DHANALAKSHMI SRINIVASAN ENGINEERING COLLEGE
PERAMBALUR-621212

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

EC6802-WIRELESS NETWORKS
UNIT I

1. State the significance of radio transmission over infrared(Apr/May 17)

Infrared light transmission is one of the important technologies used in wireless LAN. It is based on the transmission of infrared light at 900 nm wavelength.Infrared technology uses diffuse light reflected at walls, furniture etc. Or directed light when line of
sight (LOS) exists between sender and receiver.

2. List out the applications of WLAN.

Transfer of medical images Remote access to patient records Remote monitoring of patients Remote diagnosis of patients at home or in an ambulance In telemedicine Surveillance Internet supporting database.

3. What is IEEE 802.11?

The IEEE 802.11 is the first WLAN standard that has secured the market in large extent. The primary goal of the standard was the specification of a simple and robust that offers time bounded and asynchronous services.

4.Give any two requirements of HIPERLAN. Nov/Dec 2015)

- Data rates of 23.529 Mbps
- Multi-hop and Ad-hoc networking
- Support of time bounded services

5.What are the three phases in channel access in HIPERLAN-1?

- Prioritization phase
- Contention phase
- Transmission phase

6.What is meant by BRAN?

The BRAN (Broadband Radio Access Networks (BRAN) is standardized by the EuropeanTelecommunications Standards Institute (ETSI). Primary motivation of BRAN is the deregulationand privatization of the telecommunication sector. BRAN technology is independent from theprotocols of the fixed network. BRAN can be used for ATM and TCP/IP networks.

7.What is Bluetooth? Nov/Dec 2015)

Bluetooth is an inexpensive personal area Ad-hoc network operating in unlicensed bands and owned by the user. It is an open specification for short range wireless voice and data communications that was developed for cable replacement in PAN (Personal Area Network).

8.What is WIMAX?
WIMAX is the air interface for the actual radio interface network, where both fixed and mobilcan have access to the network. Its specification is IEEE 802.16.

9.What are the frequency bands of IEEE 802.16? The 802.16 standard defines a number of air interfaces that can be divided into,
10-66 GHz licensed band Below 11 GHz licensed bands Below 11 GHZ unlicensed bands

10. What is the need for WATM?
WATM systems had to be designed for transferring voice, classical data, video, multimedia etc.

PART B

1.Explain the architecture and reference model of HIPERLAN- 2 in detail(Nov/Dec2014) (Apr/May 2014) (Nov/Dec2015) (Apr/May 2015)

HIPERLAN/2 has a very high transmission rate up to 54 Mbit/s. This is achieved by making use of a modularization method called Orthogonal Frequency Digital Multiplexing (OFDM). OFDM is particularly efficient in time-dispersive environments, i.e. where the radio signals are reflected from many points

HIPERLAN/2 connections are time-division multiplexed and connection-oriented, either bidirectional point-to-point or unidirectional point-to-multipoint connections. There is also a dedicated broadcast channel through which the traffic from an AP reaches all terminals.

Physical Layer

The channeling is implemented by Orthogonal Frequency Division Multiplexing (OFDM) due to its excellent performance on highly dispersive channels. The basic idea of OFDM is to transmit broadband, high data rate information by dividing the data into several interleaved, parallel bit streams, and let each bit stream modulate a separate subcarrier. The channel spacing is 20 MHz, which allows high bit rates per channel yet has reasonable number of channels: 52 subcarriers are used per channel (48 subcarriers for data, 4 subcarriers tracking the phase for coherent demodulation). The independent frequency subchannels are used for one transmission link between the AP and the MTs

Data Link Control Layer

The Data Link Control (DLC) layer includes functions for both medium access and transmission (user plane) as well as terminal/user and connection handling (controlplane) . It consists of the following sublayers :

- Medium Access Control (MAC) protocol
- Error Control (EC) protocol (or Logical Link Control, LLC)
- Radio Link Control (RLC) protocol (also known as RCP) with the associated signalling entities:
    - DLC Connection Control

- Radio Resource Control (RCC)
- Association Control Function (ACF)

Convergence Layer

The Convergence Layer (CL) adapts service request from higher layers to the service offered by the DLC and converts the higher layer packets (SDUs) into a fixed size used within the DLC. This function makes it possible to implement DLC and PHY that are independent of the fixed network to which the HIPERLAN/2 network is connected.

There are currently two types of CLs defined: cell based and packet based. The former is intended for interconnection to ATM networks, the latter is used in a variety of configurations depending on fixed network type

Features:

- High throughput transmission
- Connection oriented
- Quality of service support
- Dynamic frequency selection
- Security support

Architecture:

Operation mode

- Centralized mode
- Direct mode

Hand over

- Sector hand over
- Radio handover
- Network handover

2. Explain in detail the Wi- Max layer. (Apr/May 2014) (Apr/May 2015) (Nov/Dec 2015)

Two types: -

- Fixed WiMAX
- Mobile WiMAX

WiMAX (**Worldwide Interoperability for Microwave Access**) is a family of wireless communication standards based on the IEEE 802.16 set of standards, which provide multiple physical layer (PHY) and Media Access Control (MAC) options.

The name "WiMAX" was created by the **WiMAX Forum**, which was formed in June 2001 to promote conformity and interoperability of the standard, including the definition of predefined system profiles for commercial vendors. The forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as

an alternative to cable and DSL".IEEE 802.16m or Wireless MAN-Advanced was a candidate for the 4G, in competition with the LTE Advanced standard.

Features:

- High data rates
- Quality of service
- Scalability
- Security
- Mobility

WiMAX physical layer
WiMAX Media access control
Spectrum Allocation for WiMAX

3.Explain any two MAC mechanism used in IEEE 802.11 WLAN systems. (Nov/Dec 2015) (Apr/May 2015)

Mechanisms

- Mandatory basic method based on a version of CSMA/CA
- An option method avoiding the hidden terminal problem
- A contention free polling method for time –bounded service

Priorities

- SIFS-Short Inter frame Spacing
- PIFS-PCF Inter frame Spacing
- DIFS-DCF Inter frame Spacing

he IEEE 802.16 MAC was designed for point-to-multipoint broadband wireless access applications. The primary task of the WiMAX MAC layer is to provide an interface between the higher transport layers and the physical layer.

The MAC layer takes packets from the upper layer, these packets are called MAC service data units (MSDUs) and organizes them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse.

The IEEE 802.16-2004 and IEEE 802.16e-2005 MAC design includes a convergence sublayer that can interface with a variety of higher-layer protocols, such as ATM TDM Voice, Ethernet, IP, and any unknown future protocol.

The 802.16 MAC is designed for point-to-multipoint (PMP) applications and is based on collision sense multiple access with collision avoidance (CSMA/CA).

The MAC incorporates several features suitable for a broad range of applications at different mobility rates, such as the following –

- Privacy key management (PKM) for MAC layer security. PKM version 2 incorporates support for extensible authentication protocol (EAP).
- Broadcast and multicast support.
- Manageability primitives.
- High-speed handover and mobility management primitives.
- Three power management levels, normal operation, sleep, and idle.
- Header suppression, packing and fragmentation for an efficient use of spectrum.
- Five service classes, unsolicited grant service (UGS), real-time polling service (rtPS), non-real-time polling service (nrtPS), best effort (BE), and Extended real-time variable rate (ERT-VR) service.

4. Explain about WATM in detail

- Wireless ATM (WATM; sometimes also called wireless, mobile ATM, wmATM) specifies a complete communication system (Acampora, 1996), (Ayanoglu, 1996).
- While many aspects of the IEEE WLANs originate from the data communication community, many WATM aspects come from the telecommunication industry .

Two main subgroups

- Radio Access Layer
- Mobile ATM

Radio Access Layer

- Radio Resource Control
- Wireless Media Access
- Wireless Data Link Control
- Handover issues
- **Location management**: WATM networks must be able to locate a wireless terminal or a mobile user.
- **Mobile routing:** Each time a user moves to a new access point, the system must reroute traffic.
- **Handover signalling:** The network must provide mechanisms which search for new access points, set up new connections and signal the actual change of the access point.
- **QoS and traffic control:** WATM should be able to offer many QoS parameters.
- The network must pay attention to the incoming traffic (and check if it conforms to some traffic contract) in a similar way to today's ATM (policing).
- **Network management:** All extensions of protocols or other mechanisms also require an extension of the management functions to control the network.

ensure wireless access, the working group discussed the following topics belonging to a radio access layer (RAL):

- **Radio resource control:** Radio frequencies, modulation schemes, antennas, channel coding etc. have to be determined.
- **Wireless media access:** Different media access schemes are possible, each with specific strengths and weaknesses for, e.g., multi-media or voice applications.

- **Wireless data link control**: This layer can apply ARQ or FEC schemes to improve reliability.
- **Handover issues**: Cells must be re-sequenced and lost cells must be retransmitted if required

5. Explain the Bluetooth architecture with relevant diagram. (May/June 2012)

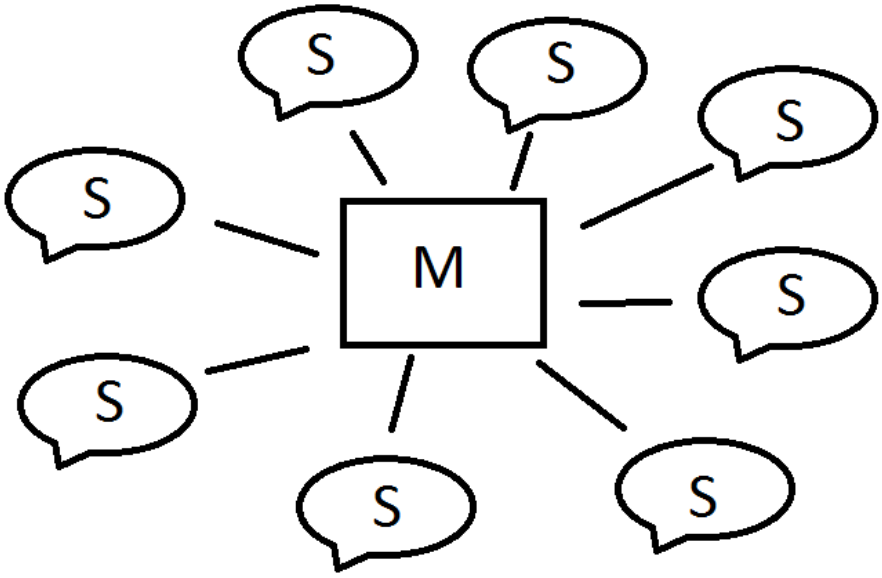
It is a short radio technology

ARCHITECTURE

- Piconet
- Scatternet

Piconets

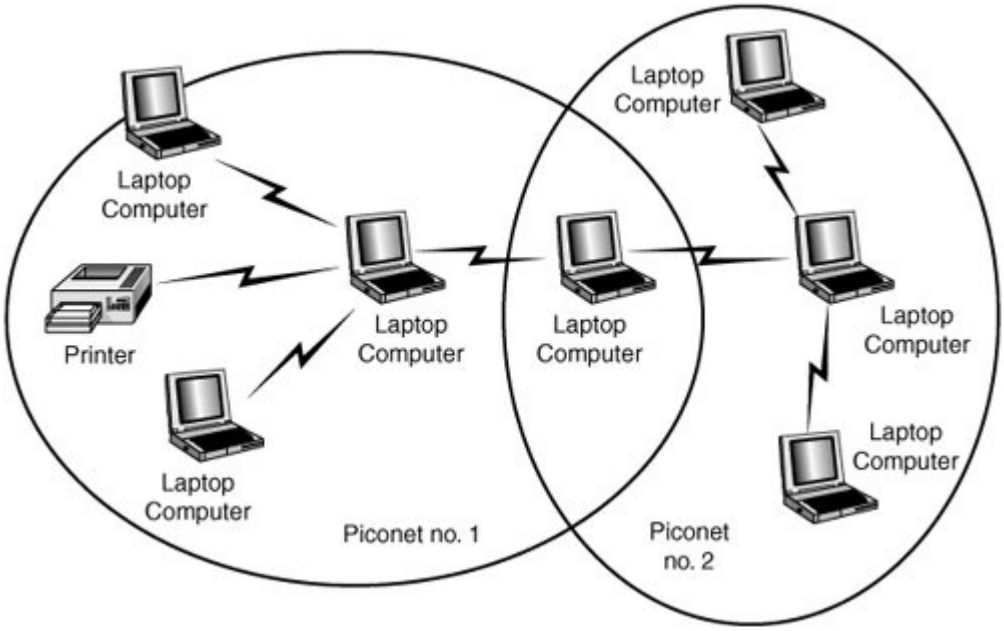
The first type of Bluetooth network is called as a piconet or a small net. It can have at the most eight stations.One of them is called as a master and all others are called as Slaves.All the slave's stations are synchronized in all aspects with the master.A piconet can have only one master station shows piconet. A master can also be called as a primary station and slaves are the secondary station.



