MOBILE COMPUTING - IITT84E

MS INFORMATION TECHNOLOGY VIII SEM

FOUTH YEAR

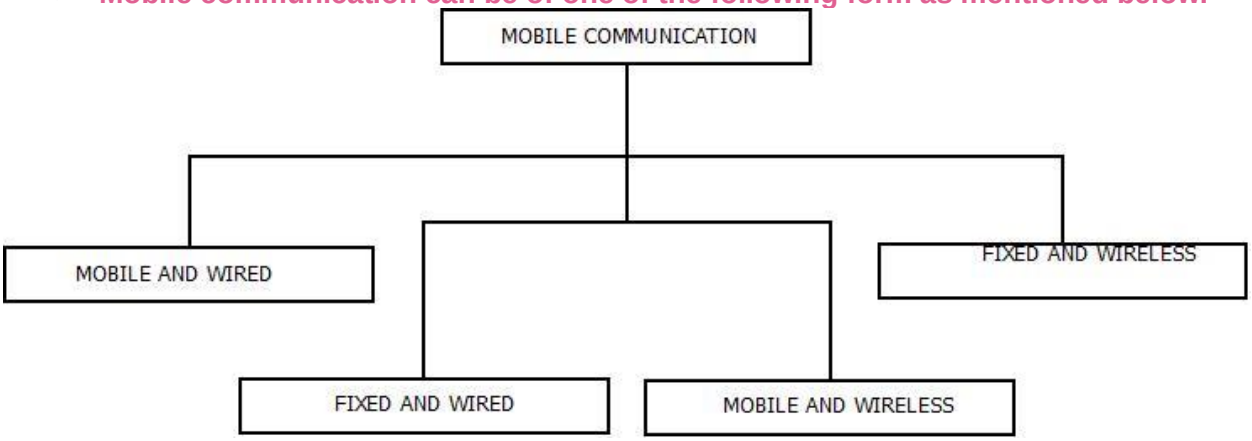
UNIT I

Mobile Computing : Introduction

- **A technology that is capable of providing an environment which enables users to transmit data from one device to other device without the use of any physical link/cables is known as Mobile Computing.**
- **It means, data transmission is done wireless-ly with the help of wireless devices such as mobiles, laptops etc.**
- **Whenever any device is connected to a network without being connected physically over a link or cable, data transmission such as messages, voice recording, videos etc. can be done be done by using the concept of mobile computing.**
- **Mobile Computing technology helps users to access and transmit data from any remote locations without being present there physically.**
- **Thus, having such a big coverage diameter, it is one of the fastest and most reliable sectors of computing technology field.**

Mobile Communication : Introduction

- **Mobile Communication is the framework that is responsible behind the working of mobile computing technology.**
- **It ensures the consistency and reliability of communication process through this framework.**
- **Mobile communication framework includes communication devise such as mobiles, laptops, as rules of conduct, fitness etc. They are responsible for delivering of smooth communication process.**
- **Mobile communication can be of one of the following form as mentioned below.**



1. **Mobile and Wired : In this configuration, Some of the devices are wired and some are mobile in nature. For Example : Laptops.**
2. **Fixed and Wired : In this configuration, The devices are fixed at a position and are connected through a physical link for communication. For Example : Office/Desktop Computer.**
3. **Mobile and Wireless : In this configuration, devices can communicate(data transmission) with each other irrespective of their position and can connect to any network without the use of any wired device. For Example : WiFi Dongle.**

Applications : Mobile Computing

- **Some of the major field in which mobile computing can be applied are:**
  - **Web or Internet access.**
  - **Global Position System(GPS).**
  - **Emergency services.**
  - **Entertainment services**
  - **Educational services.**

Signals

- physical representation of data

function of time and location
signal parameters: parameters representing the value of data
classification
continuous time/discrete time
continuous values/discrete values
analog signal = continuous time and continuous values
digital signal = discrete time and discrete values
signal parameters of periodic signals: period T, frequency f=1/T, amplitude A, phase shift φ q sine wave as special periodic signal for a carrier:

$$s(t) = At \sin(2 \pi ft t + \varphi t)$$

Antennas

Radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission
Isotropic radiator: equal radiation in all directions (three dimensional) - only a theoretical reference antenna
Real antennas always have directive effects (vertically and/or horizontally
Radiation pattern: measurement of radiation around an antenna

Signal propagation

Transmission range
communication possible q low error rate

Detection range q detection of the signal possible q no communication possible

Interference range q signal may not be detected q signal adds to the background noise

Wireless Networks : The Difference

- **The difference between Fixed Vs. Wireless networks can be seen as, wireless networks does not require any sort of cables to get the devices connect physically. It is a shared medium that can be accessed easily.**
- **While in case of fixed networks, physical configuration of devices is required in order to perform data transmission process. Every new device needs to be connected separately and physically to the network. Let's have a look at their comparisons**

Fixed Vs. Wireless Networks : Issues in Mobile Computing

- **Mobile computing technology has a number of advantages- from mobility to portability and from cloud to productivity. But, there are certain issues which do pops out while using the mobile computing technology. These are**

1. Wireless Medium

- **Since the mobile computing technology mainly focuses on wireless infrastructure, issues like cost, efficiency, delays and security needs to be considered too.**

2. Device Mobility

- **The device mobility is certainly a major advantage of mobile computing technology. But, it is one of its major issue too.**
- **The mobility feature of mobile computing technology needs to be of highest standards. It means, this configuration needs to structure the environment, every time the mobile device changes it's environment.**
- **Device mobility feature needs to work and configure itself according to the location, environment and surroundings of a mobile device on regular basis.**

3. Security Issues

- **It is one of the most discussed issue with mobile computing technology, as it arises due to the shared medium ability.**
-
  - **Data Security à Physical Security.**
  - **System Security à Network Security.**
- **Some of the most common tactics used to get rid of these issue are:**
  - **Use of VPN technology.**
  - **Use of Cryptography & Network Security.**
  - **Use of Firewall technology.**

Advantages : Mobile Computing Technology

- **Device Mobility.**
- **Simple Framework/Infrastructure.**

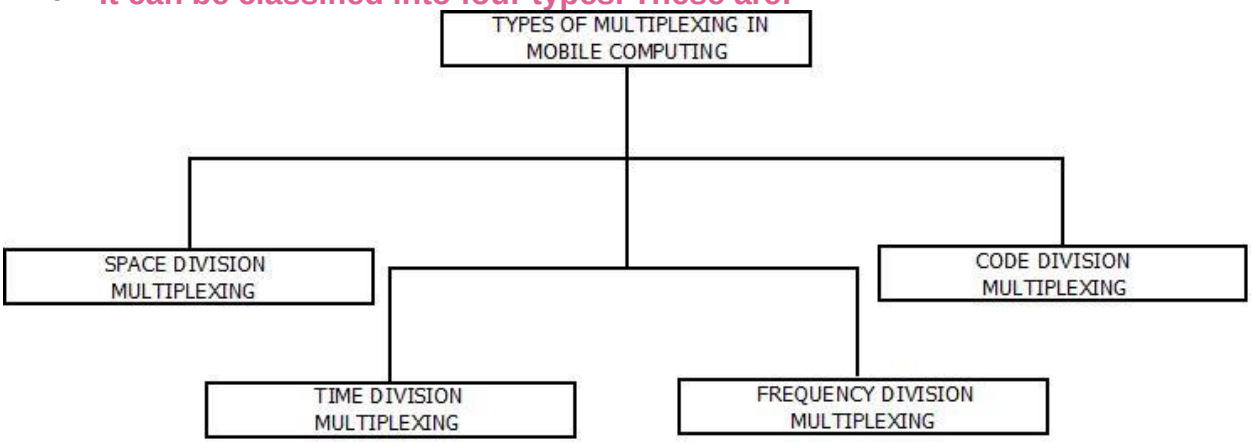
- Portability
- Better Productivity.
- Use of cloud technology.

Disadvantages : Mobile Computing Technology

- Less Secured.
- Low data transmission rates.
- High data losses.
- High on power consumption.
- Frequent network issues.

Multiplexing : Introduction

- Multiplexing is a technique in which, multiple simultaneous analog or digital signals are transmitted across a single data link.
- The concept behind it is very simple: **Proper Resource Sharing and its Utilization**.
- It can be classified into four types. These are:



ultiplexing : Frequency Division Multiplexing(FDM)

- In Frequency Division , the frequency dimension spectrum is split into bands of smaller frequency.
- FDM is used because of the fact that, a number of frequency band can work simultaneously without any time constraint

Advantages of FDM

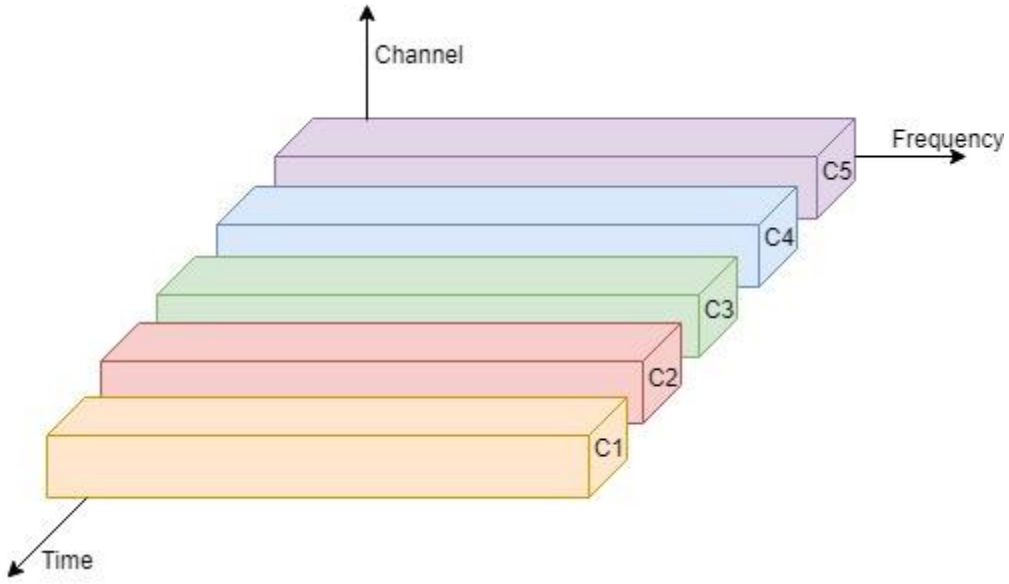
- This concept is applicable on both analog signals as well as digital signals.
- Simultaneous signal transmission feature.

Disadvantages of FDM

- Less Flexibility.
- Bandwidth wastage is high and can be an issue.

Multiplexing : Time Division Multiplexing(TDM)

- Time Division is used for a particular amount of time in which the whole spectrum is used.
- Time frames of same intervals are made such that the entire frequency spectrum can be accessed at that time frame.



Advantages of TDM

- **Single user at a time.**
- **Less complex and more flexible architecture.**

Disadvantages of TDM

- **Difficult to implement.**

Multiplexing : Code Division Multiplexing(CDM)

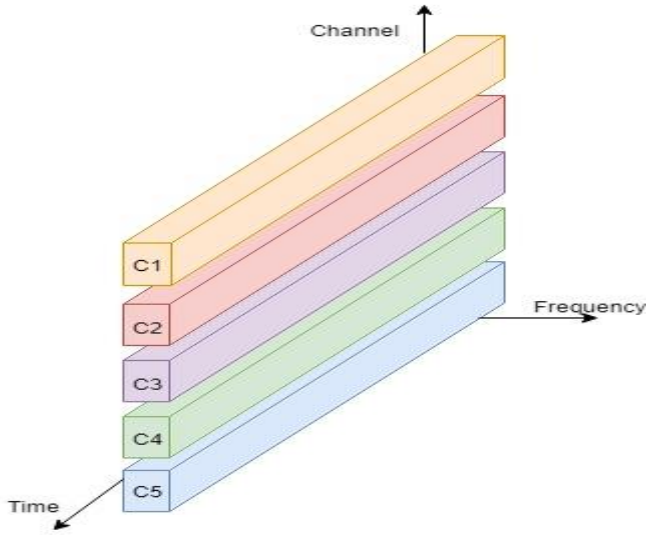
- **In Code Division Multiplexing, every channel is allotted with a unique code so that each of these channels can use the same spectrum simultaneously at same time.**

Advantages of CDM

- **Highly Efficient.**
- **Less Inference.**

Disadvantages of CDM

- **Less data transmission rates.**
- **Complex in nature**



Advantages of CDM

- **Highly Efficient.**
- **Less Inference.**

Disadvantages of CDM

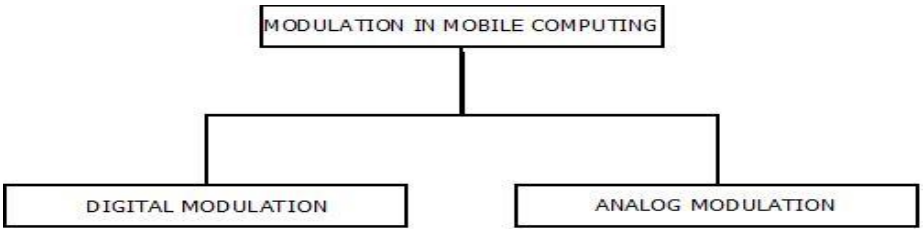
- **Less data transmission rates.**
- **Complex in nature**

