIM and in AUC.
A5 is implemented in devices.

*) But A3 & A8 was no longer secret :), because it was published on the internet in 1998.

a) Authentication:

*) Before a subscriber use any service from the GSM n/w, he or she must be authenticated.

*) Authentication is based on SIM, which stores
- → Individual Authentication key (K_i)
- → User identification (IMSI)
- → Algorithm used for authentication (A3).

*) Authentication uses a challenge - response method:

i) Access control AC generate a random number RAND as challenge.

ii) SIM within MS answers with SRES (signed response) as response.

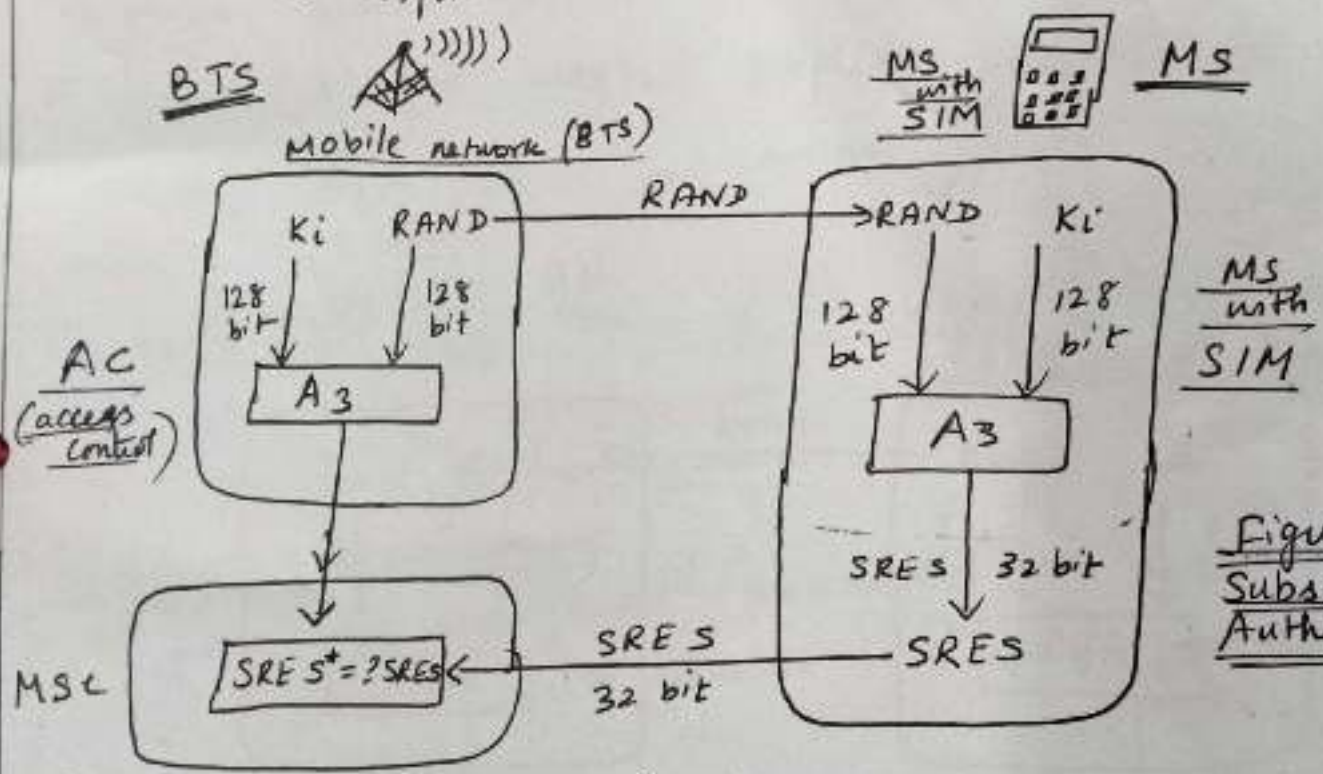


Figure: Subscriber Authentication

*) AUC generates — Random values (RAND), Signed response (SRES) & cipher keys (Kc) — for each IMSI (user identification)

and then forwards this information to HLR.

*) current VLR requests the values of RAND, SRES and K_c from HLR.

Ki → individual Key RAND → Random number	AC → Access control SRES → signed Response

*) For authentication, VLR sends the RAND to SIM.

*) Both mobile nlw & SIM perform the same operation with RAND & Ki called A_3.

*) MS sends back the SRES generated by the SIM. VLR now compare both SRES values. If they are same, VLR accepts the subscriber, otherwise the subscriber is rejected.

b) Encryption:

*) To ensure privacy, all messages are encrypted in GSM.

*) After Authentication, MS and BSS start using encryption by applying cipher key (K_c).

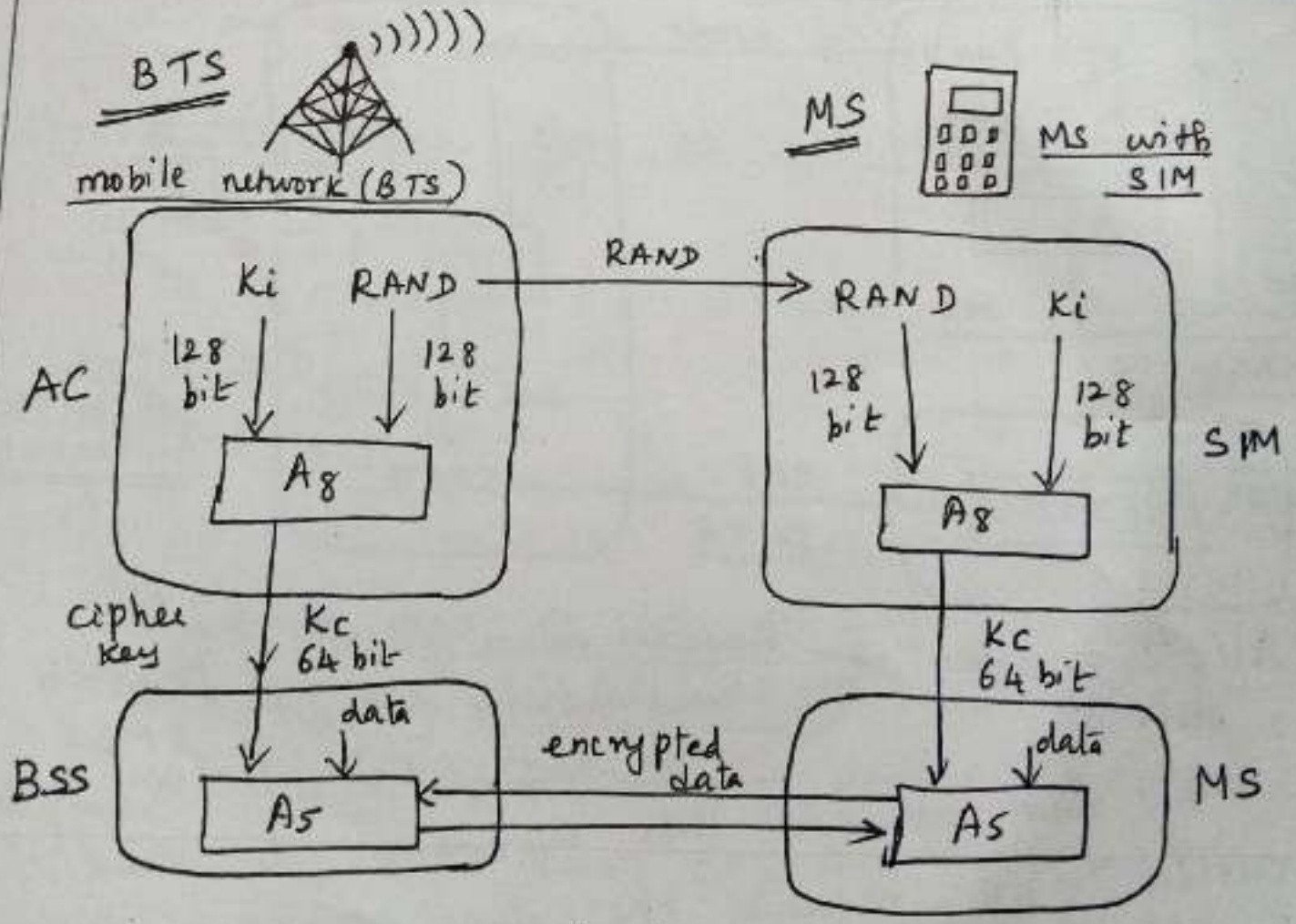


Figure: Data Encryption.

*) K_c is generated using the individual key K_i and RAND by applying A_8 algorithm.

*) SIM and mobile n/w both calculate the same K_c based on RAND.

*) MS and BTS can now encrypt & decrypt data using the algorithm A_5 and cipher key K_c.

*) K_c is a 64 bit key.

Mobility Management in GSM:

*) In mobile communication, the mobile node changes its own physical location (ie, address) in very less time.

*) Mobility of user has to be strictly supervised so that it is easier to continue call communication smoothly.

*) There are two types of mobility management,
   i) Location Management
   ii) Hand off Management.

i) Location Management:

*) Location Management procedure has 2 operations
   a) search operation b) update operation

a) Search operation:

*) search operation is invoked by a node which needs connection establishment with that of mobile node.

b) update operation: / registration operation:

*) It is also called as registration operation, it gives the information about the node's current location.

*) Search operation is supported by update

*) search overhead (cost) mainly depends on granularity and currenty of the location information. Location register is important because it stores the location related inf. of the nodes.

ii) Handoff Management:

*) Handoff Management is the second task after performing location management.

*) Aim is to ensure connectivity of the n/w with MS.

*) Handoff procedure involves many subtasks, they are:

a) Deciding the time of handoff to access point
b) Choosing new access point from many access points in mobile node's vicinity.
c) Getting resources (channels)
d) Sending information to old access point so that it can reroute the packets.

Handoff is initiated by 2 methods:

a) By Mobile node [Mobile Controlled Handoff (MCHO)].
b) By Access point [Network Controlled Handoff [NCHO]]

Handoff depends on factors such as:

i) Quality of mobile comm. b/w AP & MS.
ii) Load of current AP.
iii) Availability of resources at AP.
iv) SNR of beacon signals from AP.
v) Resources acquired for uplink & downlink channels.

Location Management	→ It assists in establishing new connections.
Handoff Management	→ It ensures the connectivity of mobile node with the n/w

Both these operations completes mobility management.

Location Management Principles:

A) Location management schemes uses many databases known as location registers for maintaining the location & service profiles.

*) One of the simple location management scheme is Home Location Registrar (HLR). It maintains location information of all mobile nodes in the network

Design issues:

1) The average time for which mobile node stays within a cell is known as cell residency time. It has to be calculated accurately.

2) As the mobile node is switched on, then its HLR has to be notified to ensure the current position of node.

3) Then the HLR contacts the current base station of cell where the node is available.

Dynamic update scheme:

→ Registration Area's (RA) based location updates are → Static update scheme.

→ Periodic updates are → dynamic update scheme.

→ example for dynamic update scheme are
  i) Movement based update
  ii) Distance based update

(7) Connection Establishment in GSM (or) Routing in GSM
(or)
Localization and calling in GSM

*) The fundamental feature of GSM system is the automatic, world wide localization of users.

*) HLR always contains the information about MS current location. As soon as the MS moves into new VLR's range, the HLR sends all the user's data needed to the new VLR.

*) Changing VLR with uninterrupted availability of all services is called as roaming.

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

1. Mobile station International ISDN number (MSISDN):

*) The only important number from the user of GSM is phone number. Phone number is associated with SIM

eg +49 179 1234567, 49 → country code (CC) of germany

179 → National destination code (NDC) (address of network provider)

1234567 → Subscriber Number (SN)

2. International Mobile Subscriber Identity (IMSI):-

*) GSM uses IMSI for internal unique identification of subscriber.

*) IMSI consists of

i) Mobile country code (MCC) → 240 for Sweden
ii) Mobile network code (MNC) → code of n/w provider
iii) Mobile Subscriber Identification number (MSIN)

3. Temporary Mobile Subscriber Identity (TMSI):-

*) To hide IMSI (which would give away the exact identity of the user), GSM uses 4 byte TMSI for local subscriber identification.

*) TMSI is selected by current VLR is only valid temporarily and within the location area of VLR.

4. Mobile station Roaming Number (MSRN):

*) MSRN also hides the identity and location of the subscriber temporarily.

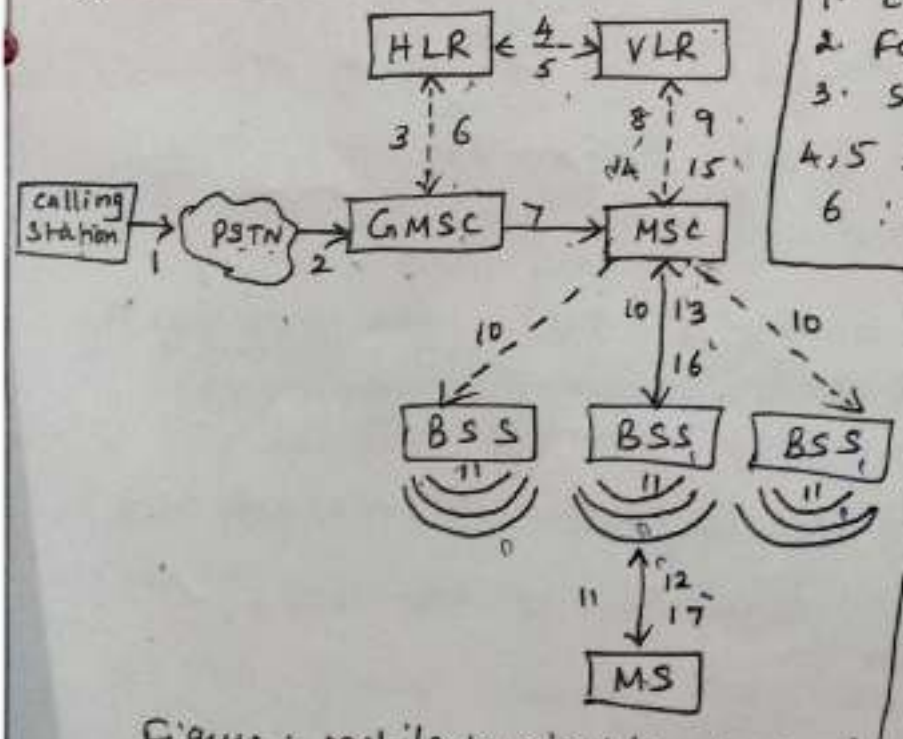
*) VLR generates this addren on request from MSC & this addren is stored in HLR.

visitor national destination code

*) MSRN contains ⇒ visitor country code (VCC)
⇒ visitor national destination code (VNDC)
⇒ Identification of current MSC & Subscriber Number

Routing in GSM:

(1) Mobile Terminating Call (MTC):



1. calling a GSM subscriber
2. Forwarding call to GMSC
3. signal call set up to HLR
4,5 : request MSRN from VLR
6 : Forward responsible MSC to GMSC.
7: Forward call to current MSC.
8,9: get current status of MS.
10,11 : paging of MS.
12, 13 & 14, ... } MS answers & security checks
15-17 : Set up connection

Figure : mobile terminating call (MTC)

Step 1: A user dials the phone number of GSM subscriber.

Step 2: The fixed network PSTN notices that the number belongs to the user in GSM network and forwards the call setup to the Gateway MSC (GMSC).

Step 3: GMSC identifies the HLR for the subscriber and signals the call set up to HLR.

Step 4: HLR now checks whether the number exists and whether the user has subscribed to the requested services and request MSRN from the current VLR

Step 5: HLR receives MSRN (mobile station roaming number)

Step 6: HLR forwards this information (MSRN) to GMSC

Step 7: GMSC now forward the call set up request to MSC.

Step 8 & Step 9: From this point on, MSC is responsible for all further steps. First, it requests the current status of MS from VLR.

Step 10: MSC initiated paging in all cells, so that location area (LA) can be easily determined

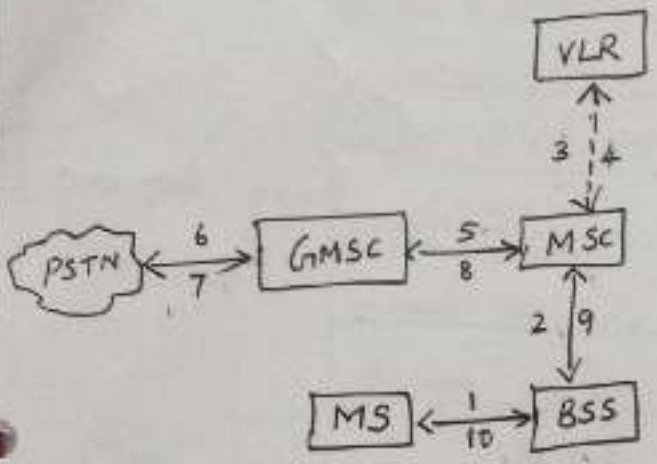
Step 11: The BTS's of all BSS's transmit this paging signal to the MS.

Step 12, Step 13, Step 14: If MS answers (12 & 13), the VLR has to perform security checks (encryption, etc).

Step 15 to 17: VLR then signals to MSC to set up a connection to the MS.

(2) Mobile originated call (MOC)

*) It is simple to perform Mobile originated call (MOC) compared to a MTC (mobile terminated call).



1, 2 : connection request
3,4 : security check
5-8 : check resources

Fig: Mobile originated call

Step 1: MS transmits a request for a new connection

Step 2: BSS forwards this request to MSC.

Step 3 & 4: MSC then checks if the user is allowed to set up a call with the requested service (3,4 and checks the availability of resources through GSM n/w into PSTN.

Steps 5-8: If all resources are available, MSC sets up a connection b/w MS and fixed network.

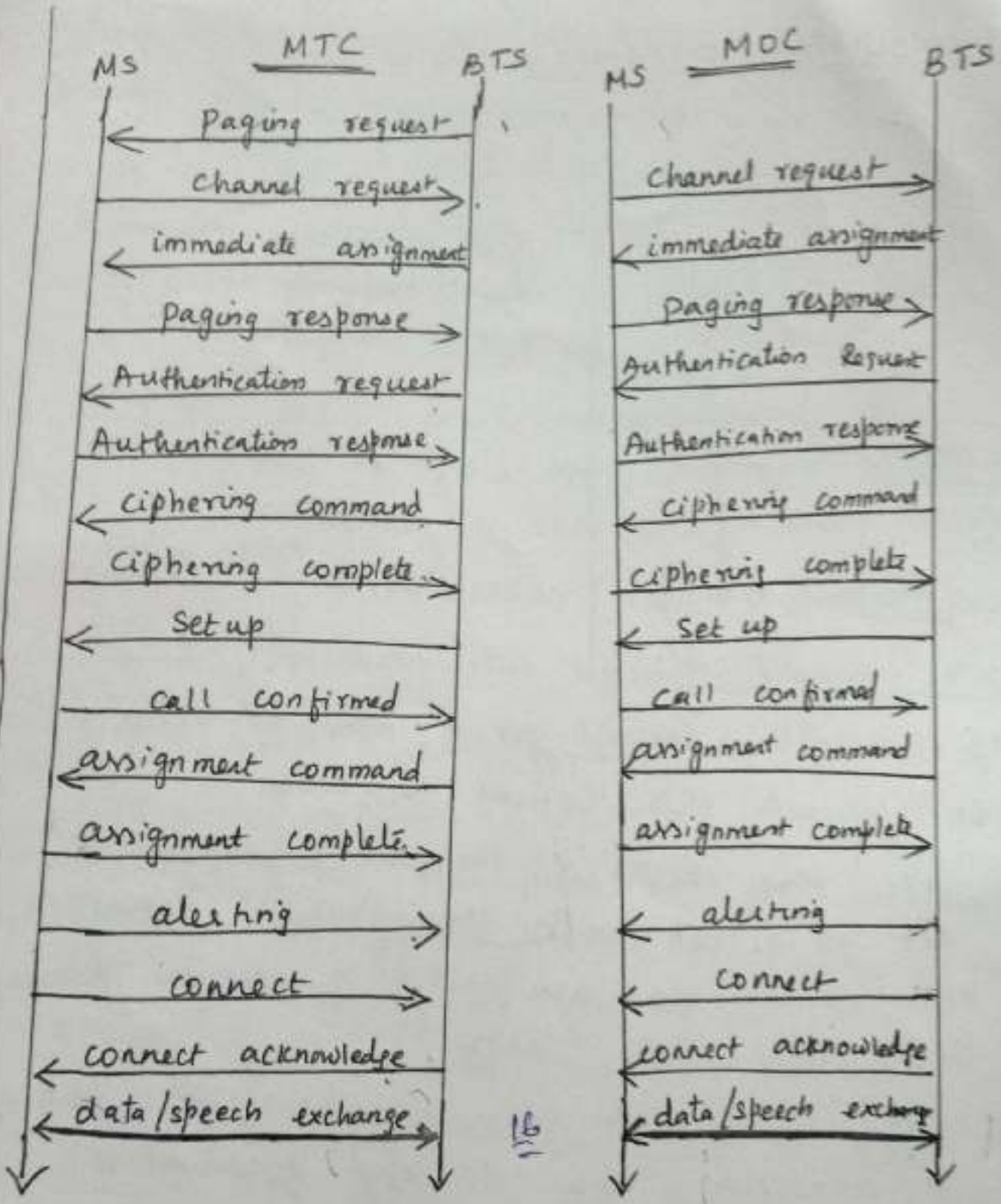
Steps 9,10: It's set up a call with the help of BSS and MS.

(3) Message Flow for MTC and MOC:

*) In addition to the steps mentioned above, other messages are exchanged b/w an MS and BTS during connection setup.

*) The figure shows the messages for MTC and MOC.

MTC → Mobile Terminated call.
MOC → Mobile originated call.



16

Figure: Message flow for MTC and MOC.

8) GSM services:

*) GSM provides 3 main categories of services.

They are
i) Bearer services
ii) Tele services
iii) Supplementary services

*) The figure shows the reference model for GSM services.

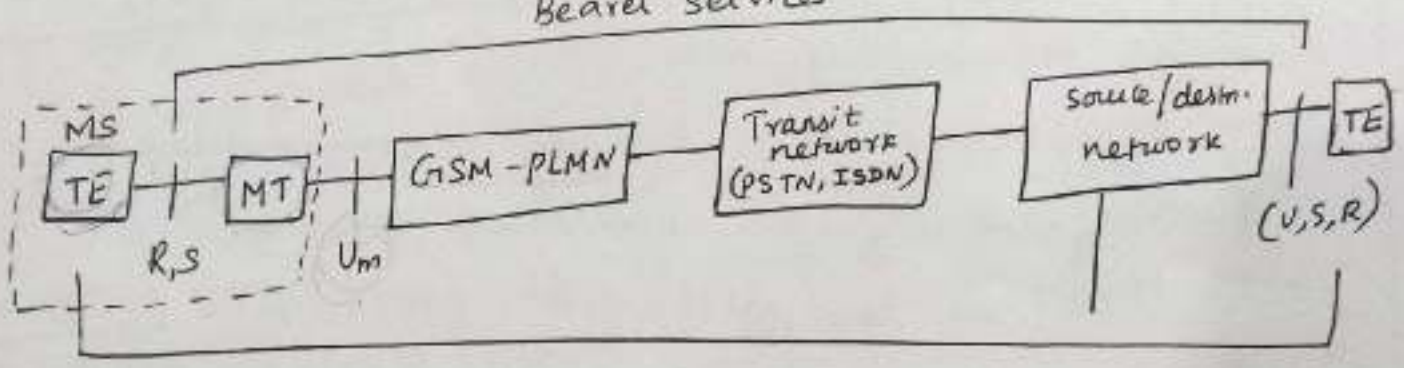


Fig: Bearer & Tele services Reference Model

*) Mobile station MS is connected to GSM public land mobile network (PLMN) via, Um interface.

*) The network is connected to transit networks eg, ISDN (integrated services digital network) or public switched telephone network (PSTN).

*) within the Mobile station MS, the mobile termination (MT) offers interface data transmission to terminal (TE). MT performs tasks such as TDMA, FDMA, coding, etc.

*) Tele services needs all 7 layers of ISO/OSI reference model.

*) Bearer Service — connection oriented
— circuit or packet switched
— need lower 3 layers of ISO/OSI reference model.

i) Bearer services/ data services :

*) Bearer services gives the subscriber the capacity to send and receive data to/from remote computers or mobile phones. Hence, bearer service is called as data services.

*) Bearer service permit
   a) either transparent or non-transparent mode and
   b) either synchronous or asynchronous data transmission.

a) Transparent bearer service:

→ Uses only the function of physical layer (layer 1) for transmitting data.

→ Data transmission has a constant delay and throughput if no transmission errors occurs.

→ There is a mechanism called FEC (forward Error correction) to increase the quality of data transmision.

b) Non- Transparent bearer service:

→ This service uses the protocol of second and third layer to implement error correction & flow control.

→ These service use transparent bearer service in addition to radio link protocol (RLP).

→ RLP comprises mechanism of High- level data link control (HDLC)

i) Data transmision can be either
   → full-duplex, synchronous with data rate 1·2, 2·4, 4·8 and 9·8 kb/s.
   (or)
   → full-duplex, asynchronous from 300 to 9600 bits/s.

ii) Teleservices:

*) GSM provides both → voice-oriented tele service &
→ non-voice teleservice.

The following are the services:

a) Telephony:

→ The main goal of GSM was to provide high quality digital voice transmission, offering the bandwidth of 3.1 KHz of analog wire phone system.
→ Special codecs are used for voice transmission, while other codecs are used for the transmission of analog data.

b) Emergency Number:

→ Another service offered by GSM is emergency no.
→ The same no. can be used throughout Europe.
→ This service is mandatory for all providers and free of charge.
→ This connection has highest priority and the connection will be automatically set up with the nearest emergency centre.

c) Short Message service (SMS):

→ This service offers transmission of text messages of size upto 160 characters.
→ SMS messages do not use the standard data channels of GSM but use the unused signalling capacity in channels.
→ Sending and receiving of SMS is possible during data or voice transmission.

d) Fax: Using modem, fax data is transmitted as digital data over the analog telephone network according to ITU-T standards T.4 and T.30

iii) Supplementary Services:

*) GSM offers Supplementary services such as
   a) user identification
   b) call direction
   c) forwarding of ongoing calls.
   d) ISDN features like
      i) close user group &
      ii) Multiparty communication are available.

(9) UMTS & IMT-2000

*) Universal Mobile Telecommunication System (UMTS) is an emerging 3G (third generation) air interface. It is developed by European carriers, manufacturers and government regulators. The International Telecommunication Union (ITU) made a request for proposals for Radio Transmission Technology (RTT) for International Mobile Telecommunication (IMT-2000) Pgm.

*) IMT-2000 Pgm was formally called as future public land mobile telecommunication system (FPLMTS)

*) IMT 2000 indicates the start of the system in the year 2000. and uses the frequency band of 2000 MHz.

*) European proposal for IMT 2000 is called UMTS. Radio interface RTT in UMTS is UMTS terrestrial radio access (UTRA).

*) UMTS fits into a bigger framework known as global multimedia mobility (GMM).

*) GMM provides an architecture to integrate.
- → mobile & fixed terminal
- → many different access n/w (GSM, ISDN, UMTS, LAN, WAN)
- → several core transport n/w. (GSM NSS+IN, TCP/IP ...)

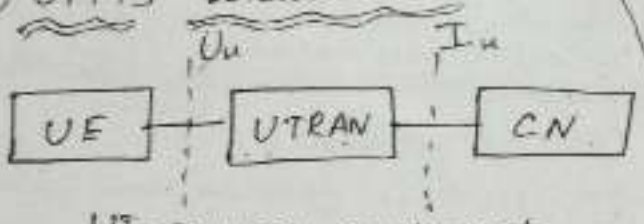
The key requirement is minimum data rate of
- → 144 Kbits/s for rural outdoor access & max speed = 500 km/hr
- → 384 Kb/s for Sub urban outdoor & max speed = 120 km/hr
- → 2 mb/s for indoor (city user) & max speed = 10 km/hr (walking)

*) UTRA adopts i) W-CDMA (wideband CDMA) for paired band (using FDD mode) and

ii) Time division CDMA (TD-CDMA) for unpaired band (using TDD mode)

→ Paired band is used for public mobile n/w & unpaired band is used for indoor applications.

Q.1) UMTS architecture



(a) Fig: Main components of UMTS

UE → user equipment
UTRAN → UMTS terrestrial radio access n/w.
CN → core n/w.

*) The fig shows the simplified UMTS architecture

*) UTRA n/w (UTRAN) handles cell level mobility and it has many radio n/w subsys (RNS)

UMTS system
1) UTRAN (UTRA network)
2) UE (user equipment)
3) CN (core network)

*) The fns of RNS are
1. Radio channel ciphering & deciphering
2. Hand over control.
3. Radio Resource Management.

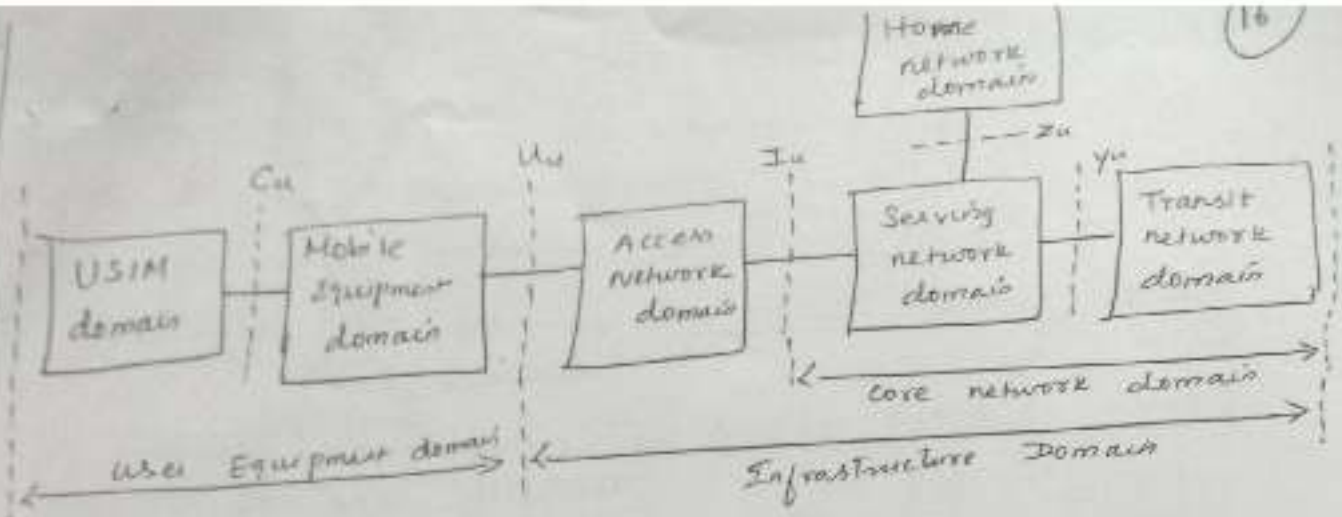
*) UTRAN is connected to user equipment (UE) via radio interface Uu (it is compared to Um interface in GSM)

*) UTRAN is connected to core n/w (CN) via Iu interface (it is compared to A interface in GSM)

The fns of CN are
→ Inter-system handover.
→ gateway to other n/ws.