Scatternet

A slave in the first piconet can act as a master in the second piconet. It will receive the messages from the master in the first piconet by acting as a slave and then delivers the message to the slaves in the second piconet as shown in the figure. So the Number of piconets, the possibility of collisions increases.This will result in degradation of performance.Therefore a device can participate in two or more piconets by means of the

time-sharing the process. To do so it must use the associated master's address and proper clock offset.



PROTOCOL STACK

- Core specification
- Profile specification

6.Explain in detail about the significance of BRAN.

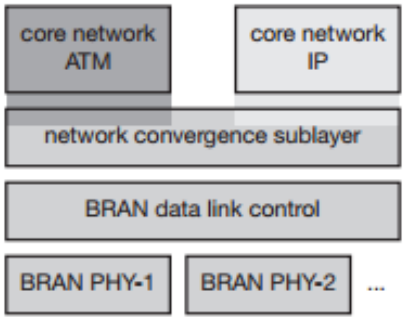
Broadband radio Access Network is standardized by ETSI

TYPES

BRAN has specified four different network types:

- HIPERLAN 1: This high-speed WLAN supports mobility at data rates above 20 Mbit/s. Range is 50 m, connections are multi-point-to-multi-point using ad-hoc or infrastructure networks.
- HIPERLAN/2: This technology can be used for wireless access to ATM or IP networks and supports up to 25 Mbit/s user data rate in a point-to-multi-point configuration. Transmission range is 50 m.
- HIPERACCESS: This technology an alternative to cable modems or Xdsl technologies. Transmission range is up to 5 km, data rates of up to 25 Mbit/s are supported.
- HIPERLINK: To connect different HIPERLAN access points or HIPERACCESS nodes with a high-speed link, HIPERLINK technology can be chosen.
- HIPERLINK provides a fixed point-to-point connection with up to 155 Mbit/s. Currently, there are no plans regarding this standard.
- Common characteristics of HIPERLAN/2, HIPERACCESS, and HIPERLINK include their support of the ATM service classes CBR, VBR-rt, VBR-nrt, UBR, and ABR.

- This technology fulfills the requirements of ATM QoS support, mobility, wireless access, and high bandwidth.
- As an access network, BRAN technology is independent from the protocols of the fixed network. BRAN can be used for ATM and TCP/IP networks as illustrated in **Fig**
- Based on possibly different physical layers, the DLC layer of BRAN offers a common interface to higher layers.
- To cover special characteristics of wireless links and to adapt directly to different higher layer network technologies, BRAN provides a network convergence sublayer.
- This is the layer which can be used by a wireless ATM network, Ethernet, Firewire, or an IP network.



Layered model of BRAN wireless access networks

7. Explain in detail about spread spectrum techniques.

Spread-spectrum telecommunications is a signal structuring technique that employs direct sequence, frequency hopping, or a hybrid of these, which can be used for multiple access and/or multiple functions. This technique decreases the potential interference to other receivers while achieving privacy. Spread spectrum generally makes use of a sequential noise-like signal structure to spread the normally narrowband information signal over a relatively wideband (radio) band of frequencies. The receiver correlates the received signals to retrieve the original information signal. Originally there were two motivations: either to resist enemy efforts to jam the communications (anti-jam, or AJ), or to hide the fact that communication was even taking place, sometimes called low probability of intercept (LPI) or low probability of detection (LPD). Although spread spectrum methods have been used for many years to establish LPD communication, the fundamental limits of covert communications were only recently studied[1] and extended for many scenarios, such as artificial noise generation[2].

Frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS), time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these techniques are forms of spread spectrum. Each of these techniques employs pseudorandom number sequences—created using pseudorandom number generators—to determine and control the spreading pattern of the signal across the allocated bandwidth. Wireless standard IEEE 802.11 uses either FHSS or DSSS in its radio interface.

Types:

- Direct Sequence spread spectrum
- Frequency hopping spread spectrum

DSSS

Direct-sequence spread spectrum (DSSS) is a spread spectrum modulation technique used to reduce overall signal interference. The spreading of this signal makes the resulting wideband channel more noisy, allowing for greater resistance to unintentional and intentional interference

- Basic operation
- Block diagram
- Working principles

FHSS

It is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver. It is used as a multiple access method in the code division multiple access (CDMA) scheme **frequency-hopping code division**

- Slow hopping
- Fast hopping

UNIT II

1.What is a Mobile IP?

Mobile IP is a protocol developed to allow internetwork mobility for wireless nodes without them having to change their IP addresses.

2.What is Care-Of Address (COA)? (Apr/May 17)

The Care of Address defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the subnet.

3.Define – Encapsulation and Decapsulation (Apr/May 17)

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 decapsulation.

4.What is DHCP?

The Dynamic Host Configuration Protocol (DHCP) is based on the bootstrap protocol (BOOTP), which provides the framework for passing configuration information to hosts on a TCP/IP network. DHCP adds the automatically allocate reusable network addresses and configuration options to internet hosts.

5.What is SIP?

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants. It is a IETF (Internet Standard) RFC 3261 protocol.

6.What are the characteristics of MANET? (Nov/Dec 16)

The characteristics of MANET are

Dynamic Topologies
Bandwidth Constraints and Variable Capacity Links
Energy Constrained Operations
Limited Physical Security

7.What are the challenging issues in ad hoc network maintenance(May/June 12)

The challenging issues in ad hoc network are

- Medium access scheme
- Routing
- Multicast routing
- Transport layer protocol
- Pricing Schemes

8.Why are ad hoc networks needed? (May/June 12)

Ad hoc networking is often needed where an infrastructure network cannot be deployed and
managed. The presence of dynamic and adaptive routing protocols enables quick formation of ad
hoc networks and is suitable for emergency situations like natural disasters, spontaneous meetings or military conflicts.

9. What is DSDV?

Distance-Vector Routing (DSDV) is a table driven routing scheme for ad-hoc mobile networks. The main contribution of the algorithm was to solve the routing loop problem.

10.List the Source-initiated On-Demand Routing Protocols.

- Ad-hoc On-Demand Distance Vector Routing (AODV)
- Dynamic Source Routing (DSR)
- Temporarily Ordered Routing Algorithm (TORA)
- Associatively Based Routing (ABR)
- Signal Stability Based Routing (SSR)

PART B

1.State the entities and terminologies used in mobile IP (Apr/may 17)

Mobile IP

The following gives an overall view of Mobile IP, and the extensions needed for the internet to support the mobility of hosts. The following material requires some familiarity with Internet protocols, especially IP. A very good overview which includes detailed descriptions of classical Internet protocols is given in Stevens (1994). Many new approaches related to Internet protocols,applications, and architectures can be found in Kurose (2003).

ENTITIES AND TERMINOLOGY

- Mobile Node
- Correspondent node
- Home network
- Foreign network
- Foreign agent
- Care of Address
- Home Agent

Mobile node (MN):

A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP. The MN keeps its IP address and can continuously communicate with any

Correspondent node (CN):

At least one partner is needed for communication. In the following the CN represents this partner for the MN. The CN can be a fixed or mobile node.

Home network:

The home network is the subnet the MN belongs to with respect to its IP address. No mobile IP support is needed within the home network

Foreign network:

The foreign network is the current subnet the MN visitsand which is not the home network.

Foreign agent (FA):

The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA (defined below),the MN. The FA can be they belong to the foreign network as opposed to the MN which is only visiting. For mobile IP functioning, FAs are not necessarily needed. Typically, an FA is implemented on a router for the subnet the MN attaches to.

Care-of address (COA):

All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is done using a tunnel, as explained later. To be more precise, the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel

Foreign agent COA:

The COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

Home agent (HA):

The HA provides several services for the MN and is located in the home network.The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry, i.e., it is informed of the MN's location by the current COA. Three alternatives for the implementation of an HA exist.

2.Explain the working mechanism of DSDV (Apr/may 17)

Destination sequence distance vector (DSDV**)** routing is an enhancement to distance vector routing for ad-hoc networks (Perkins, 1994). DSDV can be considered historically, however, an on-demand version (ad-hoc on-demand distance vector, AODV) is among the protocols currently Distance vector routing is used as routing information protocol (RIP) in wired networks. It

performs extremely poorly with certain network changes due to the count-to-infinity problem. Each node exchanges its neighbor table periodically with its neighbors. Changes at one node in the network

DSDV adds two things to the distance vector algorithm

- Sequence number
- Damping

Sequence numbers:

Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths. Sequence numbers help to apply the advertisements in correct order. This avoids the loops that are likely with the unchanged distance vector algorithm.

Damping:

Transient changes in topology that are of short duration should not destabilize the routing mechanisms. Advertisements containing changes in the topology currently stored are therefore not disseminated further. A node waits with dissemination if these changes are probably unstable. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.

3.Explain in detail about tunneling and also explain the three types of encapsulation mechanisms used in mobile IP

Tunneling is used to forward IP datagrams from a home address to a care-of-address. Types of IP tunneling are: IP-within-IP encapsulation — simplest approach, defined in RFC 2003 Minimal 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.

IP-within-IP encapsulation (see Figure 2.1.5): The entire IP datagram becomes the payload in a new IP datagram. The inner, original IP header is unchanged except to decrement time-to-live (TTL) by 1. The outer header is a full

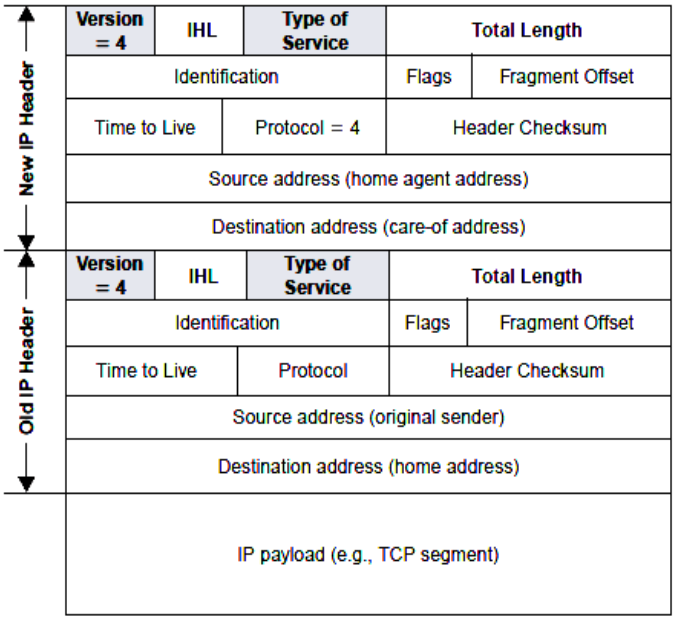


Fig 2.1.5 IP within IP encapsulation

IP header in which:

- Two fields, version number and type of service, are copied from an inner header
- The source address typically is the IP address of the home agent, and the destination address is the CoA for the intended destination.

Minimal encapsulation This results in less overhead and can be used if the mobile node, home agent, and foreign agent all agree to do so. A new header with the following fields is used between the original IP header and the original IP payload: Protocol, Header checksum, Original destination address, Original source address

The following fields in the original IP header are modified to form the new outer IP header:

- Total length
- Protocol
- Header checksum
- Source address
- Destination address.

The encapsulation (home agent) prepares the encapsulated datagram which is now suitable for tunneling and delivery across the Internet to the care-of address. The fields in the minimal forwarding header are restored to the original IP header and the forwarding header is removed from the datagram.