Modulation : Intoduction

- **Modulation is the process of converting signals from one form into other form i.e. Analog to Digital or Digital to Analog.**

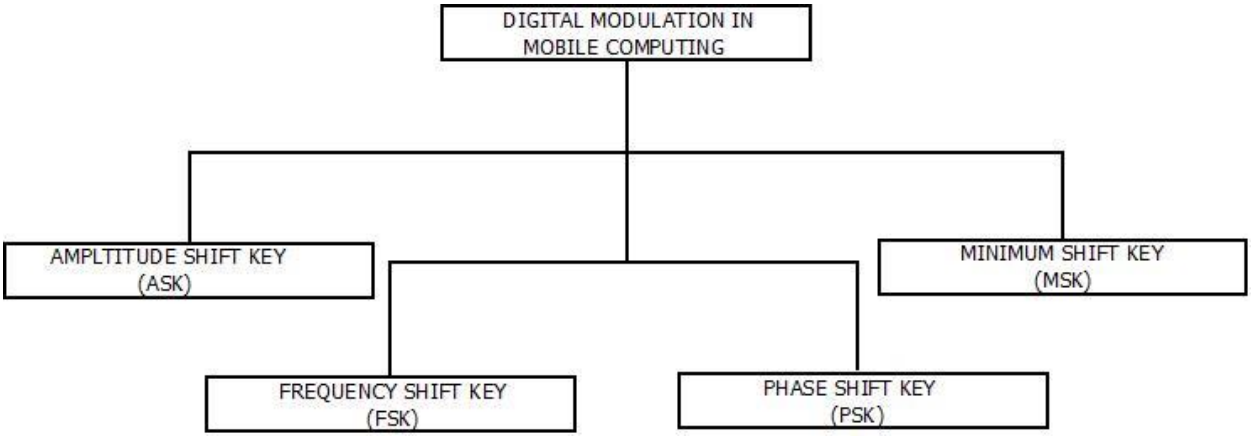
For Example : Consider an Analog transmission medium is available to transmit signals, but we have a digital signal which needs to be transmitted through this Analog medium. This can be done by converting the digital signal into analog signal. This process of conversion is called as modulation.

- **This can be classified into two types:**



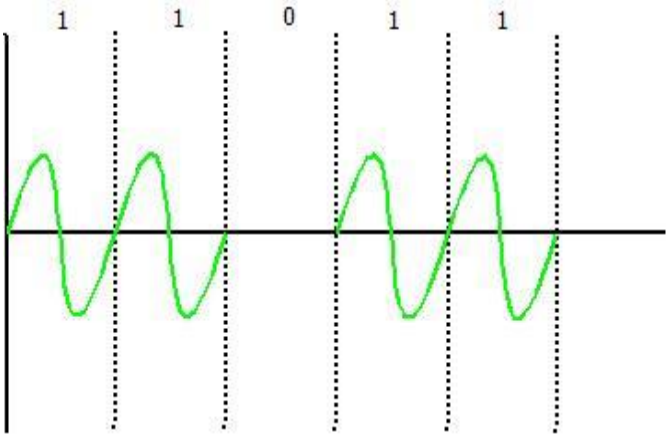
Modulation : Digital Modulation

- **Modulating a signal digitally, is a technique with the help of which digital signals/data can be converted into analog signals i.e. base band signals.**
- **This can further be classified as:**



1. Amplitude Shift Key(ASK)

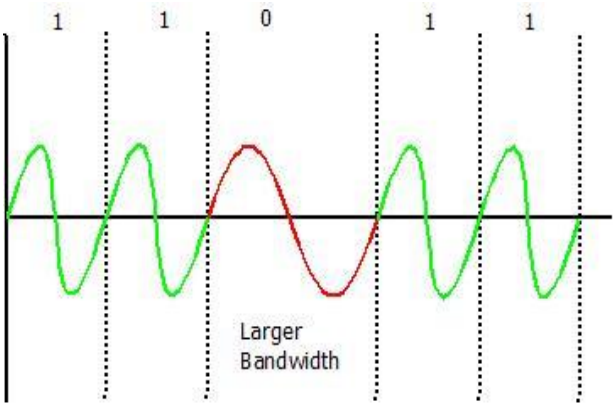
- **In Amplitude Shift Key as the name suggests, amplitude is represented by "1" and if the amplitude doesn't exists, it is represented by "0".**
- **Use of Amplitude Shift Key is very simple and requirement of bandwidth is very low.**
- **ASK is vulnerable to inference or deduction**



2. Frequency Shift Key(FSK)

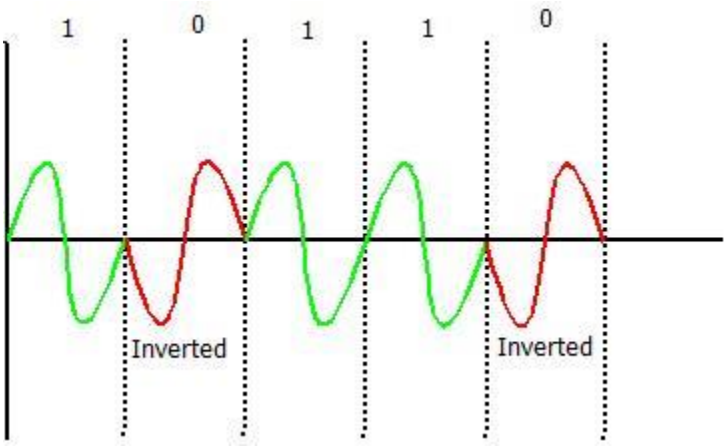
- **It uses different notations f1 and f2 are used for different frequencies.**
- **f1 is used to represent bit "1" and f2 is used to represent bit "0".**

- **Frequency Shift Key is simple too, but due to use of different frequencies for different bits, bandwidth requirement becomes high.**



3. Phase Shift Key(PSK)

- **In this, phase difference is used to differentiate between the bits i.e. "1" and "0".**
- **If the bit is "1" , simple wave is drawn and if the bit becomes "0", the phase of the wave is shifted by "180 or π"**
- **PSK is more complex than ASK and FSK and is robust too.**

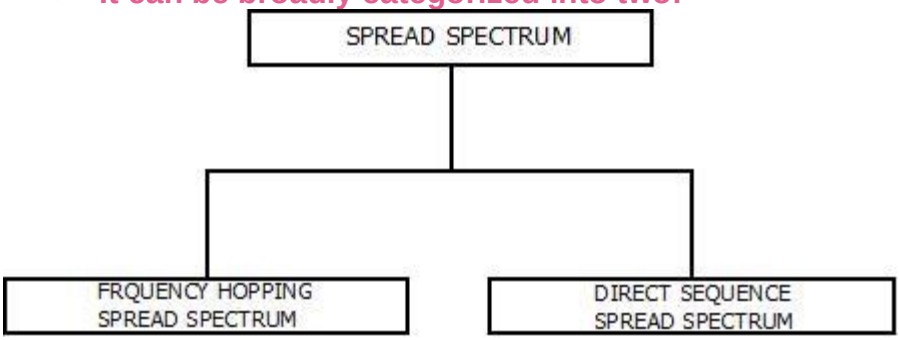


Modulation : Analog Modulation

- **Analog Modulation is a technique with the help of which analog data signals can be transmitted into digital signals i.e. Broadband Signals.**
- **This can further be classified as :**

Spread Spectrum : Introduction

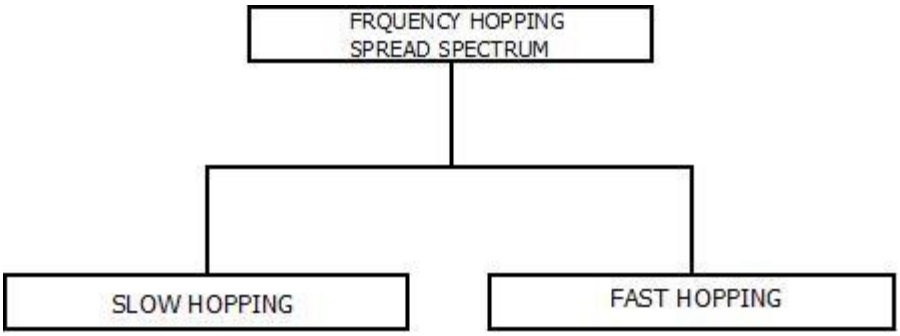
- When transmitted signals of certain frequencies are varied slightly in order to obtain greater bandwidth as compared to initial bandwidth is known as Spread Spectrum.
- Spread Spectrum technology helps in transmission of radio signals because they can easily reduce the noise and other issues that are data resistant.
- It can be broadly categorized into two:



The major reason of spectrum technology being used is because of its proper bandwidth utilization ability.

Spread Spectrum : Frequency Hopping Spread Spectrum (FHSS)

- The logic behind the use of Frequency hopping Spread spectrum is, in order to utilize bandwidth properly, we need to divide the whole available bandwidth into many channels and spread them between channels which are arranged in a continuous manner.
- The selection of frequency slots is done on random basis and based on their occupancy, frequency signals are transmitted.
- The transmitters and receivers keeps on hopping on channels available for a particular amount of time in milliseconds.
- Hence, frequency division multiplexing and time division multiplexing are implemented simultaneously in FHSS.
- FHSS can be classified as



- **Slow hopping : In slow hopping, multiple bits are transmitted on a particular or same frequency.**
- **Fast Hopping : In fast hopping, individual bits are split and are transmitted on different frequencies.**

Advantages of FHSS

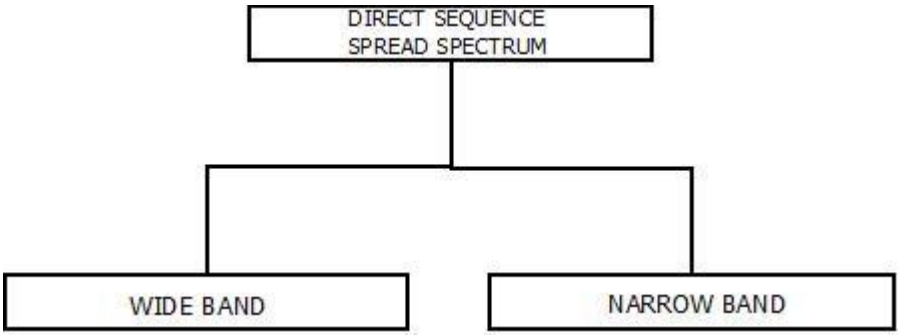
- **Secure.**
- **Simple implementation as compared to DsSS.**
- **High efficiency.**

Disadvantages of FHSS

- **Less Robust.**

Spread Spectrum : Direct Sequence Spread Spectrum(DSSS)

- **Direct Sequence Spread Spectrum is another type of spread spectrum in which data that needs to be transmitted is split into smaller blocks.**
- **Then, each data block is attached with a high data rate bit sequence and is transmitted from sender end to receiver end.**
- **At the receiver's end with the help of data rate bit sequence, data blocks are recombined again to generate the original data which was sent by the sender.**
- **If in case the data is lost, with the help of those data rate bits data blocks can be recovered.**
- **This split of data into smaller blocks is done to reduce noise and unintentional inference.**



Advantages of DSSS

- **Signals are difficult to detect.**
- **Less chances of jamming.**
- **Less reluctant to noise.**

Disadvantages of DSSS

- **Slow.**
- **Requirement of wide-band channels.**

Applications of Spread Spectrum

- **LAN technology**
- **Satellite communication technology**

UNIT II

Medium Access Control

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

3. Medium Access Control

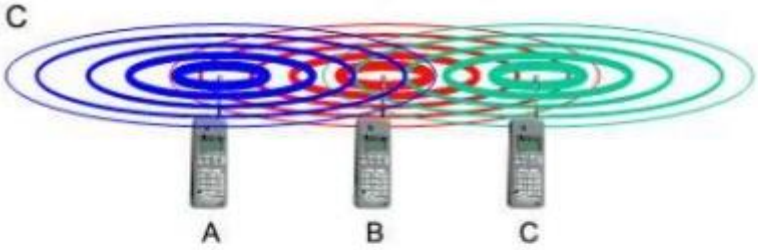
- Medium access control comprises all mechanisms that regulate user access to a medium using SDM, TDM, FDM, or CDM.
- MAC is thus similar to traffic regulations in the highway/multiplexing example.
- MAC belongs to layer 2, the data link control layer (DLC).
- Layer 2 is subdivided into the logical link control (LLC), layer 2b, and the MAC, layer 2a.
- The task of DLC is to establish a reliable point to point or point to multi-point connection between different devices over a wired or wireless medium.

3.1. Motivation for a specialized MAC

3.1.1. Hidden and exposed terminals

Hidden terminals

- A sends to B, C cannot receive A
- C wants to send to B, C senses a "free" medium (CS fails)
- collision at B, A cannot receive the collision (CD fails)
- A is "hidden" for C



Exposed terminals

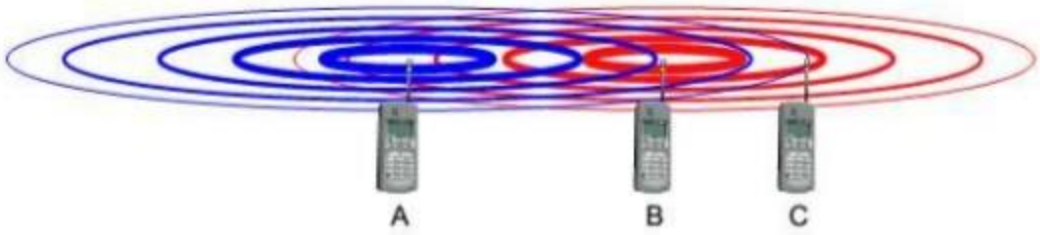
- B sends to A, C wants to send to another terminal (not A or B)
- C has to wait, CS signals a medium in use
- but A is outside the radio range of C, therefore waiting is not necessary
- C is "exposed" to B

3.1. Motivation for a specialized MAC

3.1.2. Near and far terminals

Terminals A and B send, C receives

- signal strength decreases proportional to the square of the distance
- the signal of terminal B therefore drowns out A's signal
- C cannot receive A



If C for example was an arbiter for sending rights, terminal B would drown out terminal A already on the physical layer

Also severe problem for CDMA-networks - precise power control needed!