*) UMTS specifies
1. C-plane for control inf
2. U-plane for user data.

*) The architecture has 3 layers
1. Layer 1 provides radio interface (its fns are mux & demux, modulation, spreading, synchro & power control)
2. Layer 2 is responsible for MAC connection, MAC, priority handling & scheduling & data packet
3. Layer 3 is responsible for all control fns for connection setup situated in layer 3.



(b) Figure : UMTS domain & interfaces

*) UMTs further subdivides the fig (a) architecture into domains. i) User Equipment domain
ii) Infra structure Domain

i) User Equipment domain:

*) This domain is assigned to a single user and comprises of all the functions that are needed to access UMTS service.

*) User Equipment domain has 2 domain
a) USIM domain
b) Mobile Equipment domain

*) USIM domain → contains. SIM for UMTS
→ it perform encryption & authentication of users
→ Stores all user-related data for UMTS

*) Mobile Equipment domain → is the end device.

ii) Infra structure Domain:

*) It is divided into 2 domain
i) Access Network domain
ii) Core Network domain

*) Core n/w domain is divided into 3 subdomains:

a) Serving Network domain
b) Transit Network domain
c) Home Network domain.

Access Network domain → contains the radio access network (RAN)

Serving Network domain → contains all functions currently used by a user for accessing UMTS services.

Home Network domain → All functions related to the home network of the user.

Transit network domain → it is needed if the serving n/w domain cannot directly contact the home n/w.

UMTS Radio interface.

*) The biggest difference between UMTS and GSM is the new radio interface (Uu).

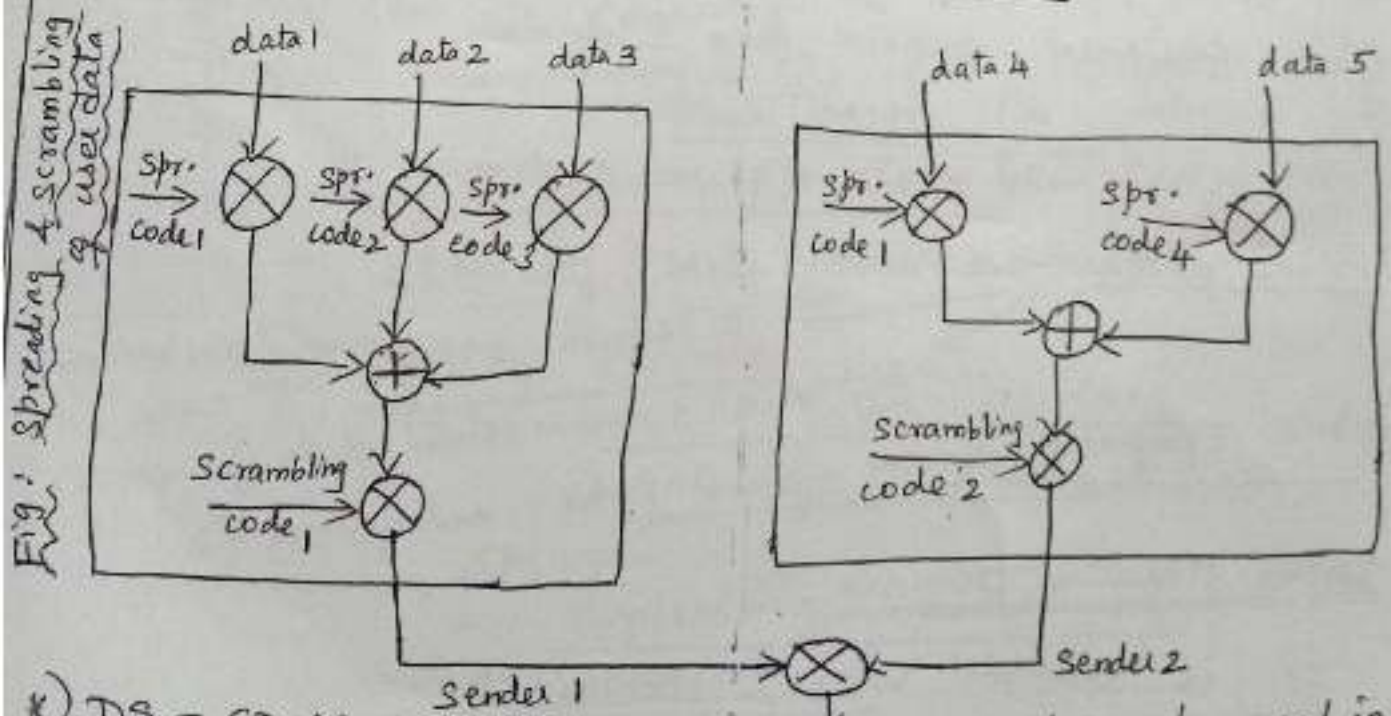


Fig: Spreading & scrambling of user data

*) DS - CDMA technology multiplies stream of bits with a chipping sequence.

*) UMTS uses a constant chipping rate of 3.84 M Chips/sec

*) The spreading codes used in UMTS are called as Orthogonal variable Spreading Factor codes (OVSF)

*) UTRA has 2 modes for spreading
① UTRA-FDD (W-CDMA)
② UTRA-TDD (TD-CDMA)

9.2) UTRA FDD Mode (W-CDMA)

FDD mode for UTRA uses wide band CDMA (W-CDMA) with direct sequence spreading.

The uplink freq. range → 1920 – 1980 MHz
The downlink freq. range → 2110 – 2170 MHz.
There are roughly 250 channels.

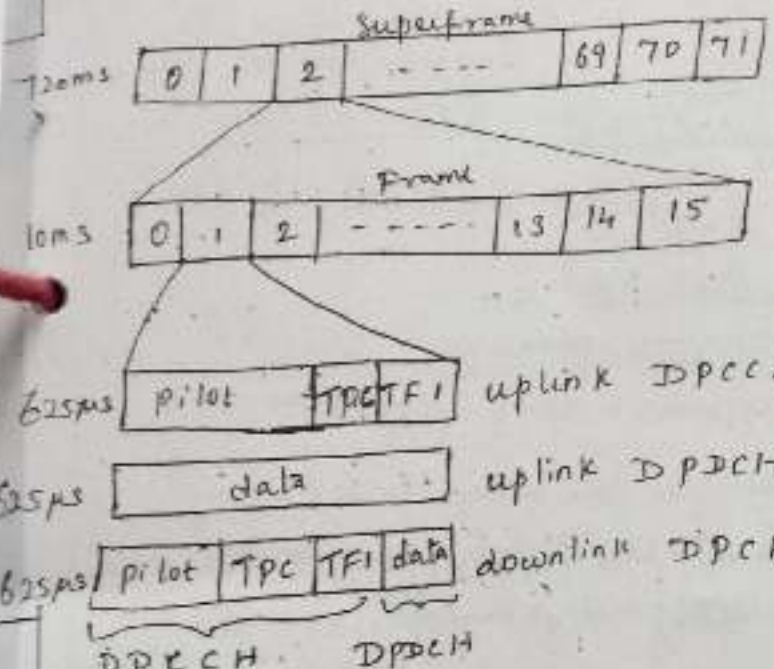


Fig: frame structure of UTRA in FDD mode

UTRA → UMTS terrestrial radio acces

Uplink

*) As in GSM there are no. of logical channels. On the uplink, uplink dedicated physical Data channel is used for tr. of data (user data) (UDPDCH)
In Uplink, the control data is transmitted thro uplink dedicated physical control channel (UDPCCH)
Both UDPDCH & UDPCCH are tr. in parallel.
For both channels diff spreading tech. faction are possible.

Downlink

*) On the downlink both control data & user data are transmitted in a single downlink dedicated Physical channel (Downlink DPCH)

*) The above diagram shows the frame structure of UTRA in FDD mode.

*) It has a superframe with a duration of 720 ms and it contains 72 frames.
*) A single frame contains 16 slots of 10ms duration. The fig shows 3 diff channels can use a slot

i) uplink DPCCH
→ It contains pilot to support channel estimation
→ Transmit power control (TPC)
→ Optional Transport format identifier (TFI)

ii) uplink DPDCH :-
It contains user data
Tx- at the same time of uplink DPCCH

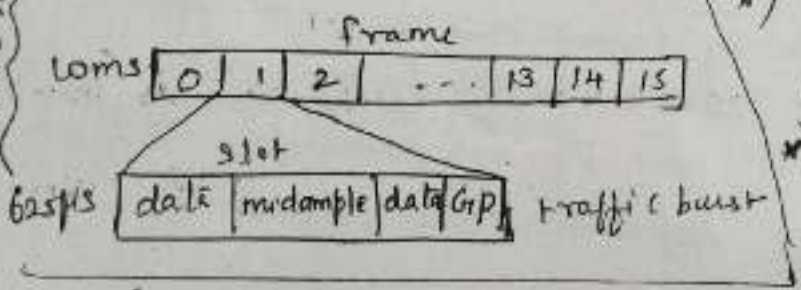
iii) Downlink DPCH :-
contains same field (Pilot, TPC, TFI & data) but in time - multiplexed version.

*) Since CDMA is used soft hand-off is possible

3.3) UTRA TDD Mode (TD-CDMA):

*) It uses Wide band TDMA/CDMA for Medium access.
*) Uplink & downlink use the same frequency.
Data rate = 2 Mbps.
*) 120 channels for user traffic (This capacity is half that of FDD)
*) Inside a frame there is 16 slots of 10ms duration
*) The fig shows the traffic burst. within a slot
The burst contains → user data
→ midample for channel estimation
→ guard period (GP) to avoid interference b/w slots
*) Each slot duration = 625 μs & contains 2,650 chips
*) Since FDD frame & TDD frame is 10ms duration hand-off is possible b/w frames.

Figure: Frame structure



(10) UMTS Hand over:

*) UMTS has two basic classes of hand overs:

i) Hard Hand over
ii) soft Hand over.

i) Hard Handover:

*) Hard handover is used in GSM & TDMA/FDMA systems.

*) UTRA-TDD use this type of hand over.

*) 2 types of hard handover
a) Inter Frequency Handover
b) Inter system Hand over

a) Inter frequency Handover:

→ changing the carrier frequency, is a hard hand over.

→ Receiving data at different frequencies at the same time requires a more complex receiver compared to receiving data from different sources at the same carrier frequency.

b) Inter system hand over:

→ Inter system handover means handover to and from GSM or other IMT-2000 system.

→ A special type of inter system handover → is the handover to satellite system (inter-segment handover)
It is also hard handover, because different frequencies are used.

*) UMTS specifies Compressed mode transmission for UTRA FDD.

*) In compressed mode, the user Equipment (UE) stops all transmission. Either spreading factor can be lowered or less data is sent using different coding schemes.

ii) Sqt Handover:

*) This is a new mechanism in UMTS compared to GSM.

*) UMTS - FDD use this type of handover.

Macro diversity property:

*) sqt handover uses Macro diversity property, this is the basic property of CDMA.

*) UE (user equipment) can receive signals from upto three different antennas, which may belong to different BS.

*) Towards UE, RNC splits the data stream & forwards it to node Bs. UE combines the received data again

*) From UE (opp. direction),

UE sends its data which is then received by all the node BS. RNC combines the data stream received from the node B S.

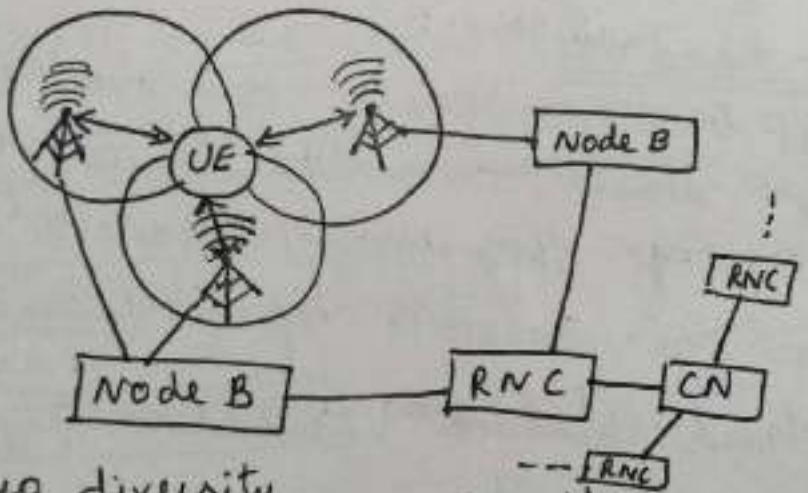


Figure:
Micro-diversity
Supporting sqt
hand over

RNC → radio n/w controller
CN → core network

*) Micro diversity makes the tranomission more robust if one path is blocked by an obstacle, then the datas can be received using another antenna.

*) During sqt hand over, UE receives power control commands from all node Bs.

*) Several nodes are connected to RNC. Several RNC's are connected with CN.

Serving RNC and Drift RNC:

*) This situation shows, where a sqt handover is performed b'w two node BS that do not belong to the same RNC.

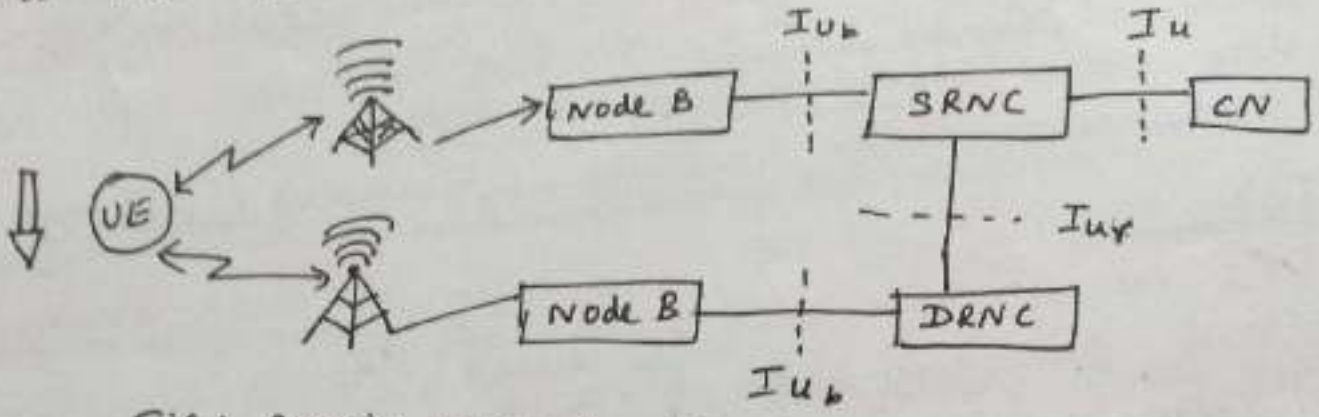


Fig: Serving RNC & drift RNC

SRNC → Serving RNC
DRNC → Drift RNC
Iu → Interface (similar to interface A in GSM)
→ Each RNC is connected with CN via Iu.
Iub → RNC is connected with node via Iub interface
Iur → connects two RNC's. (This interface is not in GSM)

*) In this case, one RNC → controls the connection & → forwards all data to & from CN.

*) If UE moves from upper cell to lower cell,
Upper RNC acts as Serving RNC (SRNC)
lower RNC acts as Drift RNC (DRNC)

*) SRNC forwards data received from CN to node B and to DRNC via Iur interface

*) This SRNC combines both data streams & forwards as a single stream of data to CN.

Different Types of handover in UMTS:

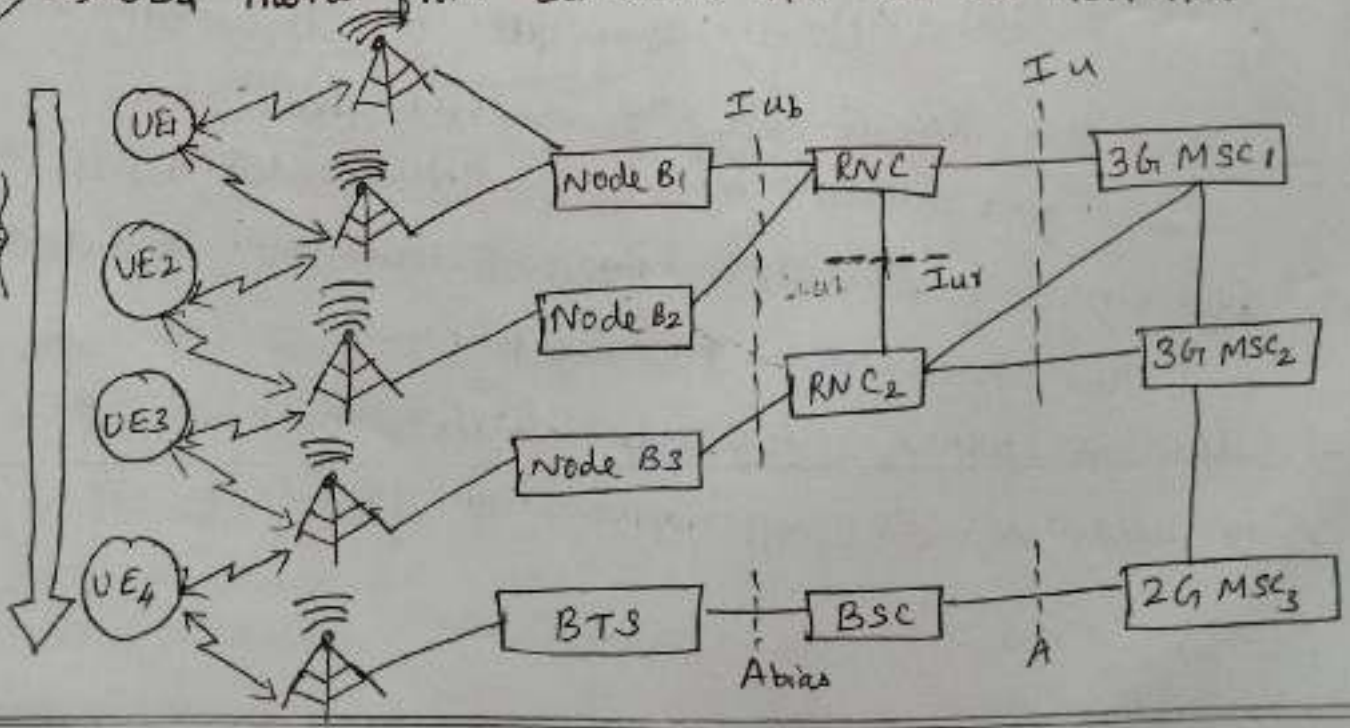
1) Intra-node B, intra-RNC:
→ UE, moves from one antenna of node B, to another antenna. This type of handover is called softer handover.
→ In this case, node B, perform combining & splitting of data streams.

2) Inter-node B, Intra-RNC:
→ UE_2 moves from node B_1 to node B_2.
→ RNC, support soft handover by combing & splitting of data.

3) Inter RNC:
→ UE_3 moves from node B_2 to node B_3.
→ Two handover takes place
a) Internal inter-RNC handover:
→ It is not visible, RNC_1 acts as SRNC & RNC_2 acts as DRNC.
→ same Iu is used all the time.
b) External inter-RNC handover:
→ Relocation of Iu takes place & the handover is called as external inter RNC handover.
→ It is a hard handover.

4) Inter MSC: MSC_2 takes over and performs a hard handover of the connection.

5) Inter System:
→ UE_4 moves from 3G UMTS n/w into 2G GSM n/w



(11) UMTS security:

a) UMTS security builds on the security of GSM, inheriting the proven GSM security features.

b) GSM subscribers roaming in a UMTS n/w are supported by GSM security features.

UMTS consists of 5 security feature groups:

i) Network Accen security:

→ A in diagram below.

→ Network accen security provides users with secure accen to UMTS services and protect against attacks on the radio accen link.

ii) Network Domain Security:

→ B in diagram below.

→ Network domain security protects against attacks on the usreline network and allows nodes in the provider domain to exchange signaling data securely.

iii) User Domain security:

→ C in diagram below.

→ User domain security provides secure accen to mobile stations.

iv) Application Domain Security:

→ D in diagram below.

→ Application domain security allows the secure exchange of menages b'w applications in the use and in the provider domain.

v) Visibility and configurability of security:

→ It allows the user to observe whether a security feature is currently in operation and if certain services depend on this security feature.

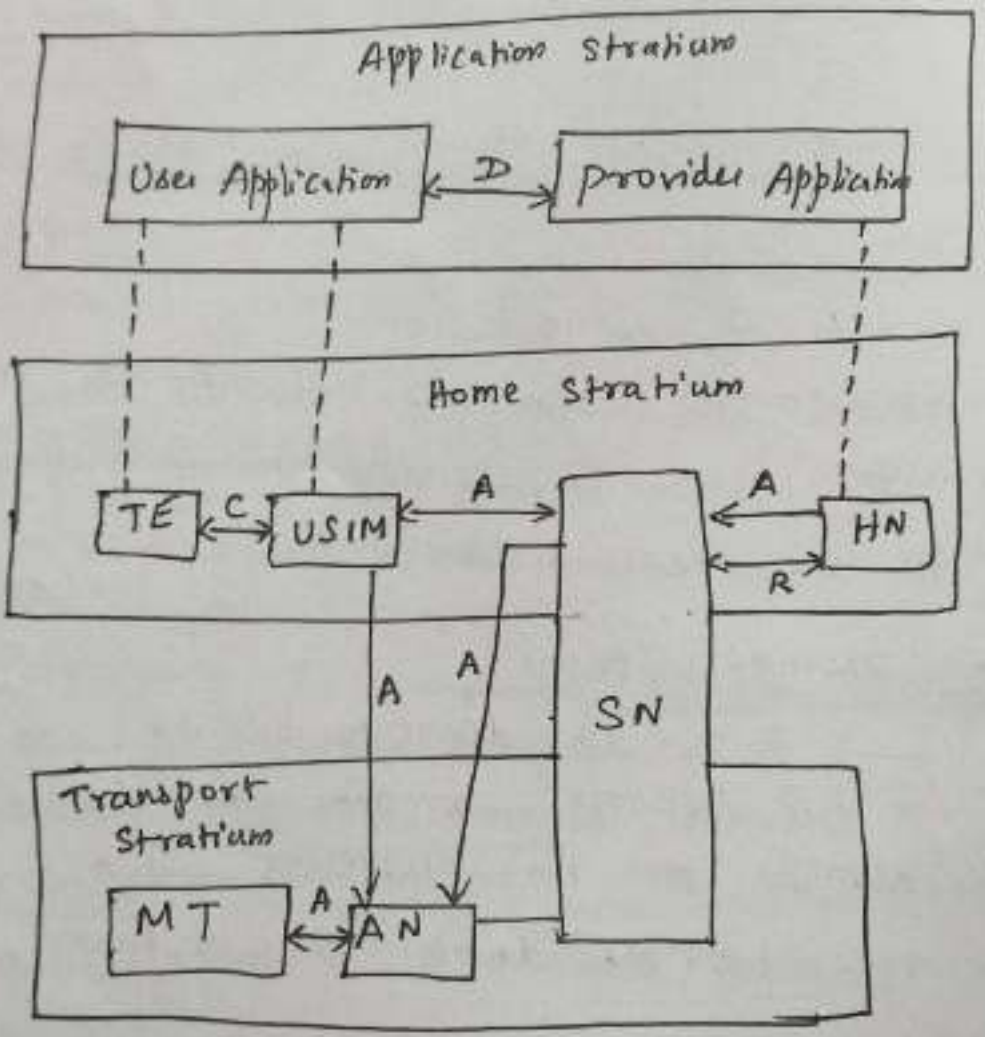


Fig: Security feature groups in UMTs

*) UMTs also provides different security features for maintaining identity confidentiality.

Security feature for Maintaining identity confidentiality:-

i) User Identity confidentiality:

→ It is maintained by ensuring the permanent User identity (IMSI) of a user using the service cannot be eavesdropped on the radio link

ii) User location Confidentiality:

*) It means that one cannot determine whether the presence of a user by eavesdropping on the radio accen link.

iii) User Untraceability:

*) It ensures that it cannot be determined if different services are available to the same user by eavesdropping on the radio accen link.

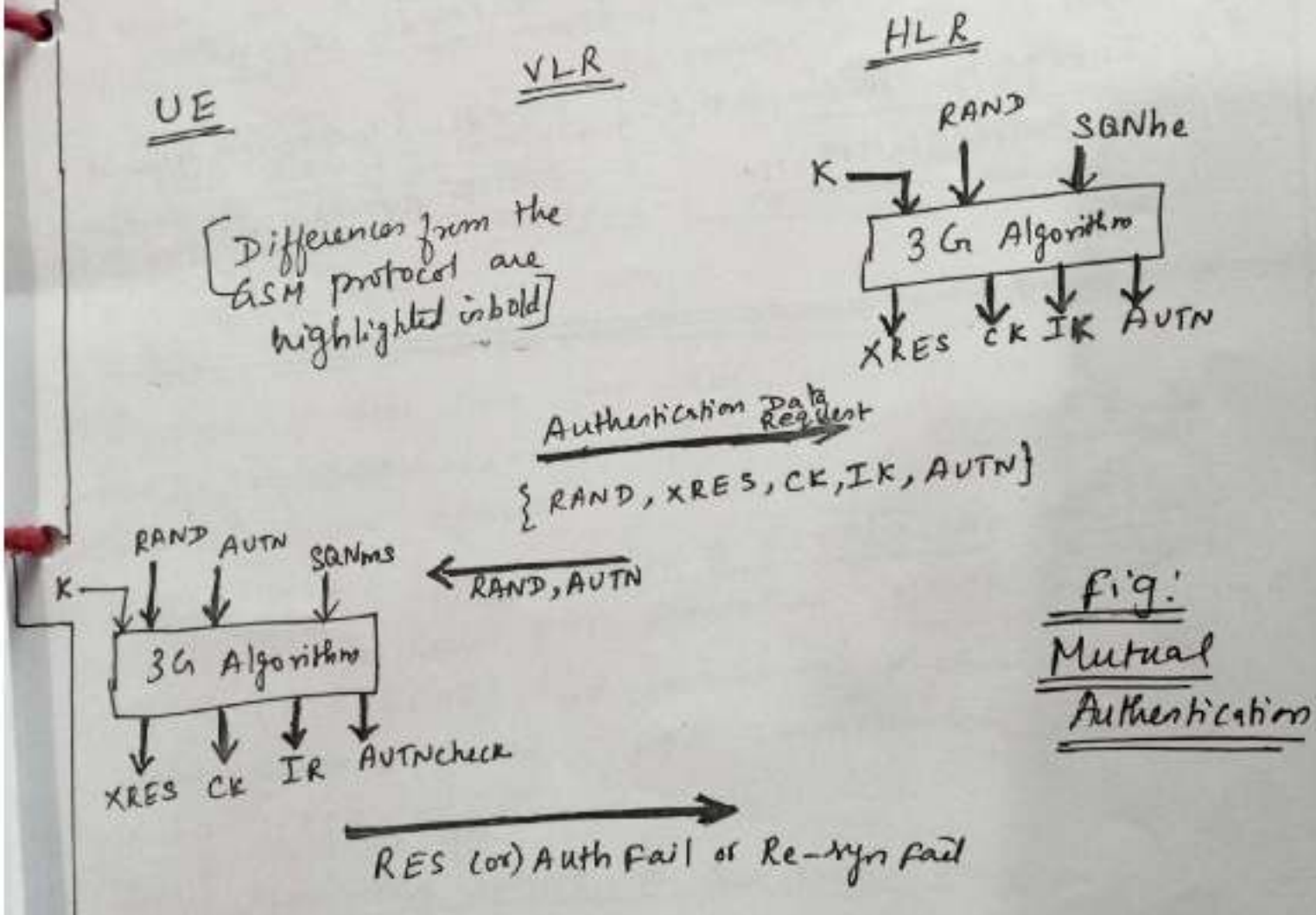


Fig: Mutual Authentication

K → subscriber Authentication Key
SQNms → Sequence number information at user
SQNhe → Sequence number information at ho system
UE → User Equipment / SIM
VLR → visitor Location Register
HLR → Home Location Register

*) Authentication quintet consists of

→ User challenge (RAND)
→ Expected user Response (XRES)
→ Encryption Key (CK)
→ Integrity Key (IK)
→ Authentication token for n/w Authentication } (AUTN)

*) User & n/w negotiate and agree on } cipher & integrity algorithms

*) Integrity mechanism & Authentication. } provide protection against active attacks on radio interfaces.

*) The satellite provider multiplexes the ... stream together with other digital TV channels and transmits it to the customer via satellite and a satellite receiver. The customer now receives the requested info with the help of a DVB adapter & multimedia PC

(12) GPRS (general packet radio service) :—

*) GPRS is a more flexible, powerful data transmission with fully packet-oriented (ie packet switching) transmission of small volume or infrequent data transmissions of medium volume, GPRS provid packet mode of transfers.

*) GPRS allows broadcast, multicast and unicast services.

*) GPRS needs additional n/w elements ie s/w & H/w.

*) In GPRS, time slots are not allocated in a fixed & predetermined manner, but on demand basics Time slots are shared by active users.

*) GPRS offers point-to-point (PTP) packet transfer service.

i) one version is called PTP connection Oriented n/w service (PTP-CONS) it maintains virtual ckt.

ii) another version is called: PTP connectionless n/w service (PTP-CLNS)

*) GPRS users can specify a QoS profile based on

i) service precedence (high, medium, low)
ii) Reliability class
iii) Delay class
iv) User data throughput

*) Reliability class 1 used for very error-sensitive applications that cannot perform error corrections themselves

class 2 could be appropriate

class 3 used for error-insensitive applications that can handle error corrections themselves.