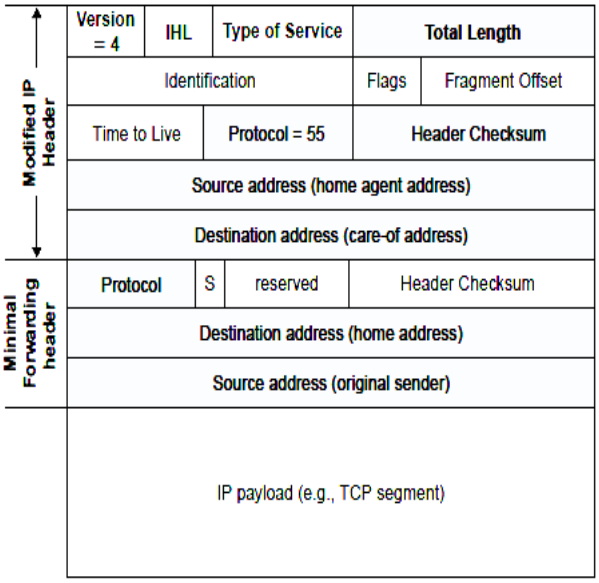
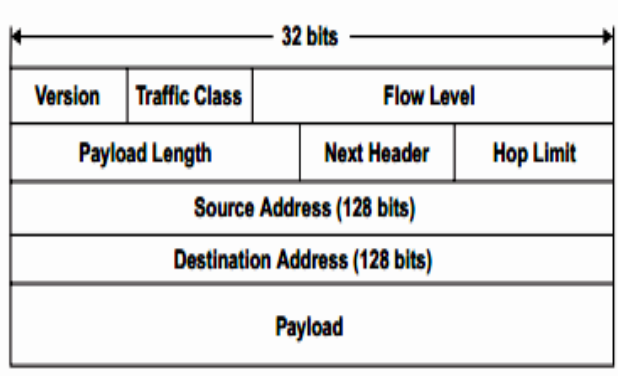


Fig 2.1.6 Minimal encapsulation

The total length field in the IP header is decremented by the size of the minimal forwarding header and the checksum field is recomputed

4.Explain in detail, the IPV6 & DHCP

Today's Internet operates over the common network layer datagram protocol, Internet Protocol version 4 (IPv4). In the early 1990s, a new design of addressing scheme was initiated within the Internet Engineering Task Force (IETF) due to the recognized weaknesses of IPv4. The result was IPv6 (see Figure 2.3.2). The single most significant advantage IPv6 offers is increased destination and source addresses.



- Version: 4-bit field to identify the IP version number
- Traffic class: 8-bit field is similar to Type of Service field in IPv4
- Flow level: This 20-bit field is used to identify a "flow" of datagrams
- Payload length: 16-bit is treated as an unsigned integer to give the number of bytes in the datagram
- Next header: This field identifies the protocol to which the contents of this datagram will be delivered (for example TCP or UDP). The field uses the same values as Protocol field in IPv4 header
- Hop limit: The contents of this field are decremented by one by each router that forwards the datagrams. If the hop limit count reaches zero, the datagram is discarded
- Source and destination address: 128-bit field

IPV6

IPv4 to 128 bits, which provides more than enough globally unique IP addresses for every network device on the planet. This will lead to network simplification, first, through less need to maintain a routing state within the network and second, through reduced need for address translation; hence, it will improve the scalability of the Internet.

IPv6 will allow a return to a global end-to-end environment where the addressing rules of the network are transparent to applications. The current IP address space is unable to satisfy the potentially large increase in number of users or the geographical needs of Internet expansion, let alone the requirements of emerging applications such as Internet-enabled personal digital assistants (PDAs), personal area networks (PANs), Internet-connected transportation, integrated telephony services, and distributed gaming.

The use of globally unique IPv6 addresses simplifies the mechanisms used for reachability and end-to-end security for network devices, functionally crucial to the applications and services driving the demand for the addresses. The lifetime of IPv4 has been extended using techniques such as address reuse with translation and temporary use allocations. Although these techniques appear to increase the address space and satisfy the traditional client/server setup, they fail to meet the requirements of new applications.

The need for an always-on environment to be connectable precludes these IP address conversion, pooling, and temporary allocation techniques, and the “plug and play” required by consumer Internet applications further increases address requirements. The flexibility o f the IPv6 address space provides the support for private addresses but should reduce the use of network address translation (NAT) because global addresses are widely available. IPv6 reintroduces end-to-end security that is not always readily available throughout an NAT-based network.

The success of IPv6 will depend ultimately on the innovative applications that run over IPv6. A key part of IPv6 design is its ability to integrate into and coexist with existing IP networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start. Selection of a deployment strategy will depend on current network environment, and factors such as the forecast of traffi c for IPv6 and availability of IPv6 applications on end systems.

IPv6 does not allow for fragmentation and reassembly at an intermediate router; these operations can be performed only by the source and destination. If an IPv6 datagram received by a router is too large to be forwarded over the outgoing link, the router simply drops the datagram and sends a *packet too big* ICMP message back to sender. The checksum field in IPv4 was considered redundant and was removed because the transport layer and data link layer protocols perform checksum.

5.Explain in detail, the Session Initiation Protocol (SIP)

SIP is used for provisioning services in IP-based mobile networks. SIP specifications define an architecture of user agents and servers (proxy server, redirect server, register) that support communications between SIP peers through user tracking, call routing, and so on. In SIP, each user is uniquely identified by an SIP universal resource indicator, which is used as the identifier to address the called user when the sending session initiation requests.

However, an IP address is associated with the user in order to route SIP signaling from the SIP register. A SIP user registers with the SIP register to indicate its presence in the network and its willingness to receive incoming session initiation requests from other users. A typical session in SIP begins with a user sending an INVITE message to a peer through SIP proxies. When the recipient accepts the request and the initiator is notified, the actual data flow begins, usually taking a path other than the one taken by the SIP signaling messages.

INTERNET REFERENCE MODEL:

Although many useful protocols have been developed in the context of OSI, the overall 7-layer model has not flourished. The TCP/IP architecture has come to dominate. There are a number of reasons for this outcome. The most important is that the key TCP/IP protocols were mature and well tested at a time when similar OSI protocols were in the development stage.

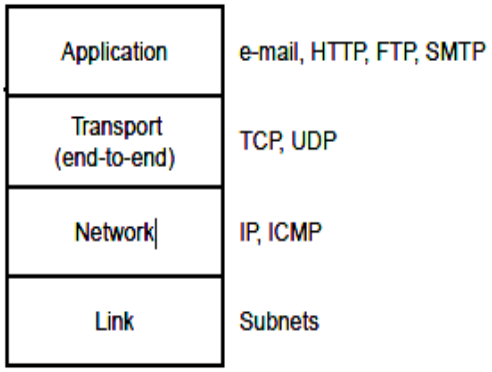


Fig 2.1.7 Internet Reference Mode

6.Explain in detail, the registration process in mobile IP.

When the mobile node receives an agent advertisement, the mobile node registers through the foreign agent, even when the mobile node might be able to acquire its own co-located care-of address. This feature enables sites to restrict access to mobility services. Through agent advertisements, mobile nodes detect when they have moved from one subnet to another.

Mobile IP registration provides a flexible mechanism for mobile nodes to communicate their current reachability information to their home agent. The registration process enables mobile nodes to perform the following tasks:

- Request forwarding services when visiting a foreign network
- Inform their home agent of their current care-of address
- Renew a registration that is due to expire
- Deregister when they return home
- Request a reverse tunnel

Registration messages exchange information between a mobile node, a foreign agent, and the home agent. Registration creates or modifies a mobility binding at the home agent, associating the mobile node's home address with its care-of address for the specified lifetime.

The registration process also enables mobile nodes to:

- Register with multiple foreign agents
- Deregister specific care-of addresses while retaining other mobility bindings
- Discover the address of a home agent if the mobile node is not configured with this information

Registration request

- Home address
- Home agent
- COA
- Identification

Registration reply

- UDP packet
- Type
- Code

7. Explain in detail, agent discovery process in mobile IP.

One initial problem of an MN after moving is how to find a foreign agent. How does the MN discover that it has moved? For this purpose mobile IP describes two methods: agent advertisement and agent solicitation, which are in fact router discovery methods plus extensions.

These advertisement messages can be seen as a beacon broadcast into the subnet. For these advertisements Internet control message protocol (ICMP) messages according to RFC 1256 (Deering,1991) are used with some mobility extensions. The agent advertisement packet according to RFC 1256 with the extension for mobility is shown in Figure 2.1.3 The upper part represents the ICMP packet while the lower part is the extension needed for mobility.

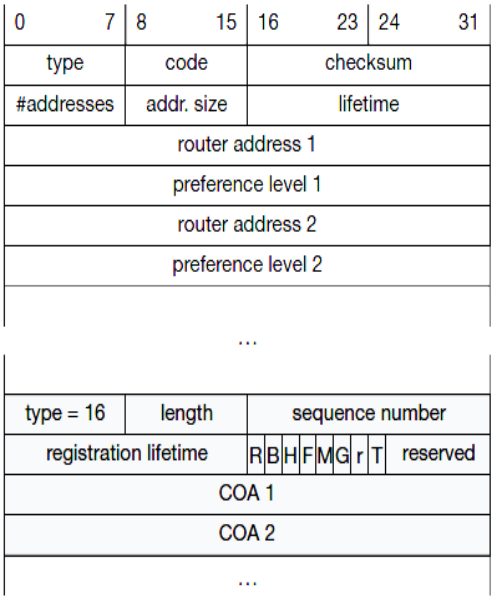


Fig 2.1.3 Agent advertisement packet

The discovery process in MIP is similar to the router advertisement process defined in ICMP. The agent discovery makes use of ICMP (Internet control message protocol) router advertisement messages, with one or more extensions specific to MIP.

A mobile node is responsible for an ongoing discovery process to determine if it is attached to its network (in which case a datagram may be received without forwarding) or to a foreign network. A transition from the home network to a foreign network can occur at any time without notification to the network layer (i.e., the IP layer).

Location management in MIP is achieved via a registration process and an agent advertisement. FAs and HAs periodically advertise their presence using agent advertisement messages. The same agent may act as both an HA and an FA — mobility extensions to ICMP messages which are used for agent advertisements. The messages contain information about the CoA associated with the FA, whether the agent is busy, whether minimal encapsulation is permitted, whether registration is mandatory, and so on.

The agent advertisement packet is a broadcast message on the link. If the mobile node gets an advertisement from its HA, it must be register its CoA and enable a gratuitous ARP. If a mobile node does not hear any advertisement, it must solicit an agent advertisement using
ICMP. Once an agent is discovered, the MN performs either registration or deregistration with the HA, depending on whether the discovered agent is an HA oran FA. The MN sends a registration request using UDP to HA through the FA(or directly, if it is a co-located CoA).

The HA creates a mobility binding between the MN's home address and the current CoA that has a fixed lifetime. The mobile node should register before expiration of the binding. Each FA maintains a list of visiting mobiles containing the following information:

- Link-layer address of the mobile node
- Mobile node home IP address
- UDP registration request source port

- Home agent IP address
- An identification field
- Registration lifetime
- Remaining lifetime of pending or current registration.

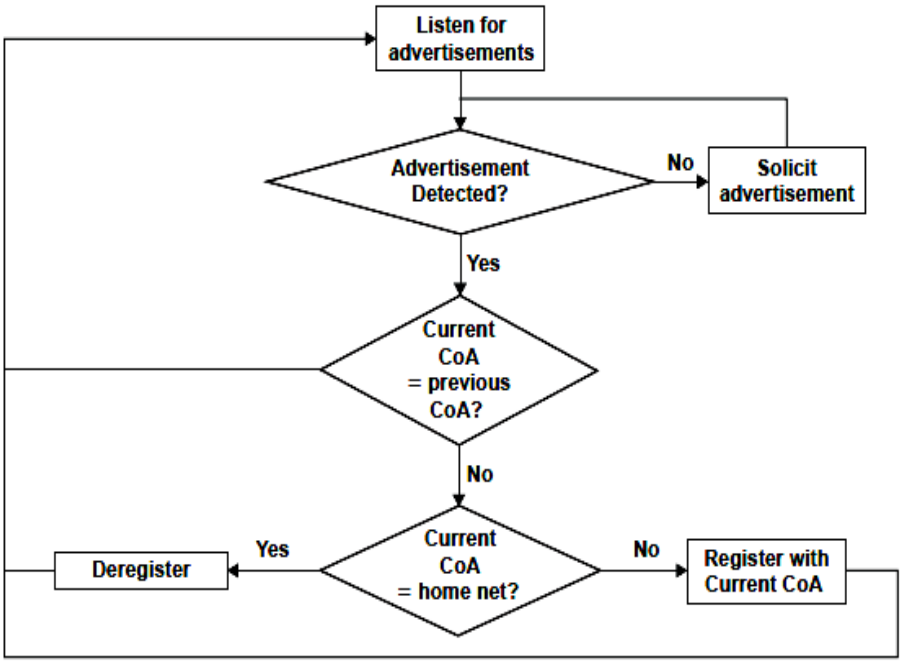


Fig 2.1.4 Agent discovery procedure

.

8.Explain with an example DSR

Dynamic source routing (DSR), therefore, divides the task of routing into two separate problems (Johnson, 1996), (Johnson, 2002a):

● **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.

● **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative.

The basic principle of source routing is also used in fixed networks, e.g. token rings. Dynamic source routing eliminates all periodic routing updates and works as follows. If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters. Any node that receives a route request does the following.

If the node has already received the request (which is identified using the unique identifier), it drops the request packet.

● If the 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 packet and broadcasts this updated route request.