3.2. SDMA

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

3.3. FDMA

- Frequency division multiple access (FDMA) comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM) scheme.
- Allocation can either be **fixed** or **dynamic**.
- FDM is often used for simultaneous access to the medium by base station and mobile station in cellular networks.
- Here the two partners typically establish a **duplex channel**, i.e., a channel that allows for simultaneous transmission in both directions.
- The two directions, mobile station to base station and vice versa are now separated using different frequencies.
- This scheme is then called **frequency division duplex** (FDD).

3.3. FDMA

- Both partners have to know the frequencies in advance; they cannot just listen into the medium.
- The two frequencies are also known as **uplink**, i.e., from mobile station to base station or from ground control to satellite, and as **downlink**, i.e., from base station to mobile station or from satellite to ground control.

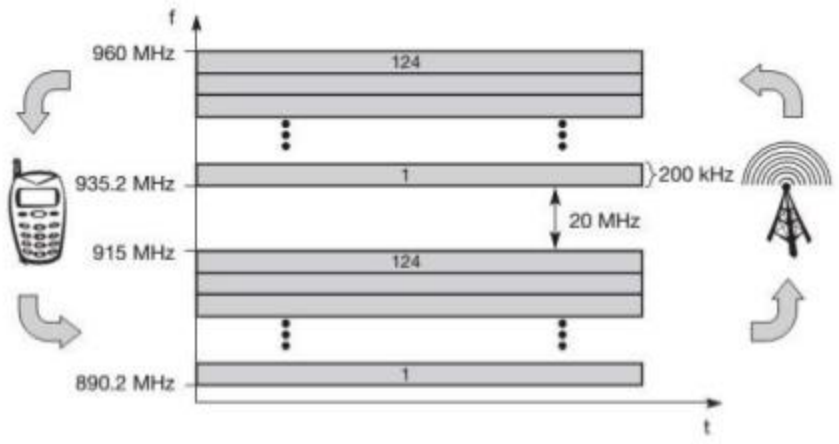


Figure 3.3
Frequency division multiplexing for multiple access and duplex

3.4. TDMA

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

3.4. TDMA

- Synchronization between sender and receiver has to be achieved in the time domain.
- Again this can be done by using a fixed pattern similar to FDMA techniques, i.e., allocating a certain time slot for a channel, or by using a dynamic allocation scheme.
- **Dynamic allocation schemes** require an identification for each transmission (e.g., sender address) or the transmission has to be announced before hand.
- MAC addresses are quite often used as identification.
- This enables a receiver in a broadcast medium to recognize if it really is the intended receiver of a message.
- **Fixed schemes** do not need an identification, but are not as flexible considering varying bandwidth requirements.

3.4. TDMA

3.4.1. Fixed TDM

- The simplest algorithm for using TDM is allocating time slots for channels in a fixed pattern. This results in a fixed bandwidth.
- These patterns guarantee a fixed delay – one can transmit, e.g., every 10 ms as this is the case for standard DECT systems.
- MAC is quite simple, as the only crucial factor is accessing the reserved time slot at the right moment.
- If this synchronization is assured, each mobile station knows its turn and no interference will happen.
- The fixed pattern can be assigned by the base station, where competition between different mobile stations that want to access the medium is solved.

3.4. TDMA

- Figure 3.4 shows how these fixed TDM patterns are used to implement multiple access and a duplex channel between a base station and mobile station.
- Assigning different slots for uplink and downlink using the same frequency is called **time division duplex** (TDD).

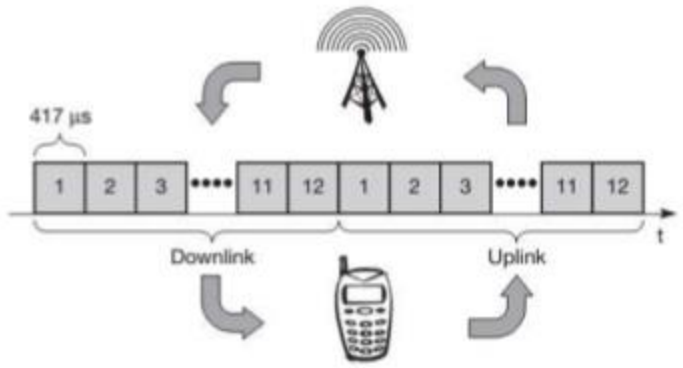


Figure 3.4
Time division multiplexing for multiple access and duplex

3.4. TDMA

- As shown in the figure, the base station uses one out of 12 slots for the downlink, whereas the mobile station uses one out of 12 different slots for the uplink.
- Uplink and downlink are separated in time.
- Up to 12 different mobile stations can use the same frequency without interference using this scheme.
- Each connection is allotted its own up- and downlink pair.
- In the example, which is the standard case for the DECT cordless phone system, the pattern is repeated every 10 ms, i.e., each slot has a duration of 417 µs.
- This repetition guarantees access to the medium every 10 ms, independent of any other connections.

3.4. TDMA

3.4.2. Classical Aloha

- A scheme which was invented at the University of Hawaii and was used in the ALOHANET for wireless connection of several stations.
- Aloha neither coordinates medium access nor does it resolve contention on the MAC layer.
- Instead, each station can access the medium at any time.
- This is a random access scheme, without a central arbiter controlling access and without coordination among the stations.
- If two or more stations access the medium at the same time, a collision occurs and the transmitted data is destroyed.
- Resolving this problem is left to higher layers (e.g., retransmission of data).

3.4. TDMA

- The simple Aloha works fine for a light load and does not require any complicated access mechanisms.
- On the classical assumption that data packet arrival follows a Poisson distribution, maximum throughput is achieved for an 18 per cent load.

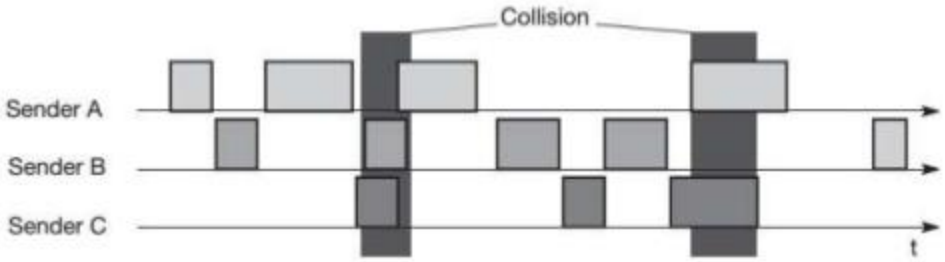


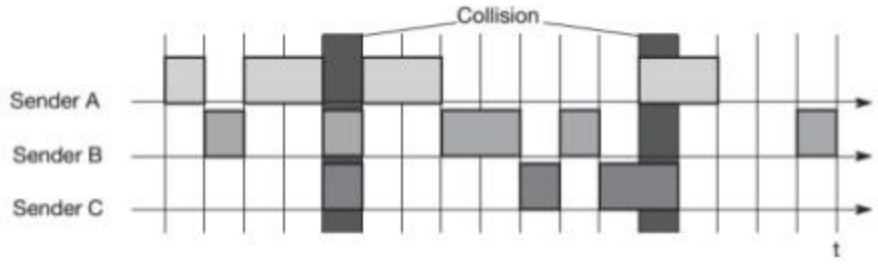
Figure 3.5
Classical Aloha multiple access

3.4. TDMA

3.4.3. Slotted Aloha

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

Figure 3.6
Slotted Aloha multiple access



3.4. TDMA

3.4.4. Carrier sense multiple access

- One improvement to the basic Aloha is sensing the carrier before accessing the medium.
- Sensing the carrier and accessing the medium only if the carrier is idle decreases the probability of a collision.
- But, as already mentioned in the introduction, hidden terminals cannot be detected.
- If a hidden terminal transmits at the same time as another sender, a collision might occur at the receiver.
- This basic scheme is still used in most wireless LANs.

3.4. TDMA

- Several versions of CSMA exist.
- In **non-persistent CSMA**, stations sense the carrier and start sending immediately if the medium is idle.
- If the medium is busy, the station pauses a random amount of time before sensing the medium again and repeating this pattern.
- In **p-persistent CSMA** systems nodes also sense the medium, but only transmit with a probability of p, with the station deferring to the next slot with the probability 1-p, i.e., access is slotted in addition.
- In **1-persistent CSMA** systems, all stations wishing to transmit access the medium at the same time, as soon as it becomes idle.
- This will cause many collisions if many stations wish to send and block each other.

3.4. TDMA

- To create some fairness for stations waiting for a longer time**, back-off algorithms** can be introduced, which are sensitive to waiting time as this is done for standard Ethernet.
- **CSMA with collision avoidance** (CSMA/CA) is one of the access schemes used in wireless LANs following the standard IEEE 802.11.
- Here sensing the carrier is combined with a back-off scheme in case of a busy medium to achieve some fairness among competing stations.
- Another, very elaborate scheme is **elimination yield – non-preemptive multiple access** (EY-NMPA) used in the HIPERLAN 1 specification.
- Here several phases of sensing the medium and accessing the medium for contention resolution are interleaved before one "winner" can finally access the medium for data transmission.

3.4. TDMA

3.4.5. Demand assigned multiple access

- A general improvement of Aloha access systems can also be achieved by reservation mechanisms and combinations with some (fixed) TDM patterns.
- These schemes typically have a reservation period followed by a transmission period.
- During the reservation period, stations can reserve future slots in the transmission period.
- While, depending on the scheme, collisions may occur during the reservation period, the transmission period can then be accessed without collision.
- Alternatively, the transmission period can be split into periods with and without collision.

3.4. TDMA

- In general, these schemes cause a higher delay under a light load (first the reservation has to take place), but allow higher throughput due to less collisions.
- One basic scheme is **demand assigned multiple access** (DAMA) also called **reservation Aloha**, a scheme typical for **satellite systems**.
- DAMA has two modes.
- During a contention phase following the slotted Aloha scheme, all stations can try to reserve future slots.
- For example, different stations on earth try to reserve access time for satellite transmission.
- Collisions during the reservation phase do not destroy data transmission, but only the short requests for data transmission.

3.4. TDMA

3.4.6 Packet Reservation Multiple Access (PRMA)

- In PRMA, slots can be reserved implicitly according to the following scheme.
- A certain number of slots forms a frame.
- The frame is repeated in time i.e., a fixed TDM pattern is applied.
- A base station, which could be a satellite, now broadcasts the status of each slot to all mobile stations.
- All stations receiving this vector will then know which slot is occupied and which slot is currently free.
- A successful transmission of data is indicated by the station's name.
- All stations wishing to transmit can now compete for this free slot in Aloha fashion.
- The already occupied slots are not touched.

3.4. TDMA

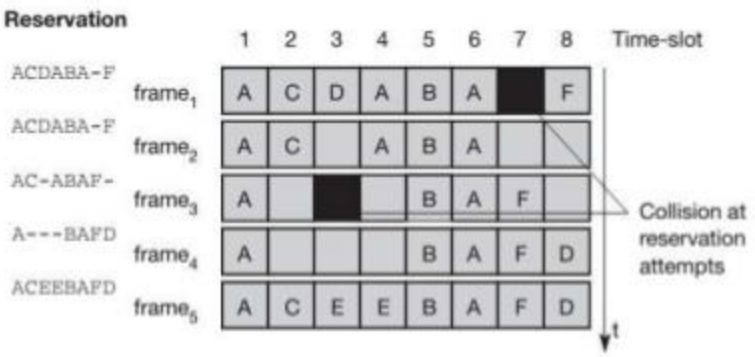


Figure 3.8
Demand assignment multiple access with implicit reservation

3.4. TDMA

3.4.7. Reservation TDMA

- An even more fixed pattern that still allows some random access is exhibited by reservation TDMA.
- In a fixed TDM scheme N mini-slots followed by N * k data-slots form a frame that is repeated.
- Each station is allotted its own mini-slot and can use it to reserve up to k data-slots.
- This guarantees each station a certain bandwidth and a fixed delay.
- Other stations can now send data in unused data-slots.