*) Delay in the GPRS is occured by channel access delay & transfer delay

*) GPRS has security services such as authentication, access control, subscribers confidentiality etc

GPRS architecture

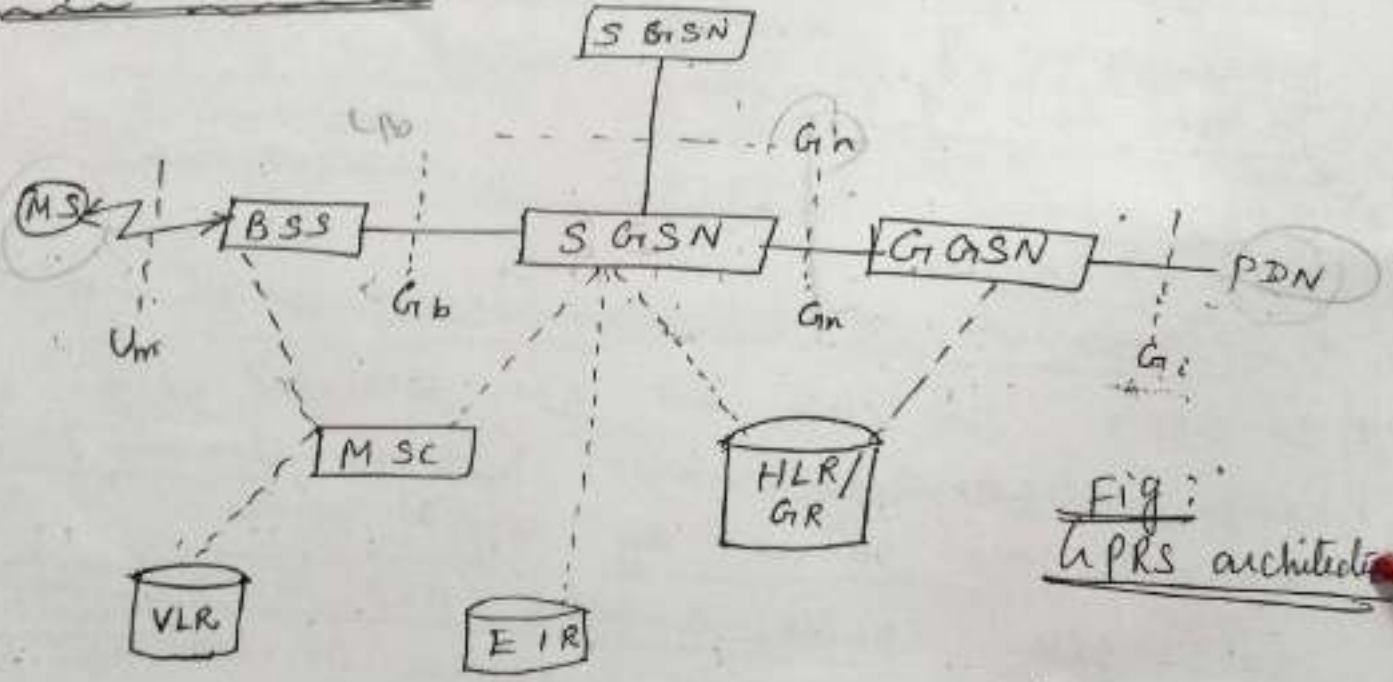


Fig: GPRS architecture

*) The above diagram is the architecture of GPRS architecture. GPRS architecture introduces 2 new elements, called as GPRS support nodes (GSN)

i) gateway GPRS support node (GGSN)

ii) Serving GPRS support node (SGSN)

i) GGSN (gateway GPRS support node):

GGSN provides a link b'w GPRS n/w and external packet data n/w (PDN), it contains routing info for GPRS users. It performs addr. conversion and tunnels data to a via encapsulation

ii) SGSN (Serving GPRS support node)

SGSN supports MS via Gb interface

*) GPRS register (GR) keeps track of the individual MS's location. GR is a part of HLR.

*) packet data is transmitted from a PDN via the GGSN & SGSN directly to the BSS and finally to the MS.

* MSC is used only for signaling

*) GGSC transfer packets to the SGSN thro' Gn interface

*) Before sending any data over GPRS nlw, the MS must attach the procedures of mobility management to the GPRS nlw.

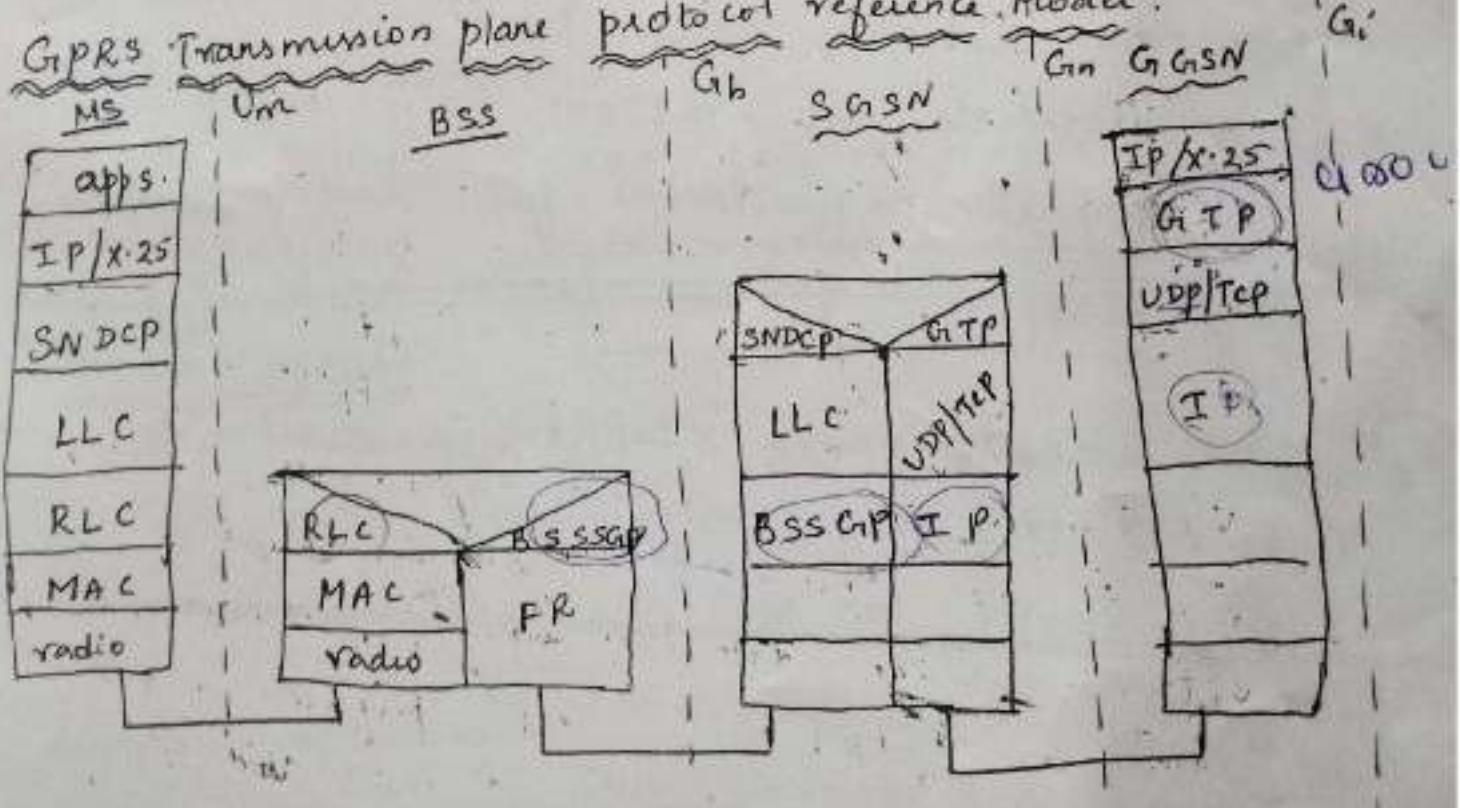
Procedures of Mobility Management are

→ assigning temporal ID called as temporary logical link identity (TLLI)

→ & assigning ciphering key sequence no. (CKSN) for data encryption

→ Mobility management provides fns such as authentication, location management & ciphering

GPRS Transmission plane protocol reference Model:



*) The figure shows the protocol architecture of transmission plane for GPRS.

*) Data transfer within GPRS is thro' GPRS tunelling protocol (GTP). GTP uses two transport protocols.

i) reliable TCP (used for transfer of X.25 packets)

ii) non reliable UDP (used for transfer IP packets)

*) The n/w protocol for GPRS is IP.

*) Base station subsystem GPRS protocol (BSSGP)

→ is used to convey routing & QOS-related inf b/w the BSS and SGSN

→ BSSGP does not perform error correction.

*) Radio link between MS and BSS is thro' Um interface. Radio link protocol (RLC) provides reliable radio link.

*) MAC controls the access

i) signalling procedures for radio channels.

ii) Mapping of LLC frames on to GSM channels.

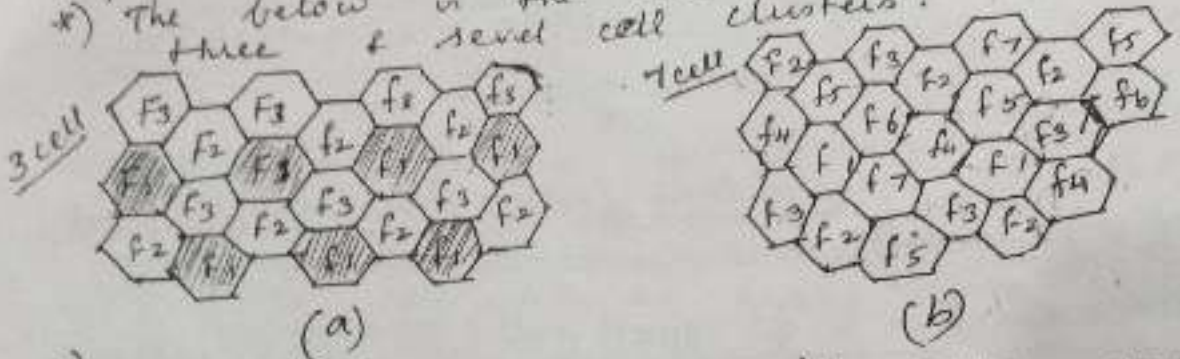
*) Um interface of GPRS is similar to GSM

*) MCM splits the high bit rate stream into many lower bit rate stream, each stream is being sent using an independent carrier frequency

(13) Cellular Systems:

*) Cellular system for mobile communication implements SDM (space division multiplexing)

*) The below is the cellular system with three & seven cell clusters.



*) Each cell covers a certain area and it has a base station (which has a transmitter & receiver).

*) The cell radii vary from tens of meters in buildings, 100 of m in cities & some Kms in country side.

*) The shape is not perfect circle or hexagon

Advantages of cellular system with small cells:

i) Higher Capacity:

SDM allows frequency reuse. If one transmitter is far away from another, the freq. can be reused. Huge cells do not allow more users ie no. of concurrent users / cell is limited. This is the reason for using very small cells in cities

ii) Less transmission power:

A receiver far away from a base station would need much more trasmit power. than Hence smaller cells are preffered.

iii) Local interference only:

Long distance b/w sender & receiver results in more interefference problems. With small cells, only local interference occurs.

iv) Robustness:

If one antenna fails, this defect only affects small area.

Disadvantage of small cell:

i) Infrastructure needed:

Each & every small cell needs an seperate antenna, switches, location register, hence makes the whole system very expensive.

ii) Hand over needed:

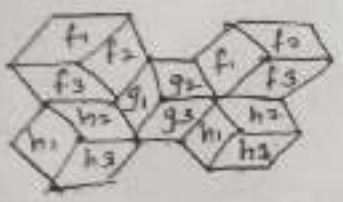
The hand over operation takes place with moving from one cell to another. If the cell size is small hand over is quite often.

iii) Frequency planning:

To avoid interference b/w transmitters using same frequency, frequencies have to be distributed carefully. Hence frequency has to be planned carefully for each & every cell.

*) The above fig shows that the cells are combined in clusters → fig (a) 3 cells form a cluster
→ fig (b) 7 cells form a cluster.

*) To reduce interference even further sectorized antennas can be used. The below fig. shows that the 3 cell cluster (f, g, h) is again divided into 3 sectors per cell. The sectors use sectorized antennas instead of omnidirectional antennas for large cell radii.



Types of allocation:

i) Fixed channel allocation (FCA)

The frequency allocated to each cell is fixed and even if the traffic load varies the freq is not changed. This scheme is FCA

ii) Borrowing channel allocation (BCA):

If one cell has a heavy load while another neighbouring cell has light load, the heavy ~~light~~ load cell can borrow some frequency from his neighbour, ie cells with more traffic are dynamically allotted more freq. This scheme is known as borrowing channel allocation.

iii) Dynamic channel allocation (DCA):

In this scheme, frequencies can only be borrowed but it is also possible to freely assign frequencies to cells. But there is a danger of interference with cells using the same frequency.

*) CDM cells are called as 'breathe' because the cell shrinks if the load increases and cover larger area under light load.

*) Higher the noise, higher path loss & higher transmission error.

UNIT - III

V.S

Mobile computing

(1) Mobile IP:

*) Whenever the user is connected to an application across the internet, it is said to be in mobile status. The routers actually uses the IP address in IP datagram to do the routing function.

*) 'Mobile IP' is similar to the hand off or roaming situation in cellular mobile network.

A) Goals, Assumptions and Requirements of Mobile IP:

*) The goal of mobile IP is: i) to enable packet transmission efficiently without any packet loss.
ii) to provide correct topological address.
iii) to enable packet transaction inspite of moving hosts from their home network.

*) Requirements required are:
i) compatability
ii) Transparency
iii) Scalability
iv) Efficiency
v) Security

*) Message delivery (packet) takes place in the Internet thro' routing mechanism with the help of IP address of the intended receiver of the packet.

*) When a host sends a packet, the header information in the packet contains the destination address.

*) In this case, the destination address specifies the receiver of the packet thro' the physical subnet of the receiver. If if the receiver address is 120.10.59.79, the receiver must be connected to the subnet 120.10.59

*) The receiver should be always connected to the subnet. Then only the packets will reach the receiver. If the receiver moves outside the subnet, the packet will not reach the intended receiver of the packet. This is done through "topologically correct address"

Quick solution:

*) A simple & fast solution to the above problem is

i) By assinging the mobile computers a new topologically correct address as it moves. ie, the computer needs to be assigned a new address as the computer moves.

ii) By designing proper routing. Routers are the 'brains' of the entire Internet system.

Goal of mobile Ip:

i) Efficiency

ii) Maintaining scalability

iii) Compatibility with the existing internet protocol and other related applications.

(B) Entities and Terminology:

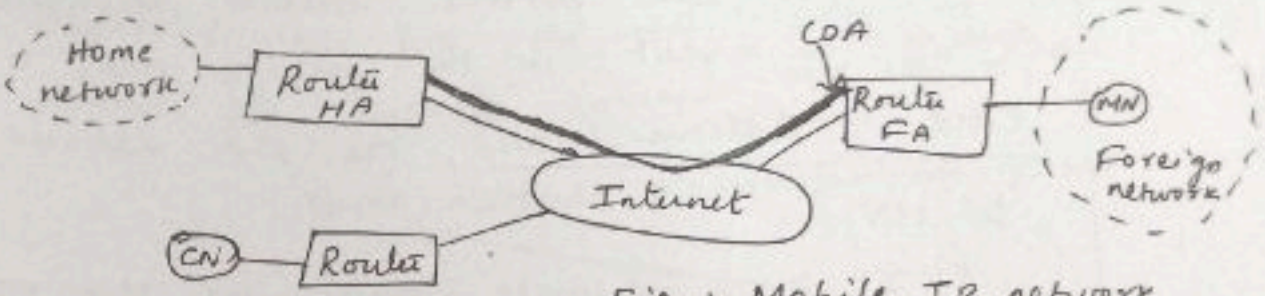


Fig: Mobile IP network

The above figure illustrates the mobile IP in an example n/w. Some of the entities shown in the figure are

i) Mobile Node (MN):

A mobile node is an end-system or router. MN keep its IP address and can continuously communicate with any other systems in the Internet. Mobile nodes are not necessary to be small devices such as Laptops with antennas or mobile phones.

ii) correspondent Node (CN):

At least one partner is needed for communica The CN can be a fixed or mobile node.

iii) Home Network (HN):

It is the subnet that supports the mobile node. within the home network no mobile IP support is required.

iv) Foreign Network (FN):

A network that is not the home n/w but that is being visited by MN.

v) Foreign Agent (FA):

*) FA can provide several services to the MN during its visit in the foreign n/w. Using Care of Address (COA), the FA delivers packets to MN.

*) It is a default router for MN.

vi) Care-of address (COA):

*) The current location of MN is defined by care-of address. All the packets sent to that of the MN are delivered to the IP address of the MN.

*) packet delivery to MN is done using a tunnel.

*) There are 2 possibilities of locating COA. They are

a) Foreign Agent COA:

COA is located at FA. ie, the COA is an IP address of the FA. Many MN using the FA can share this COA as common COA.

b) Co-located COA:

COA is called co-located if the MN temporarily acquired an additional IP address and acts as COA. Co-located addresses can be acquired using DHCP.

vii) Home Agent (HA):

*) It is located in home network and it provides several services for the MN. only at HA the tunnel for packets towards MN will start.

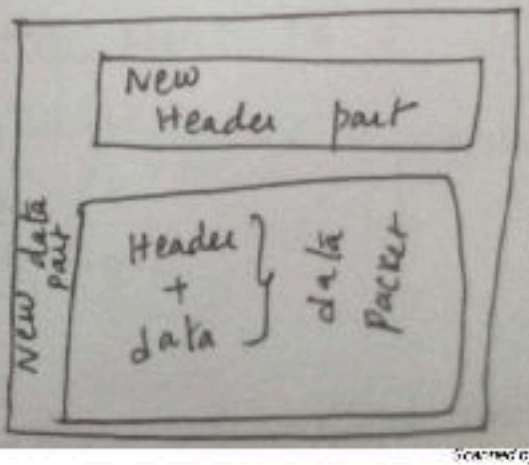
Three methods of implementation of HA

- HA can be implemented on router
- HA can be implemented on an arbitary node
- HA can be implemented on router but HA acts only as manage for the mobile nodes that belong to a virtual home network.

C) Tunelling and Encapsulation:

*) A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel end point. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunelling, ie sending a packet through a tunnel is achieved by using encapsulation.

*) Encapsulation is the process of taking a datapacket (consisting of header and data) and putting it into the data part of a new packet. The reverse operation, ie taking a packet out of the data part of another (new) packet is called decapsulation.



*) Encapsulation & decapsulation are performed when a packet is transferred from a higher protocol layer to a lower layer.

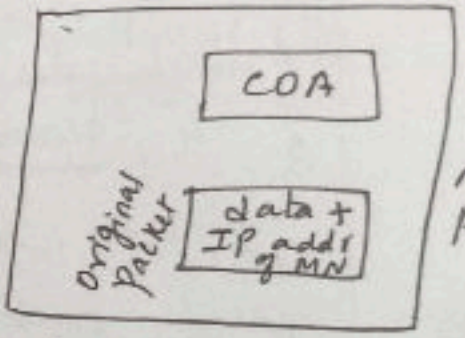
*) The inner header contains original header. The new header is also called the outer header.

The outer header (upper header) (new header) ⟶ contains COA addr.

inner header (lower header) (original header) ⟶ IP addr of MN.

*) HA takes the original packet with MN as destination and put it into the data part of the new packet.

*) The below fig. explains the process of encapsulation. The HA on receipt of the data packet for one of the MN, associated with it, carries out encapsulation



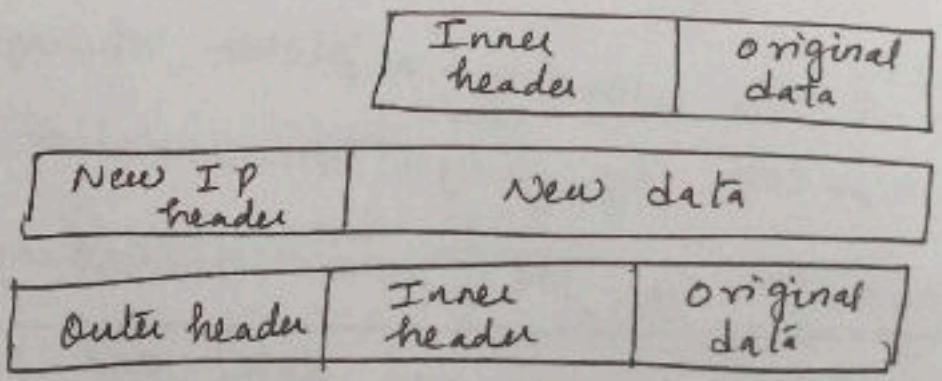


Fig: IP encapsulat

*) There are 3 types of encapsulation

1) IP – in – IP encapsulation
2) Minimal Encapsulation
3) Generic routing Encapsulation

(2) Ad- hoc networks/ Wireless Ad-hoc Network (WANET):

*) Ad hoc network is a network that is composed of individual devices communicating with each other directly. Ad hoc n/w is independent of infrastructure.

*) Ad hoc network does not need
→ Routers
→ Base station
→ Internet service providers.

*) There a several situations where users of the network cannot rely on infrastructure
i) Infrastructure is too expensive
ii) In all situations there is no possibility for the existance of intra structure

In these situations ad-hoc n/w is the only choice.

Situations where adhoc n/w is the only possible choice:

i) Instant requirement
ii) Natural Disasters
iii) Remote Areas
iv) Effectiveness.

Characteristics of Ad-hoc network:

i) Topology of ad-hoc network is dynamic in nature and changes in the topology is possible.

2) Due to wireless transmission, their physical security is limited.

3) Capacity of these network is lower when compared with wired network.

4) Adhoc n/w experience higher loss rates, higher delays and also the jitter than the fixed type of networks.

5) They use either exhaustible power supplies or batteries for getting energy.

6) A perfect "Ad-hoc n/w", it has all the seven layers from physical layer to application layer

7) Adhoc n/w does not depend on any central control or infrastructure.

8) Network density, link failure, node distributions has to be clearly defined for ad hoc n/w

MANET (Mobile Adhoc Network):

*) Mobile ad hoc n/w (MANET) has many advantages and one of the most important advantage is its "infrastructure independent" nature.

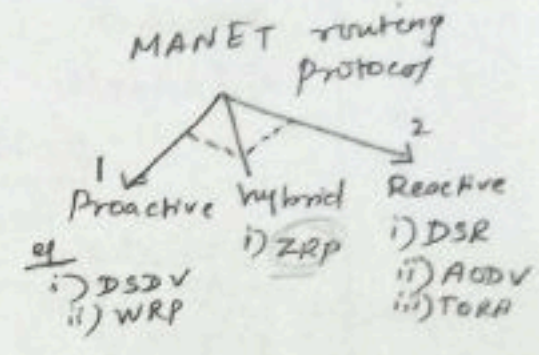
*) MANET describes mobile, wireless, distributed multihop networks that can operate independent of infrastructure.

*) MANET is developed due to military requirement where less infrastructure is required.

Types of MANET Routing:

*) MANET routing protocols are classified as

→ Pro-active (table-driven) &
→ Reactive (on-demand)



*) If a host is running a proactive protocol they will react to topology change by propogating routing related information to neighbours.

*) Routing protocols are classified as
   i) unicast
   ii) Multicast

Unicast routing protocol:

a) Proactive Protocols: → In this routing protocol, routes are constructed according to the table maintained in each node

*) Examples of proactive (table-driven) protocols are
   i) Destination sequenced Distance vector (DSDV) protocol.
   ii) Wireless Routing protocol (WRP).

b) On-demand routing protocol (or) Reactive protocol

→ In this routing protocol, routes are constructed according to the demand.
→ It tries to find or maintain routes whenever necessary.
→ examples of reactive protocol are
   i) Dynamic Source routing (DSR)
   ii) Signal Stability based Adaptive Routing (SSA)
   iii) Ad hoc Ondemand Distance vector Routing (AODV)
   iv) Temporarily ordered Routing Algorithm (TORA)

c) Hybrid routing Protocol:

A combination of reactive & proactive approach is known as Hybrid routing protocol (~~ZRP~~)

*) Example of hybrid routing protocol is Zone Routing protocol (ZRP).

Operations of DSDV:

i) DSDV is like traditional distance vector routing technique. It is also called as "Bellman-Ford routing algorithm"

ii) Each router in the network collects information from its neighbours.

iii) After gathering information, node seaches for the shortest path to route the packet.

iv) A new routing table is generated.

v) Then the router will broadcast this table to its neighbours.

vi) This procer continues till the routing information becomes stable.

Routing Algorithms:

i) Destination Sequence Distance Vector (DSDV)

ii) Dynamic Source Routing (DSR)

Features of MANET :

i) Network size
ii) connectivity
iii) Network topology
iv) User traffic
v) Operational Environment
vi) Energy → low energy n/w approach

Properties of MANET:

*) In MANET, there is no dedicated network infrastructure devices available.
*) MANET is architectureless wireless n/w.
*) Because of range limitation, for covering a short distance it has to undergo many hops.
*) gateway devices are known as weakly connected adhoc networks.
*) MANET's are mainly peer-to-peer (P2P) n/w.
*) MANET has 2 main features of wireless computing known as
   1) weak connectivity &
   2) Resource constraints.
*) There is no centralized controlling Mechanisms.

→ Proactive routing protocol — DSDV
→ Reactive routing protocol — DSR, AODV

Routing protocols

1. Proactive protocol
   - → Destination sequence Distance Vector routing (DSDV)
2. Reactive Routing protocol
   - → Dynamic source Routing (DSR)
   - → Ad hoc On Demand distance vector routing protocol (AODV)
3. Hybrid Routing protocol
   - → Zone Routing protocol (ZRP)
4. Multicast Routing protocol
   - → On Demand Multicast Routing Protocol (ODMRP)

(3)

Reactive routing protocol: Ad hoc on Demand distance vector routing Protocol (AODV):

*) AODV protocol is a reactive protocol which is constructed on DSDV protocol. While a DSDV routing protocol maintains a complete list of routes.

*) In AODV protocol routes are created only on demand.

*) Next hop routing model is essentially adopted in AODV. The routing table in the host points to the next destination. The destination IP addres of the packet received is cross checked with the routing table so as to forward the packet to the next destination.

*) The node awaits a reply after forwarding a RREQ. AODV uses the sequence number of the destination for determining the route.

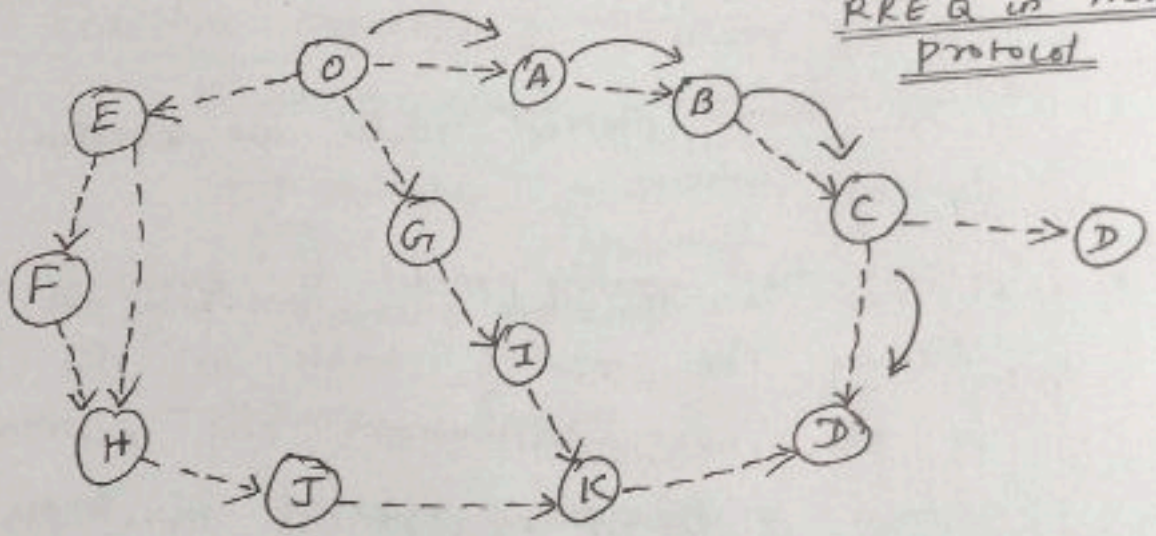
*) RREQ is identified by the broadcast ID & IP addres. Broadcast Id & Ip addres are cross checked based on the RREQ. If RREQ is a mere repetition it is ignored or else a reverse path to the origin (O) (original source) is established.

*) Reseive path is established along the intermediate nodes in the routing table based on the request.

*) When RREQ touches the destination a reply is sent in the reverse path to original source (O)

*) The fig. shows the route discovery based on AODV.

Fig: propagation of RREQ in AODV Protocol



→ Links on reverse path

↷ Links on forward path

- - → represents transmission of RREQ.

*) The figure shows the RREQ from source and RREP along the reverse path.

*) Each node transmits a HELLO message along the route so as to maintain the route in AODV. If the HELLO message is not received, it indicates as disruption in the connectivity.

*) From the source to the destination, each node registers only the next hop and not the entire route.

*) In case of disruption of a route, the origin may initiate once again a route discovery to the destination.

*) AODV make use of

i) hop-by-hop routing
ii) Sequence numbers and
iii) Beacons

Properties of AODV:

1) Reactive routing approach is used to discover/maintain the route. This is turn reduces the number of routing messages.

2) HELLO messages are used to update the nodes routing table regarding next hop.

3) AODV is bidirectional, RREP is sent along the reverse path based on RREQ

4) Due to HELLO message, there is an additional burden to the protocol.

(4) Proactive Protocol:

Destination Sequence Distance vector (DSDV)

*) DSDV routing algorithm can be used in ad-hoc n/w. It is an extension of distance vector routing algorithm. Distance vector routing algorithm has a poor performance due to count-to-infinity problem.

*) In case of adhoc n/w, each node exchanges its neighbour table periodically with its neighbours Thus changes at one node in the n/w propogate slowly thro' the n/w.