UNIT III

1.What are the advantages and disadvantages of I – TCP? (Apr/may 17)

Advantages:

- I-TCP does not require any changes in the TCP Protocol
- Transmission errors on the wireless link cannot propagate into the fixed network.
- Optimizing new mechanisms is quite simple because they only cover one single hop.

Disadvantages:

- The loss of the end-to-end semantics of TCP might cause problems if the foreign agent partitioning the connection crashes.

2.What are the advantages of Mobile TCP? (Apr/may 17)

- M-TCP maintains the TCP end-to-end semantics. The Supervisory Host (SH) does not send any ACK itself but forwards the ACKS from the MH.
- If the MH is detached, it avoids useless transmissions, slow starts or breaking connections by simply shrinking the sender's window to zero.

3.What is Snooping TCP?

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

4.What is time-out freezing?

The MAC layer informs the TCP layer about an upcoming loss of connection or that the current interruption is not caused by congestion. TCP then stops sending and freezes the current state of its congestion window and further timers. When the MAC layer notices the upcoming interruption early enough, both the mobile and correspondent host can be informed.

5.What is Selective Retransmission?

TCP acknowledgements are collective. They acknowledge in-order receipt of packets upto certain packets. Even if a single packet is lost, the sender has to retransmit everything starting from the lost packet. To overcome this problem, TCP can indirectly request a selective retransmission of packets. The receiver may acknowledge single packets and also trains of in-sequence packets.

6.What are the techniques for classical improvements?

With the goal of increasing TCPs performance in wireless and mobile environments several
scheme were proposed,
Some of them are:

- Indirect TCP
- Mobile TCP
- Snooping TCP
- Fast Transmit/ Fast Recovery
- Transmission/ time-out freezing
- Selective Retransmission

7.What is Congestion Avoidance algorithm?
In the Congestion Avoidance algorithm a retransmission timer expiring or the recACKs can implicitly signal the sender that a network congestion situation is go
The sender immediately sets its transmission window to one half of the currenat least two segments. If congestion was indicated by a timeout, the congestioone segment, which automatically puts the sender into Slow Start mode.

8.What are the algorithms used for congestion control in TCP?

- Slow start
- Congestion avoidance
- Fast transmit
- Fast recovery

9.What is Fast Retransmit algorithm in TCP?
During TCP congestion control, when three or more duplicate ACKs are received, the sender does not even wait for a retransmission timer to expire before retransmitting the segment. This process is called the Fast Retransmit Algorithm.

10.What is slow start mechanism?
Slow start is a mechanism used by the sender to control the transmission rate. The sender always calculates a congestion window for a receiver. The start size of the congestion window is one TCP packet.

PART B

1.Describe the working mechanism of traditional TCP(Apr/May 17)
Major responsibilities of TCP

- Provide reliable in-order transport of data
- Control congstions in the networks
- Control a packet low between the transmitter and the receiver

Mechanisms

- Congestion control
- Slow start
- Fast retransmit/Fast Recovery

- Implication of mobility

CONGESTION CONTROL:

A transport layer protocol such as TCP has been designed for fixed networks with fixed end-systems. Data transmission takes place using network adapters, fiber optics, copper wires, special hardware for routers etc.

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**

FAST RETRANSMIT/FAST RECOVERY:

Two things lead to a reduction of the congestion threshold. One is a sender receiving continuous acknowledgements for the same packet. This informs the sender of two things. One is that the receiver got all packets up to the acknowledged packet in sequence. In TCP, a receiver sends acknowledgements only if it receives any packets from the sender. Receiving acknowledgements from a receiver also shows that the receiver continuously receives something from the sender. The gap in the packet stream is not due to severe 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**

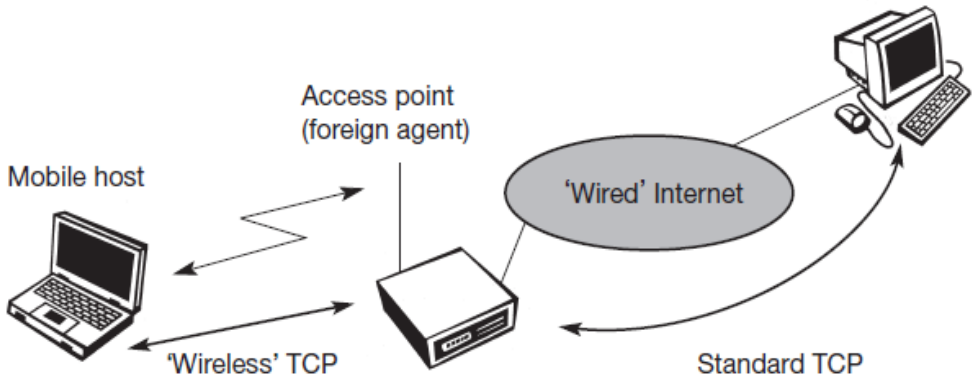
IMPLICATIONS ON MOBILITY:

While slow start is one of the most useful mechanisms in fixed networks, it drastically decreases the efficiency of TCP if used together with mobile receivers or senders. The reason for this is the use of slow start under the wrong assumptions. From a missing acknowledgement, TCP concludes a congestion situation. While this may also happen in networks with mobile and wireless end-systems, it is not the main reason for packet loss.

2.Write your understanding on indirect TCP (Apr/May 17)

INDIRECT TCP:

Two competing insights led to the development of indirect TCP (I-TCP) (Bakre, 1995). One is that TCP performs poorly together with wireless links; the other is that TCP within the fixed network cannot be changed. I-TCP segments a TCP connection into a fixed part and a wireless part. Figure 9.1 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. The correspondent node could also use wireless access. The following would then also be applied to the access link of the correspondent host..



Indirect TCP segments

However, one can also imagine separating the TCP connections at a special server, e.g., at the entry point to a mobile phone network (e.g., IWF in GSM, GGSN in GPRS).

The correspondent host in the fixed network does not notice the wireless link or the segmentation of the connection. The foreign agent acts as a proxy and relays all data in both directions. If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host. If the mobile host receives the packet, it acknowledges the packet. However, this acknowledgement is only used by the foreign agent.

If a packet is lost on the wireless link due to a transmission error, the correspondent host would not notice this. In this case, the foreign agent tries to retransmit this packet locally to maintain reliable data transport.

Similarly, if the mobile host sends a packet, the foreign agent acknowledges this packet and tries to forward it to the correspondent host. If the packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet. Packet loss in the wired network is now handled by the foreign agent.

I-TCP requires several actions as soon as a handover takes place. As Figure demonstrates, not only the packets have to be redirected using, e.g., mobile IP. In the example shown, the access point acts as a proxy buffering packets for retransmission.

3.**Explain in detail, Snooping TCP.**

One of the drawbacks of I-TCP is the segmentation of the single TCP connection into two TCP connections. This loses the original end-to-end TCP semantic. The following TCP enhancement works completely transparently and leaves the TCP end-to-end connection intact.

The main function of the enhancement is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss. A good place for the enhancement of TCP could be the foreign agent in the Mobile IP context (see Figure 3.3).

In this approach, the foreign agent buffers all packets with **destination mobile host** and additionally 'snoops' the packet flow in both directions to recognize acknowledgements (Balakrishnan, 1995), (Brewer, 1998). The reason for buffering packets toward the mobile node is to enable the foreign agent to perform a local retransmission in case of packet loss on the wireless link.

The foreign agent buffers every packet until it receives an acknowledgement from the mobile host. If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost. Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet.

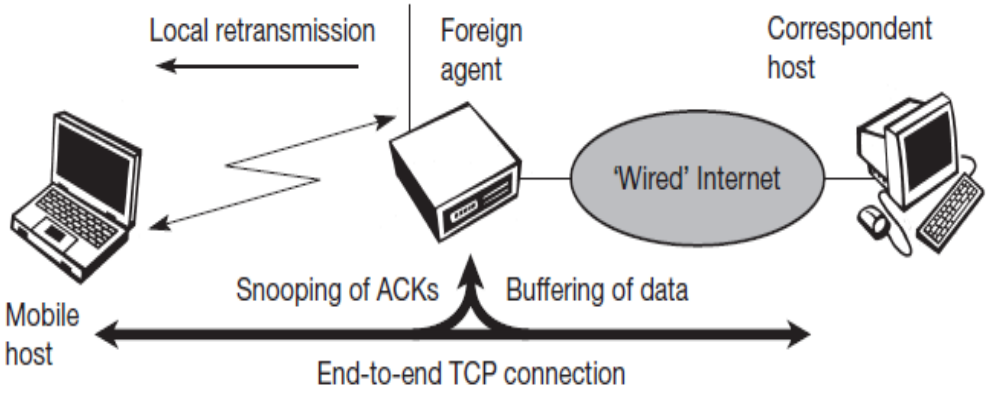


Fig 3.3 Snooping TCP as TCP Extension

To remain transparent, the foreign agent must not acknowledge data to the correspondent host. This would make the correspondent host believe that the mobile host had received the data and would violate the end-to-end semantic in case of a foreign agent failure. However, the foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host.

If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission. The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host. This avoids unnecessary traffic on the wireless link.

Data transfer from the mobile host with **destination correspondent host** works as follows. The foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP. As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host. The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the

correspondent host by TCP. Extending the functions of a foreign agent with a 'snooping' TCP has several **advantages**:

- The end-to-end TCP semantic is preserved. No matter at what time the foreign agent crashes (if this is the location of the buffering and snooping mechanisms), neither the correspondent host nor the mobile host have an inconsistent view of the TCP connection as is possible with I-TCP.

- The correspondent host does not need to be changed; most of the enhancements are in the foreign agent. Supporting only the packet stream from the correspondent host to the mobile host does not even require changes in the mobile host.

- It does not need a handover of state as soon as the mobile host moves to another foreign agent. Assume there might still be data in the buffer not transferred to the next foreign agent. All that happens is a time-out at the correspondent host and retransmission of the packets, possibly already to the new care-of address.

It does not matter if the next foreign agent uses the enhancement or not. If not, the approach automatically falls back to the standard solution. This is one of the problems of I-TCP, since the old foreign agent may have already signaled the correct receipt of data via acknowledgements to the correspondent host and now has to transfer these packets to the mobile host via the
new foreign agent.

Snooping TCP does not isolate the behavior of the wireless link as well as ITCP. Assume, for example, that it takes some time until the foreign agent can successfully retransmit a packet from its buffer due to problems on the wireless link (congestion, interference). Although the time-out in the foreign agent may be much shorter than the one of the correspondent host, after a while the time-out in the correspondent host triggers a retransmission. The problems on the wireless link are now also visible for the correspondent host and not fully isolated.

All efforts for snooping and buffering data may be useless if certain encryption schemes are applied end-to-end between the correspondent host and mobile host.

Using IP encapsulation security payload (RFC 2406, (Kent, 1998b)) the TCP protocol header will be encrypted – snooping on the sequence numbers will no longer work. Retransmitting data from the foreign agent may not work because many security schemes prevent replay attacks – retransmitting data from the foreign agent may be misinterpreted as replay. Encrypting end-to-end is the way many applications work so it is not clear how this scheme could be used in the future. If encryption is used above the transport layer (e.g., SSL/TLS) snooping TCP can be used.

4. **Explain the various issues in 2.5G/3G wireless network**

The current internet draft for TCP over 2.5G/3G wireless networks (Inamura, 2002) describes a profile for optimizing TCP over today's and tomorrow's wireless WANs such as GSM/GPRS, UMTS, or cdma2000. The configuration optimizations recommended in this draft can be found in most of today's TCP implementations so this draft does not require an update of millions of TCP stacks.

The focus on 2.5G/3G for transport of internet data is important as already more than 1 billion people use mobile phones and it is obvious that the mobile phone systems will also be used to transport arbitrary internet data.

Data rates: While typical data rates of today's 2.5G systems are 10–20 kbit/s uplink and 20–50 kbit/s downlink, 3G and future 2.5G systems will initially offer data rates around 64 kbit/s uplink and 115–384 kbit/s downlink. Typically, data rates are asymmetric as it is expected that users will download more data compared to uploading. Uploading is limited by the limited battery power. In cellular networks, asymmetry does not exceed 3–6 times, however, considering broadcast systems as additional distribution media (digital radio, satellite systems), asymmetry may reach a factor of 1,000. Serious problems that may reduce throughput dramatically are bandwidth oscillations due to dynamic resource sharing.

Latency: All wireless systems comprise elaborated algorithms for error correction and protection, such as forward error correction (FEC), check summing, and interleaving. FEC and interleaving let the round trip time (RTT) grow to several hundred milliseconds up to some seconds.