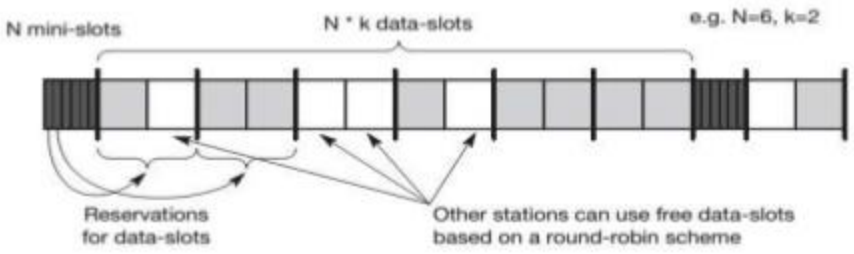


Figure 3.9
Reservation TDMA access scheme

3.4. TDMA

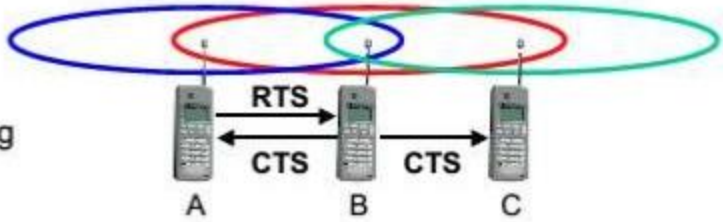
3.4.8. Multiple access with collision avoidance

- Multiple access with collision avoidance (MACA) presents a simple scheme that solves the **hidden terminal** problem, does not need a base station, and is still a random access Aloha scheme – but with dynamic reservation.
- MACA uses short signaling packets for collision avoidance.
  - **RTS** (request to send): A sender request the right to send from a receiver with a short RTS packet before it sends a data packet.
  - **CTS** (clear to send): The receiver grants the right to send as soon as it is ready to receive.
- Signaling packets contain
  - sender address
  - receiver address
  - packet size

3.4. TDMA

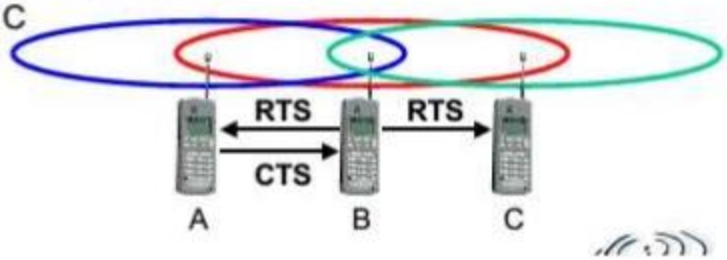
MACA avoids the problem of hidden terminals

- A and C want to send to B
- A sends RTS first
- C waits after receiving CTS from B



MACA avoids the problem of exposed terminals

- B wants to send to A, C to another terminal
- now C does not have to wait for it cannot receive CTS from A



3.4. TDMA

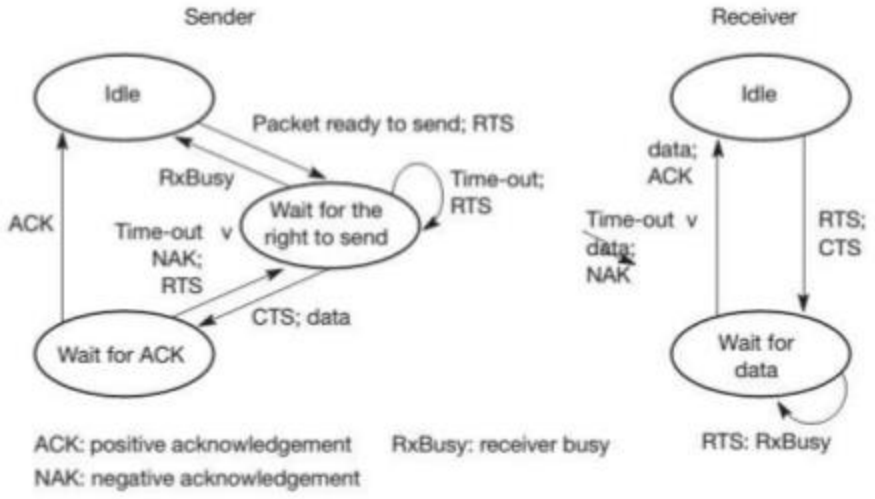


Figure 3.12
Protocol machines for multiple access with collision avoidance

3.4. TDMA

3.4.9 Polling

- Where one station is to be heard by all others, polling schemes can be applied.
- Polling is a strictly centralized scheme with one master station and several slave stations.
- The master can poll the slaves according to many schemes: round robin, randomly, according to reservations etc.
- The master could also establish a list of stations wishing to transmit during a contention phase.
- After this phase, the station polls each station on the list.
- Similar schemes are used, e.g., in the Bluetooth wireless LAN and as one possible access function in IEEE 802.11 systems

3.4. TDMA

3.4.10 Inhibit sense multiple access

- This scheme, which is used for the packet data transmission service Cellular Digital Packet Data (CDPD) in the AMPS mobile phone system, is also known as digital sense multiple access (DSMA).
- Here, the base station only signals a busy medium via a busy tone (called BUSY/IDLE indicator) on the downlink.
- After the busy tone stops, accessing the uplink is not coordinated any further.
- The base station acknowledges successful transmissions, a mobile station detects a collision only via the missing positive acknowledgement.
- In case of collisions, additional back-off and retransmission mechanisms are implemented.

3.5. CDMA

3.5.1 Spread Aloha multiple access

- CDMA senders and receivers are not really simple devices.
- Communicating with n devices requires programming of the receiver to be able to decode n different codes.
- For mobile phone systems, a lot of the complexity needed for CDMA is integrated in the base stations.
- What happens if we combine the spreading of CDMA and the medium access of Aloha or, in other words, what if we use CDMA with only a single code, i.e., without CD?
- The resulting scheme is called spread Aloha multiple access (SAMA) and is a combination of CDMA and TDMA

3.5. CDMA

- Sender A and sender B access the medium at the same time in their narrowband spectrum, so that all three bits shown cause a collision.
- The same data could also be sent with higher power for a shorter period as shown in the middle, but now spread spectrum is used to spread the shorter signals, i.e., to increase the bandwidth (spreading factor s = 6 in the example).
- Both signals are spread, but the chipping phase differs slightly.
- Separation of the two signals is still possible if one receiver is synchronized to sender A and another one to sender B.
- The signal of an unsynchronized sender appears as noise.

3.6. Comparison of S/T/F/CDMA

Approach	SDMA	TDMA	FDMA	CDMA
Idea	segment space into cells/sectors	segment sending time into disjoint time-slots, demand driven or fixed patterns	segment the frequency band into disjoint sub-bands	spread the spectrum using orthogonal codes
Terminals	only one terminal can be active in one cell/one sector	all terminals are active for short periods of time on the same frequency	every terminal has its own frequency, uninterrupted	all terminals can be active at the same place at the same moment, uninterrupted
Signal separation	cell structure, directed antennas	synchronization in the time domain	filtering in the frequency domain	code plus special receivers
Advantages	very simple, increases capacity per km²	established, fully digital, flexible	simple, established, robust	flexible, less frequency planning needed, soft handover
Dis-advantages	inflexible, antennas typically fixed	guard space needed (multipath propagation), synchronization difficult	inflexible, frequencies are a scarce resource	complex receivers, needs more complicated power control for senders
Comment	only in combination with TDMA, FDMA or CDMA useful	standard in fixed networks, together with FDMA/SDMA used in many mobile networks	typically combined with TDMA (frequency hopping patterns) and SDMA (frequency reuse)	still faces some problems, higher complexity, lowered expectations; will be integrated with TDMA/FDMA

GSM: Overview

formerly: Groupe Spéciale Mobile (founded 1982)

now: Global System for Mobile Communication q Pan-European standard (ETSI, European Telecommunications Standardisation Institute) simultaneous introduction of essential services in three phases (1991, 1994, 1996) by the European telecommunication administrations (Germany: D1 and D2) Ł seamless roaming within Europe possible q today many providers all over the world use GSM (more than 200 countries in Asia, Africa, Europe, Australia, America) q more than 1.2 billion subscribers in more than 630 networks q more than 75% of all digital mobile phones use GSM (74% total) q over 200 million SMS per month in **Germany, > 550**

billion/year worldwide (> 10% of the revenues for many operators) [be aware: these are only rough numbers…]

GSM offers

several types of connections

voice connections, data connections, short message service multi-service options (combination of basic services**)**

Three service domains

Bearer Services

Telematic Services

Supplementary Services

Architecture of the GSM system

several providers setup mobile networks following the GSM standard within each country

components l MS (mobile station) l BS (base station) l MSC (mobile switching center) l LR (location register)

subsystems l RSS (radio subsystem): covers all radio aspects l NSS (network and switching subsystem): call forwarding, handover, switching l OSS (operation subsystem): management of the network

UNIT III

Satellite Systems

History of satellite communication

1945Arthur C. Clarke publishes an essay about „Extra Terrestrial Relays“

1957 first satellite SPUTNIK 1960first reflecting communication satellite ECHO

1963 first geostationarysatellite SYNCOM

1965 first commercial geostationarysatellite Satellit„Early Bird“ (INTELSAT I): 240 duplex telephone channels or 1 TV channel, 1.5 years lifetime

1976three MARISAT satellites for maritime communication 1982 first mobile satellite telephone system INMARSAT-A

1988 first satellite system for mobile phones and data communication INMARSAT-C

1993first digital satellite telephone system 1998 global satellite systems for small mobile phones

Applications

Telecommunication

global telephone connection

backbone for global networks

connections for communication in remote places or underdeveloped areas

global mobile communication

Other applications

weather satellites

radio and TV broadcast satellites

military satellites

satellites for navigation and localization (e.g., GPS)

satellite systems to extend cellular phone systems

Basics

Satellites in circular orbits

attractive force $F_g = m\, g\, (R/r)^2$

centrifugal force $F_c = m\, r\, \omega^2$

m: mass of the satellite

R: radius of the earth (R = 6370 km)

r: distance to the center of the earth

g: acceleration of gravity ($g = 9.81\ m/s^2$)
ω: angular velocity ($\omega = 2\pi f$, f: rotation frequency)

Orbits

Four different types of satellite orbits can be identified depending on the shape and diameter of the orbit

GEO: (Geostationary Orbit):36000 km above earth surface

LEO (Low Earth Orbit): 500 -1500 km

MEO (Medium Earth Orbit) or ICO (Intermediate Circular Orbit):6000 -20000 km

HEO (Highly Elliptical Orbit):elliptical orbits

Geostationary satellites

Orbit 35.786 km distance to earth surface, orbit in equatorial plane (inclination 0°)

complete rotation exactly one day, satellite is synchronous to earth rotation

fix antenna positions, no adjusting necessary

satellites typically have a large footprint (up to 34% of earth surface!), therefore difficult to reuse frequencies

bad elevations in areas with latitude above 60° due to fixed position above the equator

high transmit power needed

high latency due to long distance (ca. 275 ms)

not useful for global coverage for small mobile phones and data transmission, typically used for radio and TV transmission

LEO systems

Orbit 500 -1500 km above earth surface

visibility of a satellite 10 -40 minutes

global radio coverage possible

latency comparable with terrestrial long distance connections, 5 - 10 ms

smaller footprints, better frequency reuse

handover necessary from one satellite to another

many satellites necessary for global coverage

more complex systems due to moving satellites

MEO systems

Orbit ca. 5000 -12000 km above earth surface comparison with LEO systems:

slower moving satellites

less satellites needed

simpler system design

for many connections no hand-over needed

higher latency, 70 -80 ms

higher sending power needed

special antennas for small footprints needed

Routing

One solution: inter satellite links (ISL)

reduced number of gateways needed

only one uplink and one downlink per direction needed for the connection of two mobile phones

Problems

more complex focusing of antennas between satellites

high system complexity due to moving parts

higher fuel consumption

Thus shorter lifetime

Localization of mobile stations

Mechanisms similar to GSM Gateways maintain registers with user data

HLR (Home Location Register): static user data
VLR (Visitor Location Register): (last known) location of the mobile station

SUMR (Satellite User Mapping Register):

satellite assigned to a mobile station

positions of all satellites

Registration of mobile stations

Localization of the mobile station via the satellite's position requesting user data from HLR

updating VLR and SUMR Calling a mobile station

localization using HLR/VLR similar to GSM

connection setup using the appropriate satellite

Handover in satellite systems

Several additional situations for handover in satellite systems compared to cellular terrestrial mobile phone networks caused by the movement of the satellites

Intra satellite handover

handover from one spot beam to another

mobile station still in the footprint of the satellite, but in another cell

Inter satellite handover

handover from one satellite to another satellite

mobile station leaves the footprint of one satellite

Gateway handover

Handover from one gateway to another

mobile station still in the footprint of a satellite, but gateway leaves the footprint

DAB: Digital Audio Broadcasting

Media access

COFDM (Coded Orthogonal Frequency Division Multiplex) SFN (Single Frequency Network)

192 to 1536 subcarrierswithin a 1.5 MHz frequency band

Frequencies

first phase: one out of 32 frequency blocks for terrestrial TV channels 5 to 12 (174 -230 MHz, 5A -12D)

second phase: one out of 9 frequency blocks in the L-band (1452-1467.5 MHz, LA -LI)

Sending power: 6.1 kW (VHF, Ø 120 km) or 4 kW (L-band, Ø 30 km)

Date-rates: 2.304 Mbit/s (net 1.2 to 1.536 Mbit/s)

Modulation: Differential 4-phase modulation (D-QPSK)

Audio channels per frequency block: typ. 6, max. 192 kbit/s

Digital services: 0.6 -16 kbit/s (PAD), 24 kbit/s (NPAD)

DAB transport mechanisms

MSC (Main Service Channel)

carries all user data (audio, multimedia, ...)

consists of CIF (Common Interleaved Frames)

each CIF 55296 bit, every 24 ms (depends on transmission mode) CIF contains CU (Capacity Units), 64 bit each

