MOBILE COMMUNICATIONS

(18KP4CSELCS4:A)

UNIT-III,IV &V

V.CHEZHIYAN
Assistant Professor
Department of Computer science
KNGAC, Thanjavur.

***Objective: To** improve skills in mobile communication technology.*

Unit - III : Wireless LAN : IEEE 802.11: System And Protocol Architecture - MAC Management-802.11a - 802.11b - Newer Development - Bluetooth: User Scenarios Architecture.

Unit – IV : Mobile Network Layer : Mobile IP: Goals Assumptions And Requirements – Entities And Terminology - IP Packet Delivery – Agent Discovery – Registration- Tunneling and Encapsulation – Optimizations– Reverse Tunneling – IPV6 – IP Micro Mobility Support – Dynamic Host Configuration Protocol- Mobile Ad-Hoc Networks: Routing – Destination Sequence Distance Vector – Dynamic Source Routing – Alternative Matrices – Overview. Mobile Transport Layer: Traditional TCP: Congestion Control – Slow Start – Fast Retransmit/Recovery – Implication of Mobility - Classical TCP Improvements - TCP Over 2.5 / 3G Wireless Networks

Unit-V : 3G: LTE Introduction - OFDM, OFDMA, SC-FDMA - LTE MIMO - TDD & FDD - Frame & sub frame - Physical logical & transport channels - Bands and spectrum - UE categories - SAE architecture - LTE SON - VoLTE - SRVCC - Security.

WLAN

Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network). Users connected by wireless LANs can move around within this limited area such as home, school, campus, office building, railway platform, etc.
Most WLANs are based upon the standard IEEE 802.11 standard or WiFi.

IEEE 802.11: System And Protocol Architecture

The architecture of the IEEE 802.11 WLAN is designed to support a network where most decision making is distributed to mobile stations. This type of architecture has several advantages. It is tolerant of faults in all of the WLAN equipment and eliminates possible bottlenecks a centralized architecture would introduce. The architecture is flexible and can easily support both small, transient networks and large, semipermanent or permanent networks. In addition, the architecture and protocols offer significant power saving and prolong the battery life of mobile equipment without losing network connectivity.

Two network architectures are defined in the IEEE 802.11 standard:

- WLANs, as standardized by IEEE 802.11, operates in two basic modes, infrastructure, and ad hoc mode.
- **Infrastructure Mode** − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet. The client transmits frames to other clients via the AP.
- **Ad Hoc Mode** − Clients transmit frames directly to each other in a peer-to-peer fashion.
-

Components of WLAN

Stations (STA) − Stations comprises of all devices and equipment that are connected to the wireless LAN. Each station has a wireless network interface controller. A station can be of two types −

- Wireless Access Point (WAP or AP)
- Client

Basic Service Set (BSS) − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories −

- Infrastructure BSS
- Independent BSS

Extended Service Set (ESS) − It is a set of all connected BSS.

Distribution System (DS) − It connects access points in ESS.

Advantages of WLANs

They provide clutter-free homes, offices and other networked places.

The LANs are scalable in nature, i.e. devices may be added or removed from the network at greater ease than wired LANs.

- The system is portable within the network coverage.

Access to the network is not bounded by the length of the cables.

- Installation and setup are much easier than wired counterparts.
- The equipment and setup costs are reduced.
-

Disadvantages of WLANs

- Since radio waves are used for communications, the signals are noisier with more interference from nearby systems.
- Greater care is needed for encrypting information. Also, they are more prone to errors. So, they require greater bandwidth than the wired LANs.

- WLANs are slower than wired LANs.

802.11 FRAME FORMAT

Types

□ control frames, management frames, data frames

□ Sequence numbers

□ important against duplicated frames due to lost ACKs

□ Addresses

□ receiver, transmitter (physical), BSS identifier, sender (logical)

□ Miscellaneous

□ sending time, checksum, frame control, data bytes.

IEEE 802.11 MAC Management

Synchronization

□ try to find a LAN, try to stay within a LAN

□ timer etc.

□ Power management

□ sleep-mode without missing a message

□ periodic sleep, frame buffering, traffic measurements

□ Association/Reassociation

□ integration into a LAN

□ roaming, i.e. change networks by changing access points

□ scanning, i.e. active search for a network
□ MIB - Management Information Base
□ All parameters concerning the present state of the wireless station and access point are stored in MIB. These can be accessed via a protocol line SNMP.

POWER MANAGEMENT

Idea: switch the transceiver off if not needed
□ States of a station: sleep and awake
□ Timing Synchronization Function (TSF)
□ For sender, it is not an issue as the transmitter knows when it is ready for sending frames.
□ Transmitter has to buffer the frame to make sure that it will transmit when the receiver is ready to receive. stations wake up at the same time periodically and listen to the transmitter.
□ Waking up at the right time needs the TSF.
□ Along with beacon, a Traffic Indication Map(TIM- containing the list of stations
for which buffering has been done in the AP.) is also sent.
□ Infrastructure
□ Traffic Indication Map (TIM)
□ list of unicast receivers transmitted by AP
□ Delivery Traffic Indication Map (DTIM)
□ list of broadcast/multicast receivers transmitted by AP
□ Ad-hoc
□ Ad-hoc Traffic Indication Map (ATIM)
□ announcement of receivers by stations buffering frames
□ more complicated - no central AP
□ collision of ATIMs possible (scalability)

802.11a

The IEEE 802.11a standard is the first standard in the IEEE 802.11 series. It defines a WiFi format for providing wireless connectivity in the 5 GHz ISM band to give raw data speeds of up to 54Mbps.

Although, alphabetically it is the first standard in the 802.11 series, t was released at the same time as IEEE 802.11b which was aimed at connectivity using the 2.4 GHz ISM band.

Using the technology of the time, IEEE 802.11a was more costly and a little more difficult to implement as it operated at 5 GHz rather than 2.4 GHz and as a result it was less widely used.

802.11a boasted an impressive level of performance. It was able to transfer data with raw data rates up to 54 Mbps and at the time it was thought to have a good range, although it could not provide the maximum data rate at its extremes.

The 802.11a standard uses basic 802.11 concepts as its base, and it operates within the 5GHz Industrial, Scientific and Medical (ISM) band enabling it to be used worldwide in a licence free band. The modulation is Orthogonal Frequency Division Multiplexing (OFDM) to enable it to transfer raw data at a maximum rate of 54 Mbps, although a more realistic practical level is in the region of the mid 20 Mbps region. The data rate can be reduced to 48, 36, 24, 18, 12, 9 then 6 Mbit/s if required. 802.11a has 12 non-overlapping channels, 8 dedicated to indoor and 4 to point to point.

802.11b

802.11b is a Wi-Fi (Wireless LAN) standard. It is used for wireless internet purposes, mainly to connect to the internet or a network wirelessly. Examples of these include personal/home networks, Internet "Hotspots" found at coffee shops, etc.

Products that use this technology include PCs via a wireless 802.11b card, wireless routers (in order to setup access points), and various handheld devices
802.11b (also referred to as 802.11 High Rate or Wi-Fi) is an IEEE standard and an extension to 802.11 that applies to wireless LAN's and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1-Mbps) in the 2.4 GHz band.
802.11b was a ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.

Bluetooth

Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the industrial, scientific and medical radio bands, from 2.402 GHz to 2.480 GHz, and building personal area networks (PANs).

Components of Bluetooth-A Bluetooth circuit is the central part of a Bluetooth and contains components such as the integrated circuit, capacitors and source of power. The course supports wired-in audio, wireless stereo, Bluetooth module and many more. The IC contains a charger and **voltage regulator**

Bluetooth Applications

In **laptops**, **notebooks** and wireless PCs.
In **mobile phones** and **PDAs** (**personal digital assistant**).
In printers.
In wireless headsets.
In wireless PANs (personal area networks) and even LANs (local area networks)
To transfer data files, videos, and images and **MP3** or MP4.