Jitter: Wireless systems suffer from large delay variations or 'delay spikes' Reasons for sudden increase in the latency are: link outages due to temporal loss of radio coverage, blocking due to high-priority traffic, or handovers. Handovers are quite often only virtually seamless with outages reaching from some 10 ms (handover in GSM systems) to several seconds (intersystem handover, e.g., from a WLAN to a cellular system using Mobile IP without using additional mechanisms such as multicasting data to multiple access points).

Packet loss: Packets might be lost during handovers or due to corruption. Thanks to link-level retransmissions the loss rates of 2.5G/3G systems due to corruption are relatively low (but still orders of magnitude higher than, e.g., fiber connections!). However, recovery at the link layer appears as jitter to the higher layers.

Large windows: TCP should support large enough window sizes based on the bandwidth delay product experienced in wireless systems. With the help of the windows scale option (RFC 1323) and larger buffer sizes this can be accomplished (typical buffer size settings of 16 kbyte are not enough).

Limited transmit: This mechanism, defined in RFC 3042 (Allman, 2001) is an extension of Fast Retransmission/Fast Recovery (Caceres, 1995) and is particularly useful when small amounts of data are to be transmitted (standard for, e.g., web service requests).

Large MTU: The larger the MTU (Maximum Transfer Unit) the faster TCP increases the congestion window. Link layers fragment PDUs for transmission anyway according to their needs and large MTUs may be used to increase performance. MTU path discovery according to RFC 1191 (IPv4) or RFC 1981 (IPv6) should be used to employ larger segment sizes instead of
Assuming the small default MTU.

Selective Acknowledgement (SACK): SACK (RFC 2018) allows the selective retransmission of packets and is almost always beneficial compared to the standard cumulative scheme.

● **Explicit Congestion Notification (ECN):** ECN as defined in RFC 3168 (Ramakrishnan,2001) allows a receiver to inform a sender of congestion in the network by setting the ECN-Echo flag on receiving an IP packet that has experienced congestion. This mechanism makes it easier to distinguish packet loss due to transmission errors from packet loss due to congestion. However, this can only be achieved when ECN capable routers are deployed in the network.

● **Timestamp:** TCP connections with large windows may benefit from more frequent RTT samples provided with timestamps by adapting quicker to changing network conditions. With the help of timestamps higher delay spikes can be tolerated by TCP without experiencing a spurious timeout. The effect of bandwidth oscillation is also reduced.

● **No header compression:** As the TCP header compression mechanism according to RFC 1144 does not perform well in the presence of packet losses this mechanism should not be used. Header compression according to RFC 2507 or RFC 1144 is not compatible with TCP options such as SACK or timestamps.

6. Explain in detail about the classical enhancements to TCP for mobility.

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. If the application requires reliable transport of the packets, it may use TCP (many applications of this kind use UDP and solve reliability on a higher, application-oriented layer).

Using TCP now requires several packets over the wireless link. 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. Assuming connections with a lot of traffic or with a long duration, this overhead is minimal. But in an example of only one data packet, TCP may need seven packets altogether.
Figure 9.4 shows an example for the overhead introduced by using TCP over GPRS in a web scenario. Web services are based on HTTP which requires a reliable transport system. In the internet, TCP is used for this purpose.

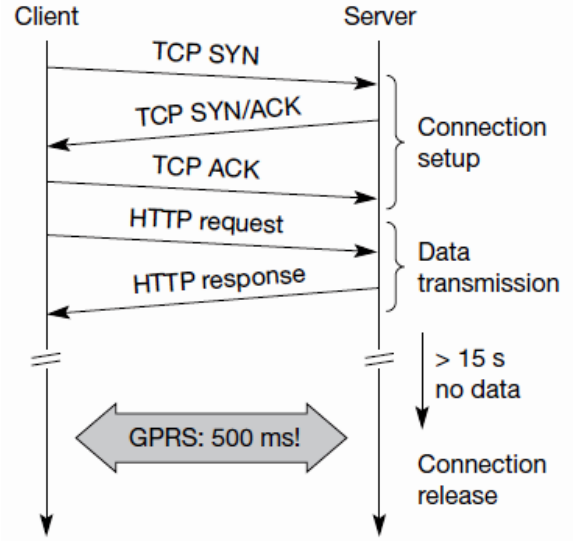


Fig 3.4 Example TCP setup connection overhead

This already requires three messages. If GPRS is used as wide area transport system, one-way delays of 500 ms and more are quite common. The setup of a TCP connection already takes far more than a second.

This led to the development of a transaction-oriented TCP (T/TCP, RFC 1644 (Braden, 1994)). 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. Similar considerations led to the development of a transaction service in WAP.

The obvious advantage for certain applications is the reduction in the overhead which standard TCP has for connection setup and connection release. However, T/TCP is not the original TCP anymore, so it requires changes in the mobile host and all correspondent hosts, which is a major disadvantage. This solution no longer hides mobility. Furthermore, T/TCP exhibits several security problems.

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover, security problems
Snooping TCP	Snoops data and acknowledgements, local retransmission	Transparent for end-to-end connection, MAC integration possible	Insufficient isolation of wireless link, security problems
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management, security problems
Fast retransmit/ fast recovery	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
Transmission/ time-out freezing	Freezes TCP state at disconnection, resumes after reconnection	Independent of content, works for longer interruptions	Changes in TCP required, MAC dependent
Selective retransmission	Retransmits only lost data	Very efficient	Slightly more complex receiver software, more buffer space needed
Transaction-oriented TCP	Combines connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent, security problems

Table3.1 overview of classical enhacnements to TCP

Table 3.1 shows an overview of the classical mechanisms presented together with some advantages and disadvantages. The approaches are not all exclusive, but can be combined. Selective retransmission, for example, can be used together with the others and can even be applied to fixed networks.

An additional scheme that can be used to reduce TCP overhead is **header compression** (Degermark, 1997). Using tunneling schemes as in mobile IP together with TCP, results in protocol headers of 60 byte in case of IPv4 and 100 byte for IPv6 due to the larger addresses. Many fields in the IP and TCP header remain unchanged for every packet. Only just transmitting the differences is often sufficient.

Especially delay sensitive applications like, e.g., interactive games, which have small packets benefit from small headers. However, header compression experiences difficulties when error rates are high due to the loss of the common context between sender and receiver. With the new possibilities of wireless wide area networks (WWAN) and their tremendous success, the focus of research has shifted more and more towards these 2.5G/3G networks. Up to now there are no final solutions to the problems arising when TCP is used in WWANs. However, some guidelines do exist.

7. Explain in detail about the time-out freezing and selective re-transmission.

TIME-OUT FREEZING

While the approaches presented so far can handle short interruptions of the connection, either due to handover or transmission errors on the wireless link, some were designed for longer interruptions of transmission. Examples are the use of mobile hosts in a car driving into a tunnel, which loses its connection to, e.g., a satellite (however, many tunnels and subways provide connectivity via a mobile phone), or a user moving into a cell

with no capacity left over. In this case, the mobile phone system will interrupt the connection. The reaction of TCP, even with the enhancements of above, would be a disconnection after a time out.

Quite often, the MAC layer has already noticed connection problems, before the connection is actually interrupted from a TCP point of view. Additionally, the MAC layer knows the real reason for the interruption and does not assume congestion, as TCP would. 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. The **advantage** of this approach is that it offers a way to resume TCP connections even after longer interruptions of the connection. It is independent of
any other TCP mechanism, such as acknowledgements or sequence numbers, so it can be used together with encrypted data. However, this scheme has some severe **disadvantages**. Not only does the software on the mobile host have to be changed, to be more effective the correspondent host cannot remain unchanged. All mechanisms rely on the capability of the MAC layer to detect
Future interruptions. Freezing the state of TCP does not help in case of some encryption schemes that use time-dependent random numbers. These schemes need resynchronization after interruption.

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. 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 (particularly those with a high path capacity, i.e., bandwidth delay- product).

Using RFC 2018 (Mathis, 1996), 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 gain in efficiency is not restricted to wireless links and mobile environments. Using selective retransmission is also beneficial in all other networks. However, there might be the minor disadvantage of more complex software on the receiver side, because now more buffer is necessary to resequence data and to wait for gaps to be filled. But while memory sizes and CPU performance permanently increase, the bandwidth of the air interface remains almost the same. Therefore, the higher complexity is no real disadvantage any longer as it was in the early days of TCP.

8.Explain in detail about Mobile TCP

Dropping packets due to a handover or higher bit error rates is not the only phenomenon of wireless links and mobility – the occurrence of lengthy and/or frequent disconnections is another problem. Quite often mobile users cannot connect at all.

A TCP sender tries to retransmit data controlled by a retransmission timer that doubles with each unsuccessful retransmission attempt, up to a maximum of one minute (the initial value depends on the round trip time). This means that the sender tries to retransmit an unacknowledged packet every minute and will give up after 12 retransmissions. No data is successfully transmitted for a period of one minute! The retransmission time-out is still valid and the sender has to wait.

The sender also goes into slow-start because it assumes congestion. What happens in the case of I-TCP if the mobile is disconnected? The proxy has to buffer more and more data, so the longer the period of disconnection, the more buffer is needed. If a handover follows the disconnection, which is typical, even more state has to be transferred to the new proxy. The snooping approach also suffers from being disconnected. The mobile will not be able to send ACKs so, snooping cannot help in this situation.

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.

The wireless side uses an adapted TCP that can recover from packet loss much faster. This modified TCP does not use slow start, thus, M-TCP needs a **bandwidth manager** to implement fair sharing over the wireless link.

The **advantages** of M-TCP are the following:

● 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.

UNIT IV

1.What are the applications of 3G?
Applications for a 3G wireless network range from simple voice-only communications to simultaneous video, data, voice and other multimedia applications

2.Name some of the wireless technology services?

- General Packet Radio Services (GPRS)
- Enhanced Data for GSM evolution (EDGE) service
- Wideband Code Division Multiple access (WCDMA)
- Universal Mobile telecommunications Services (UMTS)
- High-Speed Downlink Packet Access (HSDPA)

3.What is UMTS?
Universal Mobile telecommunications Services (UMTS) is a new radio access network based on 5 MHz WCDMA and optimized for efficient support of 3G services. UMTS can be used in both new and existing spectra.

4. What are the layers of UMTS?
The UMTS terrestrial radio access network (UTRAN) has an access layer and non access layer. The access layer includes air interface and provides functions related to OSI layer 1, layer 2, and the lower part of layer 3.
The non-access layer deals with communication between user equipment (UE) and core network (CN) and includes OSI layer 3 (upper part) to layer 7.

5.What is radio resource control (RRC)?
The radio resource control (RRC) layer broadcasts system information, handles radio resources such as code allocation, handover, admission control, measurement/control report.

6.What are the duties of Radio network control (RNC)?

- Intra UTRAN handover
- Macro diversity combining/ splitting of Iub data systems.
- Outer loop power control
- IU interface user plane setup
- Serving RNS (SRNS) relocation
- Radio resource allocation

7. What are the planes of UTRAN?

- Control plane
- User plane
- Transport network control plane.

8. What are the functions provided by 3G-MSC?

- Mobility management
- Call management
- Supplementary services
- Short message services (SMS)
- OAM (operation, administration, and maintenance) agent functionality

9. What is Transport Network Control Plane (TNCP)?

Transport Network Control Plane (TNCP) carries information for the control of transport network used within UCN.

10. What is 3G-SGSN?

The 3G-SGSN (serving GPRS Support Node) provides the appropriate signaling and data interface that includes connection to an IP-based network toward the 3G-GGSN, SS7 towards the HLR/EIR/AUC and TCP/IP or SS7 toward the UTRAN.

PART B

1.Explain the services of UMTS in detail.

3G-SGSN

- The 3G-SGSN is the main CN element for PS services.
- The 3G-SGSN provides the necessary control functionality toward the UE and the 3G-GGSN.
- It also provides the appropriate signaling and data interfaces.
- The 3G-SGSN provides the following functions:
    - **Session management:** Handles session set-up messages from/to the UE and the GGSN and operates Admission Control and QoS mechanisms.
    - ***Iu* and *Gn* MAP interface:** The 3G-SGSN is able to complete originating or terminating sessions in the network by interaction with other entities of a mobile network, e.g., GGSN, HLR, AUC. It also controls/communicates with UTRAN using RANAP.
    - **ATM/AAL5** physical connection to the UTRAN for transportation of user data plane traffic across the *Iu* interface using GPRS tunneling protocol (GTP).
    - Connection across the *Gn* interface toward the GGSN for transportation of user plane traffic using GTP. Note that no physical transport layer is defined for this interface.
    - **SMS:** This functionality allows the user to send and receive SMS data to and from the SMS-GMSC /SMS-IWMSC.