FIC (Fast Information Channel)

arries control information

consists of FIB (Fast Information Block)

each FIB 256 bit (incl. 16 bit checksum)

defines configuration and content of MSC

Audio coding

Goal

audio transmission almost with CD quality

robust against multipath propagation

minimal distortion of audio signals during signal fading

Mechanisms

fully digital audio signals (PCM, 16 Bit, 48 kHz, stereo)

MPEG compression of audio signals, compression ratio 1:10 redundancy bits for error detection and correction

burst errors typical for radio transmissions, therefore signal interleaving -receivers can now correct single bit errors resulting from interference

low symbol-rate, many symbols

transmission of digital data using long symbol sequences, separated by guard spaces

delayed symbols, e.g., reflection, still remain within the guardspace

Digital Video Broadcasting

1991 foundation of the ELG (European Launching Group) goal: development of digital television in Europe

1993 renaming into DVB (Digital Video Broadcasting) goal: introduction of digital television based on

satellite transmission

cable network technology

later also terrestrial transmission

UNIT IV

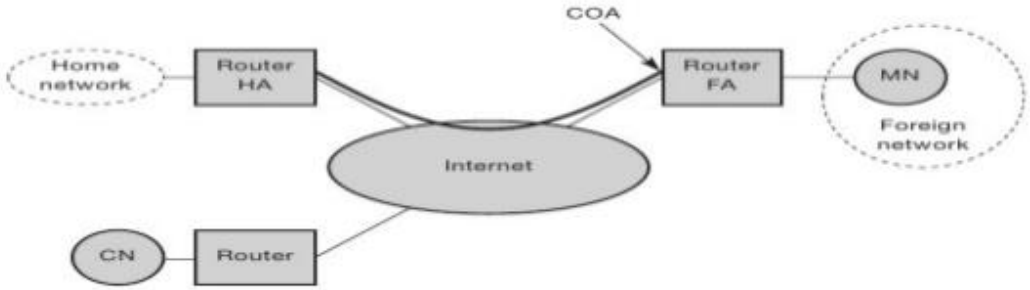
Mobile Network Layer:

Mobile Network Layer. ... It provides protocol enhancement that allows transparent routing of IP datagrams to **mobile** nodes in the internet. **Mobile** IP – Adds mobility support to the internet **network layer** protocol IP. RFC 2002 is a reference document for the complete detail about the **mobile** IP

Introduction

- In this protocols and mechanisms ***developed for the network layer*** to support mobility.
- It provides ***protocol enhancement*** that allows transparent ***routing of IP datagrams to mobile nodes in the internet***.
- **Mobile IP** – ***Adds mobility support to the internet network*** layer protocol IP.
- RFC 2002 is a reference document for the complete detail about the mobile IP.

Entities and Terminology



- **Mobile Nodes** – a host or router that ***changes its point of attachment*** from one network or subnetwork to another.
  - Mobile node change its location ***without changing its IP address***.
- **Home Agent** – a router on a mobile node's ***home network which tunnels datagrams for delivery to the mobile node*** when it is away from home.
  - Also, maintain ***current location information*** for the mobile node.
- **Foreign Agent** – router on a mobile node's visited network which provides ***routing services to the mobile node while registered***.
  - It ***detunnel and deliver the datagram*** to the mobile node that were tunneled by the mobile node's home agent

Goals, Assumptions and Requirements

- Receving of IP datagram after leaving your home network.
- Now nodes needs a so-called topologically correct address.

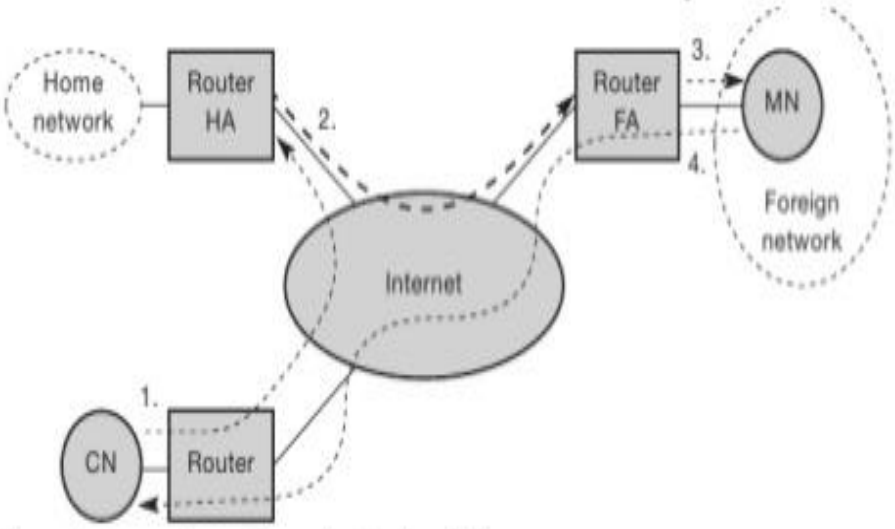
  Quick Solution

  - Assign new IP address when enter into new location.
    - Increase ***problem with higher layer protocols like TCP*** , as they rely on IP layer.
    - Routers are ***built for fast forwarding but not for fast update*** of routing table.
  - Quick solution not working.

Entities and Terminology(Cont.)

- **Correspondent Node (CN)** – ***partner through which MN is connected***. It can be a fixed or mobile node.
- **Home network** – it is ***subnet the MN belongs*** to.
- **Foreign network** – it is a ***current subnet the MN visits*** and which is not a home network.
- **Care-of Address** – it ***defines the current location of the MN*** from an IP point of view.
  - All the packets sent to the MN are ***delivered to the COA***,not directly to the IP address of the MN
  - Marks the ***tunnel endpoint*** (i.e address where packets exit the tunnel)
  - Location of COA:-
    - **Foreign agent COA** – COA could be ***located at the FA***, i.e COA is an IP address of the FA.
    - **Co-located COA** – if the MN ***temporarily acquired an additional IP address*** which acts a COA.This address is topologically correct , and the tunnel endpoint is at MN.

IP packet delivery



- CN wants to send an IP packet to the MN.
- Internet , not having info on the current location of MN, ***routes the packet to the router(Home Agent)*** responsible for the home network of MN.
- ***HA now intercept*** the packet(to find current location)
- Not found in home n/w then encapsulated and tunnelled to the COA.
- A ***new header put in front of the old header*** showing the (FA) COA as the new destination.
- ***FA now decapsulates*** the packets (remove additional header)
- Last, ***MN sends*** the packets as usual with its own ***fixed IP address as source*** and ***CN's address as the destination***.

Agent Discovery

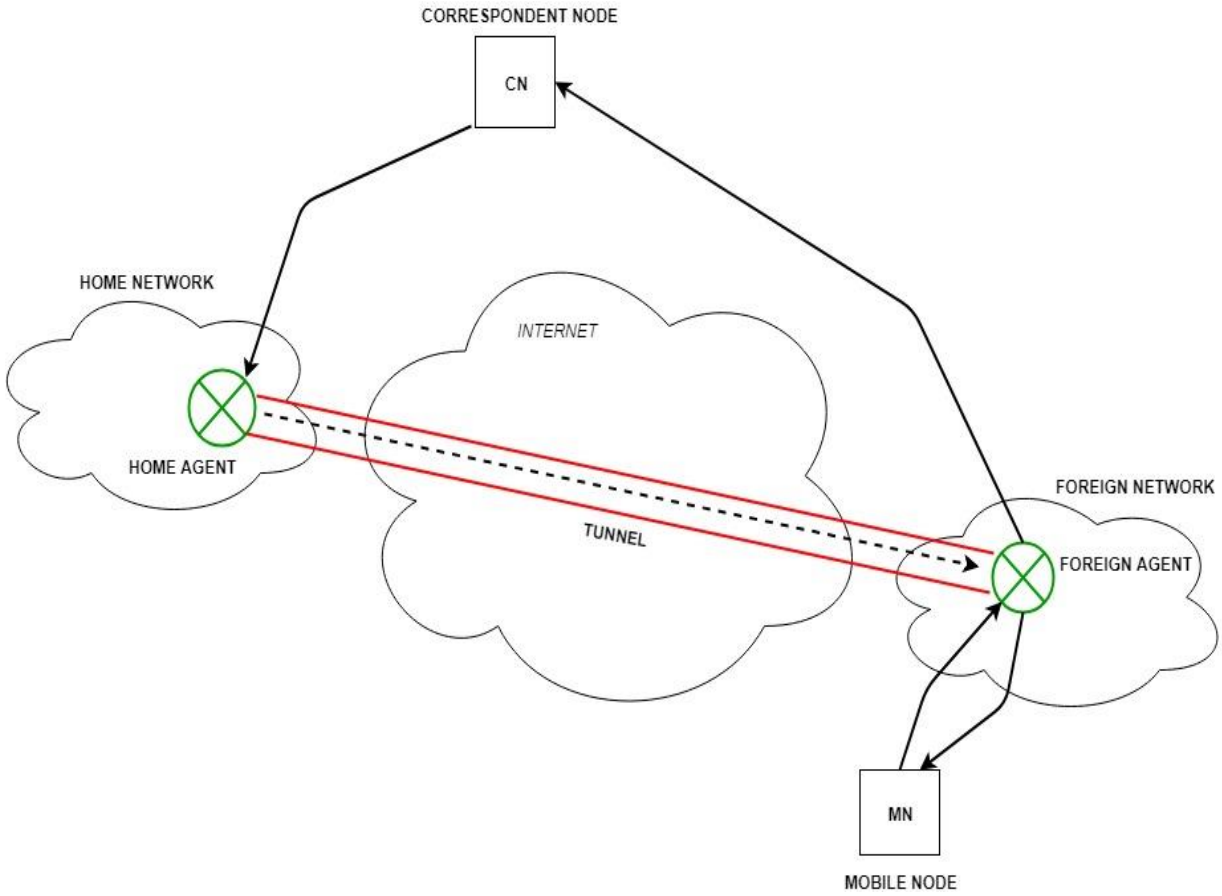
- One initial problem of an MN after moving is ***how to find a foreign agent ?***.
- Two types of methods:
  - **Agent advertisement** – in this HA and FA advertise their presence.
  - **Agent solicitation** – the mobile node send agent solicitations messages.

MOBILE IP:

Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without user's sessions or connections being dropped.

Terminologies:

- **Mobile Node (MN):**
  It is the hand-held communication device that the user caries e.g. Cell phone.
- **Home Network:**
  It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).
- **Home Agent (HA):**
  It is a router in home network to which the mobile node was originally connected
- **Home Address:**
  It is the permanent IP address assigned to the mobile node (within its home network).
- **Foreign Network:**
  It is the current network to which the mobile node is visiting (away from its home network).
- **Foreign Agent (FA):**
  It is a router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.
- **Correspondent Node (CN):**
  It is a device on the internet communicating to the mobile node.
- **Care of Address (COA):**
  It is the temporary address used by a mobile node while it is moving away from its home network.



Tunneling and encapsulation:

Tunneling: It establishes a virtual pipe for the packets available between a **tunnel** entry and an endpoint. It is the process of sending a packet via a **tunnel** and it is achieved by a mechanism called **encapsulation**. It takes place to forward an IP datagram from the home agent to the care-of-address.

Tunnelling and encapsulation

![A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved by using encapsulation

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. The reverse operation, taking a packet out of the data part of another packet, is

called de-capsulation. Encapsulation and de-capsulation are the operations typically performed when a packet is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively.The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header so that the packet is routed to the COA.The new header is called outer header.][1]

Types of Encapsulation Three types of encapsulation protocols are specified for Mobile IP:

1. **IP-in-IP encapsulation:** required to be supported. Full IP header added to the original IP packet. The new header contains HA address as source and Care of Address as destination.
2. **Minimal encapsulation:** optional. Requires less overhead but requires changes to the original header. Destination address is changed to Care of Address and Source IP address is maintained as is.
3. **Generic Routing Encapsulation (GRE):** optional. Allows packets of a different protocol suite to be encapsulated by another protocol suite.

Optimization:

Mobile IPv4 route optimization [11] is a proposed extension to the Mobile IPv4 protocol. It provides enhancements to the routing of datagrams between the mobile node and to the correspondent node. The enhancements provide means for a correspondent node to tunnel datagrams directly to the mobile node or to its foreign agent care-of address.

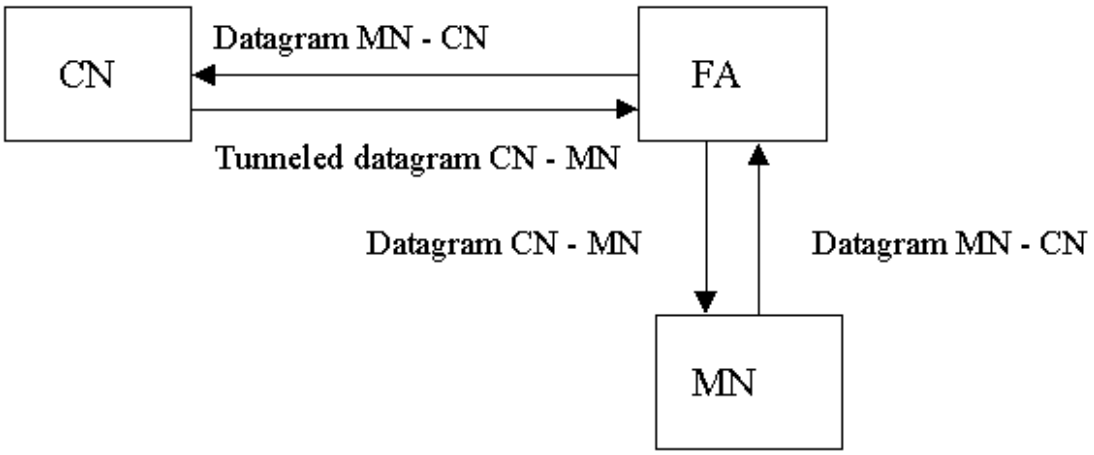
4.1 Route optimization messages and data structures

The route optimization extension adds a conceptual data structure, the binding cache, to the correspondent node and to the foreign agent. The binding cache contains bindings for mobile nodes' home addresses and their current care-of addresses. With the binding the correspondent node can tunnel datagrams directly to the mobile node's care-of address.