Architecture

Bluetooth network technology connects mobile devices wirelessly over a short-range to form a personal area network (PAN). The Bluetooth architecture has its own independent model with a **stack** of protocols, instead of following the standard OSI model or TCP/IP model.

Bluetooth communication occurs between a master radio and a slave radio. Bluetooth radios are symmetric in that the same device may operate as a master and also the slave. Each radio has a 48-bit unique device address (BD_ADDR) that is fixed.

Two or more radio devices together form ad-hoc networks called piconets. All units within a piconet share the same channel. Each piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a piconet. Thus, each active device within a piconet is identifiable by a 3-bit active device address. Inactive slaves in unconnected modes may continue to reside within the piconet.

A master is the only one that may initiate a Bluetooth communication link. However, once a link is established, the slave may request a master/slave switch to become the master. Slaves are not allowed to talk to each other directly. All communication occurs within the slave and the master. Slaves within a piconet must also synchronize their internal clocks and frequency hops with that of the master. Each piconet uses a different frequency hopping sequence. Radio devices used Time Division Multiplexing (TDM). A master device in a piconet transmits on even numbered slots and the slaves may transmit on odd numbered slots.

Newer Developments

802.11e(Mac enhancements)

802.11f(Inter-Access point protocol)

802.11g (Data rates above 20 mbit/s at 2.4GHz)

802.11h (Spectrum managed 802.11a)

802.11i (Enhanced security mechanisms)

802.11n (Next generation wireless Lan Technology).

IEEE 802.11 study groups for latest topics. The group ‘Radio Resource Measurements’ try to measure of radio resourcesThe HEW 802.11ax standard will replace both **802.11n** and 802.11ac, becoming a high-efficiency **WLAN standard** for both 2.4G and **5G** networks and focusing on multi-user environments.

UNIT – IV – MOBILE NETWORK LAYER

Mobile Network Layer

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing that is selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are placed in the header by the network layer.

The functions of the Network layer are:

Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is knowing as routing.

Logical addressing: in order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender and receiver's IP address are placed in the header by network layer. The network layer provides the means of transferring variable-length network packets from a source to destination host via one or more network.

Motivation for Mobile IP

IP Routing

- based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
- change of physical subnet implies change of IP address to have a topologically correct address (standard IP) or needs special entries in the routing tables

Specific routes to end-systems:

- requires changing all routing table entries to forward packets to the right destination
- does not scale with the number of mobile hosts and frequent changes in the location, security problems

Changing the IP-address:

- adjust the host IP address depending on the current location
- almost impossible to find a mobile system, DNS updates take long time
- TCP connections break, security problems

Mobile IP solves the following problems:

- if a node moves without changing its IP address it will be unable to receive its packets,
- if a node changes its IP address it will have to terminate and restart its ongoing connections every time it moves to a new network area (new network prefix).

Goals of Mobile IP:

The goal of a mobile IP can be summarized as: 'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and internet protocols'

Mobile IP is an internet protocol designed to support host mobility. Its goal is to provide the ability of a host to stay connected to the internet regardless o their location. Mobile IP is able to track a mobile host without needing to change the mobile host's long term IP address.
Requirements:

Transparency

- mobile end-systems keep their IP address
- continuation of communication after interruption of link possible
- point of connection to the fixed network can be changed

Compatibility

- support of the same layer 2 protocols as IP
- no changes to current end-systems and routers required
- mobile end-systems can communicate with fixed systems
- authentication of all registration messages
- only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
- world-wide support of a large number of mobile systems in the whole Internet.

Security

- authentication of all registration messages
- all the messages related to the management of mobile IP are authenticated
- the IP layer can guarantee that the IP addresses of the receiver is correct.

Efficiency and scalability

- only little additional messages to the mobile system required.
- world-wide support of a large number of mobile systems in the whole Internet.

Entities and terminology:

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 other system in the internet as long as link-layer connectivity is given. Examples are laptop, mobile phone, router on an aircraft etc.

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 visits and 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, acting as tunnel endpoint and forwarding packets to the MN.
- The FA can be the default router for the MN.
- FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.
- FA is implemented on a router for the subnet the MN attaches to.

Care-of address (COA):

- The COA 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 IP address of the MN.
- Packet delivery toward the MN is done using a tunnel, i.e., the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel.
- There are two different possibilities for the location of the COA:

  a. 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.

  b. Co-located COA:

  - The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA.
  - This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP. IP packet delivery

Home Agent (HA)

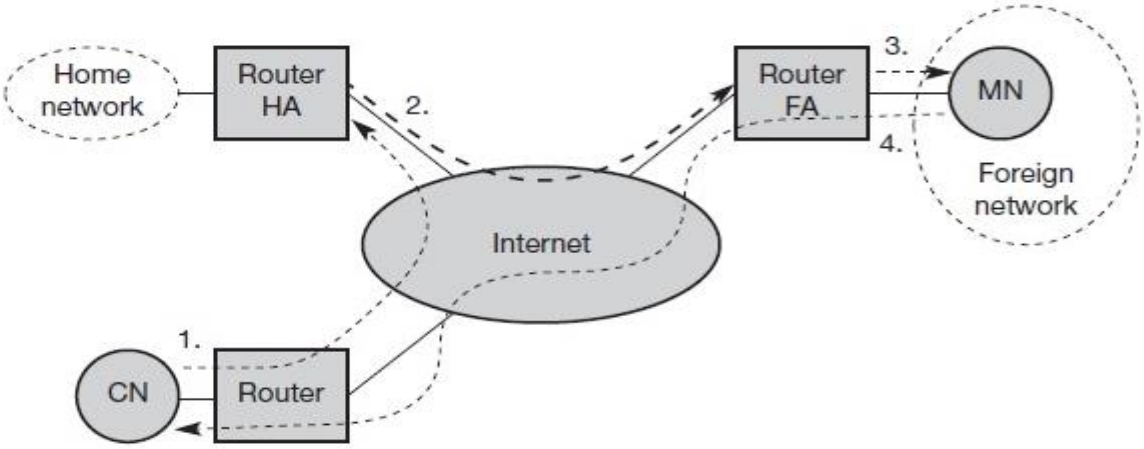
The home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist.

- Home agent can be implemented on a **router** that is responsible for the home network. This is obviously the best position, because without optimization to mobile IP, all packets for the MN have to go through the router anyway.
- If changing the router's software is not possible, the home agent could also be implemented on an **arbitrary node** in the subset. One biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign

network. A packet for the mobile node comes in via the router; the HA sends it through the tunnel which again crosses the router.

IP Packet Delivery

The mobile that is movement of MN from one location to another has to be hidden as per the requirement of mobile IP. CN may not know the exact location of MN



STEP 1: CN sends the packet as usual to the IP address of MN. With Source address as CN and Destination address as MN. The internet, which does not have any information of the current location of MN. This is done using the standard routing mechanisms of the internet.

STEP 2: The HA now diverts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet.

STEP 3: The foreign agent (FA) now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN. Again, for the MN mobility is not visible. Finally the MN Receives the packet with the Source address as CN and Destination address as MN.

STEP 4: The MN sends the packet MN as Source Address and CN as Destination Address. The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. Simple mechanism works if CN is fixed at a location if it has got mobility then the above Steps 1 to 3 are to be followed to deliver the packet from MN to CN.

Agent Discovery

This is the phase where mobile node discovers its foreign and home agents. A mobile node first determines its connected location by using ICMP router discovery messages. If it's connected location is with the local network, then the normal IP routing is used for the communication. When a mobile node determines that it has moved to a foreign network it obtains a care-of address from the foreign agent reflecting its current location.