- **Mobility management:** Handles attach, authentication, updates to the HLR and SRNS relocation, and intersystem handover.
- **Subscriber database functionality:** This database (similar to the VLR) is located within the 3G-SGSN and serves as intermediate storage for subscriber data to support subscriber mobility.
- **Charging:** The SGSN collects charging information related to radio network usage by the user.
- OAM agent functionality

3G-GGSN

The GGSN provides interworking with the external PS network. It is connected with SGSN via an IP-based network.

- The GGSN may optionally support an SS7interface with the HLR to handle mobile terminated packet sessions.
- The 3G-GGSN provides the following functions:
    - Maintain information locations at SGSN level (macro-mobility)
    - Gateway between UMTS packet network and external data networks (e.g. IP, X.25)
    - Gateway-specific access methods to intranet (e.g. PPP termination)
    - Initiate mobile terminate Route Mobile Terminated packets
    - User data screening/security can include subscription based, user controlled, or network controlled screening.
    - **User level address allocation:** The GGSN may have to allocate (depending on subscription) a dynamic address to the UE upon PDP context activation. This functionality may be carried out by use of the DHCP function.
    - **Charging:** The GGSN collects charging information related to external data network usage by the user.
    - OAM functionality

SMS-GMSC/SMS-IWMSC

- The overall requirement for these two nodes is to handle the SMS from point to point.
- The functionality required can be split into two parts.

SMS-GMSC

- The SMS-GMSC is an MSC capable of receiving a terminated short message from a service center, interrogating an HLR for routing information and SMS information, and delivering the short message to the SGSN of the recipient UE.

- The **SMS-GMSC** provides the following functions:
- Reception of short message packet data unit (PDU)
- Interrogation of HLR for routing information
- Forwarding of the short message PDU to the MSC or SGSN using the routing information.

SMS-IWMSC

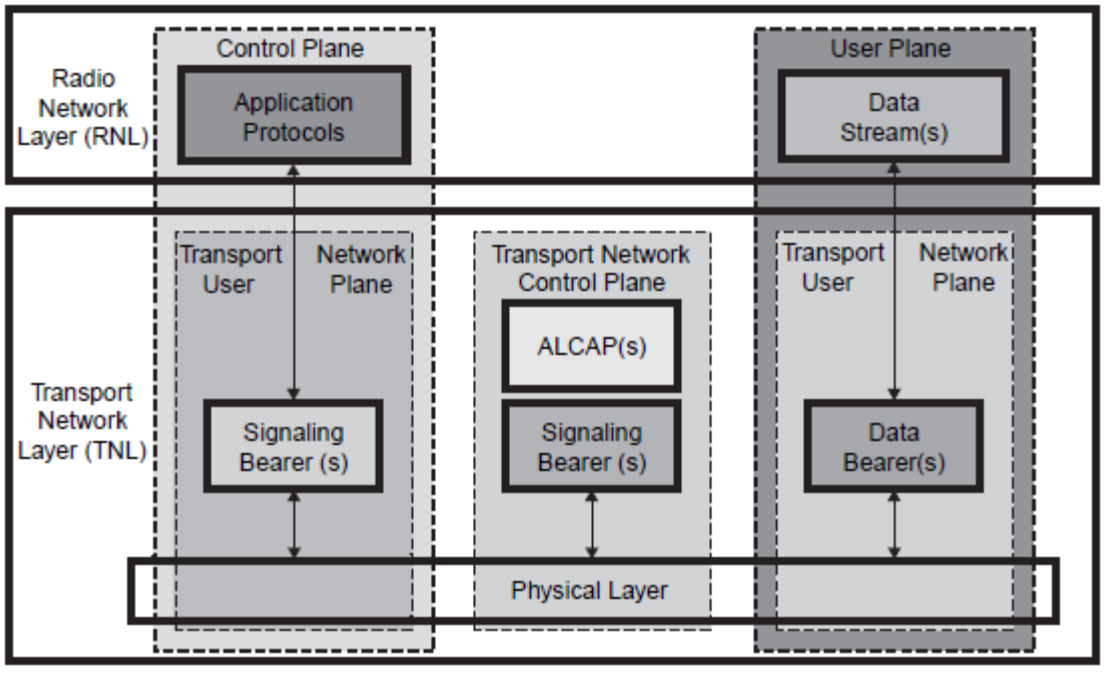
- The SMS-IWMSC is an MSC capable of receiving an originating short message from within the PLMN and submitting it to the recipient service center.

- The **SMS-IWMSC** provides the following functions:
- Reception of the short message PDU from either the 3G-SGSN or 3G-MSC
- Establishing a link with the addressed service center
- Transferring the short message PDU to the service center

2.Explain in detail, the logical interfaces of UTRAN.

In UTRAN protocol structure is designed so that layers and planes are logically independent of each other.

- The protocol structure contains two main layers,
  - Radio network layer(RNL)- all UTRAN-related functions are visible
  - Transport network layer (TNL) -deals with transport technology selected to be used for UTRAN but without any UTRAN-specific changes
- A general protocol model for UTRAN interfaces is shown in Figure 4.4.



ALCAP: Access Link Control Application Part

Fig. 4.4 **General protocol model for UTRAN interfaces.**

- The control plane is used for all UMTS-specific control signaling. It includes
    - Radio access network application part (RANAP) in *Iu*,
    - Radio network subsystem application part (RNSAP) in *Iur* and
    - Node B application part (NBAP) in *Iub*.
- The application protocol is used for setting up bearers to the UE.
- User information is carried by the user plane. The user plane includes data stream(s), and data bearer(s) for data stream(s).
- The transport network control plane carries all control signaling within the transport layer. It contains *access link control application part* (*ALCAP*) required to set up the transport bearers (data bearers) for the user plane.
- The transport plane lies between the control plane and the user plane.

***Iu* Interface**

- The UMTS *Iu* interface is the open logical interface that interconnects one UTRAN to the UMTS core network (UCN). On the UTRAN side the *Iu* interface is terminated at the RNC, and at the UCN side it is terminated at U-MSC.
- The *Iu* interface consists of three different protocol planes — the *radio network control plane* (*RNCP*), the *transport network control plane* (*TNCP*), and the *user plane* (*UP*).
- The RNCP performs the following functions:
    - It carries information for the general control of UTRAN radio network operations.
    - It carries information for control of UTRAN in the context of each specific call.
    - It carries user call control (CC) and mobility management (MM) signaling messages.
- The control plane serves two service domains in the core network, **the packet-switched (PS) domain and circuit-switched (CS) domain.**
- The CS domain supports circuit-switched services. Some examples are voice and fax. The PS domain deals with PS services.
- Some examples of PS services are Internet access and multimedia services The PS domain connects to IP networks.
- The *Iu* circuit-switched and packet-switched protocol architecture are shown in Figures 4.5 & 4.6.The control plane protocol stack consists of RANAP on the top of (SS7) protocols. The protocol layers are the signaling connection control part (SCCP), the message transfer part (MTP3-B), and signaling asynchronous transfer mode (ATM) adaptation layer for network-to-network interface (SAAL-NNI).
- The SAAL-NNI is divided into service-specific coordination function (SSCF), the service-specific connection-oriented protocol (SSCOP), and ATM adaptation layer 5 (AAL5) layers. The SSCF and SSCOP layers are specifically designed for signaling transport in

ATM networks, and take care of signaling connection management functions. AAL5 is used for segmenting the data to ATM cells.

3. Explain the LTE architecture and its protocol model in detail

- Architecture
- The core network
- Architecture reference model.
- Functional description of LTE network
- Protocol Architecture

  LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standard. The main goals of LTE is to increase the capacity and data rates of wireless data networks, improve spectrum efficiency, improve coverage, reduced latency and packet-optimized system that support mutliple Radio Access. Thus, in order to achieve the goals, the architecture of the network if different from the previous wireless data transfer network, GPRS. So, in post, a comprehensive overview of the network architecture and basic working principle of LTE network is going to be discussed.

  Basically, the LTE standard only supports packet switching with its all-IP network. The reason why LTE is designed only for packet switching is because it aims to provide seamless Internet Protocol (IP) connectivity between user equipment (UE) and the packet data network (PDN), without any disruption to the end users' applications during mobility. Due to this characteristic, voice calls and text message natively (which are typically handled by circuit-switched networks like GSM and CDMA). In LTE architecture, Evolved UTRAN (E-UTRAN) is an important role which is the air interface of LTE upgrade path for mobile networks meanwhile it is accompanied by an evolution of the non-radio aspects under the term "System Architecture Evolution" (SAE), which includes the Evolved Packet Core (EPC) network. Together LTE and SAE comprise the Evolved Packet System (EPS). Besides that, LTE network uses an eNodeB (evolved node B, essentially an LTE base station), a MME (Mobile management entity), a HSS (home subscriber server), a SGW (serving gateway), and a PGW (a packet data network gateway). These are considered as part of the EPC except eNodeB.

4. Explain the UMTS core network architecture with neat illustrations. (Apr/May 17)
UMTS Core Network Architecture

The UCN consists of a CS entity for providing voice and CS data services and a PS entity for providing packet-based services.

- The logical architecture offers a clear separation between the CS domain and PS domain.
- The CS domain contains the functional entities: mobile switching center (MSC) and gateway MSC(GMSC) (Figure 4.9).

- The PS domain comprises the functional entities: serving GPRS support node (SGSN), gateway GPRS support node (GGSN), domain name server (DNS), dynamic host configuration protocol (DHCP) server, packet charging gateway, and firewalls.
- The core network can be split into the following different functional areas:
    - Functional entities needed to support PS services (e.g. 3G-SGSN, 3G-GGSN)
    - Functional entities needed to support CS services (e.g. 3G-MSC/VLR)
    - Functional entities common to both types of services (e.g. 3G-HLR)

Other parts of the core network include :

- Network management systems (billing and provisioning, service management, element management, etc.)
- IN system (service control point (SCP), service signaling point (SSP), etc.)
- ATM/SDH/IP switch/transport infrastructure

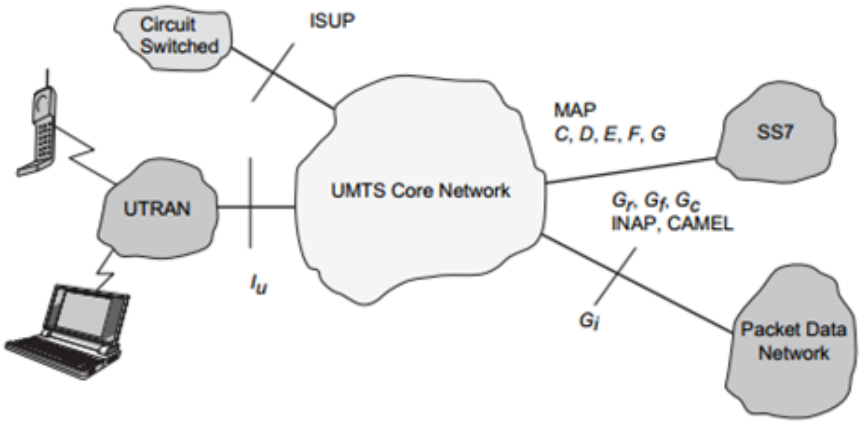
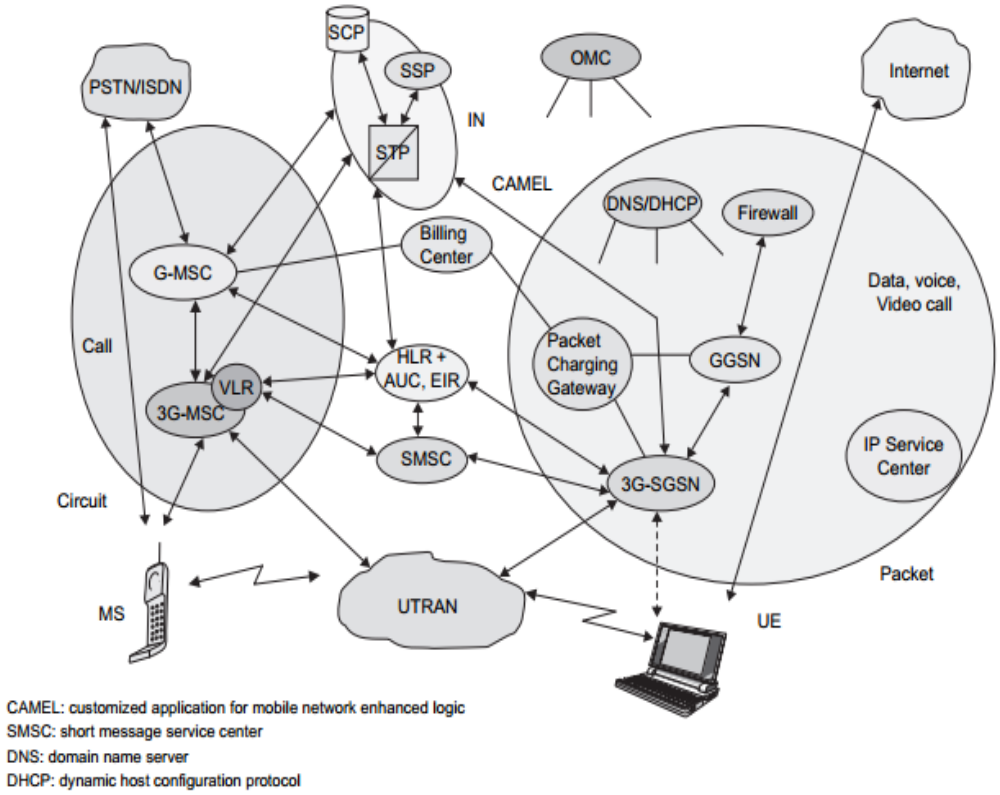


Figure 4.9 UMTS core network architecture.