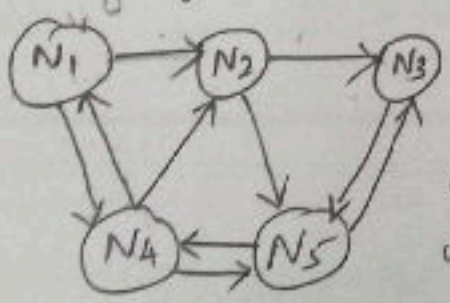
*) DSDV modifies the distance vector algorithm by adding two features as follows

i) Sequence numbers:

In DSDV, each advertisement is identified by a sequence number. These advertisement propogate along many paths in an ad-hoc n/w. Sequence number help to apply the advertisements in correct order. This helps to avoid loops.

ii) Damping:

Dynamic topology changes should not destabilize routing algorithms. This is achieved by not disseminating of the advestiments that contain changes in topology currently stored.

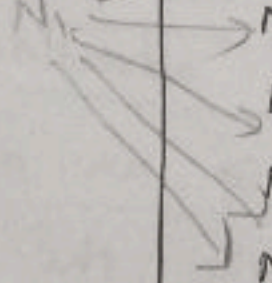


*) The working principle of DSDV algorithm can be explained considering this n/w.

*) N_1 stores the information for each node in a particular format.

*) For each node (from N_1)
- → next hop towards the node
- → metric (no. of hops)
- → sequence no. of last advertisement of this node.
- → Time at which the path has been installed first

*) Additionally the table also contains flags and setting time



Destination	Next hop	Metric	seq. no.	install time
N_1	N_1	0	$S_1 - 321$	$T_4 - 001$
N_2	N_2	1	$S_2 - 218$	$T_4 - 001$
N_3	N_2	2	$S_3 - 043$	$T_4 - 002$
N_4	N_4	1	$S_4 - 092$	$T_4 - 001$
N_5	N_4	2	$S_5 - 163$	$T_4 - 002$

*) DSDV algorithm is loop free at all instants. It has low memory requirements and a quick coverage through triggered updates.

Reactive Routing Protocol

Dynamic Source Routing (DSR)

*) Consider in ad-hoc network, when the n/w is lightly loaded, DSDV or distance vector or link state routing algorithms are used for updating routing tables. These algorithms maintain route between all nodes even though there is no data.

*) Dynamic source routing (DSR), therefore divides the task of routing into 2 seperate problems.

i) Route discovery

A node tries to discover a route to the destination node only on "need" basis. There is currently no known route and the route is discovered as and when there is a requirement to send the data packet.

ii) Route maintanence:

As long as there is a transfer of packet to the destination node, the source node makes sure that the route is maintained. This route is used for continuously sending packets. If the source node detects any problem with the current route, an effort is made to find the alternative route.

*) Working of DSR:

Dynamic source routing eliminates all periodic routing updates and works as follows:

i) If the node has already received the current request, it drops the request packet.

ii) If the node receiving the request is the destination node, it is request has reached the target.

iii) If the node is not the destination node, the node appends its own addr. to the list of traversed hops in the packet & broadcasts again.

*) Using this approach, the route request collects a list of addresses to reach the destination Above steps (i), (ii) & (iii) continues until the destination node is reached.

*) As soon as the request reaches the destination it can return the request packet containing the list to the receiver using this list in reverse order.

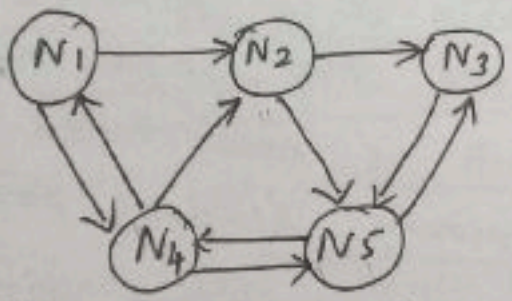
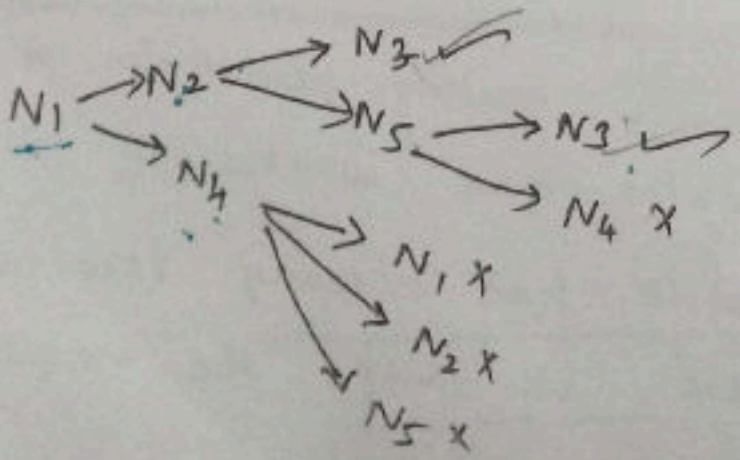


fig: route from N_1 to N_3

*) Applying route discovery to the example in this figure for a route from N_1 to N_3

*) N_1 broadcasts the reque to N_2 and N_4. The request is:

((N1), id = 42, target = N



2) N_2 then broadcasts the request to N_3 & N_5. The request is

((N1, N2), id = 42, target = N

3) N_4 then broadcast the request to N_1, N_2, N_5
The request is
$((N_1, N_4), id = 42, target = N_3)$

4) N_3 recognize itself as destination
N_5 broadcast to again N_3 & N_4
$((N_1, N_2, N_5), id = 42, target = N_3)$

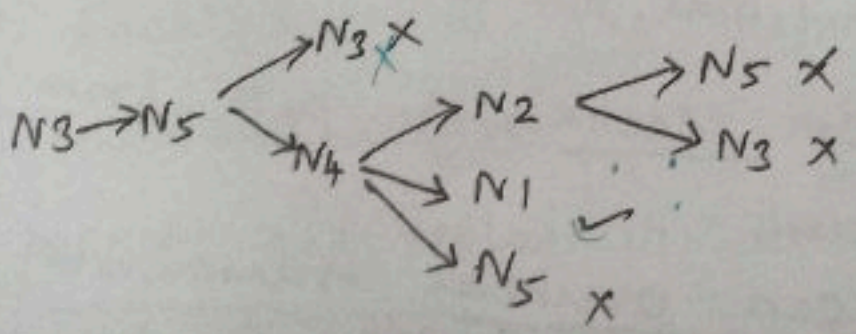
5) N_1, N_2 & N_5 drop's N_4's broadcast packet, since they have already received route request packet (N_2's broadcast reached N_5 before N_4 did)

6) N_4 drop N_5's broadcast. Finally 2 paths to destination
① $N_1 - N_2 - N_3$ & (shorter route)
② $N_1 - N_2 - N_5 - N_3$ (Longer route

*) Since the 2nd route is the longer route.
The 1st route $N_1 - N_2$ & N_3 is selected.

*) If the link is bi-directional (symmetric), the acknowledgement can be transmitted via the same path since wireless adhoc is an asymmetric, seperate path has to be found to transmit the ack. from receiver to sender.

*) The route discovery in reverse direction proceeds as follows: $N_3 - N_2 - N_1$



$N_1 - N_3$

$N_3 - N_1$

Route Discovery in Reverse direction:

1) N_3 broadcasts a route request to N_5. Only N_5 receives (((N_3), id = 27, target = N_1) this request.

2) N_5 broadcasts the request to N_3 & N_5

((N_3, N_5), id = 27, target = N_1)

N_3 drops the request.

3) N_4 broadcast the request ((N_3, N_5, N_4), id = 27, target = N_1) to N_2, N_1 & N_5.

N_5 drops the request.

N_1 recognizes itself as target.

4) N_2 broadcast the request to N_5 & N_3

((N_3, N_5, N_4, N_2), id = 27, target = N_1)

N_3 & N_5 drop the request.

*) At the end, the path from N_3 to N_1 is

$N_3 - N_5 - N_4 - N_1$.

*) The route discovery algorithm can be optimized in many ways:

i) To avoid too many broadcasts, each route request could contain a counter. Every node re-broadcasting the request increment the counter by one. If the counter value reaches maximum no. of nodes (max n/w diameter).

ii) A node can cache the path from recent route request.

iii) A node can overhear transmission from the

nodes. This information can be used to discover shorter routes.

*) Once a route is discovered, the route needs to be maintained as long as the node sends packets to the destination along the discovered route.

*) There are different approaches available for maintaining the discovered route.

i) The node listen to the next node forwarding the packet, thus getting passive acknowledgement

ii) The node could request an explicit acknowledgement

(6) Multicast Routing Protocol:
On-Demand Multicast Routing Protocol (ODMRP)

*) Under on-Demand Multicast Routing protocol (ODMRP) the multicast tree is formed by periodical JOIN packets of host source.

*) Consider the source node 's'. It will flood the JOIN_DATA packets to all other nodes in the network. When a host node receives first JOIN-DATA packet it will rebroadcast it to form a reverse path with the previous host.

*) Each host in the network acts as multicast receiver. It receives JOIN_DATA packet and replies in turn with a JOIN-TABLE packet to the upstream to establish reverse path.

r) The procen repeats until source host 's' is reached. The method of packet forwarding is for fig (i) as shown in fig (ii)

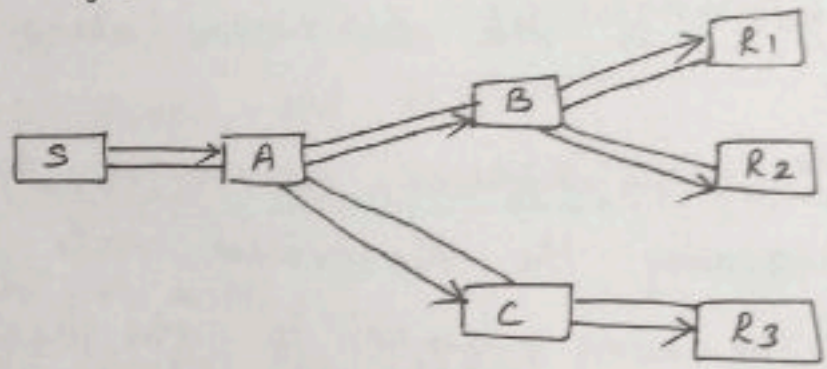


Fig (i)
Load_data packets propagation

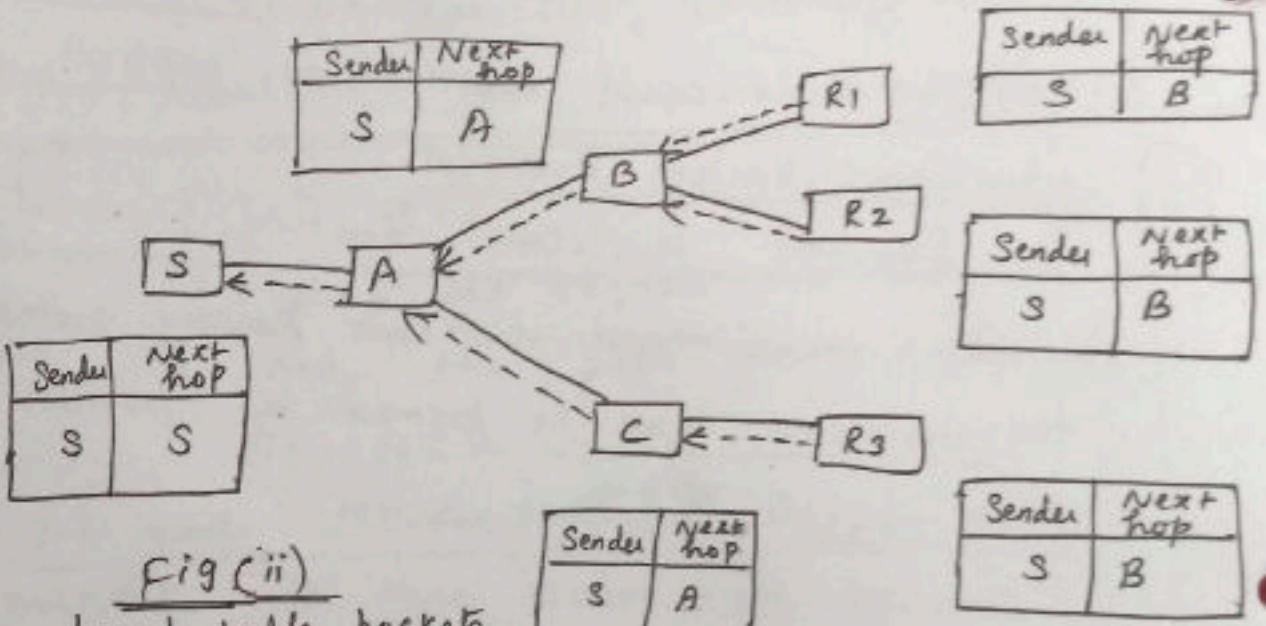


Fig (ii)
Load_table packets Propogation.

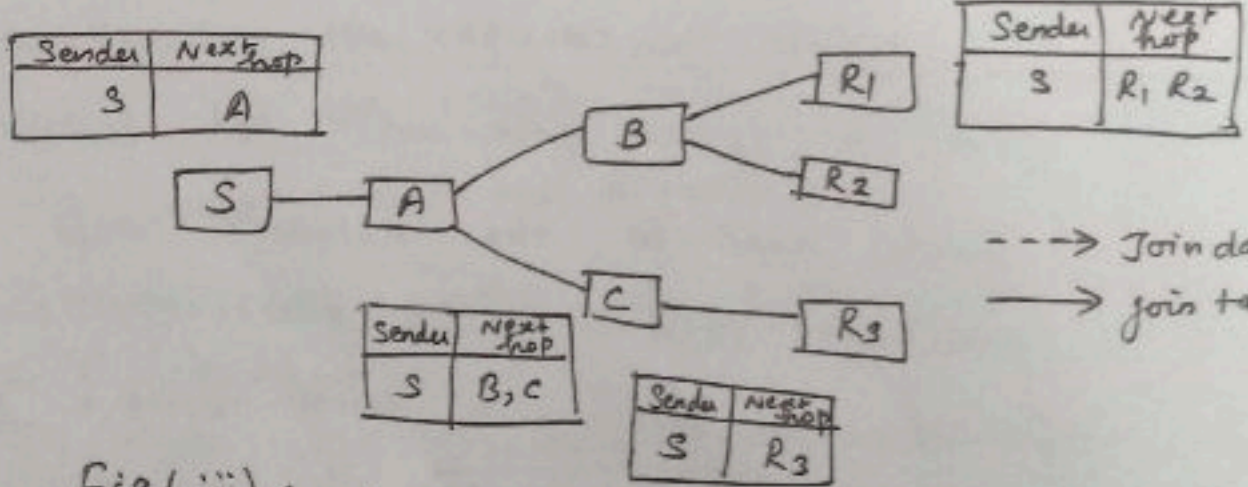


Fig (iii): Last Multicast table

Figure (i) (ii) & (iii) On-demand multicast routing protocol

*) As the JOIN-TABLE is received a host has to build a multicast table so as to facilitate future packet forwarding.

*) For example the host B receives the R_1's JOIN-TABLE as shown in figure. It will add R_1 as its next hop step. Assume B receives R_2's JOIN-TABLE. Now it will also add R_2 as its next hop step.

*) A simple final multicast table for each host is shown in fig (iii) in propagation of data packets

AODV protocol

*) The on-demand distance vector routing protocol known as multicast AODV is an extension of unicast AODV protocol. Here the multicast tree is updated whenever a new host joins the multicast group. For making the process of tree updation easier the route request packet (RREQ) is being broadcast.

*) In case, a host receives a RREQ and if the host is not a member of multicast group, then it will rebroadcast RREQ to the neighbouring members of the network.

*) But if the host is a member of multicast group and if this host receives a RREQ then it will give route reply (RREP) packet

data to the sending host (S). Now the multicast table will be updated. By these processes forward path will be created.

*) If two RREQ's are received at a time then depending upon minimum no. of hop count the one with minimum hop count will be selected.

MACT (Multicast Activation):

*) It is a multicast Activation (MACT) packet. The source S will unicast a MACT packet to the next hop step. On receiving a MACT packet the next hop will enable for source host (route with minimum hop count) and it leads to multicast tree.

*) This procedure continues till a multicast member is reached succesfully.

Multi-cast Routing:

*) In multicasting the 2 clasification → Source based Pr
→ Core based protocol

*) These clasification is based how multicast tree is constructed

Soure based protocol:

→ Attempts to maintain multicast tree for every node from source node to all the members in the multicast group

→ There will be many multicast trees in the nlw.

Core based protocol:

→ There will be one multicast tree only at core host.

→ There are several appln. served by multicasting One is video conferencing.

*) In MANET broadcasting, interference, is difficult.

(7) Hybrid Routing protocol: (11)

*) Hybrid Routing method is a combination of proactive & reactive routing technique.

*) If simultaneous usage of both protocols is not achieved, then the efficiency has to be compromised

*) so, two protocols (say X and Y), the protocol X should be used locally, while protocol Y should be used globally.

*) Example of hybrid routing is Zone Routing Protocol (ZRP).

A) Zone Routing protocol:

*) In this protocol, the network is divided into a number of zones. consider a zone Z(m, n)

where n → represents nodes
m → denotes radius

ie, a branch of nodes 'n' operate at a maximum distance 'm'.

H(i,j) → where i and j are different nodes.
→ it is the distance b/w the nodes.

$$Z(m,n) = \{ i / H(i,j) n^m \}$$

a) Architecture of zone Routing protocol:

*) The main components of the protocol's architecture are

i) Intra zone Routing Protocol (IARP)
ii) Inter zone Routing protocol (IERP)
iii) Border Cast Resolution protocol (BRP)
iv) Neighbour Discovery protocol (NDP)

$i / H(i,j) n^m$

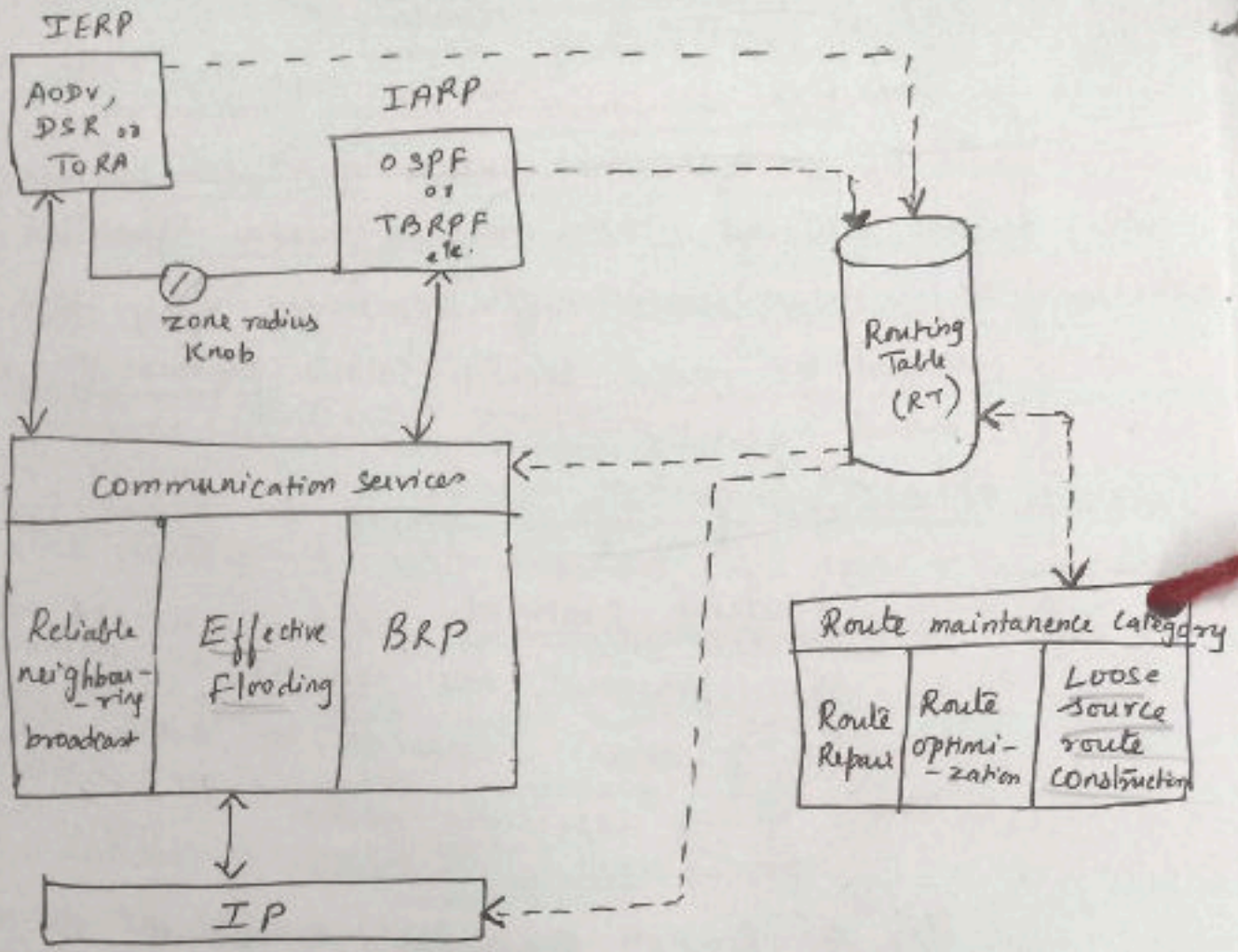


Fig: Architecture of ZRP

*) IARP covers the Routing zone which encompa the distance and routes of the nodes inside a z

*) IERP uses selective flooding under IARP.

BRP & NDP:

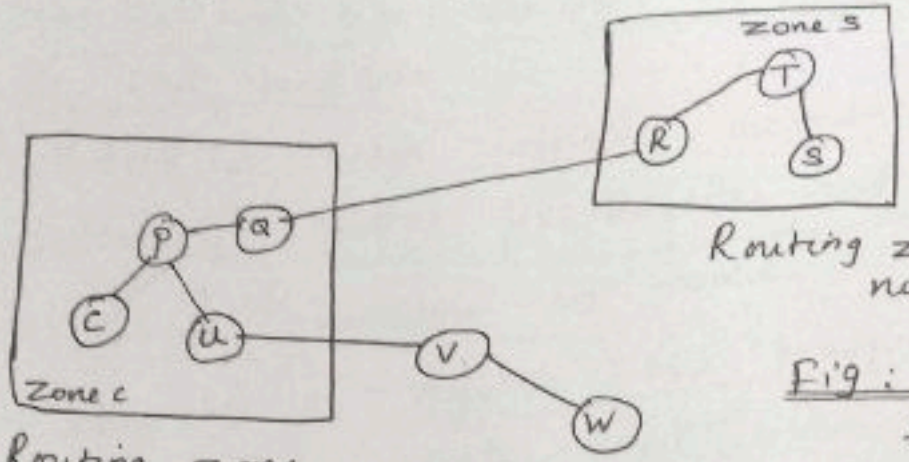
*) Datagram are conveyed to the peripheral nodes by bordercasting (BRP) resolution protocol. However, it is initially the NDP (neighbour discovery protocol) which initiates the neighbour discovery function.

b) Network with ZRP:

*) The data packet is to be sent from node C node S. We can see that node S is not within the zone and so a request is sent

to the peripheral nodes Q and U.

*) U forwards the request to the adjacent nodes and it is seen that S is along the routing zone of R and T.



Routing zone for node s

Routing zone for node c

Fig : network with ZRP.

*) A reply is thus received from s and sent to C. Thus, IRP enables to maintain the routing information proactively within the zone and reactively beyond the specific zone.

Multicast Routing :

*) In multicasting protocols, the two classification are

i) source - based protocol
ii) core - based protocol.

(8) Vehicular Ad-hoc network (VANET)

*) VANET is a special type of MANET that is used to provide communications between nearby vehicles and b'w vehicles and fixed infrastructure on the roadside.

*) VANETs were initially introduced for the vehicles of police, fire brigades and ambulances for safe travelling on road.

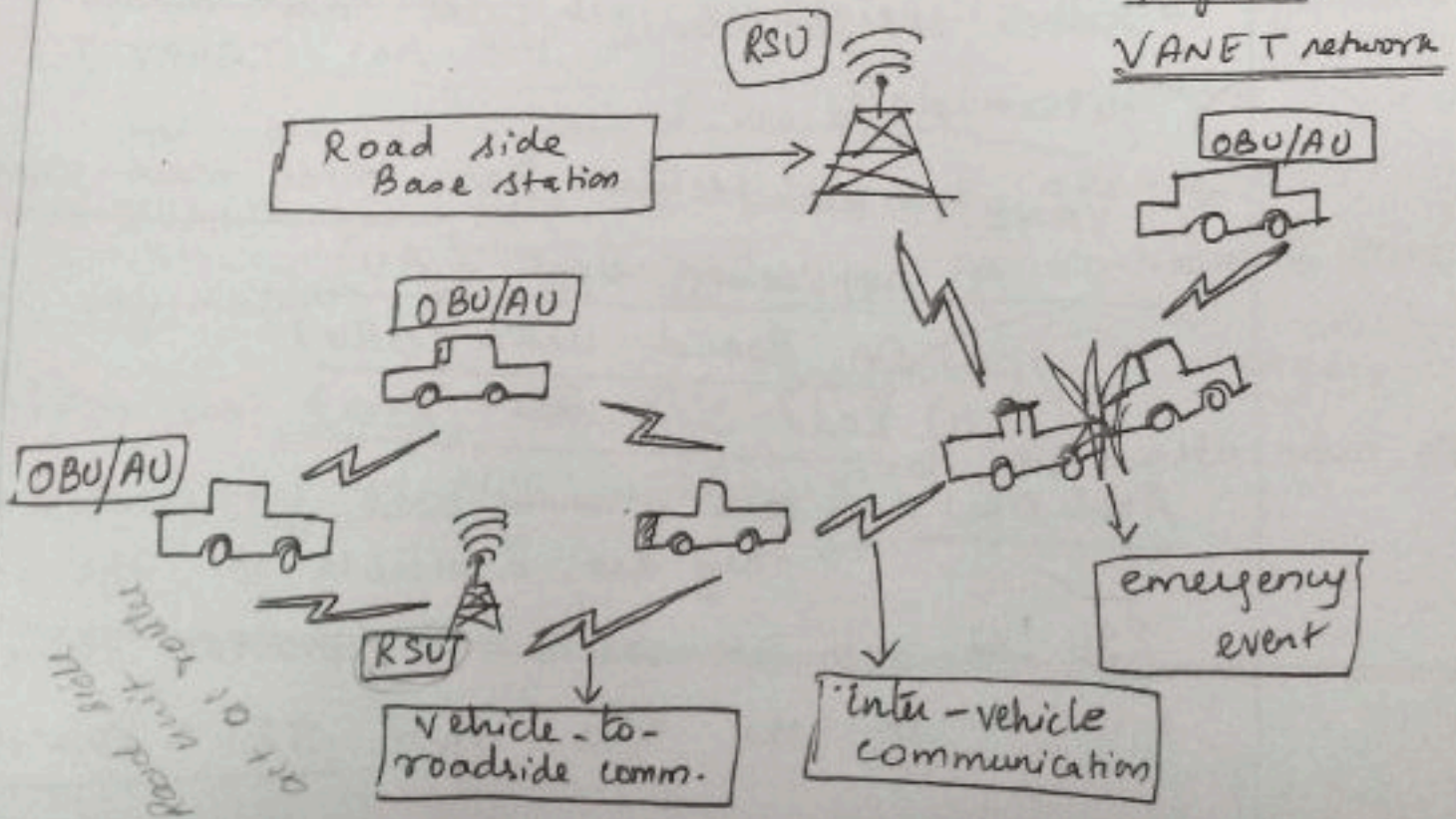
*) In order to regulate the traffic on the road and avoid accidents VANET is designed to provide real time information to the driver.

*) A vehicle can communicates within a range of about 100 to 300 meters to the other vehicle.

*) In a city or a busy highway, the diameter of the network can be several tens of km's.

Architecture of VANET:

Figure: VANET network



*) Any vehicle that goes out of the signal range in the network is excluded from the n/w and if a vehicle is coming in the range which is already in the network, can join in the n/w

*) VANET helps the driver by giving warning information in advance in the form of messages.

*) Routing protocol obtain inf from navigation service & street maps

*) Each and every vehicle is considered as node. Each node is aware of its own position with Gps devices..

*) The functionality of the geographic routing protocols is divided into 3 category namely;

i) path selection
ii) Forwarding
iii) Recovery

→ Path selection procen is not mandatory.

→ In case if the protocol fails to find the path, then it selects Forwarding strategy and selects neighbour vehicular node to forward the packet data.

*) VANET architecture has three main components

i) Application unit (AU)
ii) On Board units (OBU)
iii) Road Side units (RSU)

AU & OBU → are mainly used for consumer service
→ they are available in the vehicle.

RSU → acts as router to provide these service in the n/w thro' IEEE 802.11 p standa

OBU → are used for IP mobility management processing
↓
data collection.

*) AU can be a seperate units or integrated with OBU's and used to communicate with RSUs in the network.

Routing protocol in VANET:

*) VANET routing protocol is classified as
   i) Vehicle - to vechile based (V2V)
   ii) Vehicle - to - infrastructure based (V2I)
   iii) combined hybrid V2V & V2I communication

i) V2V adhoc n/w:
(ie, vehicle to vechile comm.)
→ It permits direct vehicular communication. It does not relay on fixed infrastructure supports.

ii) V2I adhoc n/w:
→ It permits a vehicle to roadside unit comm.
→ It focus on data and information gathering application

Uses of MANET:

1) VANET can help drivers to get advance information and warning from a nearby via menages.
2) VANET can help to broadcast geographical information to the deiver as he continues to drive.
3) Drivers can have the oppurtunity to engage in other relaxing tasks such as watch news, etc.

(9) Difference between MANET and VANET

SNO	Mobile Adhoc n/w MANET	Vehicular Adhoc n/w VANET
1.	MANET consists of a set of mobile nodes and free to move in dynamically in any direction or in any speed	VANETs is network that interconnects vehicle on the road and it is special type of MANETs.
2.	The MANET does not require and fixed infrastructure and they are operated on batteries and limited transmission range	The VANET nodes (vehicles) can communicate with certain roadside infrastructure or base station.
3.	Topology of MANET is changed randomly.	Topology changes is frequent and fast.
4.	The production cost of MANET is low.	The production cost of VANET is costlier
5.	Mobile nodes are not moved as fast as like VANET	The nodes (vehicles) in the VANET move with high velocity because of which the topology changes rapidly
6.	Density of the network is spare.	Density of the network is frequently variable.
7.	Nodes are moving a random manner in the MANET	Nodes are moving regularly in VANET
8.	Node life time depends on power source	Node life time depends on vehicle life time.