Two types of "care-of" addresses exist –

- The care-of addresses acquired from a Foreign Agent: An IP address of a Foreign Agent that has an interface on the foreign network being visited by a Mobile node.
- The collocated care-of address: This represents the current position of the Mobile Node on the foreign network and can be used by only one Mobile node at a time.

Agent Advertisement

- HA and FA periodically send advertisement messages into their physical subnets
- MN listens to these messages and detects, if it is in the home or a foreign network (Standard case for home network)
- MN reads a COA from the FA advertisement messages

- **Registration** (always limited lifetime!)
  - MN signals COA to the HA via the FA, HA acknowledges via FA to MN
  - These actions have to be secured by authentication

- **Advertisement**
  - HA advertises the IP address of the MN (as for fixed systems), i.e. standard routing information
  - routers adjust their entries, these are stable for a longer time (HA responsible for a MN over a longer period of time)
  - packets to the MN are sent to the HA,
  - independent of changes in COA/FA

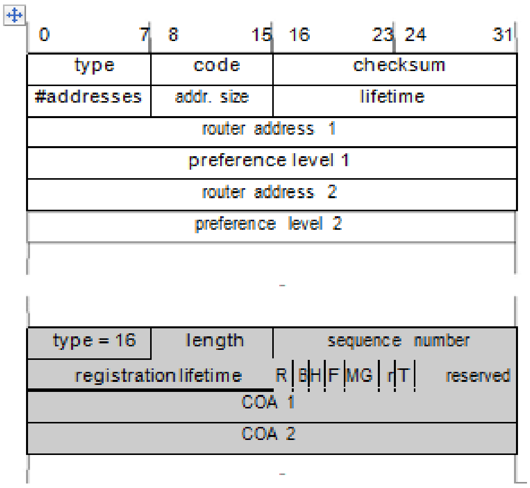


Figure 8.3
Agent advertisement packet (RFC 1256 + mobility extension)

- type = 16
- R: registration required
- H: home agent
- M: minimal encapsulation
- r: =0, ignored
- reserved: =0, ignored

length = 6 + 4 * #COAs
- B: busy, no more registrations
- F: foreign agent
- G: GRE encapsulation
- T: FA supports reverse tunneling

Agent Solicitation

• If no agent advertisements are present or the inter-arrival time is too high, and an MN has not received a COA the mobile node must send agent solicitations. These solicitations are again based on RFC 1256 for router solicitations. Care must be taken to ensure that these solicitation messages do not flood the network, but basically an MN can search for an FA endlessly sending out solicitation messages.

Registration

• Having received a COA, the MN has to register with the HA. The main purpose of the registration is to inform the HA of the current location for correct for-warding of packets. Registration can be done in two different ways depending on the location of the COA

• If the COA is at the FA, registration is done as illustrated in Figure. The MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now sets up a mobility binding containing the mobile node's home IP address and the current COA.

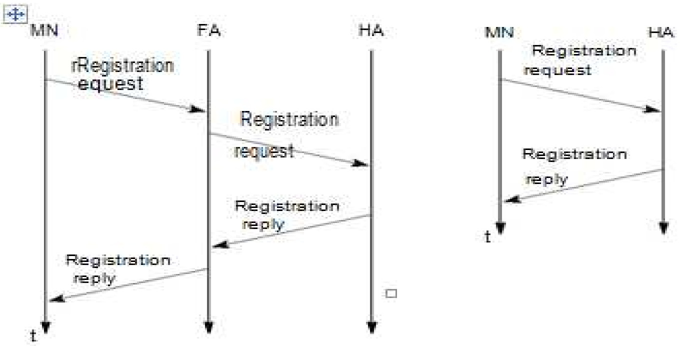
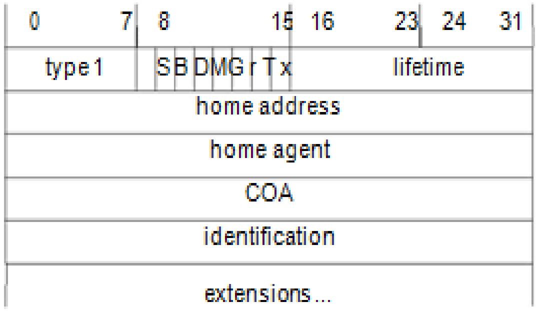


Figure 8.4 Registration of a mobile node via the FA or directly with the HA

Mobile IP registration request:

• If the COA is co-located, registration can be simpler, as shown in Figure . The MN may send the request directly to the HA and vice versa.



0 7	8 15	16 23 24 31
type 1	S B D M G r T x	lifetime
home address		
home agent		
COA		
identification		
extensions ...		

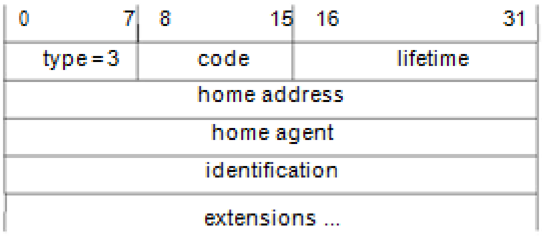
Figure 8.5
Registration request

S: simultaneous bindings
• B: broadcast datagrams • D: decapsulation by MN
• M minimal encapsulation • G: GRE encapsulation
• r: =0, ignored • T: reverse tunneling requested • x: =0, ignored

Mobile IP registration reply

• UDP packets are used for registration requests. The IP source address of the packet is set to the interface address of the MN, the IP destination address is that of the FA or HA.

Figure 8.6
Registration reply



• **Lifetime** denotes the validity of the registration in seconds. A value of zero indicates deregistration; all bits set indicates infinity.

• The **home address** is the fixed IP address of the MN.

• **home agent** is the IP address of the HA, and **COA** represents the tunnel endpoint

• . The 64 bit **identification** is generated by the MN to identify a request and match it with registration replies. This field is used for protection against replay attacks of registrations.

• The **extensions** must at least contain parameters for authentication.

Tunneling and Encapsulation

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

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

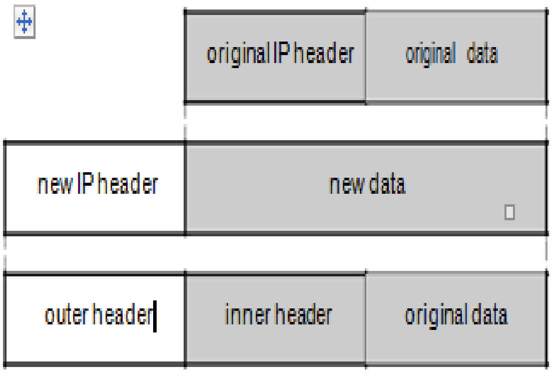
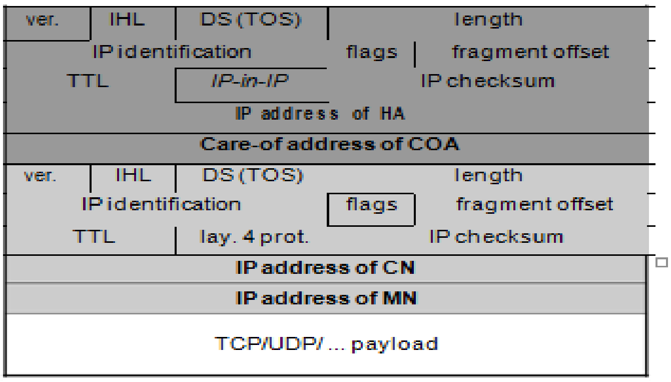


Figure 8.7
IP encapsulation

•

i i) IP-in-IP-encapsulation: .