Logical architecture of the UMTS core network

3G-MSC

- The 3G-MSC is the main CN element to provide CS services.
- The 3G MSC provides the interconnection to external networks like PSTN and ISDN.
- The following functionality is provided by the 3G-MSC:
  - **Mobility management:** Handles attach, authentication, HLR, SRNS relocation, and handover.
  - **Call management:** Handles call set-up messages from/to the UE.
  - **Supplementary services:** Handles call-related supplementary
  - **CS data services**: The IWF provides rate adaptation and message translation for circuit mode data services.
  - Vocoding
  - **SS7, MAP and RANAP interfaces:** The 3G-MSC is able to complete originating or terminating calls in the network.
  - ATM/AAL2 Connection to UTRAN for transportation of user plane traffic across the *Iu* interface.
  - **Short message services (SMS):** Allows the user to send and receive SMS data.
  - **VLR functionality:** The VLR is a database that may be located within the 3G-MSC and can serve as intermediate storage for subscriber data.

IN and CAMEL.OAM (operation, administration, and maintenance) agent functionality.

5. With neat illustration explain UMTS terrestrial radio access network.

UTRAN (short for "Universal Terrestrial Radio Access Network") is a collective term for the network and equipment that connects mobile handsets to the public telephone network or the Internet. It contains the base stations, which are called Node B's and Radio Network Controllers (RNCs)which make up the UMTS radio access network.This communications network, commonly referred to as 3G (for 3rd Generation Wireless Mobile Communication Technology), can carry many traffic types from real-time Circuit Switched to IP based Packet Switched. The UTRAN allows connectivity between the UE (user equipment) and the core network.

The RNC provides control functionalities for one or more Node Bs. A Node B and an RNC can be the same device, although typical implementations have a separate RNC located in a central office serving multiple Node Bs. Despite the fact that they do not have to be physically separated, there is a logical interface between them known as the Iub. The RNC and its corresponding Node Bs are called the Radio Network Subsystem (RNS). There can be more than one RNS present in a UTRAN.

There are four interfaces connecting the UTRAN internally or externally to other functional entities: Iu, Uu, Iub and Iur.[3] The Iu interface is an external interface that connects the RNC to the Core Network (CN). The Uu is also external, connecting the Node B with the User Equipment (UE). The Iub is an internal interface connecting the RNC with the Node B. And at last there is the Iur interface which is an internal interface most of the time, but can, exceptionally be an external interface too for some network architectures. The Iur connects two RNCs with each other.

- Physical layer
- Datalink layer
- Network layer

6. Explain the HSDPA objective and its operation in detail.

- IP core network Architecture
- Adaptive modulation and coding
- Fast HARQ
- UMTS Channel cards

HSDPA CHANNELS

- High Speed Downlink shared Channel
- High Speed Shared Control Channel
- High Speed Dedicated Physical Control Channel

7. Write short notes on

(i) Firewall

- This entity is used to protect the service providers' backbone data networks from attack from external packet data networks.
- The security of the backbone data network can be ensured by applying packet filtering mechanisms based on access control lists or any other methods deemed suitable

(ii) DNS/DHCP

- The DNS server is used, as in any IP network, to translate host names into IP addresses, i.e., logical names are handled instead of raw IP addresses.
- Also, the DNS server is used to translate the access point name (APN) into the GGSN IP address. It may optionally be used to allow the UE to use logical names instead of physical IP addresses.

A dynamic host configuration protocol server is used to manage the allocation of IP configuration information by automatically assigning IP addresses to systems configured to use DHCP

UNIT V

1.What are the challenges of 4G? (Apr/May 17)

- Multimode user terminals
- Wireless System Discovery and Selection
- Terminal Mobility
- Network Infrastructure and QoS Support
- Security and Privacy
- Fault tolerance and Survivability
- Multiple Operators and Billing Systems
- Personal Mobility

2. Define Multi Carrier Modulation (MCM) (Apr/May 17)

Multi Carrier Modulation (MCM) is a baseband process that uses parallel equal bandwidth sub channels to transmit information and is normally implemented with Fast Fourier Techniques (FFT) techniques.

3.Define Cognitive Radio

The Federal Communications Commission FCC defined Cognitive Radio as "A radio that can change its transmitter parameters based on interaction with the environment in which it operates.

4. What is meant by receiver diversity?

The Single Input Multiple Output (SIMO) configuration of the radio channel is known as receiver diversity. The input the channel is single transmitter signal that feeds two receiver paths. Depending on multipath fading and the correlation between two receiver gain is achieved in the form of fading resistance.

5. What is Smart Antenna?

A Smart Antenna is a multi- element antenna where the signals received at each antenna element are intelligently combined to improve the performance of the wireless system.

6.List out the applications of 4G technologies.

- Virtual Presence
- Virtual Navigation
- Tele-Medicine
- Tele-Geo-Processing applications
- Gaming
- Crisis detection and prevention
- Education
- Cloud Computing

7. What are the goals of 4G?

The ambitious goal of 4G is to allow everyone to access the Internet anytime and everywhere. The provided connection to Internet will allow users to access all types of services including text, databases and multimedia. Unlike 3G, 4G is IP based, that is every user connected to the Internet will have an IP address.

8. What are the techniques to improve network survivability in different layers?

- Prevention
- Network design and capacity allocation
- Traffic Management and restoration

9. What are the main issues in terminal mobility of 4G?

- Location Management

  With location management, the system tracks and locates a mobile terminal fir possible connection
- Handoff Management

Handoff management maintains ongoing communications when the terminal roams.

10. What are the main functions of Cognitive Radio?

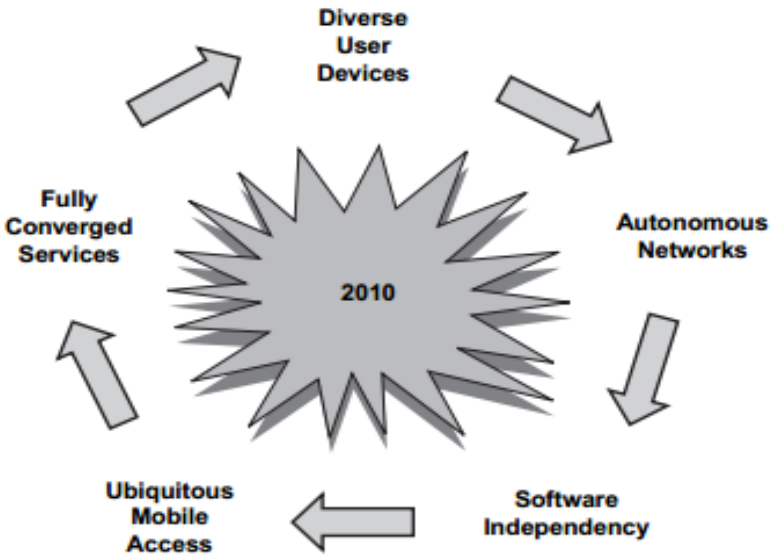
The main functions of Cognitive Radio are Spectrum Sensing, Dynamic Spectrum Management and Adaptive Communications**.**

PART B

1.Explain in detail, the 4G vision, features and challenges of 4G with applications.

Some key features of 4G mobile networks are as follows :

- High usability: anytime, anywhere, and with any technology
- Support for multimedia services at low transmission cost
- Personalization
- Integrated services



4G features

- 4G networks are all-IP-based heterogeneous networks that will allow users to use any system at anytime and anywhere.
- 4G systems provide not only telecommunications services, but also data and multimedia services. To support multimedia services, high-data-rate services with system reliability will be provided. At the same time, a low per-bit transmission cost will be maintained by an improved spectral efficiency of the system. Personalized services are provided by 4G networks.
- Users can use multiple services from any service provider at the same time.
- Table lists the key challenges and their proposed solutions.

- Figure shows the carriers migration from 3.5G to 4G systems.

	Key challenges	Proposed solutions
Mobile Station		
Multimode user terminals	To design a single user terminal that can operate in different wireless networks, and overcome design problems such as limitations in device size, cost power consumption, and backward compatibilities to systems	A software-defined radio approach can be used: the user terminal adapts itself to the wireless interfaces of the networks.
Wireless system discovery	To discover available wireless systems by processing the signals sent from different wireless systems (with different access protocols and incompatible with each other)	User- or system-initiated discoveries, with automatic download of software modules for different wireless systems
Wireless system selection	Every wireless system has its unique characteristics and role. The proliferation of wireless technologies complicates the selection of the most suitable technology for a particular service at a particular time and place.	The wireless system can be selected according to the best possible fit of user QoS requirements, available network resources, or user preferences.
System		
Terminal mobility	To locate and update the locations of the terminals in various systems. Also, to perform *horizontal* (within the same system) and *vertical* (within different systems) handoff as required with minimum handover latency and packet loss	Signaling schemes and fast handoff mechanisms are proposed.

Network infrastructure and QoS support	To integrate the existing non-IP-based and IP-based systems, and to provide QoS guarantee for end-to-end services that involves different systems	A clear and comprehensive QoS scheme for the UMTS system has been proposed. This scheme also supports interworking with other common QoS technologies.
Security	The heterogeneity of wireless networks complicates the security issue. Dynamic reconfigurable, adaptive, and lightweight security mechanisms should be developed	Modifications in existing security schemes may be applicable to heterogeneous systems. Security handoff support for application sessions is also proposed.
Fault tolerance and survivability	To minimize the failures and their potential impacts in any level of tree-like topology in wireless networks.	Fault-tolerant architectures for heterogeneous networks and failure recovery protocols are proposed.
Service		
Multioperators and billing system	To collect, manage, and store the customers' accounting information from multiple service providers. Also, to bill the customers with simple but detailed information.	Various billing and accounting frameworks are being proposed to achieve this goal.
Personal mobility	To provide seamless personal mobility to users without modifying the existing servers in heterogeneous systems.	Personal mobility frameworks are proposed. Most of them use mobile agents, but some do not.

4G Key challenges and their proposed solutions

2. Explain the Cognitive Radio architecture, functions and its Network Applications.

- Spectrum can be efficiently shared in a more flexible fashion by a number of operators/users/systems.
- The CR paradigm can be viewed as an enabling technology that will benefit several types of users by introducing new communications and networking models for the whole wireless world.
- It creates better business opportunities for the incumbent operators and new technical dimensions for smaller operators.
- It helps shape an efficient approach regarding spectrum requirements and usage in the next generation wireless networks.
- The CR can be regarded as an extension of SDR.

- In 2003, the IEEE Committee on Communications and Information Policy (CCIP) recommended CR for consideration by the FCC as a means to conserve valuable spectrum utilization.
- The CR focuses on applying software capabilities that have been developed to support algorithm control across a wide spectrum of signal processing technologies to add smarts to the software that allows it to determine when frequencies are free to use and then use them in the most efficient manner possible.
- Most of the research work currently is focusing on spectrum sensing cognitive radio, particularly on the utilization of TV bands for communication.
- The essential problem of spectrum sensing CR is the design of high quality sensing devices and algorithms for exchanging spectrum sensing data between nodes.
- A simple energy detector cannot guarantee accurate detection of signal presence.
- This calls for more sophisticated spectrum sensing techniques and requires that information about spectrum sensing be exchanged between nodes regularly.
- It is possible to implement CR features, the ability to detect and avoid (protect) incumbent users while using conventional radio transmitter/receiver architectures and techniques.
- The goal of CR is to relieve radio spectrum overcrowding, which actually translates to a lack of access to full radio spectrum utilization.