Every time the home agent receives a datagram that is destined to a mobile node currently away from home, it sends a binding update to the

correspondent node to update the information in the correspondent node's binding cache. After this the correspondent node can directly tunnel packets to the mobile node. Thus direct bi-directional communication is achieved with route optimization, as shown in Figure 3.

Figure 3. Direct routing with route optimization and foreign agent care-of address.

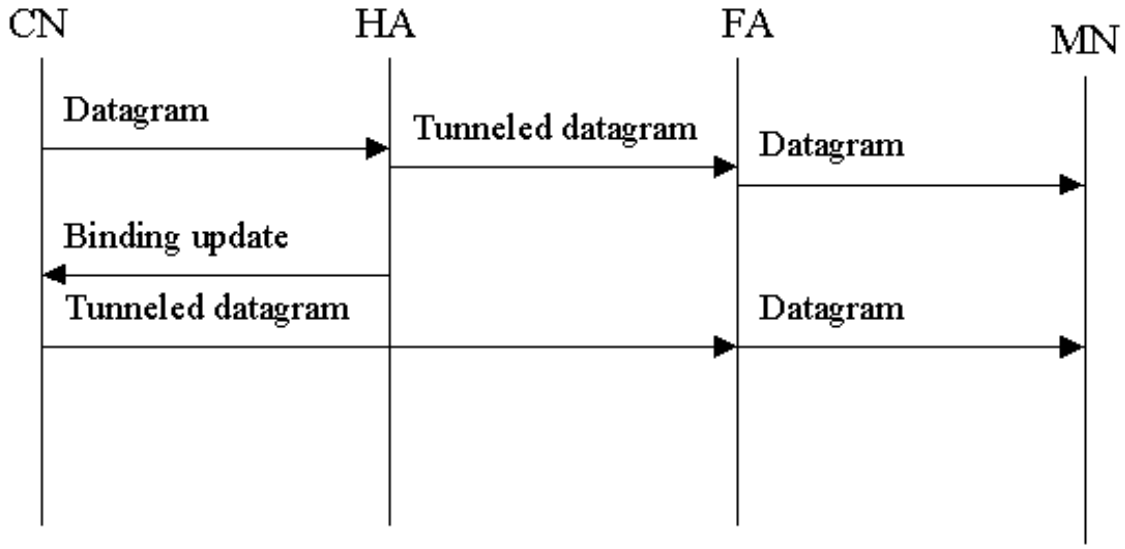


Route optimization adds four new UDP-messages to the Mobile IPv4 protocol:

- Binding update informs the correspondent node or foreign agent of the mobile node's new location. It is sent by the home agent or in the case of previous foreign agent notification, by the new foreign agent, as shown in Figure 4. The binding update contains the care-of address and the home address of the mobile node and also the lifetime of the binding. It also must contain a mobile IP authentication extension. An identification number may also be present to provide a way of matching updates with acknowledgements and to protect against replay attacks.
- Binding acknowledgement is sent by the correspondent node or the foreign agent in response to the binding update. It contains the mobile node's home address and a status code. It also contains an identification number, if there was one in the corresponding binding update.

- Binding request is sent by the correspondent node to the home agent to request a binding update. It contains the home address of the queried mobile node and possibly an identification number.
- Binding warning is sent by the previous foreign agent in response to receiving a tunneled datagram for a mobile node for which it has a binding and for which it is not acting as the current foreign agent. The binding warning is sent to the home agent. It contains the home address of the mobile node and the address of the correspondent node that does not have up to date information of the mobile node's current care-of address. With this information the home agent can send a binding update to the correspondent node.

Figure 4. Binding update to correspondent node



4.2 The effect on static routes

As the correspondent node learns the care-of address of the mobile node from the binding update, it can tunnel datagrams directly to the mobile node's care-of address [11]. Thus only the first datagrams are routed via the home agent. This reduces the network load and also reduces the delays caused by routing. Thus the optimization is valuable to mobile nodes that visit networks located far from their home agent.

However, the overhead caused by tunneling is not decreased. The correspondent node's use of minimal encapsulation [10] is a partial remedy, if both the encapsulator and the decapsulator support it. Ingress filtering [3]

may also prevent the mobile node from sending datagrams directly to the correspondent node. The use of direct reverse tunneling from the care-of address to the correspondent node's address is a possible solution to ingress filtering. However, it is not possible with foreign agent care-of addresses, since the current reverse tunneling standard [8] requires the foreign agent to tunnel all packets to the home agent of the mobile node.

4.3 Smooth handoffs with route optimization

In the static case the protocol is fairly simple, but handoffs somewhat complicate the situation. When the correspondent node has an out of date entry for the mobile node's care-of address it tries to send the tunneled datagram to the mobile node's previous location and the datagram is lost. To solve this problem the protocol includes the previous foreign agent notification mechanism, which adds a binding cache to the foreign agent. [3]

When a mobile node moves to a new subnetwork it sends a registration request to the new foreign agent. The registration request may contain a previous foreign agent notification extension. Upon receiving such a request the foreign agent builds a binding update and sends it to the previous foreign agent. The previous foreign agent can then, after authenticating the update, create a binding for the mobile node. With this binding it can re-tunnel datagrams to the mobile node's new care-of address. The re-tunneling requires foreign agent care-of addresses in order for the agents to act as tunnel endpoints. [3]

The previous foreign agent notification mechanism provides temporary localization of the handoffs. It does not reduce the signaling load between the home agent and the mobile node, but reduces the number of datagrams lost due to correspondent nodes with out-of date bindings.

4.4 Security considerations

Since the correspondent nodes and foreign agents have binding caches, which change the routing of datagrams destined to mobile nodes, the binding updates must be authenticated. The authentication is performed in a similar manner as in base Mobile IPv4. All binding updates contain a route optimization or smooth handoff authentication extension. This extension contains a hash, which is calculated from the datagram and the shared secret. [11]

The correspondent node and the mobile node's home agent need a security association [5]. This association is used for the authentication of the binding updates. Since the mobile node sends a binding update directly to its previous foreign agent, they also need a security association. If the security associations are not preconfigured they can be established via a key management protocol such as ISAKMP [6] or SKIP [7]. [11]

4.5 General deployment requirements

In order to make use of the binding updates the correspondent nodes must be able to process and authenticate them and be able to encapsulate datagrams [11]. To establish this the network stacks of the operating systems require changes. Since correspondent nodes need to establish a security association with the home agent and foreign agents need to establish one with the mobile node, a widely deployed key management system is obviously needed. Otherwise only nodes with statically configured security associations can benefit from the binding updates.

Dynamic host configuration protocol:

Dynamic Host Configuration Protocol. **Dynamic Host Configuration Protocol** (**DHCP**) is a **network** management **protocol** used to dynamically assign an **IP** address to nay device, or node, on a **network** so they can communicate using **IP** (Internet **Protocol**). **DHCP** automates and centrally manages these configurations.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows:

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.

- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

There are following benefits of DHCP:

Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

Ad hoc Networks:

Wireless mobile ad hoc networks are self-configuring, dynamic **networks** in which nodes are free to move. ... MANETs usually have a routable **networking** environment on top of a Link **Layer ad hoc network**. MANETs consist of a peer-to-peer, self-forming, self-healing **network**.

MANET stands for Mobile adhoc Network also called as wireless adhoc network or adhoc wireless network that usually has a routable networking environment on top of a Link Layer ad hoc network.. They consist of set of mobile nodes connected wirelessly in a self configured, self healing network without having a fixed infrastructure. MANET nodes are free to move randomly as the network topology changes frequently. Each node behave as a router as they forward traffic to other specified node in the network.

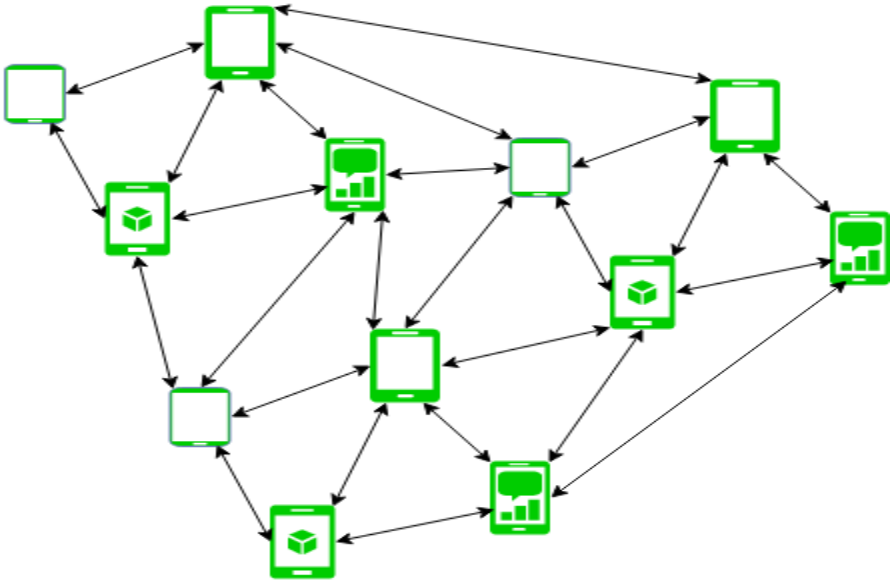


Figure - Mobile Ad Hoc Network

MANET may operate as standalone fashion or they can be the part of larger internet. They form highly dynamic autonomous topology with the presence of one or multiple different transceivers between nodes. The main challenge for the MANET is to equipped each devices to continuously maintain the information required to properly route traffic. MANETs consist of a peer-to-peer, self-forming, self-healing network MANET's circa 2000-2015 typically communicate at radio frequencies (30MHz-5GHz). This can be used in road safety, ranging from sensors for environment, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, etc.

Characteristics of MANET –

- **Dynamic Topologies:** Network topology which is typically multihops, may change randomly and rapidly with time, it can form unidirectional or bi-directional links.
- **Bandwidth constrained, variable capacity links:** Wireless links usually have lower reliability, efficiency, stability and capacity as compared to wired network.The throughput of wireless communication is even less than a radio's maximum transmission rate after dealing with the constraints like multiple access, noise, interference conditions, etc.
- **Autonomous Behavior:** Each nodes can act as a host and router, which shows its autonomous behavior.
- **Energy Constrained Operation:** As some or all the nodes rely on batteries or other exhaustible means for their energy.Mobile nodes are characterized with less memory, power and light weight features.
- **Limited Security:** Wireless network are more prone to security threats. A centralized firewall is absent due to its destributed nature of operation for security, routing and host configuration.
- **Less Human Intervention:** They require minimum human intervention to configure the network, therefore they are dynamically autonomous in nature.

Pros and Cons of MANET –

Pros:

1. Seperation from central network administration.
2. Each nodes can play both the roles ie. of router and host showing autonomous nature.
3. Self configuring and self healing nodes, does not require human intervention.

Cons:

1. Resources are limited due to various constraints like noise, interference conditions, etc.
2. Lack of authorization facilities.
3. More prone to attacks due to limited physical security.

Routing

Differences between wired n/w and ad-hoc n/w

- **Asymmetric link** – signal quality uneven in both direction of the link.
- **Redundant links** – wired n/w have few redundant links while ad-hoc will have many redundant links.
- **Interference** – it is very high in case of wireless ad-hoc n/w
- **Dynamic topology** – change in topology is very frequent which affects the routing table and routing methods.

DSDV Routing

- **D**estination **S**equence **D**istance **V**ector is an enhancement to ditance vector routing for ad-hoc network.
- **Distance Vector** – exchange distance vector to its neighbors for all destination.
- Problem with DV is the cout-to-infinity.
- DSDV adds two things to the DV
  - **Sequence No.** - each routing adv. comes with a seq. no. Seq. no. help to ***apply the advertisement in correct order.***
  - ***Damping*** – ***Transient change in topology*** that re of short duration should not destabilize the routing mechanisms.