Figure 8.8
IP-in-IP encapsulation



- The version field **ver** is 4 for IP version 4.
- The internet header length (**IHL**) denotes the length of the outer header in 32 bit words. **DS(TOS)** is just copied from the inner header,
- The **length** field covers the complete encapsulated packet.
- TTL must be high enough so the packet can reach the tunnel endpoint.
- The next field, here denoted with **IP-in-IP**, is the type of the protocol used in the IP payload. This field is set to 4, the protocol type for IPv4 because again an IPv4 packet follows after this outer header.
- IP **checksum** is calculated as usual.
- The next fields are the tunnel entry as source address (the **IP address of the HA**) and the tunnel exit point as destination address (the **COA**).

ii)Minimalencapsulation:

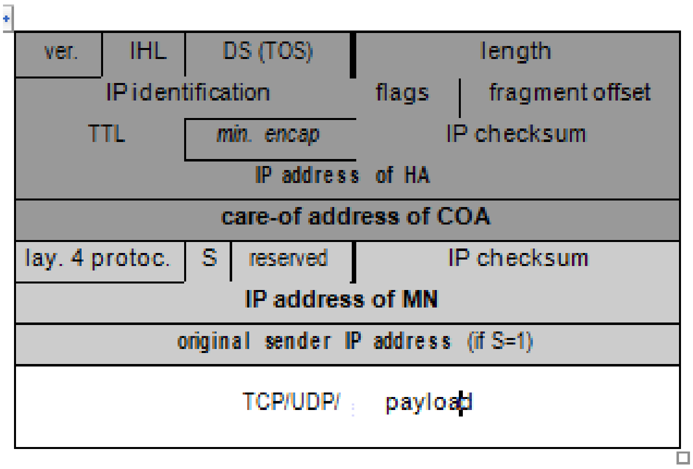
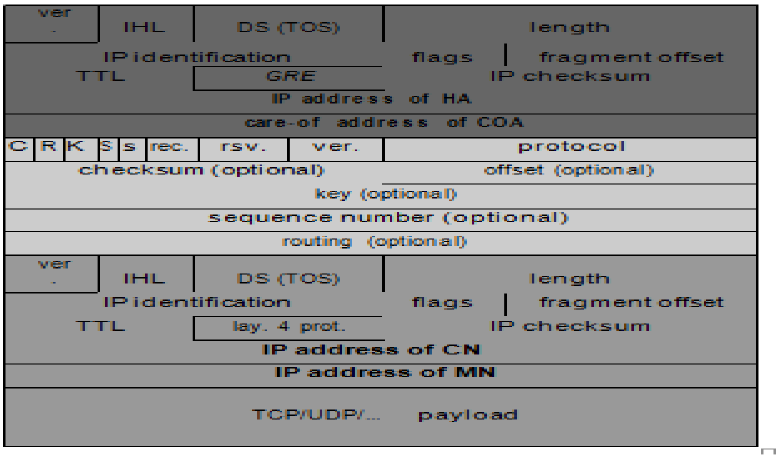


Figure 8.9
Minimal encapsulation

- avoids repetition of identical fields
- e.g. TTL, IHL, version, TOS
- only applicable for unfragmented packets, no space left for fragment **identification.**

iii)Generic routing encapsulation:

Figure 8.11
Protocol fields for GRE according to RFC 1701



- While IP-in-IP encapsulation and minimal encapsulation work only for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP. Generic routing encapsulation (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.

- A minimal GRE header uses only 4 bytes; nevertheless, GRE is flexible enough to include several mechanisms in its header.

- The C bit indicates if the checksum field is present and contains valid information. If C is set, the checksum field contains a valid IP checksum of the GRE header and the pay-load.
- The R bit indicates if the offset and routing fields are present and contain valid information. The offset represents the offset in bytes for the first source routing entry. The routing field, if present, has a variable length and contains fields for source routing.
- If the C bit is set, the offset field is also present and, vice versa, if the R bit is set, the checksum field must be present. The only reason for this is to align the following fields to 4 bytes. The checksum field is valid only if C is set, and the offset field is valid only if R is set respectively.
- GRE also offers a **key** field which may be used for authentication. If this field is present, the **K** bit is set.
- The sequence number bit **S** indicates if the **sequence** number field is present, if the s bit is set, strict source routing is used.
- **reserved** fields must be zero and are ignored on reception. The **version** field contains 0 for the GRE version.
- The **ver-sion** field contains the value zero. The **protocol** type, again, defines the protocol of the payload following RFC 3232.

Optimizations

i) Optimization of packet forwarding

- Change of FA

• packets on-the-fly during the change can be lost

• new FA informs old FA to avoid packet loss, old FA now forwards remaining packets to new FA

• this information also enables the old FA to release resources for the MN

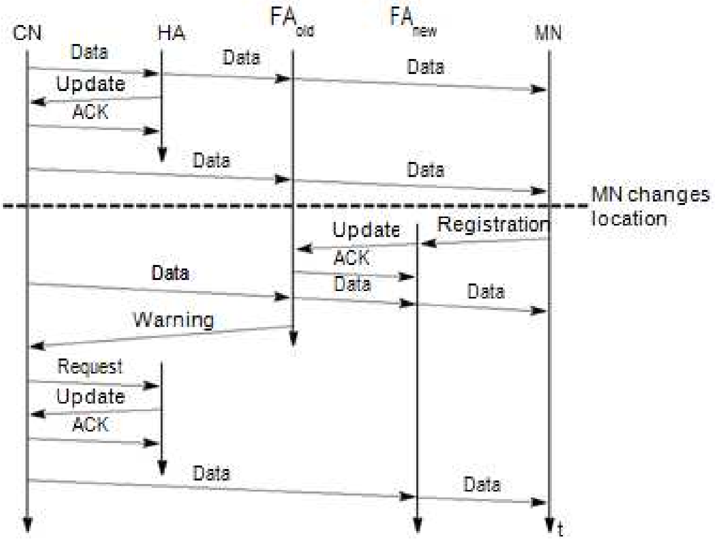


Figure 8.13
Change of the foreign agent with an optimized mobile IP

Triangle routing has the MN correspond directly with the CN using its home address as the SA

• Firewalls at the foreign network may not allow that

• Multicasting: if a MN is to participate in a multicast group, it needs to use a reverse tunnel to maintain its association with the home network.

• TTL: a MN might have a TTL that is suitable for communication when it is in its HM. This TTL may not be sufficient when moving around. When using a reverse tunnel, it only counts as a single hop. A MN does not want to change the TTL every time it moves.

Solution: reverse tunneling

Reverse tunneling

• Routers accept often only "topologically correct" addresses.

• a packet from the MN encapsulated by the FA is now topologically correct

• Multicast and TTL problems solved

• Reverse tunneling does not solve

• all problems with firewalls, the reverse tunnel can be abused to circumvent security mechanisms.

• Optimization of data paths, i.e. packets will be forwarded through the tunnel via the HA to a sender.

• The new standard is backwards compatible

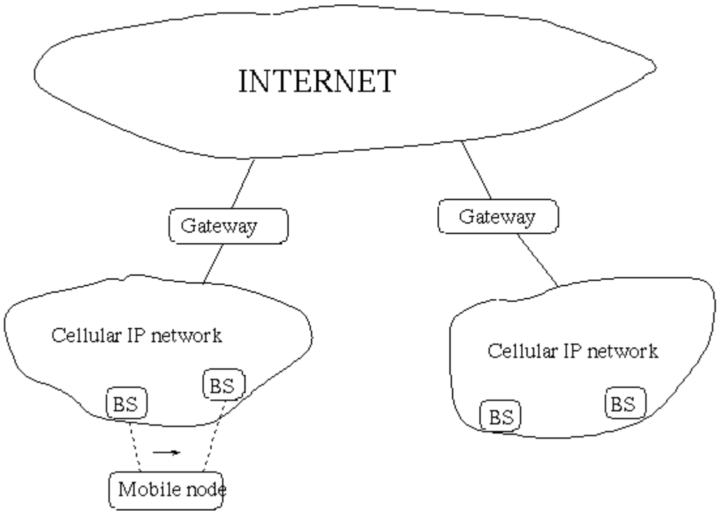
•the extensions can be implemented easily

IP Micro-mobility support:

The **micro mobility** term **means** the **mobile** node's movements inside a network. The **mobile** nodes may change their point of connection to the Internet very frequently.