	MANET	VANET
9.	Banduidth used in the MANET is in hundreds of Kbps.	Banduidth used in the VANET is in ranges of thousands of Kbps.
10.	The geographical range of MANET is upto 100m	The geographical range of MANET is upto 300 feet
11.	The reliability is medium in MANET.	The rediability is high in VANET

(10) Security in VANET:

*) VANET is vulnerable to many security attacks. This is because of the open access nature.

*) The attackers are clasified into 3 classes

i) Insider Vs outsider
ii) Active Vs passive &
iii) Malicious Vs Rational attackers

A) Security practices in VANET:

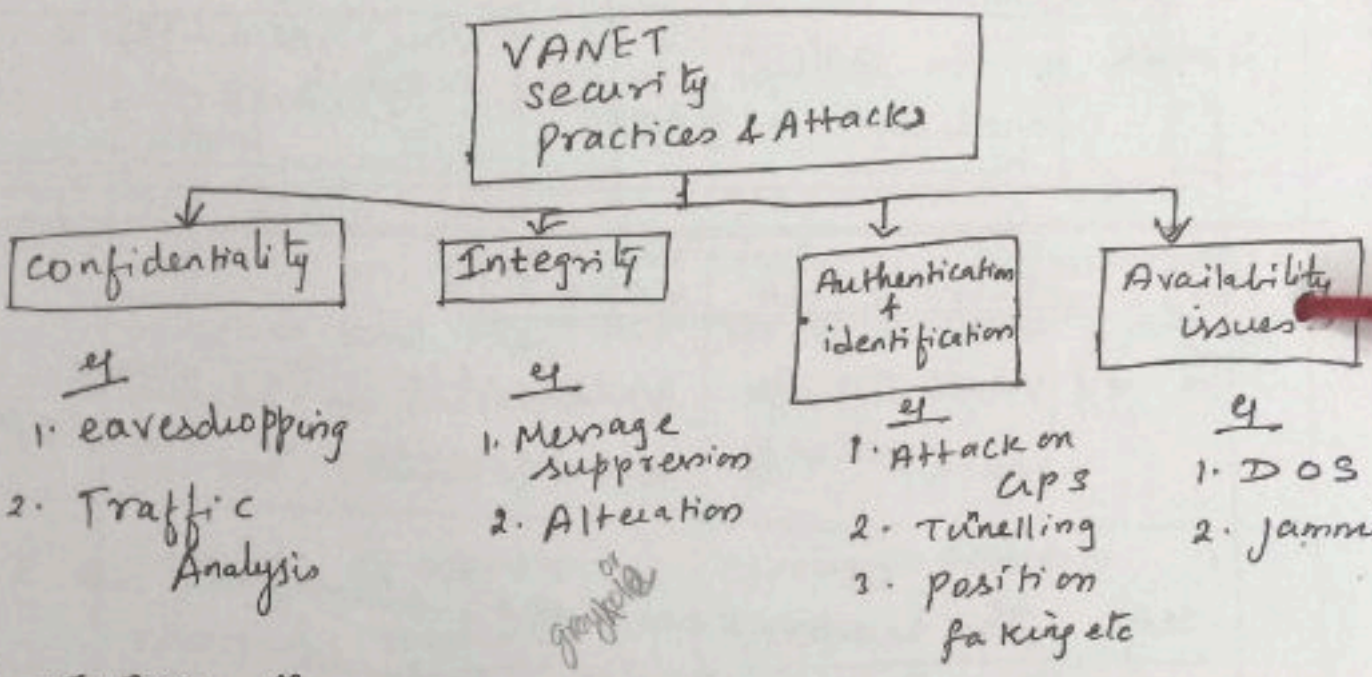
The major VANET security practices are

1. confidentiality
2. Integrity
3. Availability

*) Attacks in VANET n/w is clasified as

1. Network attack
2. Timing attack
3. Social attack
4. Monitoring attack &
5. Application attack, etc

*) There are also attackers such as
— Selfish Driver
— Malicious attacker
— pranksters, etc.
but each class of attackers makes different types of attacks.



B) Types of Attacks in VANET:

1. Denial of service [DOS] Attack:

*) DOS attack can even prevent sending and receiving of messages to other vehicles from the network.

*) DOS attacker either → jams the n/w comm- medium
(or) makes control of resourc of vehicl

2. Sybil Attack:

*) Sybil attack sends multiple copies of messa to other vehicles so that it misguides the vehicle telling that there is traffic jam ahea to it and it has to take another route

3. Meoage suppression Attack:

*) In this attack, the attacker can choose som packets and drop it. Sometimes those packets may contain a critical required information. The goal of this attacker is to deny the collision and jamming information from reaching the knowledge of concerned authorities.

4. Alteration Attack:

This type of attack, takes ploce where the attacker try to change or modify an existing data.

5. Spamming:

*) This attack, → consumes network bandwidth.
→ increases transmission latency

*) In this attack, the attacker attacks the n/w by sending many advertisement meoage.

6. Identity Discloser:

*) In this attack, the attacker sends malicious code to the target node and get required data from it.

C) Security Requirements in VANET

*) An efficient VANET has to satisfy many security requirements.

Some security needs include:

1. Authentication
2. Privacy
3. Availability
4. Integrity
5. Non repudiation.

Trap door

(11) SECURITY in MANETs:

*) The aim of security solutions in MANET is to provide security services like,

i) confidentiality
ii) Integrity
iii) Anonymity
iv) Availability

A) Security issues in MANET:

*) It is very important to protect the protocol stack of MANET. The table shown below describes the security issues in each layer of protocol stack.

*) In MANET, security has to be provided to "deliver data bits from one node to another node".

S.NO	Layer in protocol stack	Security issues in each layer
1.	Physical layer	Preventing the signal jamming deniel of service attacks.
2.	Data link layer	Protecting wireless MAC protocol and to provide link layer security support.
3.	Network layer	Protecting the ad-hoc routing protocol and forwarding protocols.
4.	Transport layer	Securing and authenticating, end-to-end communications through data encryption techniques.
5.	Application layer	Detection & prevention of virus, worms, malicious codes, etc

Table : Security issues in MANET

*) Two approaches for securing MANET (20)

i) Proactive approach

→ prevents attacks through cryptographic techniq
→ it is used for ensuring correctness of routing states.

ii) Reactive approach:

→ detects threats (attackers).
→ it is used for protecting packet forwarding functions.

B) Multifence security solution:

*) In MANET multi-hop connectivity is provided through distributed protocols in link layer & n/w layer.

*) Three security components are

a) Prevention
b) Detection
c) Reaction.

*) A better security approach is to have both proactive & reactive methods together and also the three components has to be included.

Prevention component → prevent the attacker from entering the system.

Detection component → detects the attackers

Reaction component → identifies the attackers & avoids them from doing adverse effects.

Network layer security:

*) It is concerned with protecting → adhoc routing protocol & → forwarding protocols

*) protocols are of two types

a) Secure adhoc routing protocol &
b) Secure packet forwarding protocol

c) Message Authentication Primitives:

*) Messages are being transmitted between the nodes in the network. These messages has to be authenticated. There are three cryptographic primitives for authentication. They are

i) Message Authentication code.
ii) Digital signature.
iii) One-way HMAC key chain

i) Message Authentication code:

→ In this technique, two nodes share a common secre Symmetric key (K).
→ They can generate & check a message with the help of hash function (h).
→ HMAC is the popular security primitive used in n/w layer

ii) Digital Signature:

→ It is based on asymmetric key cryptography.
→ It includes signing/verification or encryption/decryption
→ If public key is known to all nodes, then each node can verify digital signature.

iii) One-way HMAC Key chain:

→ There are many one way cryptographic fn's are available.
→ The computations incorporated in one-way key-chain based authentication is less and an authenticator can verify layer no. of receivers.

*) MN itself decapsulates the packets & HA encapsulates the packets. There is no need for FA any more. Where as in IP v4 encapsulation & decapsulation is done by FA.

(12) Dynamic Host Configuration Protocol (DHCP):

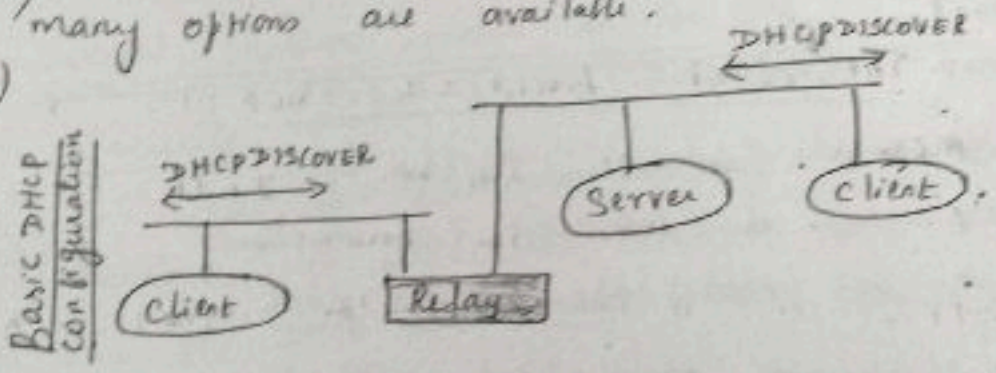
*) DHCP is mainly used for the installation & maintenance of the comp n/w simple. Whenever a new computer joins an already existing n/w, the DHCP provides the following necessary info.

i) address of a DNS server & default router
ii) Subnet mask
iii) Domain name
iv) IP address.

*) The unique feature of DHCP is to provide an IP address for the new node entering into the n/w.

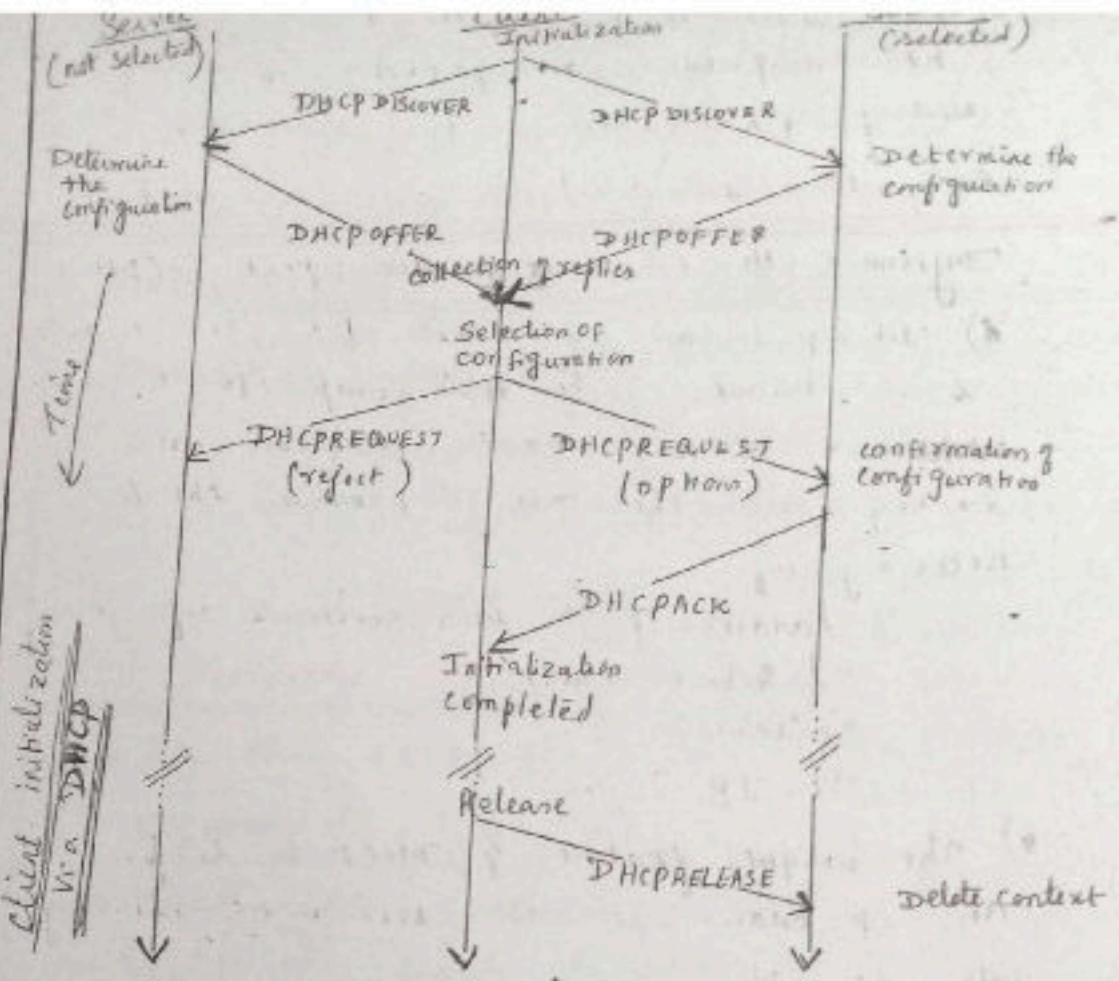
*) The basic DHCP mechanisms are very simple, many options are available.

*)



*) The fig shows the basic DHCP operation It works on the basics of client/server Model.

As shown in fig, each node (client) sends a request to server. The server responds to these requests. Suitable Relays are needed for the request to be forwarded to the server.



*) The above fig shows one client and two servers.

The client broadcast DHCP DISCOVER message into the subnet. In this eg two servers receive this broadcast from the client.

*) Once the server receives the request, each server has to provide the client with some information, including the clients Ip address via a DHCP OFFER message.

*) The client can choose one of the offered configurations. The client inturn replies to the server, accepting one of the configuration

and rejecting the other using DHCPREQUEST. If the server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients. The server with the configuration accepted by the client now confirms the configuration using DHCPACK. This completes the initialization phase.

*) If a client leaves a subnet, it should release the configuration received by the server using DHCPRELEASE.

*) The configuration a client gets from a server is only leased for a certain amount of time. Therefore the client has to reconfirm the configuration from time to time. Otherwise the server will free the configuration. This is mainly done to take care of crashed-out nodes or the nodes that may have moved out without releasing the context.

Several problems related to the use of DHCP:

1. Security
   There has been no authentication of DHCP messages. i.e MN cannot trust a DHCP server and the DHCP server cannot trust the mobile node.
2. There is no protocol for server-server configuration i.e One DHCP server cannot communicate with another DHCP server
3. An administrator has to take care that every DHCP server has its own addr. space for clients This typically results in address space fragmentation

13). Optimization of Mobile IP

Consider a situation that an Italian and a French meet at Singapore. Let us further assume that the Italian has some data on his laptop and wants to transfer the same from his laptop to the ~~Italian~~ Laptop of the French who is only few meters away. They may choose to use mobile IP for mobility support. When the Italian transmits a packet to the French (at Singapore), the data packets travels to France (from Singapore). The HA at France encapsulates the data and tunnels the same to the COA of the French at Singapore. Even though the senders & receiver are only a few meters away from each other, the data travels almost all over the globe before it reaches its destination. This is known as triangular routing and is non-optimized behaviour of mobile IP. The triangle is made up of 3 segments

i) CN — HA
ii) HA — COA/CN
iii) MN — CN

*) One way to optimize the route is to inform the CN of the current location of the MN. The CN can thus learn the location by caching it in a binding cache which is a part of the local routing table for the CN. The optimized mobile IP protocol has 4 messages

4)

:

4 messages are

i) Binding request :

Any CN that wants to know the current location of and MN sends the binding request to the corresponding HA. HA must verify if MN has permitted HA to reveal the MN's current location. If such permission exists, HA sends a binding update back.

ii) Binding Update :

This is the message sent by HA to CN informing CN of the current location of MN. CN receiving binding update may be expected to send an acknowledgment back

iii) Binding Acknowledgment :

The CN return this acknowledge after receiving a binding update message.

iv) Binding Warning :

Finally, if a node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends a binding warning to the HA of the MN. The warning contains the IP address of the MN and the address of the node.

Sequence of operation for optimization :

*) The fig illustrates the operation of the 4 messages. The sequence of operation are as follows :

1) CN request a current location of the MN. The request is sent to HA.

2) HA checks if MN has permitted for the information. If permission is available HA sends the update message to CN. The update message contains the COA address of MN.

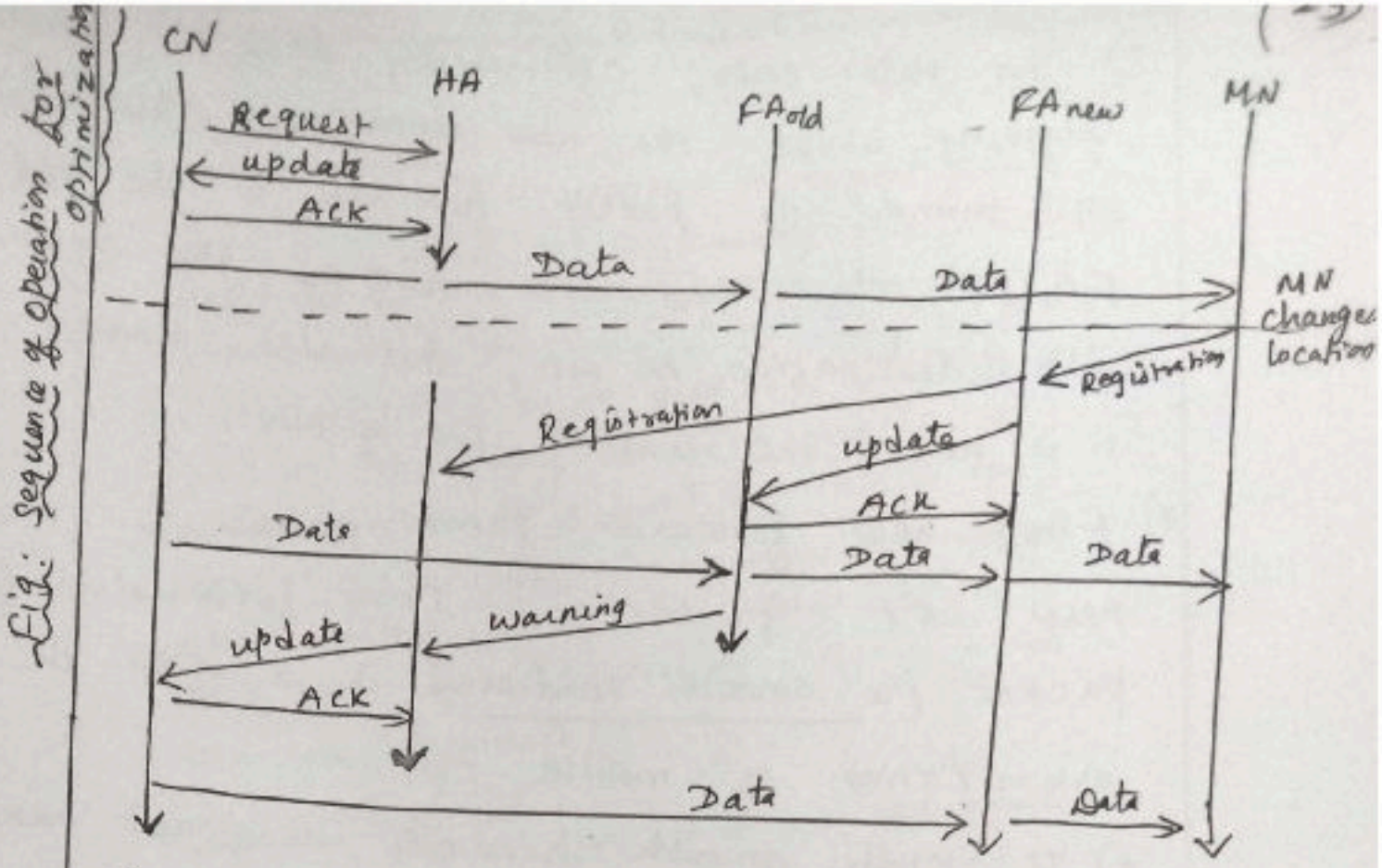


Fig: Sequence of Operation for optimization

3) The CN updates the mobility binding of MN after acknowledging the update message.

4) If CN has the data packet to be transferred to MN, the CN sends the packet directly to FA_{old}. FA_{old} is the current FA for MN.

*) Let us consider the situation that the MN has moved its location & registered with a new foreign agent FAnew. This registration is also forwarded to HA to update its location data base.

*) Furthermore, FAnew informs FAold about the new registration of MN. This message is passed via update message, which is acknowledged by FA_{old}.

*) In this case, CN surely does not know anything about the new location. Thus CN still tunnels its packet for MN to the old FA FAold. The FAold now notices the packet with destination as MN, but also knows that it is not the current FA of MN.

*) FAold now forwards these packets to the new COA of MN. This forwarding of packet (ie smooth handover) is a step in optimization of mobile IP.

*) If such smooth handover does not take place, all packets meant for MN might be lost in transmission.

*) Another option is → FA old sends a binding warning message to HA. HA in turn sends an update to CN, so that CN can update its binding cache. CN will acknowledge the update message. Then CN sends all further data packets meant for MN to FAnew.

14

Difference b'w wired n/w & adhoc wireless network

related to routing are gn. below :-

1. Asymmetric links:

If a node A receives a signal from node B, it is not necessary that there should be a link in the reverse direction from node B to node A. It may have a better link, or a good link or a weak link or there may not be a link in the reverse direction (B – A). This is the case of wireless n/w. where as in wired n/w routing info is transmitted in the same path on both direction. Hence wired n/w's are symmetric

2) Redundant links:

In a wired n/w, there are redundant links, mainly to survive link failures. Generally lower level of redundancy exists in wired n/w and it is controlled by n/w administrator In ad-hoc n/w there is no controller for redundancy. Adhoc n/w has high redundancy.

3) Interference:

In wired n/w, links exists only where a wire exists and connections are planned by n/w administrators. This is not the case of wireless ad hoc n/w's. Links come & go depending on transmission characteristics. One transmission might interfere with another one. Interference thus creates new problem by links b'w nodes. (in ad-hoc n/w)

wireless → Interference high in ad-hoc n/w. → unplanned link.

"unplanned" wired – planned link hence less interference

4) Dynamic Topology:

wireless There is frequent changes in the topology of the n/w in case of adhoc n/w a topology changes for very short period of time

In adhoc n/w, the frequent changes in the routing table's routing algorithms have to be changed immediately.

wired In wired n/w the routing algorithms are updated too slowly.

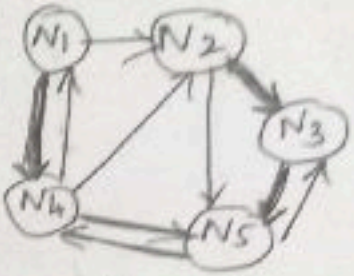
wireless 5) Consider the fig (a) at time t_1, node N_1 wants to send data to N_3 and needs an acknowledgement. N_1 choose the path N_1, N_2, N_3 for this it requires 2 hops, where as acknowledgement cannot take the same path, N_3 chooses N_3, N_5, N_4, N_1. This takes 3 hops. In wired n/w same no of hops takes in both direction. In wireless the assumption becomes wrong leading to misinterpretations of measurements & efficiencies.

6) At time t_2, the topology has changed. Now N_3 cannot take the path N_3, N_5, N_4, N_1 to reach N_1, but take the same path N_3, N_2, N_1 (as data was sent) to transmit the acknowledgement.

wireless Thus as topology changes the path to transmit data & ack. also changes from time to time.

eg - 9 adhoc n/w

fig (a)

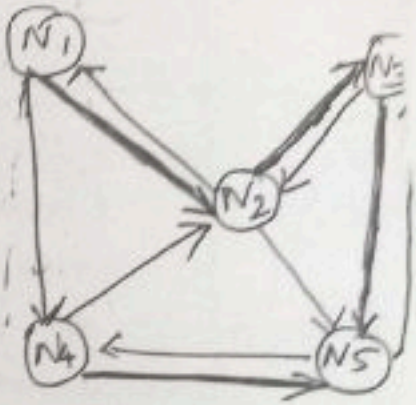


time = t_1

→ Good link

⇢ weak link

fig (b)



time = t_2

*) Adhoc n/w using mobile nodes face additional problems due to hardware limitations. Due to frequent update of n/w information
→ there is wastage of battery power.
→ wastage of Bandwidth

Some more difference b/w adhoc n/w & wired n/w

Wireless
1. Traditional routing algorithms are not suited for ad-hoc n/w. Traditional routing algorithm work
→ less efficiently (distance vector algorithm) or
→ fail completely (Link state algorithm).
These algorithm cannot handle situations such as asymmetric link, highly dynamic topology and interference

2. In wired n/w, layer 3 knowledge is good enough to define good path. In case of adhoc n/w (wireless) layer 3 knowledge alone is not sufficient to help the routing algorithms to find a suitable path b/w a source & destination. Lower three layers offer help to wireless n/w.

3. Wireless n/w takes too long time to collect the current status & disseminate it again, due to frequent topological change, centralized approached cannot be used.

4. Ad hoc n/w is connectionless

5. In wireless n/w flooding concept works only if the load is low, but it is inefficient.

6. One of the main metric in wireless n/w is hop counting

V. Selshiya

UNIT IV

Mobile computing

1) Mobile TCP:

*) Transport layer is responsible for the following functions

i) Performing checksum checks on user data

ii) Multiplexing / demultiplexing of data to / from application.

*) UDP (or) TCP is used as protocol.

UDP → connectionless and does not guarantee reliability in data delivery

TCP → connection oriented and guarantee reliability

→ TCP is more complex

*) The mobile link may have cases of dropping packets that may be due to reasons other than hand off related problems of higher error rates in the wireless links. packets may be dropped due to disconnections. Mobile links totally failing for an extended period is not an un common phenomenon.

*) The timer doubles its duration for each incidence of unsuccessful retransmission attempt. The max. time allowed is one minute. Retransmission will be finally given up after 12 attempts. Sender will start slow rate as it assumed congestion as the reason for no ack

Goals of M-TCP:

i) Improvement of throughput
ii) Lowering delay
iii) To maintain end-to-end TCP semantic
iv) To provide more efficient handoff
v) To adapt to the problems due to length and frequency disconnections.

*) In case of I-TCP, M-TCP splits a single TCP connections into two parts.

The two parts are

i) Normal TCP connection b/w standard host and supervisory host.
ii) Optimized connection b/w Mobile host and supervisory host.

Advantage of M-TCP:

i) End-to-End semantics is maintained.
ii) When MH is disconnected, retransmissions are avoided.
iii) NO buffering of data in SH.

Disadvantages with M-TCP:

i) packet loss is propagated to the sender. M-TCP assumes the reason for packet loss is low bit error rate, that may not be valid
ii) Modification of TCP on mobile host requires changes in MH protocol.

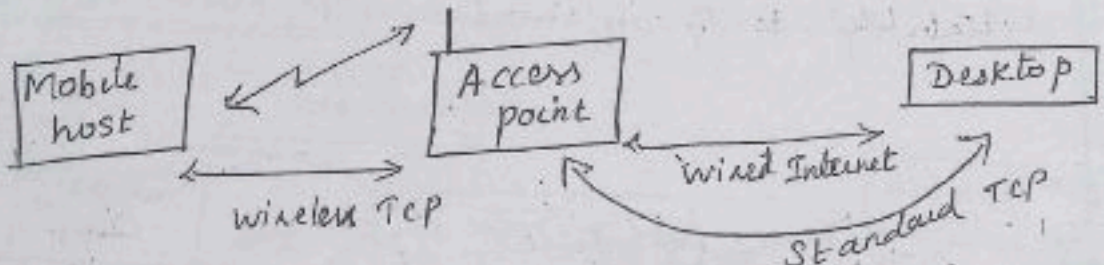
Classical TCP improvements:

Mobility links are prone to higher error rates as compared to fixed networks. So, in a mobile networks packet loss is a common phenomenon. This packet loss cannot be compensated by a simple retransmission. TCP may end up retransmitting the same packet over a bad link. Detecting these duplicates in layer two is not a comfortable option.

When TCP mechanism detects missing acknowledgements through time outs cannot decipher the reason of packet loss. The reason can be any one of the following three:

i) congestion in the medium
ii) Transmission link error
iii) problems of rerouting traffic.

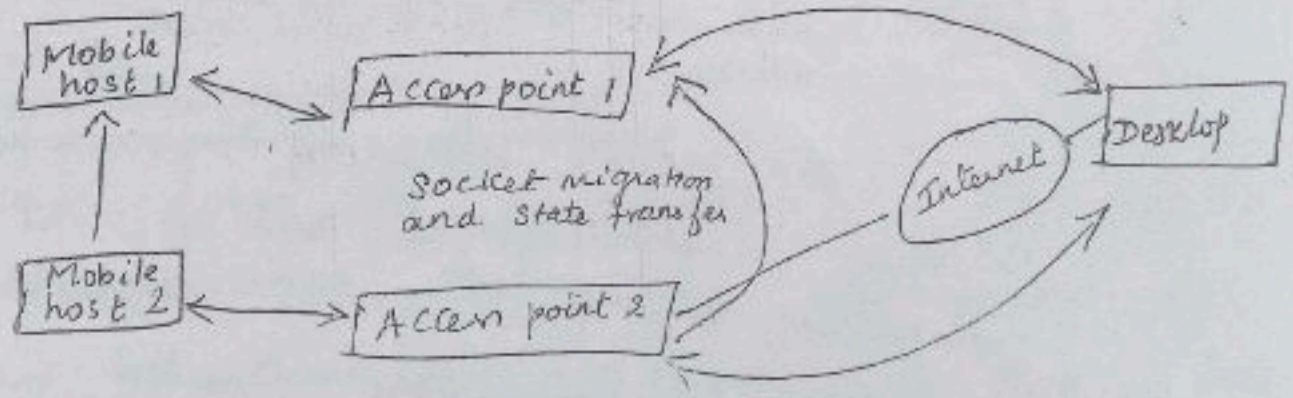
Indirect TCP:



One possible method of taking care of missing acknowledgements but at the same time maintaining TCP standards is defined in Indirect TCP. The above fig explains the possible method of using I-TCP. In this, there is a wireless host that is connected to a fixed n/w through a wireless link.