DSDV Routing

- If the ***sequence number*** of one node in the ***newly received same as the corresponding sequence number*** in the routing table , then the ***metric will be compared*** and the route with ***the smallest metric will be used.***

DSDV Example

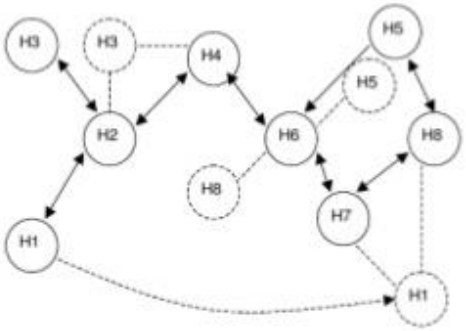
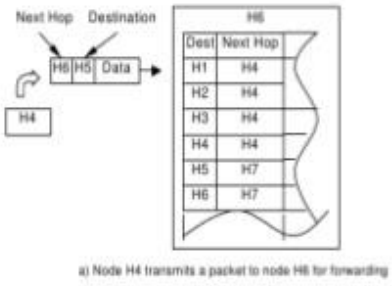
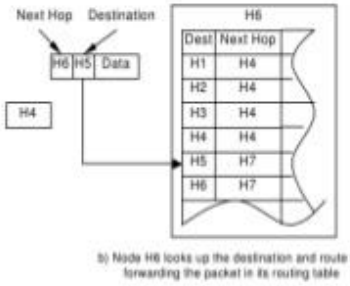


Table 1: The routing table of node H6 at one instant [7]

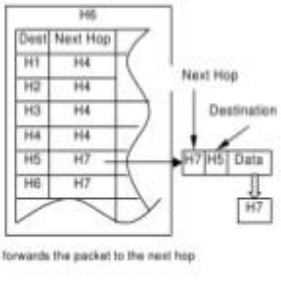
Dest	Next Hop	Metric	Seq.No.	Install
H1	H4	3	S406_H1	T001_H6
H2	H4	2	S128_H2	T001_H6
H3	H4	3	S564_H3	T001_H6
H4	H4	1	S710_H4	T002_H6
H5	H7	3	S392_H5	T001_H6
H6	H6	0	S076_H6	T001_H6
H7	H7	1	S128_H7	T002_H6
H8	H7	2	S050_H8	T002_H6



a) Node H4 transmits a packet to node H6 for forwarding



b) Node H6 looks up the destination and route for forwarding the packet in its routing table



a) Node H6 forwards the packet to the next hop

Dynamic source Routing:

DSR

- **D**ynamic **S**ource **R**outing

  Problem associated with DSDV

- Previous routing exchange routing information with all nodes , although currently their may be no data to exchange.
- Cause unnecessary traffic and consumes more battery power.
- DSR , divides the task into two :-
  - **Route discovery** – a node ***only discover*** route to a destination **want to send somthing** to this destination.
  - **Route maintenance** – if a node is continuously sending packet via a route, it has to ***make sure that the route is held upright***.
- DSR eliminates all periodic routing updates.

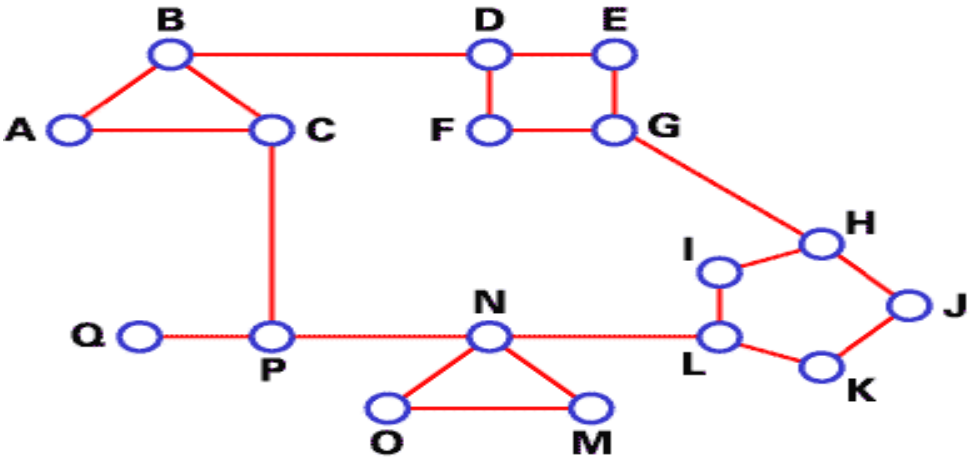
DSR

- If the node receive a route request:-
  - If the node has ***already received the request*** (which is identified using the unique identifier) , it drops the request packet.
  - If node recognizes its ***own address as the destination*** , the request has reached its target.
  - Otherwise, the ***node appends its own address*** to a list of traversed hops in the packets and broadcast this update request.
- Destination may ***receive several list containing*** different paths from the initiator.It could return the ***best path***, ***the first path*** or ***several path***.

Hierarchical Algorithm:

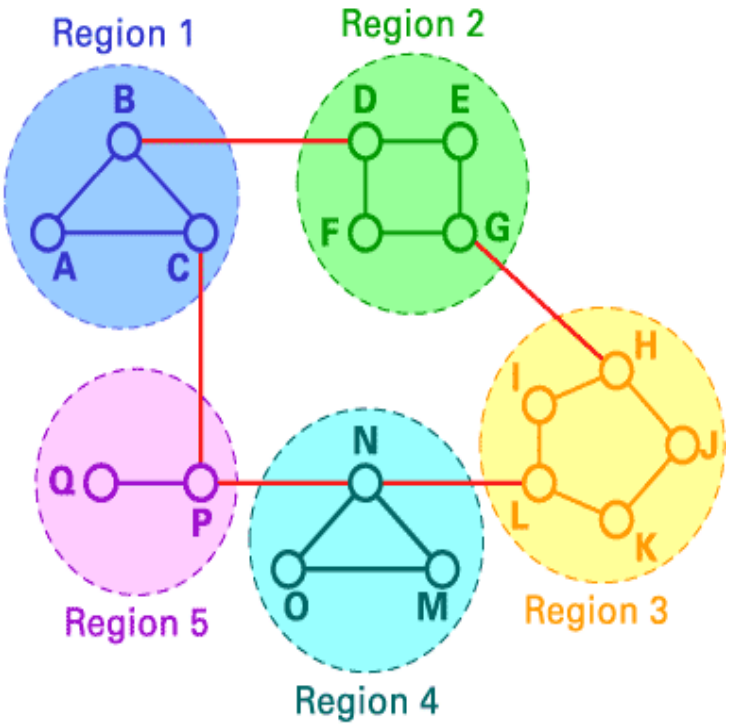
As you see, in both LS and DV algorithms, every router has to save some information about other routers. When the network size grows, the number of routers in the network increases. Consequently, the size of routing tables increases, as well, and routers can't handle network traffic as efficiently. We use **hierarchical routing** to overcome this problem. Let's examine this subject with an example:

We use DV algorithms to find best routes between nodes. In the situation depicted below, every node of the network has to save a routing table with 17 records. Here is a typical graph and routing table for A:



Destination	Line	Weight
A	---	---
B	B	1
C	C	1
D	B	2
E	B	3
F	B	3
G	B	4
H	B	5
I	C	5
J	C	6
K	C	5
L	C	4
M	C	4
N	C	3
O	C	4
P	C	2
Q	C	3

Network graph and A's routing table



Destination	Line	Weight
A	---	---
B	B	1
C	C	1
Region 2	B	2
Region 3	C	2
Region 4	C	3
Region 5	C	4

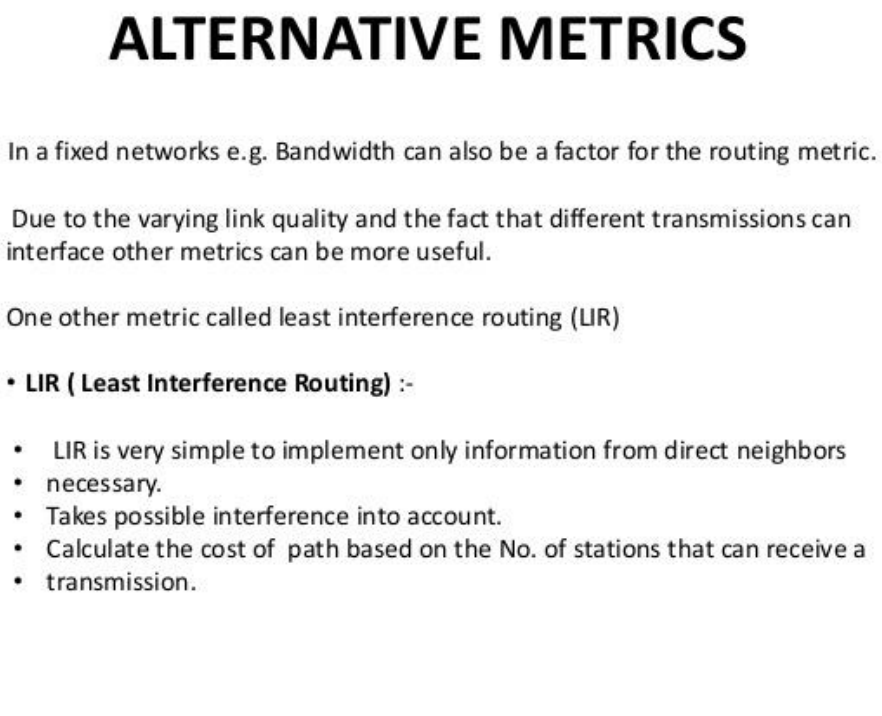
In hierarchical routing, routers are classified in groups known as **regions**. Each router has only the information about the routers in its own region and

has no information about routers in other regions. So routers just save one record in their table for every other region. In this example, we have classified our network into five regions (see below).

If A wants to send packets to any router in region 2 (D, E, F or G), it sends them to B, and so on. As you can see, in this type of routing, the tables can be summarized, so network efficiency improves. The above example shows two-level hierarchical routing. We can also use three- or four-level hierarchical routing.

In three-level hierarchical routing, the network is classified into a number of **clusters**. Each cluster is made up of a number of regions, and each region contains a number or routers. Hierarchical routing is widely used in Internet routing and makes use of several routing protocols.

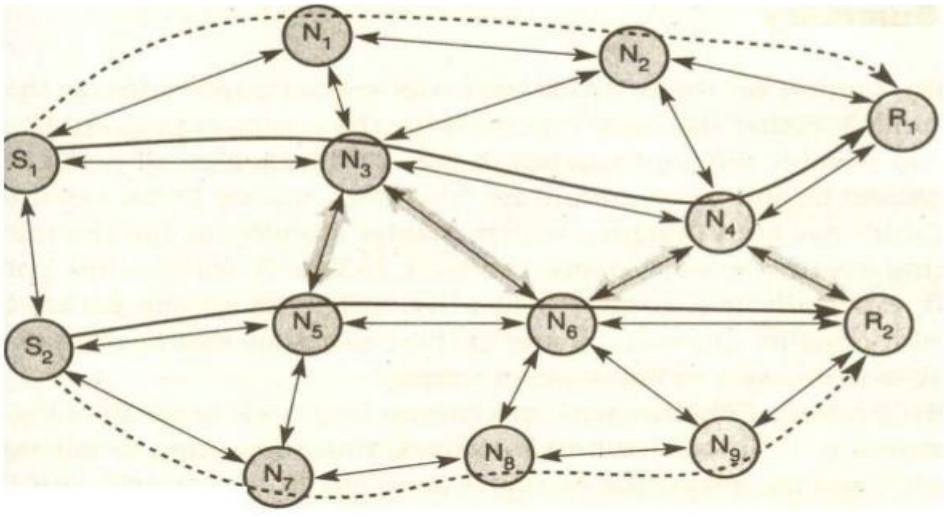
Alternative Metrics:



- MMRCR:- (Max-Min Residual Capacity routing)
-
- Calculate the cost of path based on a probability function of successful;
- transmissions and interference.

LRR (Least Resistance Routing)

- Calculate the cost of path based on interference, jamming & other
- transmissions.



File systems – Motivation

Goal

• efficient and transparent access to shared files within a mobile environment while maintaining data consistency.

Problems

• limited resources of mobile computers (memory, CPU, ...)
• low bandwidth, variable bandwidth, temporary disconnection
• high heterogeneity of hardware and software components (no standard PC architecture)
• wireless network resources and mobile computer are not very reliable
• standard file systems (e.g., NFS, network file system) are very inefficient, almost unusable

Solutions

• replication of data (copying, cloning, caching)
• data collection in advance (hoarding, pre-fetching)

UNIT –V

Mobile Transport Layer:

The **transport layer** is the **layer** in the open system interconnection (OSI) model responsible for end-to-end communication over a network. It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.

Traditional TCP:

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite, often simply referred to as TCP/IP. TCP is reliable, guarantees in-order delivery of data and incorporates congestion control and flow control mechanisms. TCP supports many of the Internet's most popular application protocols and resulting applications, including the World Wide Web, e-mail, File Transfer Protocol and Secure Shell. In the Internet protocol suite, TCP is the intermediate layer between the Internet layer and application layer.

The major responsibilities of TCP in an active session are to:

• Provide reliable in-order transport of data: to not allow losses of data.

• Control congestions in the networks: to not allow degradation of the network performance,

• Control a packet flow between the transmitter and the receiver: to not exceed the receiver's capacity.

Congestion Control:

A transport layer protocol such as TCP has been designed for fixed networks with fixed end- systems. Congestion may appear from time to time even in carefully designed networks. The packet buffers of a router are filled and the router cannot forward the packets fast enough because the sum of the input rates of packets destined for one output link is higher than the capacity of the output link. The only thing a router can do in this situation is to drop packets.

A dropped packet is lost for the transmission, and the receiver notices a gap in the packet stream. Now the receiver does not directly tell the sender which packet is missing, but continues to acknowledge all in sequence packets up to the missing one. The sender notices the missing acknowledgement for the lost packet and assumes a packet loss due to congestion. Retransmitting the missing packet and continuing at full sending rate would now be unwise, as this might only increase the congestion. To mitigate congestion, TCP slows down the transmission rate dramatically. All other TCP connections experiencing the same congestion do exactly the same so the congestion is soon resolved.