Cellular IP

The cellular IP protocol provides mobility and handoff support for very frequently moving hosts. However, it is also capable of handling rarely moving and totally static hosts as well. The cellular IP is intended to be used in local or metropolitan area networks. One of the main differences to the other micro mobility solutions is that in cellular IP the location management for idle mobile hosts is different from hosts that are actively transmitting or receiving data.



The base stations periodically broadcast beacon signals and mobile hosts use them to locate the nearest base station. A mobile host can send an IP packet to the Internet by sending it to the nearest base station. The base station then routes the packet to the cellular IP gateway providing access to the Internet.

All the cellular IP nodes are responsible of maintaining a cache containing routing information. An entry in the cache binds the mobile node's IP address with the direction where the mobile node is located. When a mobile node sends an IP packet, it goes through the necessary cellular IP nodes and after that the nodes have the necessary information about the mobile node's location. Every cellular IP node knows only the next hop to the downlink direction. The mobile node's reverse direction packets can be delivered through the same path.

HAWAII

- HAWAII stands for Handoff-Aware Wireless Access Internet Infrastructure
- No HA is involved when MN is in home domain where MN is identified by its IP address

- When MN moves to HAWAII domain (foreign domain) , it obtains co-located COA (step 1)
- and registers with HA (step 2)
- This CCoA remains unchanged as long as MN in foreign domain (therefore no need to notify HA unless MN moves to new domain)
- MN sends registration request to new BS (step 3)
- the BS intercepts registration request and sends out hand-off update message, which reconfigures all routers on the paths from the old and new BS to the so-called crossover router (step 4)
- The BS then sends a registration reply to MN as if it were the FA

Hierarchical Mobile IPv6

Hierarchical Mobile IPv6 (HMIPv6) has been proposed to accommodate frequent mobility of the mobile nodes and reduce the signaling load in the Internet. Though it is being considered as an efficient local mobility management protocol, its performance may vary widely depending on the various mobility and traffic related parameters. Therefore, it is essential to investigate the effects of these parameters and conduct in-depth performance study of HMIPv6.

For the analysis of HMIPv6, we present a new analytical method using the mobility model based on imbedded Markov chain and a simplistic hierarchical network model. Based on these models, we analytically derive the location update cost, packet tunnelling cost, and total signaling cost, respectively, in HMIPv6. In addition, we investigate the effects of various parameters such as the speed of a mobile node, binding lifetime, and packet arrival rate on the total signaling cost generated by a mobile node during its average MAP domain residence time. The analytical results demonstrate that the signaling load generated by HMIPv6 decreases as the speed of a mobile node and binding lifetime get larger, and its packet arrival rate gets smaller.

DHCP: Dynamic Host Configuration Protocol

Application

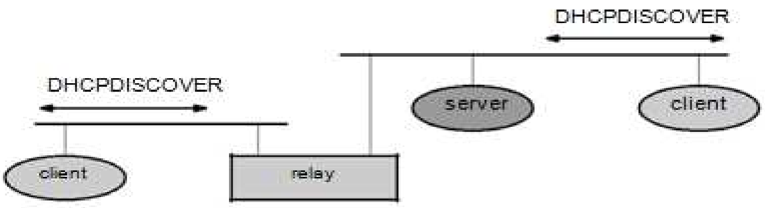
• Simplification of installation and maintenance of networked computers

• Supplies systems with all necessary information, such as IP address, DNS server address, domain name, subnet mask, default router etc.

• Enables automatic integration of systems into an intranet or the internet, can be used to acquire a COA for mobile IP

Client/Server-Model

Figure 8.17
Basic DHCP
configuration



• The client sends via a MAC broadcast a request to the DHCP server.

• The client broadcasts a DHCPDISCOVER into the subnet.

• Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters. The client can now choose one of the configurations offered. The client in turn replies to the servers, accepting one of the configurations and rejecting the others using DHCPREQUEST.

- If a server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients. The server with the configuration accepted by the client now confirms the configuration with DHCPACK. This completes the initialization phase.

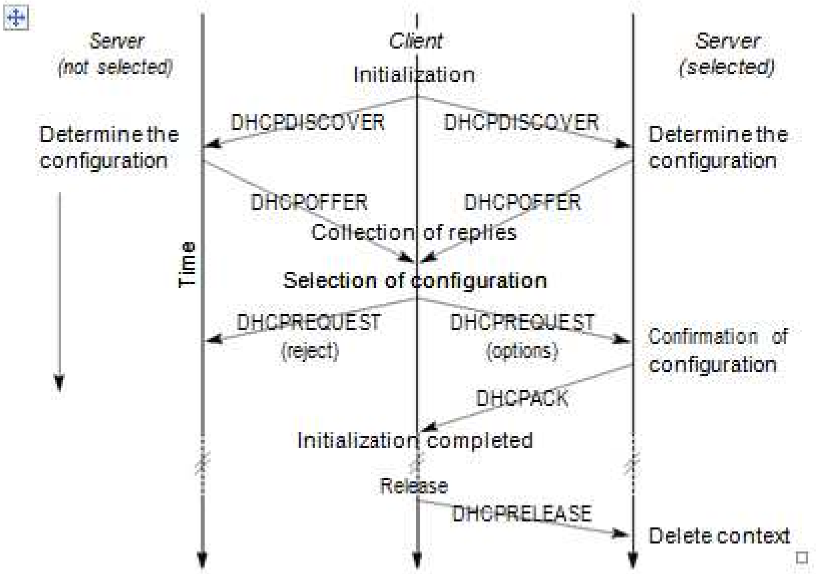
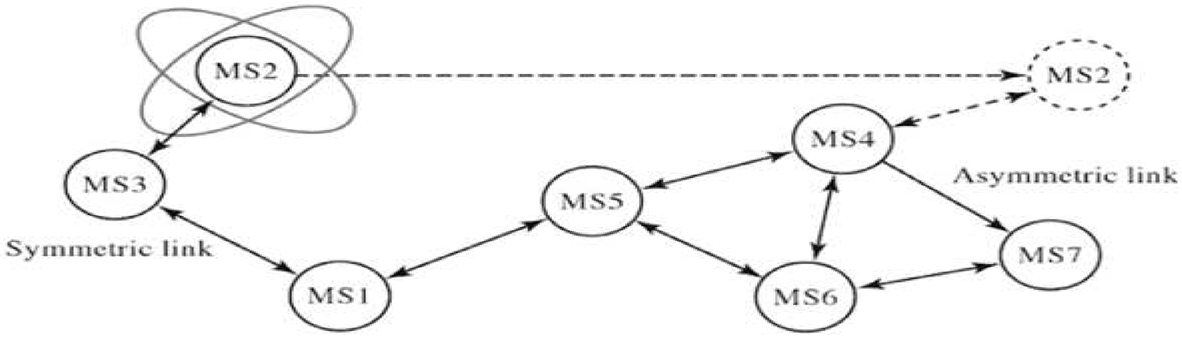


Figure 8.18 Client initialization via DHCP

Mobile Adhoc Network (MANET)

- A MANET consists of a number of mobile devices that come together to form a network as needed, without any support from any existing internet infrastructure or any other kind of fixed stations.
- A MANET can be defined as an autonomous system of nodes or MSs(also serving as routers) connected by wireless links, the union of which forms a communication network modeled in the form of an arbitrary communication graph.
- In a MANET, no such infrastructure exists and network topology may be changed dynamically in an unpredictable manner since nodes are free to move and each node has limiting transmitting power, restricting access to the node only in the neighboring range.
- MANETs are basically peer-to-peer, multi-hop wireless networks in which information packets are transmitted in a store and forward manner from a source to an arbitrary destination, via intermediate nodes as given in the figure:



Applications of MANET

- **Defense applications:** Many defense applications require on the fly communications set-up, and ad hoc/sensor networks are excellent candidates for use in battlefield management.
- **Telemedicine:** The paramedic assisting the victim of a traffic accident in a remote location must access medical records (e.g. X-rays) and may need video conference assistance from a surgeon for an emergency intervention. In fact, the paramedic may need to instantaneously relay back to the hospital the victim's X-rays and other diagnostic tests from the site of the accident.
- **Education via the internet:** Educational opportunities available on the internet or remote areas because of the economic infeasibility of providing expensive last-mile wire line internet access in these areas to all subscribers.
- **Vehicular area network:** This a growing and very useful application of adhoc network in providing emergency services and other information. This is equally effective in both urban and rural setup. The basic and exchange necessary data that is beneficial in a given situation.