The wireless host is connected to an access point, standard TCP is used between mobile node and the access point wireless TCP is used. Any computer in the Internet recognizes the access point wireless TCP is used. Any computer in the Internet recognizes the access point as a standard TCP connection.

In this arrangement, FA acts as the proxy and delays data from mobile host to correspondent host and vice versa. The acknowledgement is sent to FA when a packet meant for mobile host is sent by the correspondent host. FA tries to maintain link b/w itself and mobile host. If there are errors in transmission to mobile host, FA tries to retransmit the lost packet so that link reliability is maintained.



Some of the advantages of I-TCP:

1. I-TCP does not require any change in TCP.
2. Transmission errors in wireless link can not propagate to fixed network.

iii) Different solutions can be tested and used without disturbing the stability of the Internet.

iv) optimized TCP can use precise time-outs to guarantee retransmissions as fast as possible

v) Different transport layer protocol is allowed b/w FA and mobile host.

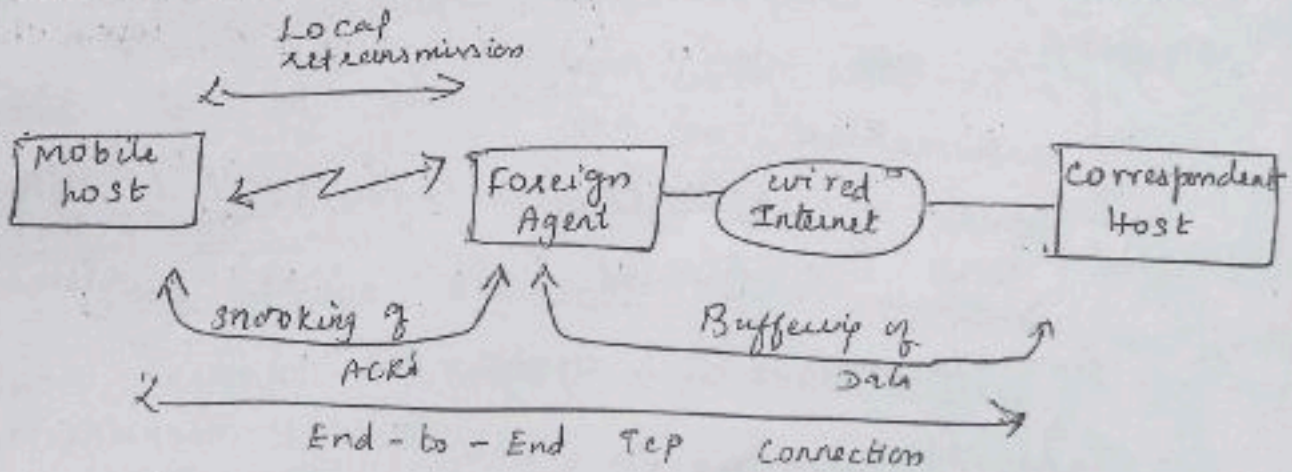
Introduction of segmentation in I-TCP throws up some disadvantages as follows:

i) If the FA connection to mobile host crashes, it may cause problems. The sender may receive an acknowledgment (from FA), whereas the receiver may have not received it.

ii) An increased handoff latency may give rise to some practical difficulties.

iii) FA must be a trusted entity

Snooping TCP:



One major problem with I-TCP is the segmentation of single TCP connection into two TCP connections. By doing such segmentation, end-to-end TCP semantic is lost.

The above fig. shows the arrangement where end-to-end semantic of TCP is not lost. The main fn. of the scheme is to locate a foreign agent close to the mobile host. FA performs fast local retransmissions where there is a packet loss. In this scheme, the FA buffers all the packets with destination mobile host. FA also "snoops" for flow of acknowledgement on both sides. The reason for buffering packet is for facilitating retransmissions to the mobile host in case of packet loss due to transmn errors.

In such case, mobile host retransmits.

Some of the advantages of snooping TCP are:

i) End to end TCP semantic is preserved.
ii) Most of the enhancements are in FA.
iii) No complicated handoff mechanism is required.
iv) It does not matter if the new FA uses this enhancement or not

Some of the disadvantages of this system are

i) Snooping TCP does not isolate problems of wireless link as good as I-TCP.
ii) Introduction to additional mechanism
   i) using negative acknowledgement
   ii) Snooping & buffering data may become meaningless if there is any end-to-end encryption scheme is in operation.

2) Wireless Application Protocol (WAP)

*) The wireless Application protocol was popularly known as WAP. It was founded in the year 1997.

*) The main objective of this WAP forum was,

i) To bring diverse internet contents like web pages, push services, etc.

ii) To provide better protocol suite to support world wide wireless communication.

iii) To support wireless networks like GSM, UMTS etc.

*) Many solutions were derived by "WAP forum". All solutions must meet the following requirements

i) Scaleable :

The protocols and other services should be able to be in scale with the customer need

ii) Interoperable :

It allows the terminals and softwares from several vendors to communicate with many networks of different providers.

iii) Efficient :

To provide proper quality of service suitable to the requirements of wireless and the mobile networks

iv) Reliable:

To provide predictable and consistent platforms for deployment of services.

v) Secure:

It should have provisions to secure data and to preserve data integrity and devices.

*) WAP forum published

Version 1.0	in the year	April 1998
Version 1.1	in the year	May 1999
Version 1.2	in the year	Nov 1999
Version 1.2.1	in the year	June 2000

WAP Architecture:

*) The figure shows the overview of WAP architecture, its protocols and components compared with the internet architecture

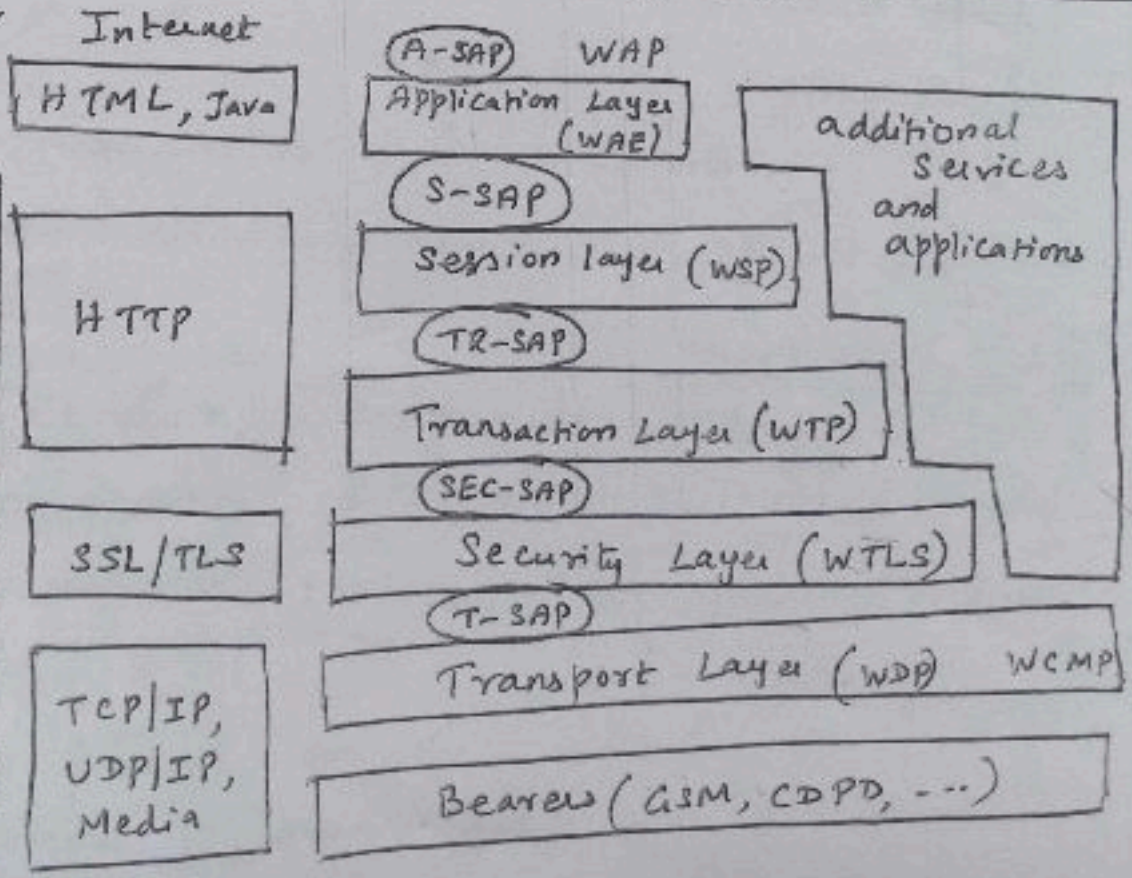


Figure: Components and interface of WAP 1.x architecture

WAP architecture has 5 layers (5)

1. Bearer Service (GSM, CDPD, ...)
2. Transport Layer (WDP)
3. Security Layer (WLTS)
4. Transaction Layer (WTP)
5. Session Layer (WSP)
6. Application Layer (WAE)

i) Bearer service:

*) The basis for transmission of data is formed by different bearer services.

*) WAP does not specify bearer service, but uses existing data services.

*) Examples are
   → message service [Short message service (SMS) of GSM]
   → circuit switched data [high speed circuit Switched data in GSM (HSCSD)]
   → packet switched data [general packet radio Service (GPRS) in GSM]

*) No special interface b/w bearer service and the transport layer

ii) Transport Layer with WDP:

*) Next layer is transport layer with wireless datagram protocol (WDP) and additional wireless control message protocol (WCMP).

*) This layer offers bearer independent, consistent datagram oriented service to higher layer of WAP architecture.

*) T-SAP (Transport Layer Servica accen point) is the interface b'w Transport layer & Security layer.

iii) Security Layer with WTLS:

*) Security Layer with wireless Transport Layer Security protocol WTLS offers services at Security SAP (SEC-SAP).

*) WLTS offers data integrity, privacy, authenti- and denial-of-servica protection.

*) Security SAP (SEC-SAP) acts as the interface b'w Security layer & Transaction Layer.

*) WTLS is based on transport Layer security (TLS, SSL, Secure Socket layer as in internet.

iv) Transaction Layer with WTP:

*) Transaction Layer with wireless transaction Protocol (WTP) offers light weight transaction service at transaction SAP (TR-SAP)

*) TR-SAP acts as an interface b'w transaction layer & session Layer.

v) Session Layer with WSP:

*) Session layer with wireless session protocol (WSP) offers 2 services i) connection oriented & ii) connectionless

*) S-SAP (Session-SAP) acts as an interface b'w Session Layer and Application Layer.

vi) Application Layer with WAE :

*) The application Layer with wireless application Environment (WAE) offers a framework for the integration of different WWW and mobile telephony applications.

*) It offers many protocols & services with special service access points.

*) This layer supports HTML & Java as in internet

Integration of WAP components :

i) Transport Layer & Bearer service of WAP is compared with the TCP or UDP over IP of Internet.

If WAP architecture offer IP service } WDP.
then UDP is used as

ii) Security Layer of WAP is compared to SSL, TLS layers of internet.

iii) The role of session layer & Transp layer is compared with HTTP in Internet. HTTP does not offer all the additional mechanisms.

iv) Application Layer offers similar features as HTML and java in Internet.

*) The figure shows the integration of WAP compo-ent

Left side → different fixed network
(Traditional internet, public switching telephone n/w)

*) we cannot change Protocols & services of these existing networks.

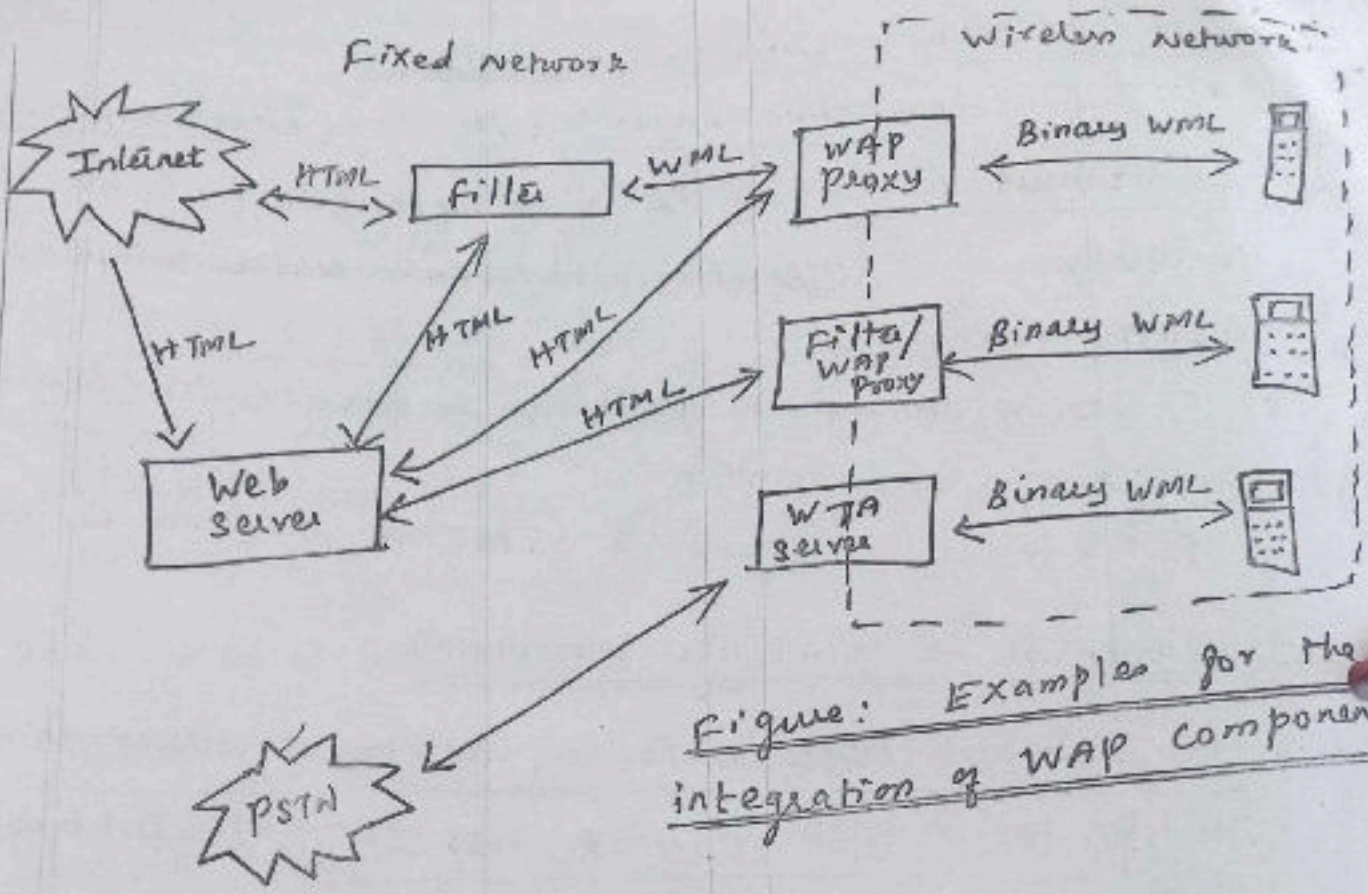


Figure: Examples for the integration of WAP components

3) Wireless Datagram Protocol (WDP)

*) Wireless Datagram protocol operates on top of bearer services.

*) T-SAP acts as an interface b/w transport layer (WDP) & security Layer (WTLS)

*) NO special interface b/w bearer service and the transport Layer WDP.

T-SAP WDP:

*) T-SAP WDP offers consistent datagram transport service independent of bearer service.

*) Transport Layer (WDP) & bearer service of WAP can be roughly compared to the services offered by TCP/IP (or) UDP/IP of internet.

*) If WAP architecture offers IP service, then the UDP is used as WDP.

WDP Service Parameters

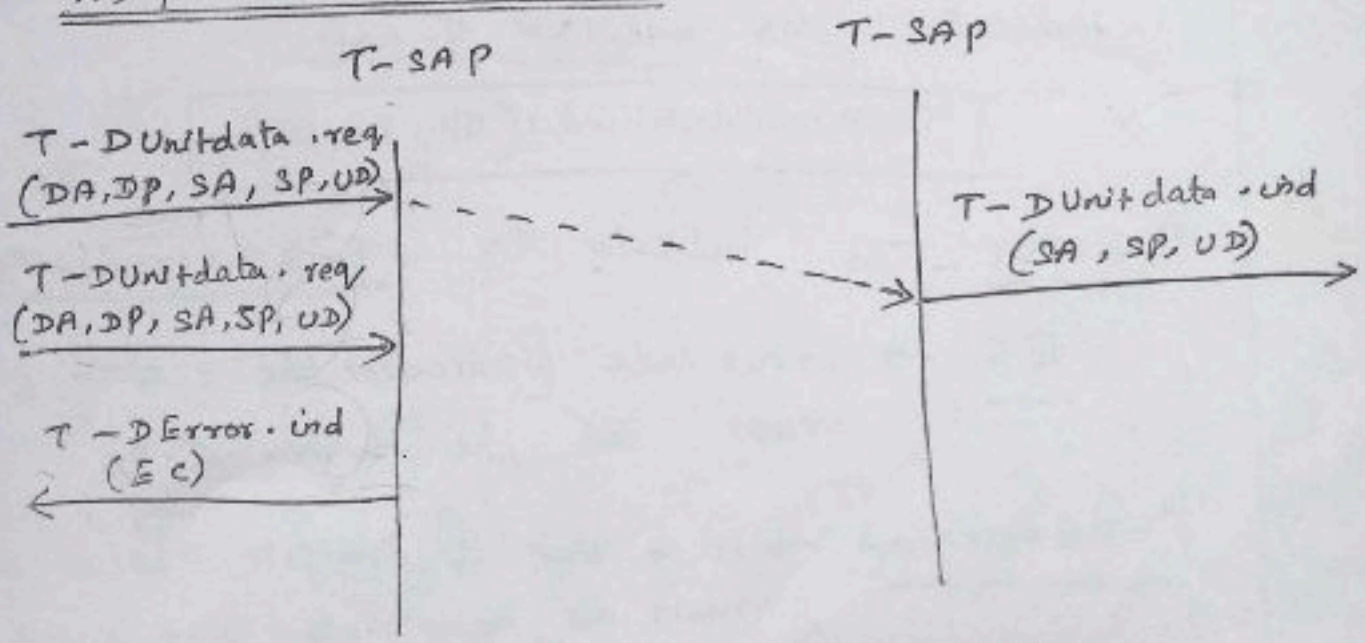


Figure: WAP Service Primitives

*) WDP offers source and destination port numbers used for multiplexing and demultiplexing of data.

*) WDP service primitives send a datagram - T-DUnitdata·req.

*) The parameters of T-DUnitdata·req are

→ Destination address (DA)
→ Destination port (DP)
→ Source address (SA)
→ Source Port (SP) &
→ User data (UD)

} Mandatory

T-Dunitdata·req (DA, DP, SA, SP, UD)

*) Destination & Source address are unique address for receiver & sender of user data. These could be either telephone no., Ip address or any other unique address.

*) T-Dunitdata·ind is a service primitive which indicates the reception of data

T-Dunitdata·ind (SA, SP, UD)

*) Error is indicated by T-DError·ind (EC)

EC → error code [indicates the reason for the error to the higher layer]

T-DError·ind → it is use to indicate local problems such as user data size is too large
→ it does not indicate problems with peered service.

Wireless control Message protocol (WCMP):

*) When error occurs when WDP datagrams are sent from one WDP entity to another (eg, destination is not reachable), WCMP provides error handling mechanism for WDP.

*) WCMP contains control messages that resembles Internet control message protocol (ICMP) message.

*) WCMP is used by WDP nodes to report errors.

*) In IP-based n/w, ICMP will be used as WCMP.

WCMP messages are

→ destination unreached (route, port, address unreachable)
→ Parameter problem (errors in the packet header)
→ Message too big
→ Reassembly failure
→ echo request/reply.

4) Wireless Transport Layer Security (WTLS)

*) WTLS is integrated on the top of WDP.

*) WTLS provides different levels of security (Privacy, data integrity & authentication) for low bandwidth and high-delay bearer n/w.

*) WTLS supports datagram and connection-oriented transport layer protocols

WTLS establishing a secure session:

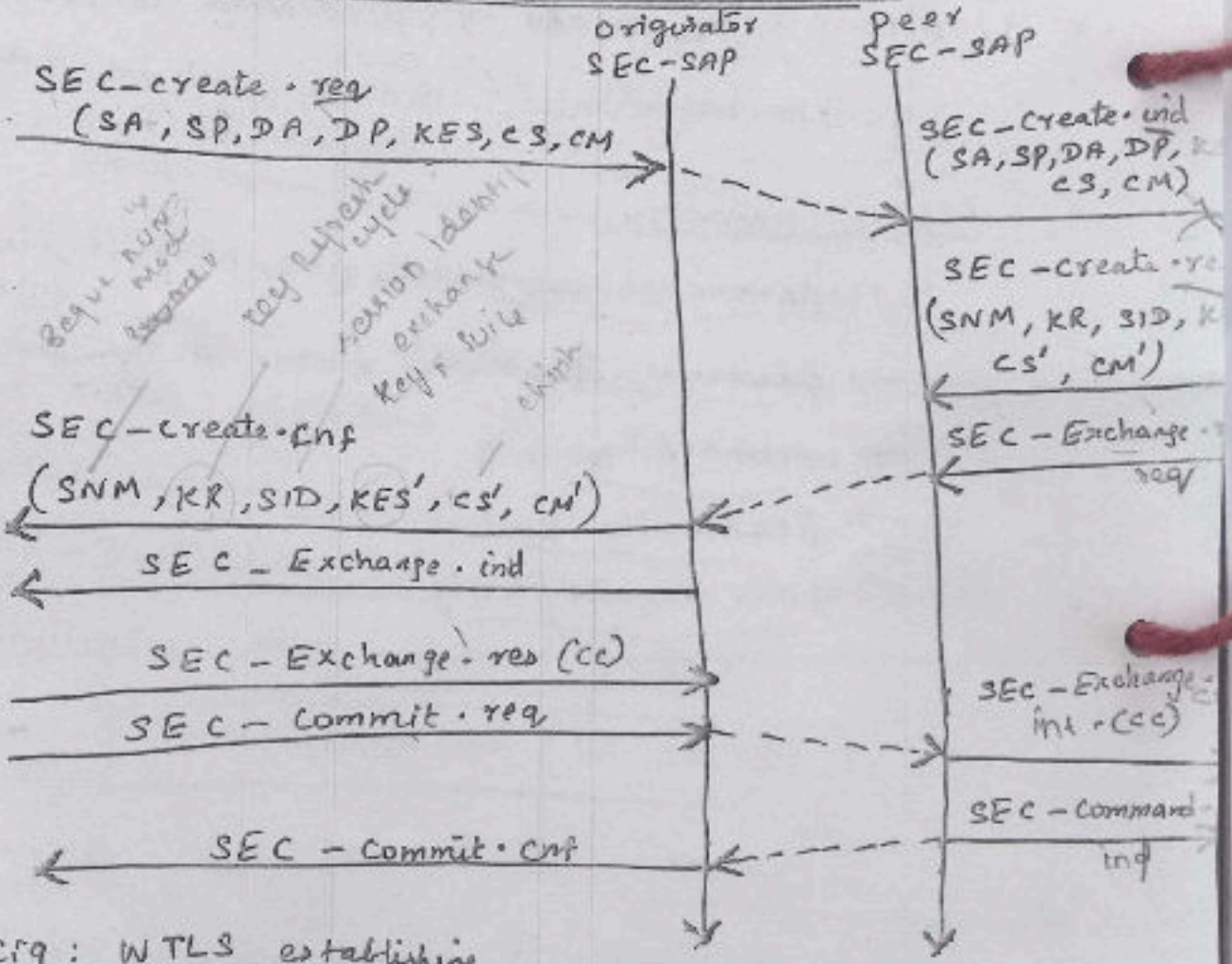


Fig: WTLS establishing a secure session

*) Session establishment consists of several st

*) The figure shows the sequence of service primitives needed for "full handshake".

* req → request
* ind → indicati
* res → respons
* cnf → Confirma

Full handshake process for secure session setup: (9)

SEC_create.req & SEC_create.ind:

SEC_create.req (SA, SP, DA, DP, KES, CS, CM)

SEC_create.req → secure session creation request

SA → Source address
DA → Destination address
KES → Key exchange suite
CM → Compression Method
SP → Source port
DP → Destination port
CS → cipher suite

SEC_create.ind → secure session creation is indicated

SEC_create.res:

.res → response
SNM → sequence no. mode
KR → Key Refresh cycle
SID → Session identifier
KES' → Key exchange suite
CS' → cipher suite
CM' → Compression method

*) SEC_Exchange primitive:

peer issues a SEC_Exchange.req

SEC_Exchange.req → peer wishes to perform public key authentication with the client

originator responses with SEC_Exchange.res (CC)

CC → client certificate.

originator also responses SEC_commit.req.

*) certificate is delivered to the peer side & SEC_com is indicated

*) peer sends back the confirmation to the originator SEC_commit.cnf

This is "full handshake" process for secure session setup.

*) WLTS datagram transfer: (SEC-Unitdata)

After setting up a secure connection b/w two peers, user data can be exchanged. This is done using SEC-Unitdata.

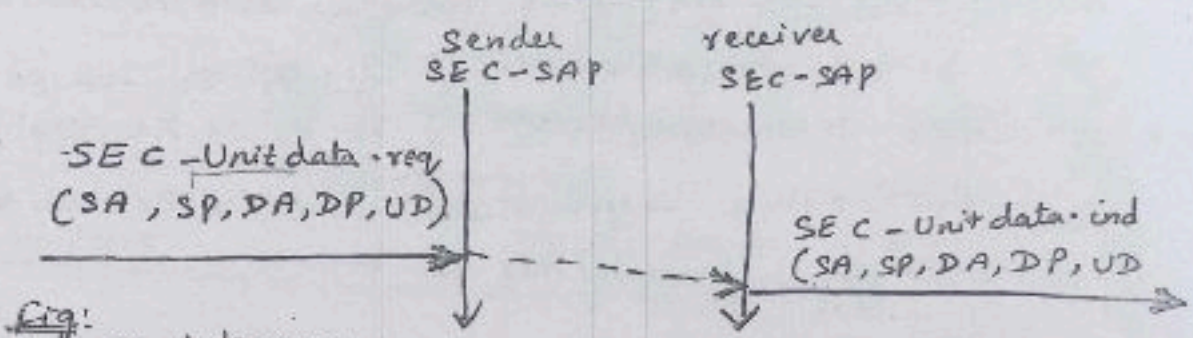


Fig: WLTS datagram Transfer

SEC-Unit data parameters

→ SA → Source Address
SP → Source port
DA → Destination Address
DP → Destination port
UD → User data

*) SEC-Unit data of WTLS is similar to T-Dunit data of WDP.

*) Higher layers use SEC-Unit data instead of T-Dunit data.

*) In WTLS, due to the computational power of handheld devices, the encryption provided is not very strong.

*) If application requires stronger security, it is up to an application or user to apply stronger encryption

5) Wireless Transaction protocol (WTP):

*) WTP is on the top of either Transport layer WDP or security layer (WTLS).

*) WTP is designed to run on very thin clients, such as mobile phones.

*) WTP provides services such as
- → improved reliability over datagram services
- → improved efficiency over connection oriented service
- → support for transaction-oriented services such as web browsing

*) Three classes of WTP, they are

i) WTP class 0 → provides unreliable message transfer without any result message.

ii) WTP class 1 → provides reliable message transfer without result message.

iii) WTP class 2 → provides reliable request/response message transfer.

*) In WTP, reliability is achieved by
- → duplicate removal
- → retransmission
- → Acknowledgement
- → unique transaction identifiers.

*) WTP allows:
- → Asynchronous transaction
- → Abort of Transaction
- → concatenation of message
- → Report success or failure of reliable msg

*) Services offered by WTP:

i) TR-Result → to send back the result of previous initiated tran

ii) TR-Invoke → to initiate new transaction

iii) TR-Abort → to abort existing transaction

*) Two acknowledgement in WTP:

i) User Acknowledgement
ii) Automatic Acknowledgement.

a) WTP class 0:

*) Class 0 offers unreliable transaction service without result message (ack)

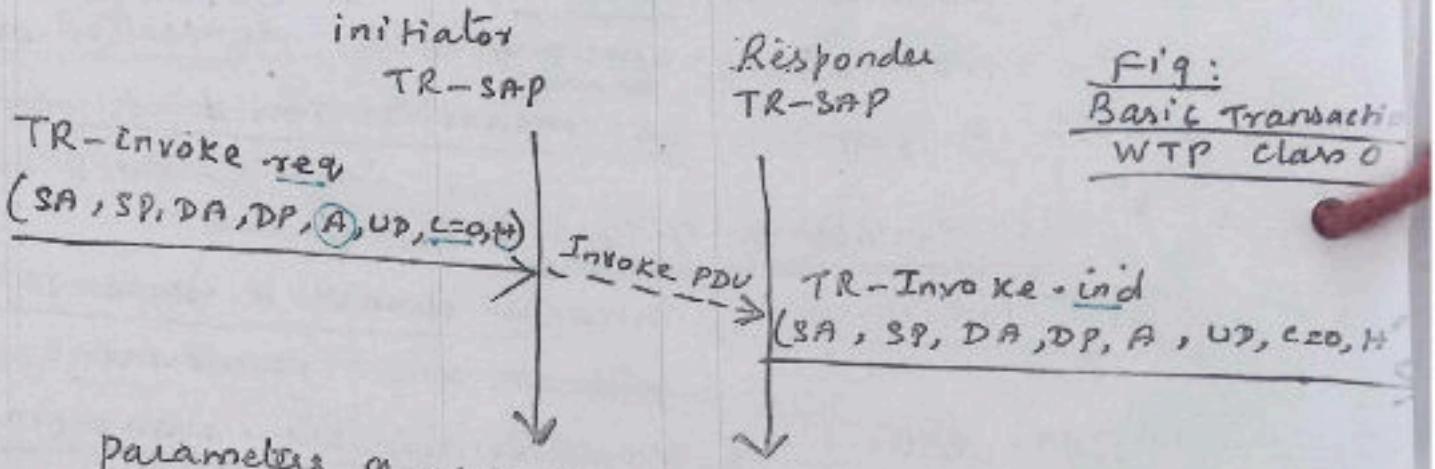


Fig: Basic Transaction WTP class 0

Parameters of WTP class 0:

→ Source address (SA), Source port (SP), Destination (D addr.
Destination port (DP)
→ A → Acknowledgement
→ C=0 → class 0
→ H → Handle [provides simple index to uniquely identify the transaction
H' → Handle at responder's side

*) The initiator sends invoke PDU, the responder receives it. The responder then generates TR-Invoke.ind. The responder does not acknowledge the message and the initiator does not perform any retransmission.

b.) WTP class 1 (without user Acknowledgement)

class 1 offers reliable transaction & without result message (ack)

Class 1 ⇒ no user acknowledgement

*) Initiator send ⟶ TR-Invoke.req
Responder signals ⟶ TR-Invoke.ind & acknowledges automatically without user intervention.