Slow Start:

TCP's reaction to a missing acknowledgement is quite drastic, but it is necessary to get rid of congestion quickly. The behavior TCP shows after the detection of congestion is called slow start. The sender always calculates a congestion window for a receiver. The start size of the congestion window is one segment (TCP packet). The sender sends one packet and waits for acknowledgement. If this acknowledgement arrives, the sender increases the congestion window by one, now sending two packets (congestion window = 2).

This scheme doubles the congestion window every time the acknowledgements come back, which takes one round trip time (RTT). This is called the exponential growth of the congestion window in the slow start mechanism. But doubling the congestion window is too dangerous. The exponential growth stops at the congestion threshold. As soon as the congestion window reaches the congestion threshold, further increase of the transmission rate is only linear by adding 1 to the congestion window each time the acknowledgements come back.

The congestion window itself is set to one segment and the sender starts sending a single segment. The exponential growth starts once more up to the new congestion threshold, then the window grows in linear fashion.

Fast retransmit/fast recovery:

The congestion threshold can be reduced because of two reasons. First one is if the sender receives continuous acknowledgements for the

same packet. It informs the sender that the receiver has got all the packets up to the acknowledged packet in the sequence and also the receiver is receiving something continuously from the sender. The gap in the packet stream is not due to congestion, but a simple packet loss due to a transmission error. The sender can now retransmit the missing packet(s) before the timer expires. This behavior is called fast retransmit. It is an early enhancement for preventing slow-start to trigger on losses not caused by congestion.

The receipt of acknowledgements shows that there is no congestion to justify a slow start. The sender can continue with the current congestion window. The sender performs a fast recovery from the packet loss. This mechanism can improve the efficiency of TCP dramatically. The other reason for activating slow start is a time-out due to a missing acknowledgement. TCP using fast retransmit/fast recovery interprets this congestion in the network and activates the slow start mechanism.

The advantage of this method is its simplicity. Minor changes in the MH's software results in performance increase. No changes are required in FA or CH.

- The disadvantage of this scheme is insufficient isolation of packet losses. It mainly focuses on problems regarding Handover.
- Also it effects the efficiency when a CH transmits already delivered packets.

Implication on mobility:

- Slow Start mechanism in fixed networks decreases the efficiency of TCP if used with mobile receivers or senders.
- Error rates on wireless links are orders of magnitude higher compared to fixed fiber or copper links. This makes compensation for packet loss by TCP quite difficult.
- Mobility itself can cause packet loss. There are many situations where a soft handover from one access point to another is not possible for a mobile end-system.
- Standard TCP reacts with slow start if acknowledgements are missing, which does not help in the case of transmission

errors over wireless links and which does not really help during handover.

- This behavior results in a severe performance degradation of an unchanged TCP if used together with wireless links or mobile nodes

Indirect TCP:

Indirect TCP segments a TCP connection into a fixed part and a wireless part. The following figure shows an example with a mobile host connected via a wireless link and an access point to the 'wired' internet where the correspondent host resides.

Indirect TCP segments a TCP connection into a fixed part and a wireless part. The following figure shows an example with a mobile host connected via a wireless link and an access point to the 'wired' internet where the correspondent host resides.

Advantages of I-TCP

- No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
- Simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
    1. transmission errors on the wireless link do not propagate into the fixed network
    2. therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop s know
- It is always dangerous to introduce new mechanisms in a huge network without knowing exactly how they behave. New optimizations can be tested at the last hop, without jeopardizing the stability of the Internet.
- It is easy to use different protocols for wired and wireless networks.

Disadvantages of I-TCP

- Loss of end-to-end semantics:- an acknowledgement to a sender no longer means that a receiver really has received a packet, foreign agents might crash.

- Higher latency possible:- due to buffering of data within the foreign agent and forwarding to a new foreign agent
- Security issue:- The foreign agent must be a trusted entity

Snooping TCP:

The main drawback of I-TCP is the segmentation of the single TCP connection into two TCP connections, which loses the original end-to-end TCP semantic. A new enhancement, which leaves the TCP connection intact and is completely transparent, is Snooping TCP. The main function is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss.

Advantages of snooping TCP:

- The end-to-end TCP semantic is preserved.
- Most of the enhancements are done in the foreign agent itself which keeps correspondent host unchanged.
- Handover of state is not required as soon as the mobile host moves to another foreign agent. Even though packets are present in the buffer, time out at the CH occurs and the packets are transmitted to the new COA.
- No problem arises if the new foreign agent uses the enhancement or not. If not, the approach automatically falls back to the standard solution.

Disadvantages of snooping TCP

- Snooping TCP does not isolate the behavior of the wireless link as well as I -TCP. Transmission errors may propagate till CH.
- Using negative acknowledgements between the foreign agent and the mobile host assumes additional mechanisms on the mobile host. This approach is no longer transparent for arbitrary mobile hosts.
- Snooping and buffering data may be useless if certain encryption schemes are applied end-to end between the correspondent host and mobile host. If encryption is used above the transport layer, (eg. SSL/TLS), snooping TCP can be used.

Mobile TCP:

Both I-TCP and Snooping TCP does not help much, if a mobile host gets disconnected. The M-TCP (mobile TCP) approach has the same goals as I-TCP and snooping TCP: to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems. M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to end semantics of TCP, and to provide a more efficient handover. Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections. M-TCP splits the TCP connection into two parts as I-TCP does. An unmodified TCP is used on the standard host-supervisory host (SH) connection, while an optimized TCP is used on the SH-MH connection.

The SH monitors all packets sent to the MH and ACKs returned from the MH. If the SH does not receive an ACK for some time, it assumes that the MH is disconnected. It then chokes the sender by setting the sender's window size to 0. Setting the window size to 0 forces the sender to go into persistent mode, i.e., the state of the sender will not change no matter how long the receiver is disconnected. This means that the sender will not try to retransmit data. As soon as the SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value. The sender can continue sending at full speed. This mechanism does not require changes to the sender's TCP.

Advantages of M-TCP:

- It maintains the TCP end-to-end semantics. The SH does not send any ACK itself but forwards the ACKs from the MH.
- If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0.
- As no buffering is done as in I-TCP, there is no need to forward buffers to a new SH. Lost packets will be automatically retransmitted to the SH.

Disadvantages of M-TCP:

- As the SH does not act as proxy as in I-TCP, packet loss on the wireless link due to bit errors is propagated to the sender. M-TCP assumes low bit error rates, which is not always a valid assumption.
- A modified TCP on the wireless link not only requires modifications to the MH protocol software but also new network elements like the bandwidth manager.

Transmission/time-out freezing:

Often, MAC layer notices connection problems even before the connection is actually interrupted from a TCP point of view and also knows the real reason for the interruption. The MAC layer can inform the TCP layer of an upcoming loss of connection or that the current interruption is not caused by congestion. TCP can now stop sending and 'freezes' the current state of its congestion window and further timers. If the MAC layer notices the upcoming interruption early enough, both the mobile and correspondent host can be informed. With a fast interruption of the wireless link, additional mechanisms in the access point are needed to inform the correspondent host of the reason for interruption. Otherwise, the correspondent host goes into slow start assuming congestion and finally breaks the connection.

As soon as the MAC layer detects connectivity again, it signals TCP that it can resume operation at exactly the same point where it had been forced to stop. For TCP time simply does not advance, so no timers expire.

Advantages:

- It offers a way to resume TCP connections even after long interruptions of the connection.
- It can be used together with encrypted data as it is independent of other TCP mechanisms such as sequence no or acknowledgements

Disadvantages:

- Lots of changes have to be made in software of MH, CH and FA.

Selective retransmission:

A very useful extension of TCP is the use of selective retransmission. TCP acknowledgements are cumulative, i.e., they acknowledge in-order receipt of packets up to a certain packet. A single acknowledgement confirms reception of all packets upto a certain packet. If a single packet is lost, the sender has to retransmit everything starting from the lost packet (go-back-n retransmission). This obviously wastes bandwidth, not just in the case of a mobile network, but for any network.

Using selective retransmission, TCP can indirectly request a selective retransmission of packets. The receiver can acknowledge single packets, not only trains of in-sequence packets. The sender can now determine precisely which packet is needed and can retransmit it. The advantage of this approach is obvious: a sender retransmits only the lost packets. This lowers bandwidth requirements and is extremely helpful in slow wireless links. The disadvantage is that a more complex software on the receiver side is needed. Also more buffer space is needed to resequence data and to wait for gaps to be filled.

Transaction-oriented TCP:

Assume an application running on the mobile host that sends a short request to a server from time to time, which responds with a short message and it requires reliable TCP transport of the packets. For it to use normal TCP, it is inefficient because of the overhead involved. Standard TCP is made up of three phases: setup, data transfer and release. First, TCP uses a three-way handshake to establish the connection. At least one additional packet is usually needed for transmission of the request, and requires three more packets to close the connection via a three-way handshake. So, for sending one data packet, TCP may need seven packets altogether. This kind of overhead is acceptable for long sessions in fixed networks, but is quite inefficient for short messages or sessions in wireless networks. This led to the development of transaction-oriented TCP (T/TCP).

T/TCP can combine packets for connection establishment and connection release with user data packets. This can reduce the number of packets down to two instead of seven. The obvious advantage for certain applications is the reduction in the overhead which standard TCP has for connection setup and connection release. Disadvantage is that it requires changes in the software in mobile host

Wireless Application Protocol(WAP) : Introduction

- **Wireless Application Protocol is a programming model which is made on the concept of World Wide Web(WWW) programming model and the hierarchical design is somehow similar to TCP/IP protocol stack design.**
- **WAP is a standard which enables the mobile devices to interact, exchange and transmit information over the internet. It is a De-Facto standard.**
- **As, WAP is based upon the concept of World Wide Web, the backend functioning also remains similar i.e. HTML is used on WWW and Wireless Mark-up Language(WML) is used in WAP for using the WAP services.**
- **Since the WAP model is developed, it is accepted as a wireless protocol globally that is capable of working on multiple wireless technology such as mobile, printers, pagers etc.**
- **Another reason for opting and making WAP as De-Facto standard was its ability of creating web applications for mobile devices.**

Wireless Application Protocol Model : Working

- **WAP model comprises of 3-Levels that are : Client, Gateway and Origin Server.**
- **The WAP user agent sends a request via mobile to WAP gateway by using encoded WAP protocol i.e. called as encoding request.**
- **The encoding request is translated through WAP gateway and is further forwarded in the form of HTTP request to the server side where scripts are available.**
- **Response from the scripts and content is picked up as requested, through HTTP and is forwarded to the WAP gateway once again.**
- **The required HTTP response is then forwarded in decode format to the client protocol stack as the final response for the initial request made by client.**

Advantages : Wireless Application Protocol

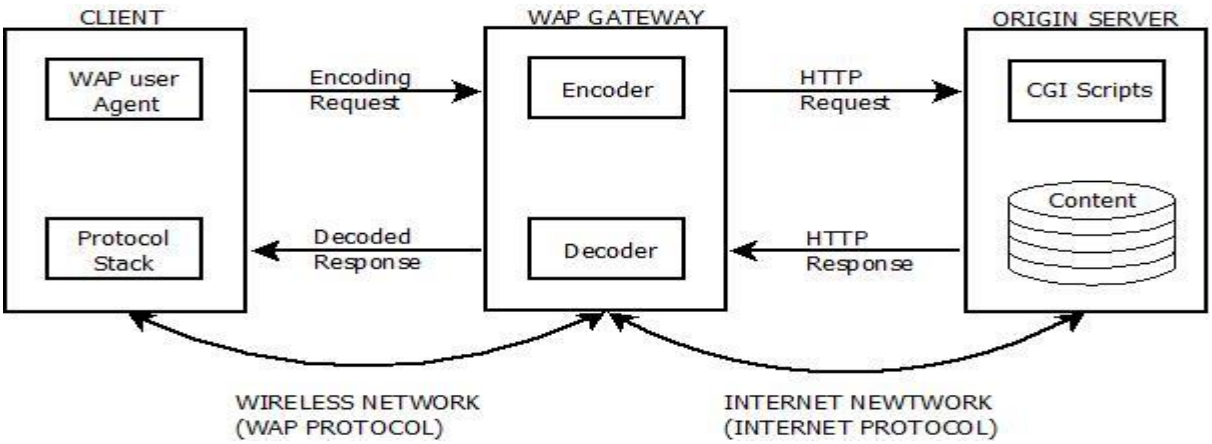
- **Fast paced technology.**
- **Open source-Free.**
- **Can be implemented on multiple platform.**
- **Independent of network standard.**
- **Higher controlling options.**

Disadvantages : Wireless Application Protocol

- **Fast Paced Technology**
- **Less Secured.**
- **User interface(UI) is small.**
- **Less availability.**

Applications : Wireless Application Protocol

- **E-mails access.**
- **Weather forecasting.**
- **Flight information.**
- **Movie & cinema information.**
- **Traffic updates.**


CLIENT
WAP user Agent
Protocol Stack
Encoding Request
Decoded Response
WAP GATEWAY
Encoder
Decoder
HTTP Request
HTTP Response
ORIGIN SERVER
CGI Scripts
Content
WIRELESS NETWORK
(WAP PROTOCOL)
INTERNET NEWTWORK
(INTERNET PROTOCOL)