Destination - sequenced distance vector routing

- Destination sequenced distance vector routing (DSDV) is a table driven routing protocol for MANET based on Bellman-Ford algorithm.
- DSDV was developed by **C. Perkins and P. Bhagwat in 1994**. The main contribution of the algorithm was that the algorithm works correctly, even in the presence of the loops in the routing table.
- As we know, each mobile node maintains a routing table with a route to every possible destination in the network and the number of hops to the destination.
- Each entry in the table contains a sequence number assigned by the destination node.
- The sequence numbers allow the node to distinguish stale routes from new ones, and help avoid formation of routing loops.

- **A new route broadcast contains:**
  - The destination address.
  - The number of hops required to reach the destination.
  - The sequence number of the information received about the destination and a new sequence number unique to the broadcast.
- If there multiple routes are available for the same destination, the route with the most recent sequence number is used. If two updates have the same sequence number, the route with smaller metric is used to optimize the routing.

Advantages

- Destination sequenced distance vector routing was one of the early algorithms available. It is suitable for creating ad-hoc networks with small no. of nodes.

Disadvantage

- Destination sequenced distance vector routing requires a regular update of its routing tables, which uses more battery power and a small amount of bandwidth even when the network is idle.
- This algorithm is not suitable for highly dynamic networks.

Dynamic source routing:

- Dynamic source routing is an on-demand routing protocol which is based on source routing.
- It is very similar to AODV in that it forms a route on demand when a transmitting computer requests one. But, it uses source routing instead of relying on the routing table at each intermediate device. Many successive refinements have been made to dynamic source routing.
- This protocol works in two main phases:
  - Route discovery
  - Route maintenance
- When a node has a message to send, it contacts to the route cache to determine whether is it has a route to the destination. If an active route to the destination exists, it is used to send a message.
- Otherwise a node initiates a route discovery by broadcasting a route request packet. The route request stores the destination address, the source address, and a unique identification number.

- Each device that receives the route request checks whether it has a route to the destination. If it does not, it adds its own address to the route record of the packet and then rebroadcasts the packet on its outgoing links.
- To minimize the no. of broadcasts, a mobile rebroadcasts a packet only if it has not seen the packet before and its own address was not already in the route record.

Mobile Transport Layer

• TCP originally designed for

– Fixed end-systems

– Fixed, wired networks

Traditional TCP

TCP congestion control

- packet loss in fixed networks typically due to (temporary) overload situations
- router have to discard packets as soon as the buffers are full
- TCP recognizes congestion only indirect via missing acknowledgements, retransmissions unwise, they would only contribute to the congestion and make it even worse

TCP slow-start algorithm

- sender calculates a congestion window for a receiver
- start with a congestion window size equal to one segment
- exponential increase of the congestion window up to the congestion threshold, then linear increase
- missing acknowledgement causes the reduction of the congestion threshold to one half of the current congestion window
- congestion window starts again with one segment

Classical TCP improvements:

TCP fast retransmit/fast recovery

- TCP sends an acknowledgement only after receiving a packet
- if a sender receives several acknowledgements for the same packet, this is due to a gap in received packets at the receiver
- however, the receiver got all packets up to the gap and is actually receiving packets
- therefore, packet loss is not due to congestion, continue with current congestion window (do not use slow-start)
- Change of foreign agent often results in packet loss
  - TCP reacts with slow-start although there is no congestion

- Forced fast retransmit
  - as soon as the mobile host has registered with a new foreign agent, the MH sends duplicated acknowledgements on purpose
  - this forces the fast retransmit mode at the communication partners

- additionally, the TCP on the MH is forced to continue sending with the actual window size and not to go into slow-start after registration

- **Advantage**
  - simple changes result in significant higher performance
- **Disadvantage**
  - further mix of IP and TCP, no transparent approach

Transmission/time-out freezing:

Mobile hosts can be disconnected for a longer time

• no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux. with higher priority traffic

• TCP disconnects after time-out completely

TCP freezing

• MAC layer is often able to detect interruption in advance

• MAC can inform TCP layer of upcoming loss of connection

• TCP stops sending, but does now not assume a congested link

• MAC layer signals again if reconnected

Advantage

• scheme is independent of data

Disadvantage

• TCP on mobile host has to be changed, mechanism depends on MAC layer

Selective retransmission:

TCP acknowledgements are often cumulative

• ACK n acknowledges correct and in-sequence receipt of packets up to n

• if single packets are missing quite often a whole packet sequence beginning at the gap has to be retransmitted (go-back-n), thus wasting bandwidth

Selective retransmission as one solution

- RFC2018 allows for acknowledgements of single packets, not only acknowledgements of in-sequence packet streams without gaps
- sender can now retransmit only the missing packets

Advantage

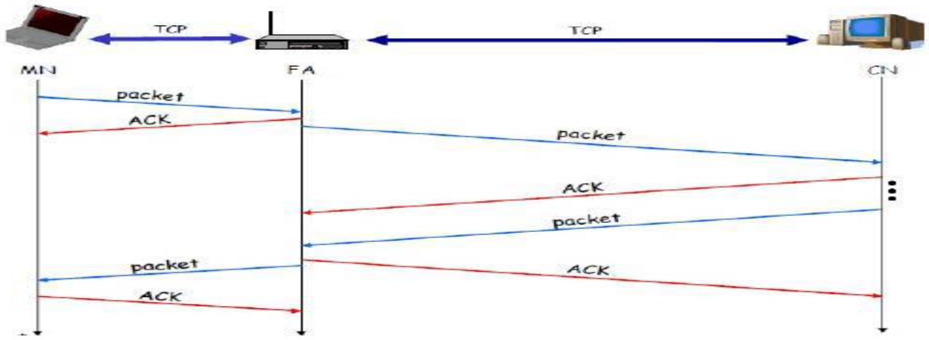
- much higher efficiency

Disadvantage

- more complex software in a receiver, more buffer needed at the receiver.