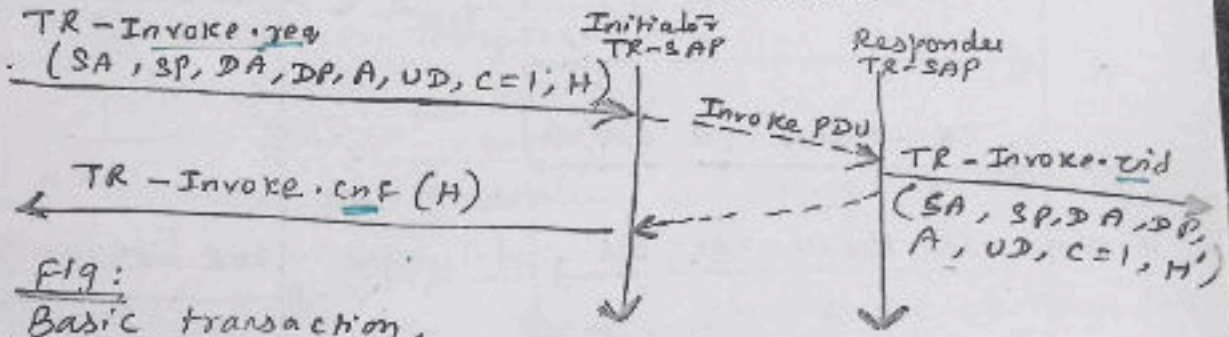
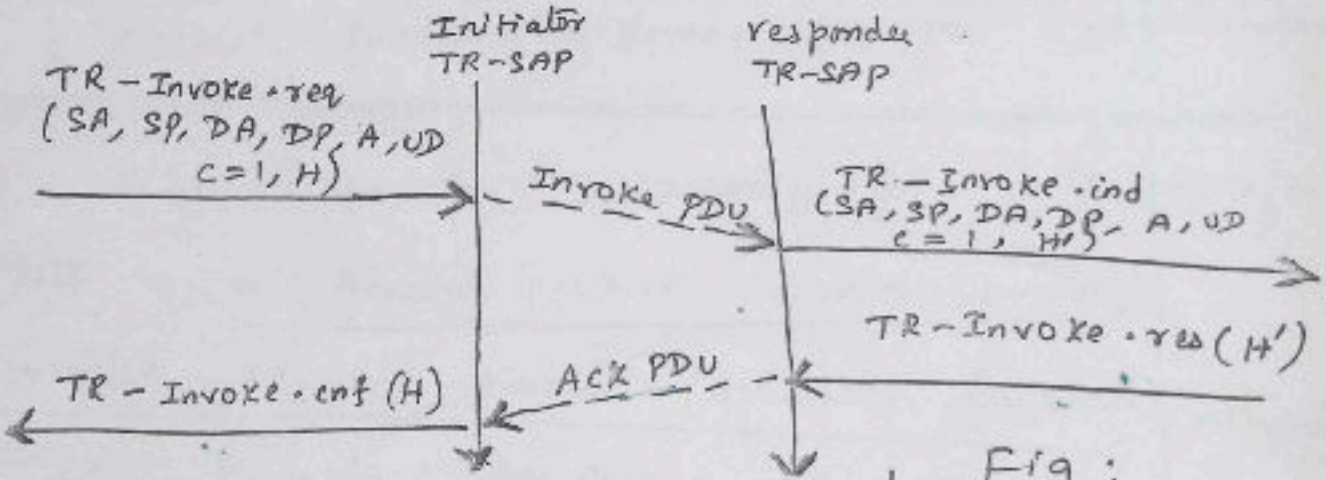


Fig: Basic transaction, WTP class 1, no user acknowledgement

ii) WTP class 1 (with user acknowledgement)



*) In this fig, the responder does not send the ack. automatically but waits for TR-Invoke.res service primitives from the user.

Fig: Basic transaction WTP class 1, with user acknowledge

c) WTP class 2 [No user Acknowledgement]

Class 2 provides classic reliable request/response transaction from many client/server.

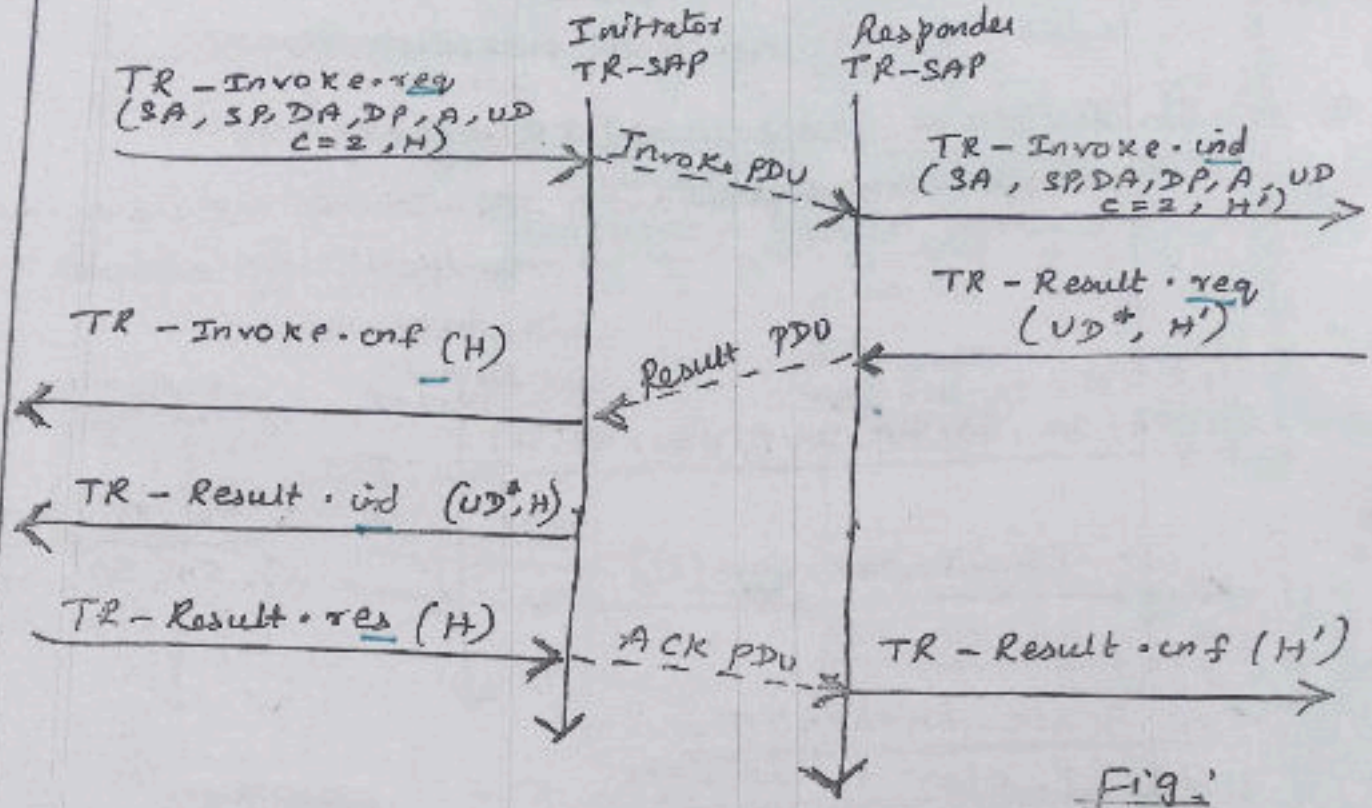


Fig:
Basic Transaction
WTP Class 2
no user Acknowledge

6) Wireless Session protocol (WSP)

*) WSP is designed to operate on the top of transaction service WTP (or) Transport layer WTP

*) For both types, security is inserted using WTLS security layer.

*) Features provided by WSP:

i) Session Management:

*) Sessions can be
- → Session Establishment (from client to server)
- → Session Released
- → Session Suspending
- → Session resuming

*) Assume a mobile device is being switched off - it would be useful for the user to be able to continue operation at exactly the point where the device was switched off.

ii) Capacity negotiation:

*) Clients and servers agree upon a common level of protocol functionality during session Establishment

iii) Content encoding:

WSP uses binary encoding for data transfer

*) WSP is a general purpose session protocol

*) Wireless session protocol / browsing (WSP/B) which comprises protocols & services suited for browsing type application.

Features of WSP/B:

i) HTTP/1.1 functionality
ii) Exchange of session headers
iii) Push & pull data transfer
iv) Asynchronous requests.

WSP/B over WTP:

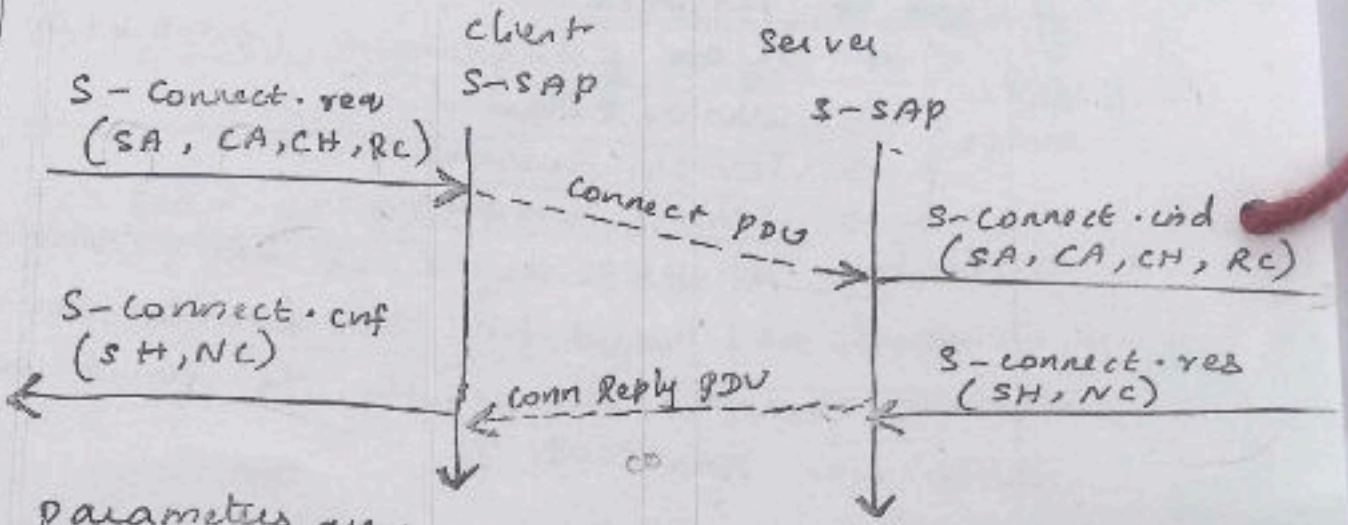
*) WSP/B uses the 3 service classes of WTP

Class 0 → for session resume, session management

Class 1 → for confirmed push

Class 2 → for method invocation, session resume & session management

WSP/B Session Establishment:



parameters are:

→ Server address (SA), client address (CA)
Client Header (CH), Requested capabilities (RC)
Server Header (SH), Negotiated Capabilities (NC) (needed for capacity negotiation)

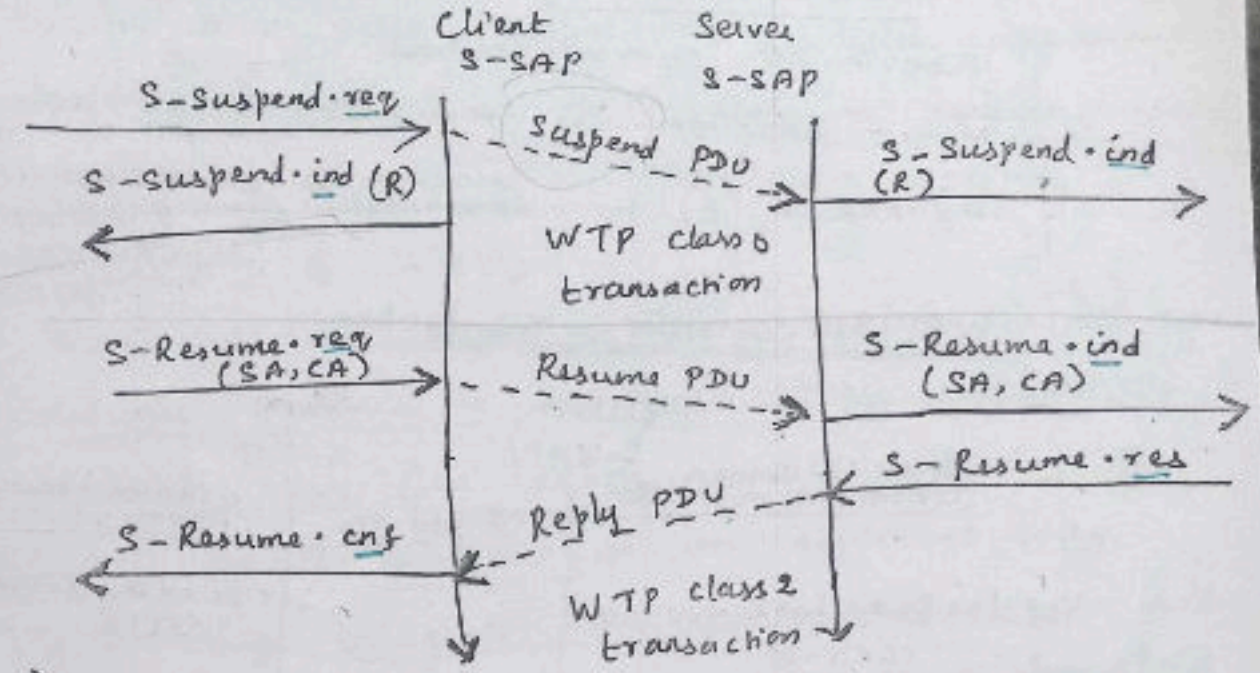
*) WTP transfer Connect PDU to Server S-SAP where S-Connect.ind indicates a new session.

If the server accepts the new session, it answers with S-connect.res

*) Server S-SAP transfer Connreply PDU back to the client.

*) S-connect.cnf confirms the session establishment

WSP/B session suspension and resume :



i) WSP/B session suspension & resume is shown in the figure

ii) Client suspends session with S-Suspend·req

iii) Client S-SAP transfers Suspend PDU to server with class 0 transaction (unconfirmed, unreliable)

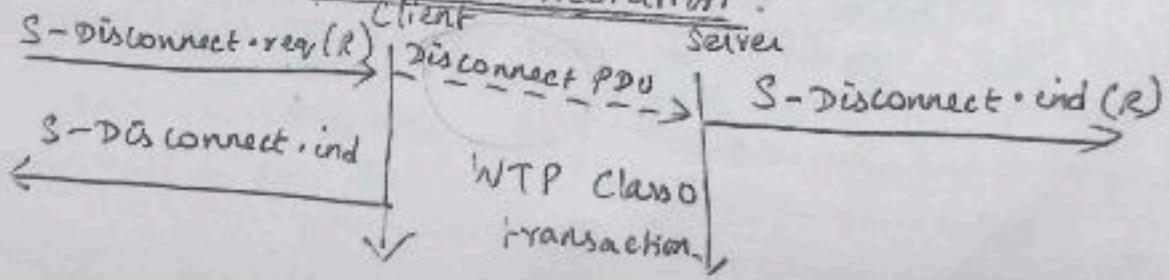
iv) WSP/B suspend the signal with S-Suspend·ind on the client and server side.

R → Reason for suspension.

v) Later the client resume the suspended session with S-Resume·req

vi) Resuming session is a confirmed operation using S-Resume·cnf

WSP/B Session Termination :

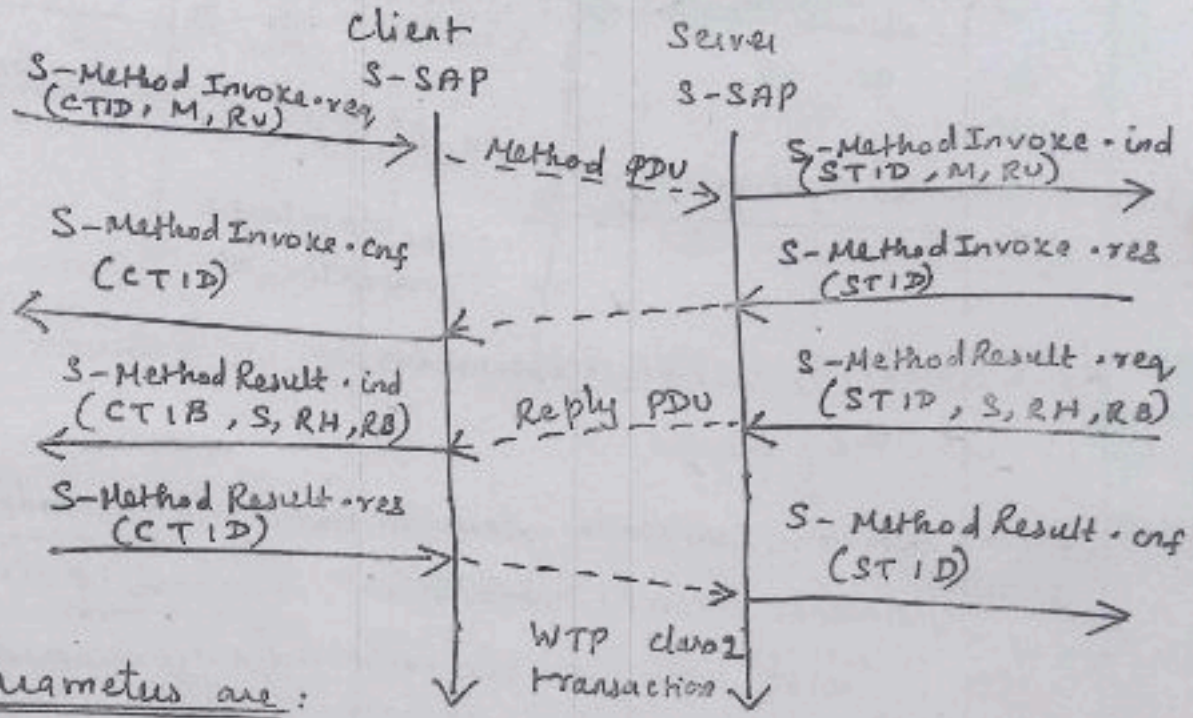


i) Terminating a session is done by using S-Disconnect.req - This service primitive aborts all current method.

ii) Disconnection is indicated by S-Disconnect.ind

iii) Reason (R) for disconnection ← network error, protocol error, peer request, congestion

WSP/B completed Transaction:



Parametes are:

CTID → Client Transaction identifier
STID → Server Transaction identifier
RU → request URI
M → Method, S → Status
RH → response header, RB → response Body

i) Client requests an operation with S-Method Invoke.Re
ii) WTP class 2 transaction transport method PDU to Serv
iii) On server side S-Method Invoke.ind indicates request
iv) The request is sent back to client using S-Method Re

.req → request | .ind → indication
.res → response | .cnf → Confirmation

7) Wireless Application Environment (WAE):

*) The main idea behind the wireless application environment (WAE) is to create a general purpose application environment based on existing technologies of WWW.

*) WAE allows service providers, software manufacturers, hardware vendors to integrate their applications so that they can reach a wide variety of different wireless platform in an efficient way.

*) WAE has integrated different technologies and adapted them to use in low power handheld devices.

*) HTML
Java script
HDML (hand held device markup language)
} form the basis of wireless mark up language (WML) & scripting language (WML script).

*) Exchange format for business card
Phone book vcard
Calendars vcalendar
} are included in WAE.

*) Web are accessed using URL location.

*) Wide range of mobile tele communication technologies have been adopted & integrated into wireless telephony application (WTA).

*) WAE focus on devices with
→ Limited capabilities
→ narrow band environment
→ special security & access control features

WAE logical Model

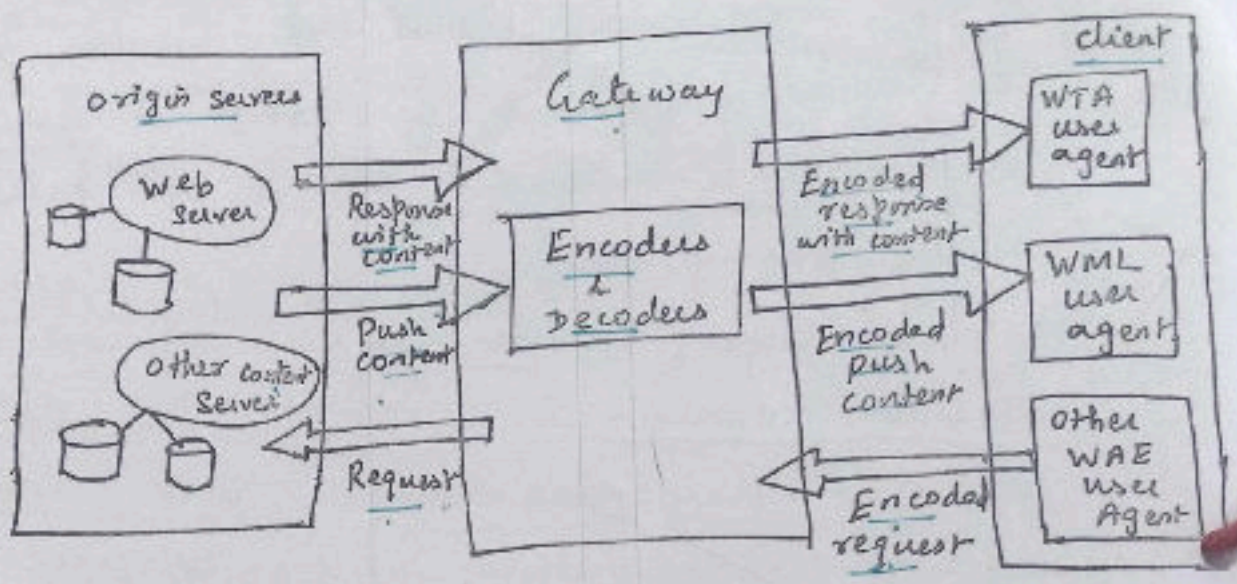


Fig: WAE logic model

*) WAE adopts a model that closely follows the WWW model, but assumes additional gateway that can enhance transmission efficiency.

Steps:

i) A client issues an encoded request to a remote server. ii) Encoding is needed to minimize data sent over the air and 2) to save resources on the hand held devices.

ii) Decodees in a gateway translate this encoded request into a standard request as understood by origin server.

iii) Origin Server respond to this request. The gateway now encodes the response (with content) and transfers the encoded response (with content) to the client.

WTA Telephone Agent

iv) Origin server pushes the content to the gateway. The gateway encodes the pushed content and transmits the encoded push content to the client.

*) Several user agents (UA) resides within a client.
User agents includes items such as
- browsers
- phone book
- message editors

*) WAE does not specify no. of UA or their functionality

*) Client has
- WTA user agent
- WML user Agent
- other WAE user agent

WAE Development:

*) WAE specification development includes
- → integration of existing or emerging technologies
- → Integration of intelligent telephone networks
- → Integration of Server side aspects
- → development of application suite for wireless client.

Goal of WAE:

i) The main goal of WAE is to minimize over-the-air traffic & (save) resource consumption on hand held devices.

ii) Another goal is that logical model of WAE shows more details than the general overview

8) Wireless Telephony Application (WTA)

*) Wireless Telephony Application (WTA) is a collection of telephony specific extensions for
→ call & feature control mechanisms
→ merging data networks & voice networks

*) If a user wants to make phone calls and access all the features of mobile phone as like traditional mobile phone, this is possible using
→ Wireless Telephony Application (WTA)
→ WTA user agent.
→ Wireless Telephony Application Interface (WTAI)

*) WTA extends basic WAE application model.

Features of WTA:

i) Content push:

*) WTA origin server can push content. Push can take place without prior client request.

ii) Access to Telephony functions:

*) Wireless telephony application interface (WTAI) provides many functions to handle telephony events like (call accept, call set up, change of phone entries, etc).

iii) Repository for event handlers:

*) Repository represents a persistent storage on the clients to offer WTA services.

*) Examples for resources are WML decks, WML Script objects

Resources are loaded using WSP or pre-installed

*) The main motivation of repository is to react very quickly for events like call accept, otherwise it would take too long to load the content from the server.

iv) Security Model:

*) Security model is very important for WTA because many frauds happens with wrong phone no.

*) WTA allows clients to connect only to trustworthy gateways.

Libraries in WTA:

*) Three classes of libraries in WTA are

a) Common network service:

i) Call control library → contains fns for call setup accept & release.

ii) Network text library → contains fns to send, rea & delete text messages

iii) phonebook Library → Contains fns for the manipulation of phone entries (read, writ delete

iv) Miscellaneous Library → contains fns to indicate incoming data, email, fax.

b) Network specific services:

→ contains operator specific libraries

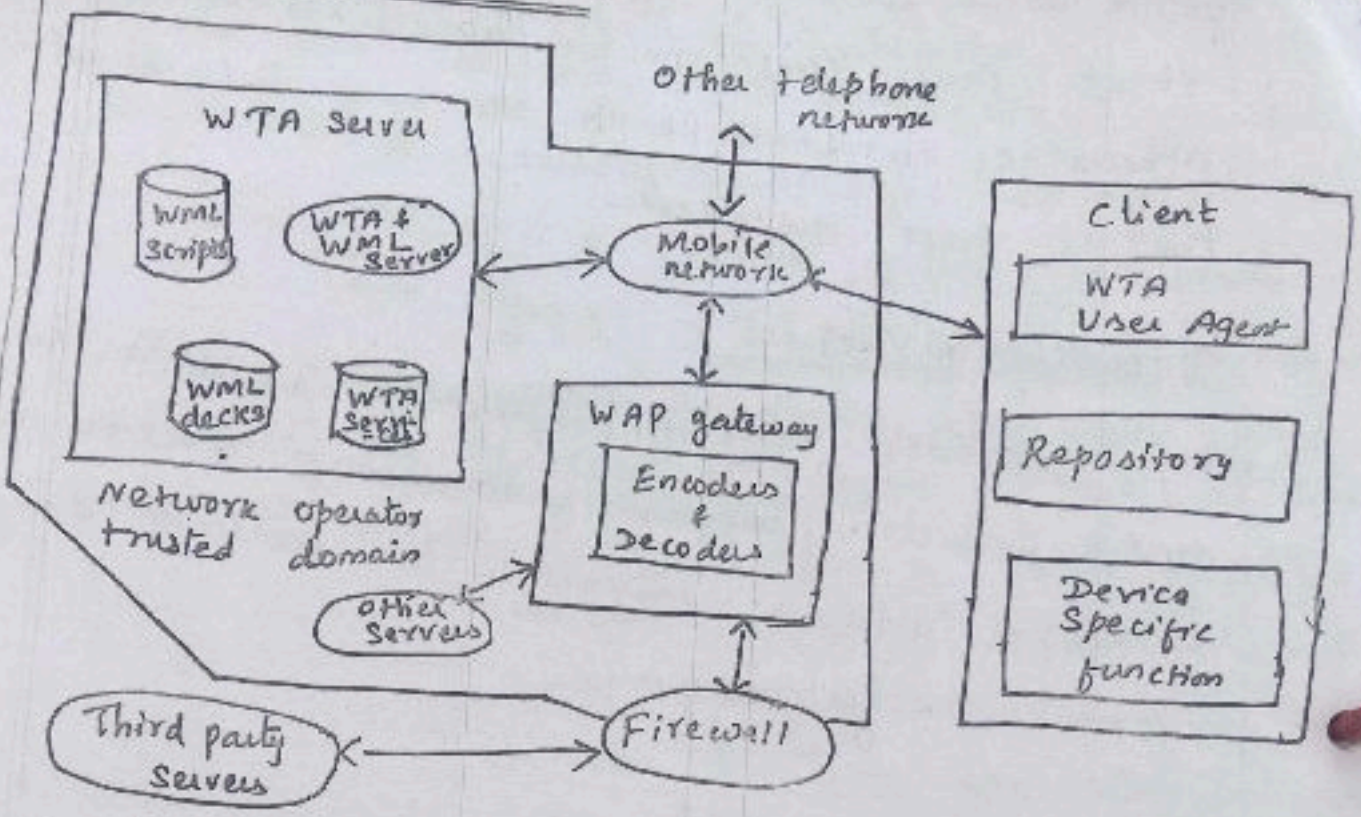
c) Public services:

→ contains publicly available functions

eg. "make call".

WTA public . makecall ("57832158");

WTA architecture:



*) The client is connected via a mobile network with a WTA server, WAP gateway and other telephone network.

*) WTA user agent is running on client.

*) Client may have voice and data connections over the mobile network.

*) WTA user agent has a very rigid and real-time Context management for browsing the web Compared to standard WML user agent.

*) Firewall is useful to connect third party servers outside the trusted domain

9) Wireless Markup Language (WML):

*) Wireless Markup Language (WML) is based on the standard HTML.

*) WML is a document manipulation language. It is tag-based

*) WML is specified as an XML document type

*) When designing WML, several constraints of wireless handheld devices have been taken into account

i) wireless link always have very limited capacity compared to wire.

ii) Hand held devices have small displays, limited user input facilities, limited memory, and low performance computational resource

iii) Processing power is getting lower.

iv) Performance of handheld devices is close to desktop devices.

WML Metaphor:

*) WML is capable of implementing two types of metaphor a) Desk b) card

Two types: Desk, card

→ A WML document is made up of multiple cards.

→ Cards can be grouped together into a desk.

→ WML desk is similar to HTML page, it is identified by URL

→ WML browser fetches desks as required from origin servers

→ In desk, the cards are linked with each other.