3. Write short notes on

- SIMO
- MISO
- MIMO

- **Single-input, multiple-output:**
  - There are *N* antennas at the receiver.
  - There are *N* sets of noise sources that are added coherently and result in an *N*-fold increase in noise power.
  - Hence, the overall increase in SNR will be:

$$\text{SNR} \approx \frac{N^2 \times (\text{signal power})}{N \times (\text{noise})} = N \times \text{SNR}_0$$

$$C \approx B \log_2 [1 + N \times \text{SNR}_0]$$

- **Multiple-input, single-output:**
  - The total power is divided into *M* transmitter branches.
  - If the signals add coherently at the receiving antenna, we get an *M*-fold increase in SNR as compared to SISO.
  - The overall increase in SNR is approximately

$$\text{SNR} \approx \frac{M^2 \cdot [(\text{signal power})/M]}{\text{noise}} = M \times \text{SNR}_0$$

Multiple-input, multiple-output:

- MIMO systems can be viewed as a combination of MISO and SIMO channels.
- In this case, it is possible to achieve approximately an *MN*-fold increase in the average SNR0 giving a channel capacity equal to

$$C \approx B \log_2(1 + M \times N \times \text{SNR}_0)$$

Assuming $N \geq M$, we can send different signals using the same bandwidth and still be able to decode correctly at the receiver. Thus, we are creating a channel for each one of the transmitters. The capacity of each one of these channels is roughly equal to

$$C_{\text{single}} \approx B \log_2\left(1 + \frac{N}{M} \times \text{SNR}_0\right)$$

Since we have *M* of these channels (*M* transmitting antennas), the total capacity of the system is

$$C \approx MB \log_2\left(1 + \frac{N}{M} \times \text{SNR}_0\right)$$

4. Write short notes on MIMO OFDM.

- OFDM and MIMO techniques can be combined to achieve high spectral efficiency and increased throughput.
- The OFDM-MIMO system transmits independent OFDM modulated data from multiple antennas simultaneously.

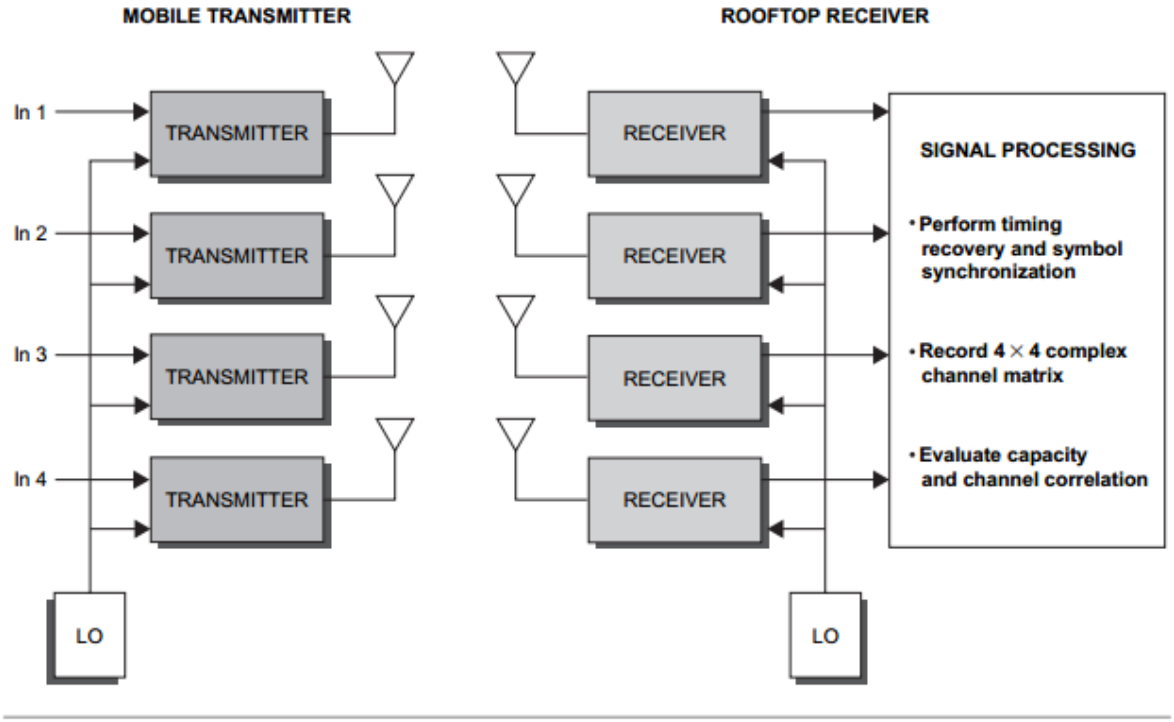
At the receiver, after OFDM demodulation, MIMO decodes each subchannel to extract data from all transmit antennas on all the subchannels

5. Explain smart antenna technologies in detail.

- Smart antenna techniques, such as multiple-input multiple-output (MIMO) systems, can extend the capabilities of the 3G and 4G systems.
- MIMO systems use multiple antennas at both the transmitter and receiver to increase the capacity of the wireless channel
- With MIMO systems, it may be possible to provide in excess of 1 Mbps for 2.5G wireless TDMA EDGE and as high as 20 Mbps for 4G systems.

- With MIMO, different signals are transmitted out of each antenna simultaneously in the same bandwidth and then separated at the receiver.
- High capacities are theoretically possible, unless there is a direct line of-sight between the transmitter and receiver.
- The number of transmitting antennas is M, and the number of receiving antennas is N, where **N≥M**.
- Four cases:
  - **Single-Input, Single-Output (SISO)**
  - **Single-Input, Multiple-Output (SIMO)**
  - **Multiple-Input, Single-Output (MISO)**
  - **Multiple-Input, Multiple-Output (MIMO)**
- **Single-input, single-output:** The channel bandwidth is *B*, the transmitter power is *Pt*, the signal at the receiver has an average signal-to-noise ratio of SNR0, then the Shannon limit on channel capacity *C* is

$$C \approx B \log_2(1 + \mathrm{SNR}_0)$$



6.Explain in detail about the Multi carrier modulation (MCM) .

- Multicarrier modulation (MCM) is a derivative of frequency-division multiplexing.
- Forms of multicarrier systems are currently used in DSL modems and digital audio/video broadcast (DAB/DVB).
- MCM is a baseband process that uses parallel equal bandwidth subchannels to transmit information and is normally implemented with fast Fourier transform (FFT) techniques.
- **Advantages of MCM:**
  - Better performance in the inter-symbol-interference environment
  - Avoidance of single-frequency interferers
- **Limitations:**
  - MCM increases the peak to-average ratio of the signal, and
  - To overcome inter-symbol-interference a cyclic extension or guard band must be added to the data.
  - The difference, D, of the peak-to-average ratio between MCM and a single carrier system is a function of the number of subcarriers, N :

    D(dB) = 10 logN

- Loss in signal-to-noise ratio (SNR):

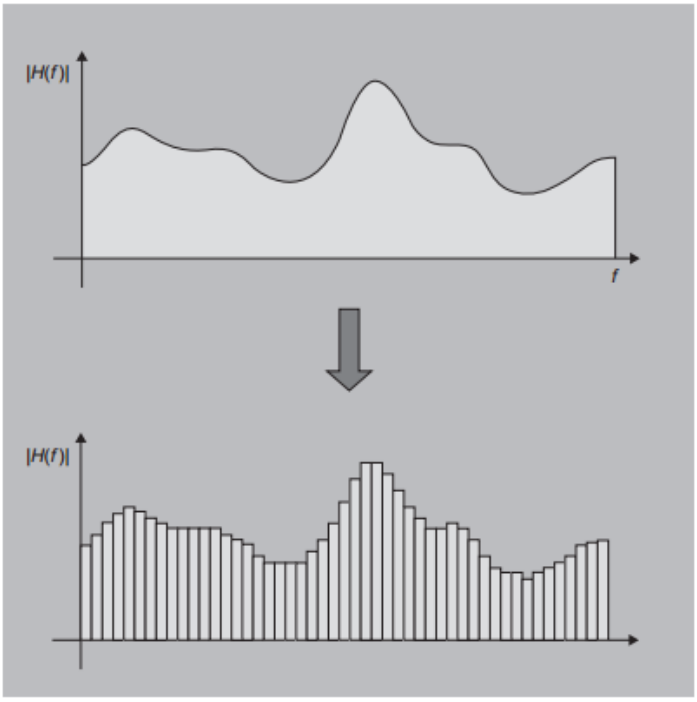
$$(\text{SNR})_{\text{loss}} = 10 \log \frac{L_b + L_c - 1}{L_b} \text{ (dB)}$$

Where L_b **-- the original length of block,**

L_c **-- channel's response is of length**

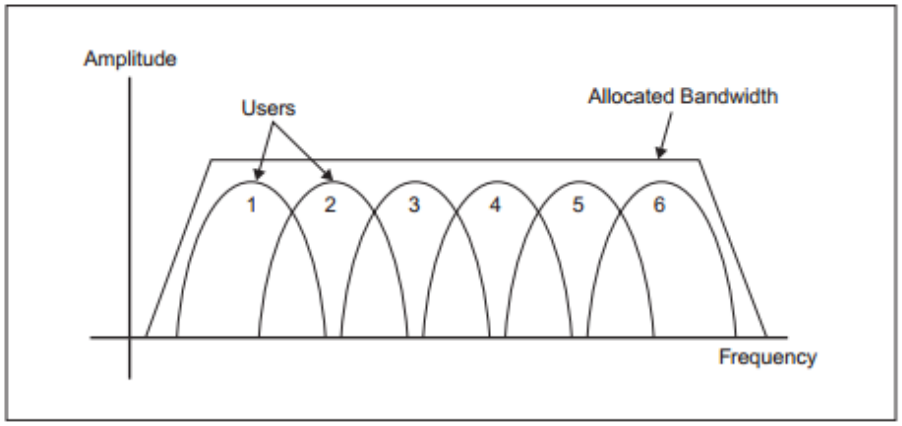
$L_b + L_c - 1$ **--New length of the cyclically extended symbol**

- The new symbol of length $\mathbf{L_b + L_c - 1}$ sampling periods has no inter-symbol interference.
- Two different types of MCM are**:**
  - **Multicarrier code division multiple access (MC-CDMA) and**
  - **Orthogonal frequency division multiplexing (OFDM) using time division multiple access (TDMA)**
- Similar to single-carrier CDMA systems, the **users are multiplexed with orthogonal codes to distinguish users in MC-CDMA.**
- However, in MC-CDMA, each user can be allocated several codes. Eitherway, multiple users simultaneously access the system.
- In OFDM with TDMA, the users are assigned time slots to transmit and receive data.
- Typically **MC-CDMA uses quadrature phase shift keying (QPSK) for modulation**, while **OFDM with TDMA could use** more high-level modulations, such as **multilevel quadrature amplitude modulation (M-QAM)** (where M 4 to 256).



A broadband channel divided into many parallel narrowband channels.

- The OFDM divides a broadband channel into many parallel subchannels.
- The subchannel pulse shape is a square wave (see Fig 5.4).
- The OFDM receiver senses the channel and corrects distortion on each subchannel before the transmitted data can be extracted.
- This ensures that even though subchannels overlap, they do not interfere with each other (Fig.5.5)



Overlapping subchannels

7. Elaborate Adaptive modulation and Coding with time slot scheduler

- TCP/IP is designed for a highly reliable transmission medium in wired networks where packet losses are interpreted as congestion in the network.
- A wireless network uses a time varying channel where packet losses may be common due to severe fading. This is misinterpreted by TCP as congestion which leads to inefficient utilization of the available radio link capacity.
- There is a need for a system with efficient packet data transmission using TCP in 4G. This can be achieved by using a suitable automatic repeat request (ARQ) scheme combined with an adaptive modulation and coding system, and a time-slot scheduler that uses channel predictions.
- This way, the lower layers are adapted to channel conditions while still providing some robustness through retransmission.
- The time-slot scheduler shares the spectrum efficiently between users while satisfying the QoS requirements.
- If the channel quality for each radio link can be predicted for a short duration, then ARQ along with an adaptive modulation and coding system can be selected for each user to satisfy the bit error rate (BER) requirement and provide high throughput.
- The scheduler uses this information about individual data streams (along with predicted values of different radio links and selected modulation and coding systems by the link layer) and distributes the time slots among the users.
- The planning is done so that the desired QoS and associated priority to different users are guaranteed while channel spectrum is efficiently utilized.

Channel type	Capacity (Mbps)	Normalized capacity with respect to SISO
SISO	3.45 B	1.0
SIMO	5.66 B	1.64
MISO	5.35 B	1.55
MIMO (with same input)	7.64 B	2.21
MIMO (with different input)	15 B	4.35

Comparison of channel capacity for different channel types.