Indirect TCP:

- Splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
- no changes to the TCP protocol for hosts connected to the wired Internet,.
- optimized TCP protocol for mobile hosts
- hosts in the fixed part of the node do not notice the characteristics of the wireless part



Advantages

- no changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
- transmission errors on the wireless link do not propagate into the fixed network
- simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
- therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop is known

Disadvantages

- loss of end-to-end semantics, an acknowledgement to a sender does now not any longer mean that a receiver really got a packet, foreign agents might crash
- higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent

Snooping TCP:
"Transparent" extension of TCP within the foreign agent

• Buffering of packets sent to the mobile host

• lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission)

• the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs

• changes of TCP only within the foreign agent

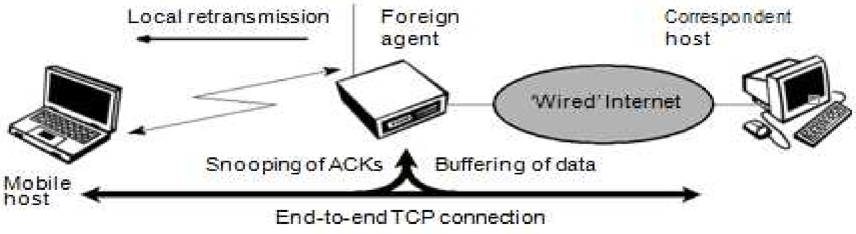
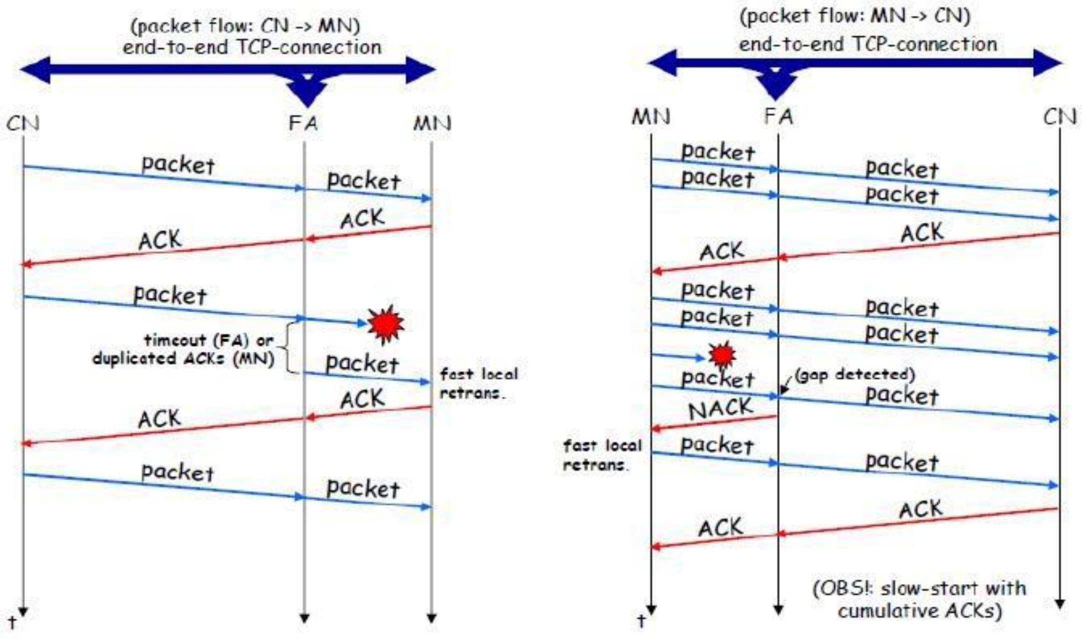


Figure 9.3
Snooping TCP as a transparent TCP extension

- **Data transfer to the mobile host**
  - FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
  - fast retransmission possible, transparent for the fixed network
- **Data transfer from the mobile host**
  - FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
  - MH can now retransmit data with only a very short delay
- **Integration of the MAC layer**
  - MAC layer often has similar mechanisms to those of TCP
  - thus, the MAC layer can already detect duplicated packets due to retransmissions and discard them

- **Problems**

  - snooping TCP does not isolate the wireless link as good as I-TCP
  - snooping might be useless depending on encryption schemes



Mobile TCP:

- Special handling of lengthy and/or frequent disconnections

M-TCP splits as I-TCP does

- unmodified TCP fixed network to supervisory host (SH)
- optimized TCP SH to MH

Supervisory host

- no caching, no retransmission
- monitors all packets, if disconnection detected

- set sender window size to 0
- sender automatically goes into persistent mode
- old or new SH reopen the window

Advantages

- maintains semantics, supports disconnection, no buffer forwarding

Disadvantages

- loss on wireless link propagated into fixed network
- adapted TCP on wireless link.

Transaction oriented TCP:

TCP phases

- connection setup, data transmission, connection release
- using 3-way-handshake needs 3 packets for setup and release, respectively
- thus, even short messages need a minimum of 7 packets!

Transaction oriented TCP

- RFC1644, T-TCP, describes a TCP version to avoid this overhead
- connection setup, data transfer and connection release can be combined
- thus, only 2 or 3 packets are needed

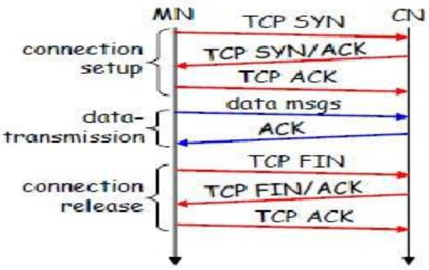
Advantage

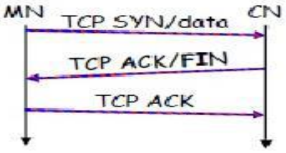
- Efficiency

Disadvantage

Requires changed TCP

- Mobility not longer transparent





LONG TERM EVOLUTION

Long – term evolution or LTE is a standard for wireless technology based upon GSM/EDGE and UMTS/HSPA technologies. It offers increased network capacity and speed to mobile device users. It is an extension of the 3G technology for high-speed mobile communications.

LTE-Advanced is an improvement over LTE that meets the criteria of 4G wireless communications as laid down by IMT-Advanced standards. It provides greater speeds and better quality of communications.

Both LTE and LTE-A are used for mobile broadband communications and in VoIP.

Features of LTE

- LTE was specified by The 3rd Generation Partnership Project (3GPP) release 8 was first adopted in European countries as early as 2009.
- Experientially, users get improved streaming, downloads and even uploads.
- LTE has peak data rate of 100 Mbps for downlink and 50 Mbps for uplink.
- It provides high speed communications with reduced latency.
- It has scalable bandwidth capacity.
- The upper layers of LTE are based on TCP/IP. So, it is an all-IP network that supports mixed data, voice, video and messages.