→ User communites with WML browser through a series of WML cards

WML Features:

*) WML has following features
i) Support for user inputs
ii) Support for text and messages
iii) Task invocation controls.
iv) MMI independence
v) context and state management
vi) Narrow band optimization
vii) User interaction

User interaction

→ WML supports different elements for user i/p
→ Eg. text entry, password entry, option selection, controls for task invocation.
→ input either by — soft keys (or) touch
— Physical Keys (or) button
— voice input

Navigation:

With HTML browsers, WML offers
— browsing history
— hyperlinks
— other international navigation element

Card Elements:

*) A card elements contains
→ Text
→ Input-fields
→ Images
→ Links, etc

Example [Module of WML]:

```
<WML>
    <card id = "no1" title = "card1"
      ---------- Hello ! ------
    </card>
    <card id = "no2" .....
    ---------- Welcome to the WML ! ----
    </card>
</WML>
```

*) WML document is nothing but XML document.

*) For the about WML module, the result is

Result:

---Card1 ... Hello!		... Card2 .... Welcome to WML!

+) In WML, it is easier to write and display information with many cards in a deck.

UNIT V

Mobile Computing

V. SELSHIYA

V. Selshiya

(1) Mobile Device operating Systems:

*) The mobile operating system (OS) performs two main responsibilities as:

i) Managing Resources
ii) Providing different interfaces

i) Managing Resources:

*) The main responsible of mobile OS is to provide effective utilization of memory, CPU, files and other attached devices namely display, camera, speaker, mike & KB.

*) Some applications of smartphone include recording, listening music, watching video, browsing web, text messaging, email, etc.

*) Smart phones allows the above said multiple applications to be running simultaneously. Each application may require multiple tasks to be done which in turn might have multiple threads.

*) It is explained with an example, a mobile user might watching a video, at the same time he might answering an incoming call, and also get a message that he wants to see while the call is still going on.

*) This scenario requires simultaneous execution of multiple tasks and all these tasks might use the same set of resources, where the OS plays a vital role so that the different tasks do not interfere with each other.

ii) Providing different interfaces:

*) The mobile OS provides interactive interfaces to the device user and also interfaces with several devices and the n/w.

*) The OS takes care of
   i) i/p from KBy board.
   ii) sending o/p to display screen
   iii) recognizing interface with other devices like mobiles, computers, printers, etc.

*) The interfaces of mobile phones vary from device to device ie, one device may have touch screen and the other might have physical keyboard. Thus OS is easily configurable.

*) some popular Mobile OS are
   → Symbian OS
   → Android OS
   → Windows Mobile
   → Palm OS
   → iOS
   → Blackerry OS.

2) Special Constraints and Requirements of Mobile OS:

(A) Special constraints:

*) The operating system of mobile device needs to differ significantly from a general purpose OS because of the following constraints:

i) To make the device to enter into low power sleep mode as soon as possible.

ii) The complex computations need to be avoided.

iii) The mobile OS need to be booted much faster as soon as it is switched on when compared to the desktop, because the number of times the desktop is switched on per day is much lower than the mobile device.

iv) Size of the mobile OS kernel needs to be very small.

Some other constraints:

i) Limited Memory:

→ when compared to desktop/laptop, a mobile device uses much less permanent and volatile storage.

→ To manage this limited memory, mobile OS must be as small as possible.

ii) Limited screen size:

*) To make the mobile device portable, the size of the mobile should be small.

*) New innovative user interfaces needs to be supported by mobile OS.

iii) Miniature keyboard:

*) Normally, the mobile devices are provided with
→ a small sized display screen as keyboard in touch mobiles
(or)
→ a small keypad.
(or)
→ by using a style.

iv) Limited battery power:

*) Mobile devices need to be lightweight as possible and the mobile device should have a small battery, to manage size & weight.

*) In order to reduce the power consumption, the procesor and the display screen has to be put in the sleep mode within a few minutes of inactivity.

v) Limited and fluctuating bandwidth of the wireless medium:

*) The wireless medium is vulnerable to atmospheric noise, which results in high bit error rate.

*) Mobile OS needs to run complex protocols

*) There is possibility of ⇒ short term fades due to atmospheric noise, movement of some objects, movement of mobile devices.

⇒ Long term fade due to hand off.

*) Uninterrupted communication is obtained by techniques namely

→ data caching
→ Pre-fetching
→ Integration.

b) Special Requirements

*) Mobile OS needs some special requirements which is not present in the traditional OS.

i) Support for specific communication protocol:

*) The mobile device needs to be communicated with the base station and also other mobile devices and computers. It requires an enhanced communication support with various generations such as 1G, 2G, 3G, etc in which the mobile device is deployed.

*) For web browsing and communication with other personal devices such as pendrive & head set, the mobile devices are equipped with USB and other types of ports.

*) Bluetooth connections are preferable for Mobile OS.

*) Mobile OS requires multiple interfacing protocols and hardware interface.

*) Mobile device needs to support TCP/IP & wireless LAN.

ii) Support for a variety of input mechanisms:

*) Mobile OS needs to support a variety of input mechanism. The variety of input mechanism are → miniature Keyboard for inexpensive device
→ Qwerty KB for sophisticated devices
→ Recent mobile devices with touch screen
→ Stylus based i/p mechanisms.

iii) Compliance with open standards:

*) Mobile OS should follow open standards to
→ to facilitate the thirty party s/w development
→ to reduce the cost of development.

*) The user interface and networking capabilities of mobile OS need to be designed by keep in mind the different shape & size of smart phones

iv) Extensive library support:

*) Extensive library support is required by the mobile OS for cost effective development of third party applications.

*) Extensive library support includes
→ email
→ SMS
→ MMS
→ multimedia, bluetooth, GSM & GPRS functionalities.

v) Support for Integrated Development Environment (IDE):

*) Mobile OS need to have their own IDE for effective s/w development & good performance of developed s/w.

*) Eclipse can be used to develop applications.

*) All smartphone vendors now actively promote software development on their platform for increased availability of third party applications.

3) Commerical Mobile operating systems:

*) Some popular Mobile os are:-

i) palm os
ii) Symbian os
iii) iOS
iv) Android os
v) Blackberry os &
vi) Windows Mobile.

i) Palm os:

*) It is a proprietary os that was developed by palm computing in 1998.

*) To have ease of use with the provision of touch screen based GUI, the palm os was designed.

*) palm os was upgraded to use in

→ Smart phones
→ Wrist watches
→ hand held gaming consoles
→ bar code readers.
→ GPS devices

→ Nowadays palm os was not popular, but it was popular a decade ago.

Features of palm OS:

→ Simple single tasking OS.
→ It has elementary memory management system
→ It supports handwritting recognition system for user input.
→ It supports sound playback and recording capabilities.
→ It uses a proprietary format to store Calendar, address, task and note entries.
→ The different interfaces supported include USB, infrared, Bluetooth & Wi-Fi connections.
→ It uses simple security schemes, in which the device can be locked by password.
→ It supports Hotsync technology for data synchronization with desktop computers.
→ Palm OS supports palm emulator, which emulates the palm hardware on a PC.

ii) Symbian OS:

*) Symbian OS was developed through collaboration with manufacturers like NOKia, Ericsson, panasonic & Samsung.

*) When grogle announced Android as an open OS in 2008, the market of Symbian OS started to come down.

*) To counter this, Symbian source code was published under Eclipse Public License (EPL) in 2010 & Nokia announced in 2011 that it will move away from Symbian OS & use Windows phone 7 OS in its smartphones.

*) Symbian OS is a
→ real time, preemptive
→ 32 bit OS, runs on ARM processor
→ micro kernal based.

*) When the application is not running, the CPU is switched into low power mode.

Major Flavours of Symbian OS:

The major flavours of Symbian OS are
i) Series 60.
ii) UIQ Interface.

i) Series 60:

→ It is the leading smartphone platform in the world.
→ It is easy to use interface & supports features such as → rich content downloading
→ MMS.
→ It is mainly used in → Nokia smart phones
→ Samsung headsets.

ii) UIQ interface:

→ It is earlier known as User Interface Quartz it was developy by UIQ technology.
→ It provides capabilities for third party application developers to develop applications.

Features Symbian OS.

i) It supports preemptive multitasking scheduling & memory protection.

ii) Communication & n/w ing protocol: It supports number of communication & networking protocols like TCP, UDP, WAP, etc.

iii) optimization: It is optimized for low power & memory requirements.

iv) programming: It supports event-based programming

v) Security: Full length encryption and certification management is supported by Symbian OS.

vi) Messaging: Support SMS, MMS, EMS, POP3.

vii) carbide is an Integrated Development Environment toolkit that is available for c++ application development on Symbian OS.

4) Software Development kit : [commercial.]

Most popular Mobile OS are

i) iOS
ii) Android
iii) Blackberry
iv) Windows Mobile

4-1) iOS: [iphone operating System]

*) Apple developed iOS as iphone's operating Syste during Jan 2007, which is originally named a iphone OS and later renamed as iOS.

*) iOS are fully owned and controlled by Apple and hence it is closed and proprietary O:

*) Apple does not include lincense iOS for installation on third-party hardware.

*) iOS include internal accelerometers used for
→ shaking the device as undo command
→ rotating the device in 3 dimension
→ switching the screen from portrait to landscape, etc

*) iOS was the sleek mobile device. iphone made a revolution in the smart phone market.

Components of iphone iOS :-

*) iphone operating system consists of four layers, as shown below

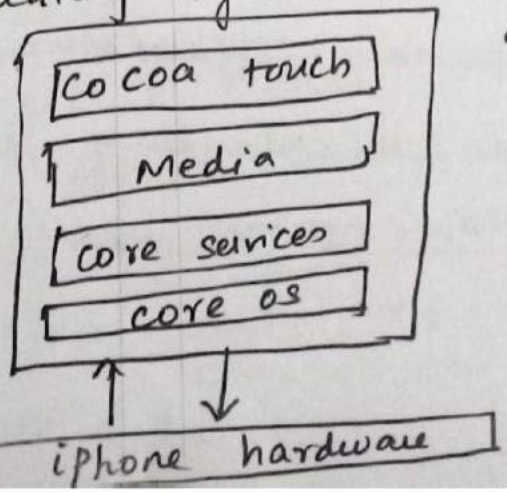


Figure : iphone os

*) Core OS:

→ It is the bottom most layer (4th layer) of the stack
→ It form the foundation of operating system
→ It takes contiol of
  → memory management
  → Networking
  → file system &
  → other operating system Task.
→ It can directly interact with H/w.

Core Service layer:

→ It forms the 3rd layer of the stack. It forms the foundation layer for the other layers.
→ It provides basic accen to iOS services. It has components namely
  i) Addren book
  ii) Collections
  iii) Networking
  iv) File acces
  v) SQLite
  vi) Core Location
  vii) Networr services
  viii) Threading
  ix) URL Utilities & Preference

Media Layer:

→ It forms the 2nd layer of the stack.
→ The media layer of iOS provides multimedia services which can be used in ipad and iphone appln.
→ This layer provides iphone os with video, audio graphic & animation capabilities
→ with this layer, many iphone applications can be developed.

*) The iphone OS is similar to the MAC OS x desig. but there is some difference in the architectural design where cocoa layer of stack are not the same as MAC OS x design.

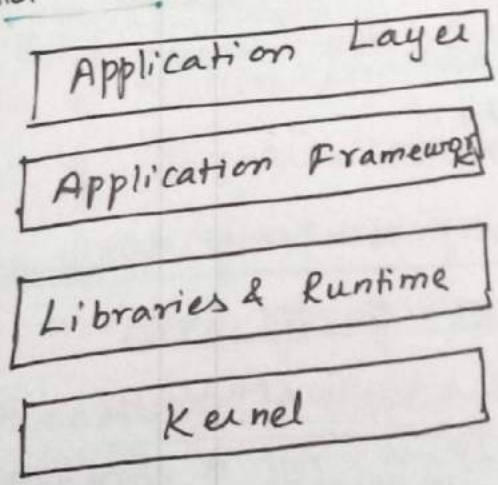
4.2) Android OS:

Features of Android:

1. Android provides the ability to use either a Phone based keyboard or a touchscreen.
2. Android SDK works in Eclipse environment.
3. Android provides RDBMS SQLite for data storage and data sharing across various applications.
4. It has several pre-installed applications such as Gmail, Maps, voice search etc.
5. It support java based applications.
6. Android can run multiple apps at the same time.

Android software stack:

The Android code is structured into 4 Layers:



i) Application Layer:

A set of basic functions such as web browser, email client, SMS program, maps, Calendar and repository management programs which is written using J2ME java programming language comes

ii) Application framework:

*) A standard structure for different applications is implemented using this application framework.

*) A set of services provided by this application framework are:

⇒ Managers → Allows an application to display custom alerts on the status bar

⇒ Content providers → enable applications to access data from other applications.

iii) Libraries & Runtime:

*) The libraries are written using multiple languages such as C & C++.

*) Java interfaces are used to call these libraries. It includes surface manager, 2D and 3D graphics, Medic codecs like MPEG-4 and MP3, SQL data base SQLite and web browser engine called Webkit.

*) The two components of Android runtime are

a) A set of libraries

b) Dalvik virtual machine

→ It is not a traditional Java virtual m/c but a custom VM designed to run multiple instances efficiently.

iv) Kernel:

*) Based on the version of Linux Kernel, Android Kernel is developed.

*) Android allows applications to run concurrently, thus it supports multitasking. For eg, sending an email & hearing music at the same time.

*) Android implements its mobile device drivers, process management, memory management and also networking functions based on Linux kernel code.
*) It does not support the full set of GUI libraries.

Advantage of Android OS:

i) Android allows applications to run concurrently.
ii) Multitasking is possible with this OS.
iii) It has open platfoom and suitable for many mobile phones.
iv) It supports libraries and robust in nature.
v) It has an integrated web browsing.
vi) It uses java as programming language and it is user friendly.

4.3) Blackberry OS:

*) It is a proprietary OS specially designed for blackberry smartphons which is produced by RIM (Research in Motion Limited).
*) The details of its architecture won't be released due to its proprietary in nature.
*) It deploys a very good email system at the user level.
*) It supports instant mailing while maintaining a high level of security through on-device hardware-based-message-encryption.

4.4) Windows Mobile:

*) Micosqt corporation developed an operating system in the yeau 1996 namely windows CE
CE → consumer Electronics.

*) The company also designed pocket pc 2000 os in the yeau 2000. As the usage of mobile phone increases, based on pocket PC 2000, micuosqt introduced its windows mobile OS in the yeau 2003.

*) Windows Mobile OS is the OS for mobile phones.

Family of windows Mobile:

*) Windows Mobile is a family of 3 OS.

1) Windows Mobile Standaud → it is used in smautphones.
2) Windows Mobile Profesional → It is used in Smauphones.
3) Windows Classic → It is mainly used for PDA's and not used for cell phones.
→ Pocket PC 2000 is renamed as windows classic.

Features of windows Mobile OS:

i) Provides virtual Environment.
ii) NO true Multitasking is supported.
iii) Graphics/window/Event Manager (GWE) componeat handles all input & output.
iv) Application development is similau to Win32 environment.
$v) Security is provided thuó cryptogeaphic libraay.

music at the same time

Unlike Apple iOS and Blackberry OS:

*) Windows mobile OS can be used for any type of mobile phone, whereas iOS and RIM blackberry OS is mainly designed to use only for iphone and Blackberry.

*) To reduce the number of versions and to simplify the design of OS, microsoft defined a hardware specifications for hand-held computers.

*) Windows mobile OS also intended to make the cell phones manufactured by different vendors appear uniform.

Family of Windows Mobile:

*) Windows Mobile is now a family of three OS:

i) Windows Mobile Standard → it is used in Smartphones

ii) Windows Mobile Professional → it is used in smartphones

iii) Windows Classic → it is mainly for PDA
→ not for cell phones
→ Pocket PC 2000 is renamed as Windows Classic with touch screen based.

Features of Windows Mobile OS:

i) Provides virtual environment
ii) No True multitasking is supported.
iii) The graphics/windows/Event Manager (GWE) component handles all i/p & o/p.
iv) Security is provided thro' cryptographic library
v) Application development is similar to win32 environment

Evolution of Micosoft Mobile OS:

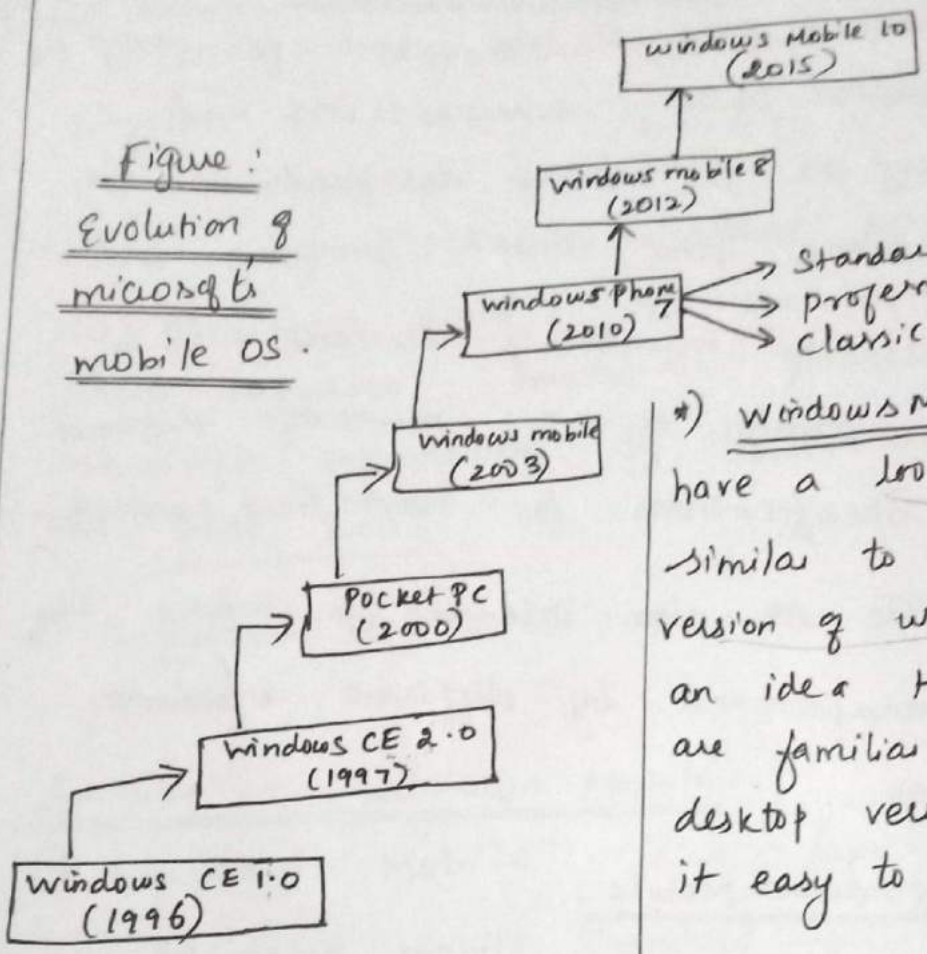


Figure: Evolution of micosoft mobile OS.

*) Windows Mobile (2003) have a look & feel that is similar to the desktop version of windows with an idea that users who are familiar with the desktop versions may find it easy to operate.

*) The main competitors of windows phone 7 are a) Android & b) ios.

*) The features of windows Phone 7:

i) Support screen resolution of 800x840 pixel.
ii) These devices have accelerometer & compass.
iii) It provides touch screen inteface.
iv) It also support screen rotation.

5) M- Commerce (Mobile Commerce):-

*) Mobile commerce, shortly called as M-commerce is an important application of Mobile computing.

*) It involves buying and selling of commodities and services through wireless handled devices such as mobile phones and PDA's.

*) Mobile payment is a natural evolution of e-payment schemes and has found an important place in M-Commerce.

Applications of M-commerce:

*) M-commerce applications can be broadly classified into

i) Buisness to consumer (B2C) Applications
ii) Buisness to Buisness (B2B) Applications.

i) Buisness to consumer (B2C) Applications:

*) In this type a product/service can be sold by a buisness firm to a consumer.

Examples:

a) Advertising

→ Mobile Advertising is a form of advertising via mobile phone.

→ Based on the current location of a user, a good targeted advertising can be done.

→ Network service providers also keep track of the history of the purchase made by the customer by directing advertisements to mobile phones.

b) Comparison Shopping:

→ Mobile phones are used to get the comparitive pricing analysis of a product at different stores consumers can see the price of different products at different shops by scanning the bar code of the product using their mobile phones.

*) They can then decide which shop is suitable for buying the product.

*) Consumers can also get product reviews from different consumers.

c) Information about a product:

*) Additional information about the product can be accessed thrugh mobile phones.

*) For example, let us assume that the consumer is buying a medicine from medical shop, but he cannot be able to read the dosage instruction given in spanish language. He can scan the bar code on the pack using his mobile phone and request for inst. in English language for easy reading

d) Mobile Ticketing: (m-tickets)

*) Mobile phones can be used to purchase movie tickets called as m-tickets using credit cards. Once the payment is received, a unique bar code is sent to the purchaser's mobile phone by SMS.

*) customers can also book train tickets using mobile phone.

Structure of Mobile commerce:

*) Mobile commerce has two sets of program namely,

i) Client-side programs → run on the webbrowsers installed on the user's mobile devices.

ii) Server-side programs → Performing data base access and computations on severs.

*) The various layer of mobile commerce architecture is shown in below figure:

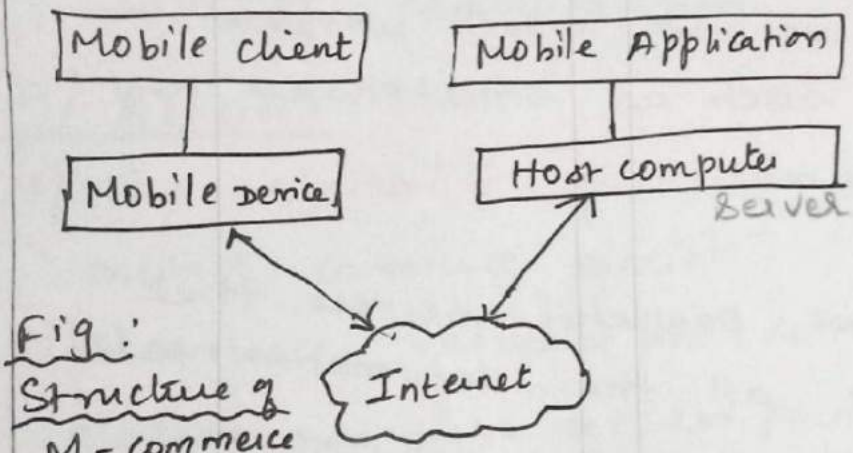


Fig: Structure of M-commerce

*) The layers are
i) Mobile devices
ii) Mobile client
iii) Mobile Application
iv) Host compute
v) Mobile Middleware
vi) Network.

i) Mobile Device:

*) Mobile device acts as the interface part of the mobile commerce to the users.

*) The users specify their request through appropriate interface, which is then transmitted through the internet of the m-commerce appln. on the internet.

*) The results are then displayed in the suitable formats.

ii) Mobile client:

*) Mobile client is a software application that is used for data collection

*) Depending on the type of mobile device used for data collection, the mobile client is available in different variations.

*) Mobile client can run either in offline mode or disconnected mode.

iii) Mobile Application:

*) It is a software application developed specifically for use on small wireless computing devices such as smartphones and tablets.

iv) Host computers:

*) Host computers are powerful servers that process and store all the information needed for the mobile commerce applications.

*) Most application programs used in the mobile commerce are hosted on these.

*) Mobile commerce applications consists of three major components:

i) Web Servers → help interact with mobile client.

ii) Data base Servers → to store data

iii) Application Programs → It is a middleware that implements the buisness logic of the mobile commerce applications.

v) Mobile Middleware:

*) The main purpose of mobile middleware is to seamlessly and transparently map the internet content to mobile phones that may sport a wide variety of OS, markup languages, microbrowsers & protocols.

*) To provide secure transactions, most mobile middleware also handle encrypting and decrypting communication.

vi) Network:

*) The availability of wireless networks makes the mobile commerce possible.

*) The user requests are delivered either to the closest wireless access point or to Base station.

*) Wired networks are optional in many mobile commerce systems.

*) Host computers are generally connected to these wired networks such as internet. So, user requests are routed to these servers using the standard transport provided by the network.

Features required by device for enabling M-commerce

i) Camera
ii) Internet
iii) RFID
iv) SMS & MMS
v) Ability for scanning bar codes
vi) Efficient display system.

6) Prons and cons of M-commerce:

Advantage & Disadvantage of M-commerce:

*) M-commerce has its own advantage & disadvantage

Advantage:

i) Mobile handheld devices can be personalized.

ii) The advantages of using M-commerce in buisness organization includes cost savings, buisness opportunities etc.

iii) M-commerce is user friendly, providing light weight, flexibility, etc.

iv) Mobile devices are personalized, thereby providing an additional level of convenience to the customers.

Disadvantage:

i) Mobile devices do not offer graphics, do not offer processing power of a pc

ii) The small screens of mobile devices limit the complexity of applications, ie, limit text typing capabilities.

iii) Biggest disadvantage is security (lack of security) Unless a customer is extremely careful, he may fall to various types of frauds.

iv) Restricted Bandwidth limits.

7) Security of M-commerce:

Security Issues:

i) Users of mobile devices can be difficult to trace because of roaming of the users.

ii) Mobile devices go on-line and off-line frequently

iii) The attackers would be very difficult to trace.

iv) Another security risk unique to the mobile device is the risk of loss or theft.

v) A mobile device that is stolen by frauds are difficult to track and prevent.

vi) A major problem in security is the lack of any satisfactory mechanism.

vii) Authentication mechanism has to be improved for M-commerce devices.

8) Mobile payment Systems:

*) A number of mobile payment methods are available via,

1) Micro payment
2) Credit card
3) Bank Payment

*) Payment is usually made by the service providers eg bank.

Mobile payment Schemes:

a) Micro payment based M-payment

*) It is intended for payment for small purchases such as items from vending machines

*) The mobile device can communicate with the vending machine directly using a bluetooth or wireless LAN connection and then the micropayment is carried out

*) Micro payment can also be implemented through the cooperation of mobile phone operator and a third party service provider. This approach is used for vending beverages from coca-cola machin

b) Credit card based M-payment

*) In the credit card based M-payment, the credit card number is linked to his mobile phone number.

*) When the customer makes an M-payment transaction with a merchant, the credit card is charged and the value is credited to the merchant's account.

c) Bank account based M-payment:

*) In this scheme, the bank account of the customer is linked to his mobile phone number.
*) When the customer makes an m-payment to a vendor through bluetooth or wireless LAN connectivity with the vendor's machine, the bank account of the customer is debited and the vendor is credited to the vendor's account.

Properties of Mobile payment System:

The mobile payment system should have the following properties:

i) Easy to use: The m-payment request must be easy for the customer to use.

ii) General purpose:

→ The m-payment system should be usable irrespective of the m-commerce transaction ie, customer-to-customer (C2C), B2B or B2C transactions. Payments should also be possible for both micro and macro payments.

iii) Interoperability:

→ It should be usable across different platforms, networks and applications.

iv) Trust:

→ The m-payment should be trustworthy. That is, the customer should be reasonably sure that credit or debit card related information that he is supplying would not be misused.

v) cost:

→ The mobile payment should not impose a high overhead cost.

vi) Swiftness:

→ The response time of the m-payment system should be reasonable.

vii) Global payment:

→ It should be possible to make payments to vendor across the globe using the m-payment system.

Mobile payment solutions.

*) The various types of mobile payment solutions are

i) SMS based payment
ii) Bar code based payment
iii) Near field communication (NFC) based payment.
iv) Mobile wallet.

i) SMS based payment:

*) In this, customer send a text message for the payment and the payment is added to his phone bill.

ii) Bar code based payment:

*) In this type, the bar code is used to pay the transaction. Immediate after the bar code is scanned at the trade point-of-scale and respective amount on the purchase is deducted from the wallet balance of the user.

iii) Near field communication (NFC) based payment:

*) This type of payment requires the user to install certain payment application such as visa pay wave, Mastercard Pay pass, etc.

*) For paying the transaction amount, user enables the payment app and necessary details are transferred to the pos m/c through bluetooth

iv) Mobile Wallet:

*) A user may have a number of ATM cards. The mobile wallet helps to keep these under the single wallet and make payment whenever necessary.

*) Some examples of mobile wallet are Paypal, google wallet, paytm, etc.

Process of Mobile Payment

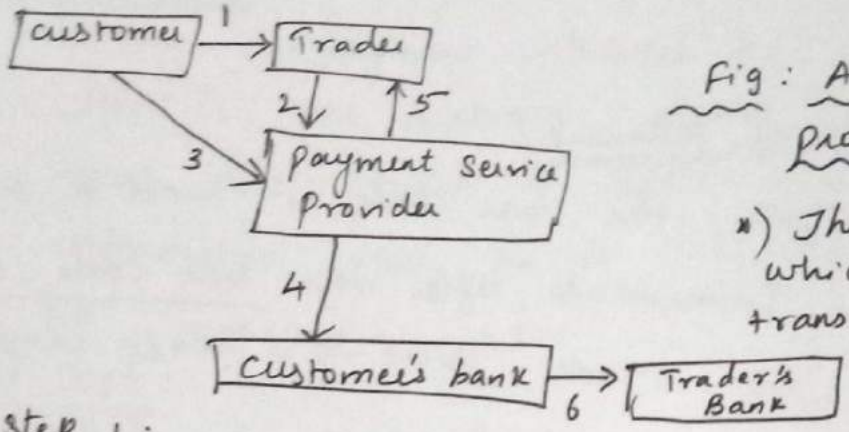


Fig: A mobile payment process model

*) The steps through which mobile payment transaction is performed is explained below.

Step 1: customer places the order with the trader for some goods.

Step 2: The trader now securely transfers the order to the selected payment service provider over the internet

Step 3: The customer then authenticates with the payment service.

Step 4: The payment service providers formats the transaction detail appropriately and securely routes the transaction authorization request through its payment gateway to the selected customer's bank.

Step 5: The merchant is informed of the payment status

Step 6: For a succesful transaction, the customer's bank transfers the requested amount to the trader's bank account.

*) It does not support the full set of standard GNU libraries, it makes it difficult to reuse the existing Linux applications.

*) Android allows applications to run concurrently, thus it supports multitasking. For example, Sending an email and hearing music at the same time.