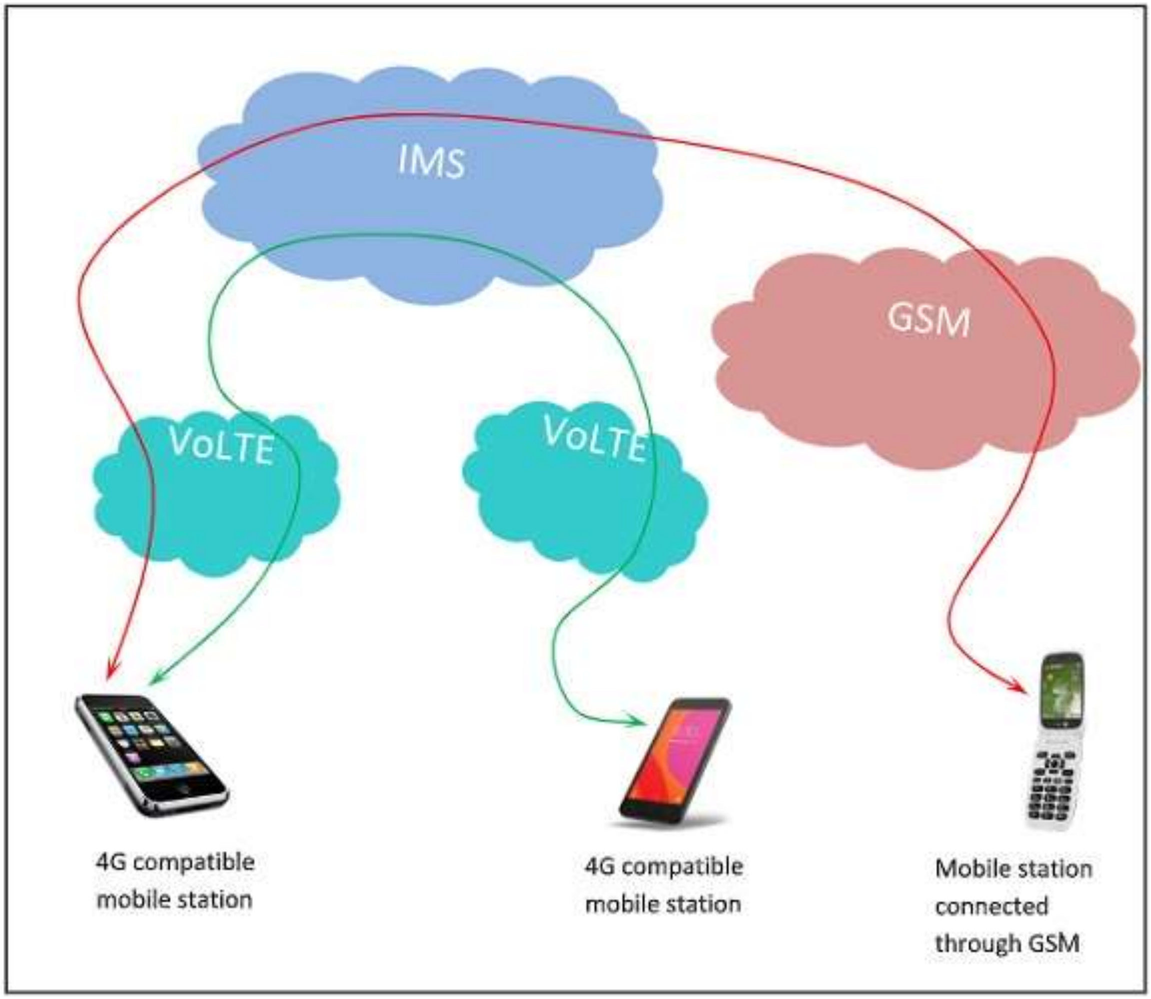
Features of LTE-Advanced

- LTE-Advanced (LTE-A) meets the specifications of IMT-Advanced standard for 4G technology. It was specified by 3GPP release 10.
- Its peak data rates are 1000 Mbps for downlink and 500 Mbps for uplink.
- 3GPP laid down that that all LTE-A devices should be backward-compatible with standard LTE.

VOLTE

- Voice over long-term evolution or Voice-over LTE (VoLTE) are the standards in all-IP networks for voice communication as well as data communication over 4G LTE networks.
- VoLTE offers services like creating, provisioning and managing high-speed voice, data, multimedia and messaging services on a 4G wireless network for mobile and portable devices. It uses the IP multimedia subsystem (IMS) to deliver the services.
- It transmits everything through only packets and thus supports only packet switching. So, all data from any circuit-switched networks like GSM need to be converted to packets

before they are transmitted by VoLTE. The communication is depicted in the following diagram −


IMS
GSM
VoLTE
VoLTE
4G compatible mobile station
4G compatible mobile station
Mobile station connected through GSM

OFDM

OFDM is main air interface technology used to move from third to fourth generation. It uses multiple carrier signals at different frequencies, sending some of the bits on each channel.

OFDMA

OFDMA uses a combination of FDMA and TDMA by allowing different users to use a subset of the subcarriers at different times.

Frequency selective fading only affects some subcarriers– Can easily be handled with a forward error-correcting code More importantly, OFDM overcomes inter symbol interference (ISI)

SC-FDMA

SC-FDMA is a multiple access technique which has similar structure abd performance as OFDMA. It performs an extra DFT operation and frequency equalization operation on transmitter and receiver.

The most obvious **difference between** the two schemes is that **OFDMA** transmits the four QPSK data symbols in parallel, one per subcarrier, while **SC-FDMA** transmits the four QPSK data symbols in series at four times the rate, with each data symbol occupying a wider M x 15 kHz bandwidth.

LTE MIMO

MIMO, Multiple Input Multiple Output is a technology that was introduced into many wireless communications systems including 4G LTE to improve the signal performance.

MIMO is basically an antenna technology as it utilizes a number of antennas to provide the performance improvements.

The basic concept of MIMO utilizes the multipath signal propagation that is present in all terrestrial communications. Rather than providing interference, these paths can be used to advantage.

The transmitter and receiver have more than one antenna and using the processing power available at either end of the link, they are able to utilize the different paths that exist between the two entities to provide improvements in data rate of signal to noise.

LTE MIMO modes

> ***Single antenna , Transmit diversity, Open loop spatial multiplexing, Close loop spatial multiplexing , Closed loop with pre-coding, Multi-User MIMO, MU-MIMO, Beam-forming & MIMO.***

What is the difference between the LTE FDD and TDD frame structures?

LTE-FDD implies that downlink and uplink transmission take place **in** different, sufficiently separated, frequency bands, while **TDD** implies that downlink and uplink transmission take place **in** different, non overlapping time slots. ... **FDD** does this by dividing the frequency band allotted into two discrete smaller channels.

Sub Frames

Ten sub frames

Each **frame** is divided into ten equally sized **subframes** of 1 ms in length (Tsubframe = 30720 · Ts). A **Special subframe** has three past DwPTS(Downlink Pilot Time Slot),GP (Guard Period) and UpPTS (Uplink Pilot Time Slot) and all of these have configurable lengths while the sum of the lengths has to be 1 ms or 14 symbols

LTE physical channels

The LTE physical channels vary between the uplink and the downlink as each has different requirements and operates in a different manner.

Downlink-_*Physical*_*Broadcast Channel (PBCH), Physical Control Format Indicator Channel (PCFICH), Physical Downlink Control Channel (PDCCH), Physical Hybrid ARQ Indicator Channel (PHICH)*

Uplink:-Physical Uplink Control Channel (PUCCH), Physical Uplink Shared Channel (PUSCH) , Physical Random Access Channel (PRACH)

LTE logical channels

The logical channels cover the data carried over the radio interface. The Service Access Point, SAP between MAC sublayer and the RLC sublayer provides the logical channel.

- ***Control channels:*** these LTE control channels carry the control panel information
  - ***Broadcast Control Channel (BCCH) :*** This control channel provides system information to all mobile terminals connected to the eNodeB.
  - ***Paging Control Channel (PCCH) :*** This control channel is used for paging information when searching a unit on a network.

- ***Common Control Channel (CCCH) :*** This channel is used for random access information, e.g. for actions including setting up a connection.
- ***Multicast Control Channel (MCCH) :*** This control channel is used for Information needed for multicast reception.
- ***Dedicated Control Channel (DCCH) :*** This control channel is used for carrying user-specific control information, e.g. for controlling actions including power control, handover.

Traffic channels:These LTE traffic channels carry the user-plane data:

- ***Dedicated Traffic Channel (DTCH) :*** This traffic channel is used for the transmission of user data.
- ***Multicast Traffic Channel (MTCH) :*** This channel is used for the transmission of multicast data.

LTE transport channels

The LTE transport channels vary between the uplink and the downlink as each has different requirements and operates in a different manner. Physical layer transport channels offer information transfer to medium access control (MAC) and higher layers.

- ***Downlink:***

  - ***Broadcast Channel (BCH) :*** The LTE transport channel maps to Broadcast Control Channel (BCCH)
  - ***Downlink Shared Channel (DL-SCH) :*** This transport channel is the main channel for downlink data transfer. It is used by many logical channels.
  - ***Paging Channel (PCH) :*** To convey the PCCH
  - ***Multicast Channel (MCH) :*** This transport channel is used to transmit MCCH information to set up multicast transmissions.

Uplink:

- ***Uplink Shared Channel (UL-SCH) :*** This transport channel is the main channel for uplink data transfer. It is used by many logical channels.
- ***Random Access Channel (RACH) :*** This is used for random access requirements.

LTE Frequency Bands, Spectrum

There are many frequency bands allocated to accommodate available spectrum in different countries for LTE (FDD & TDD) which are numbered and have defined limits. Radio channel numbers are also allocated.

The spectrum requirements and hence the frequency band allocations for LTE are different for FDD and TDD.

- ***FDD LTE bands:*** FDD spectrum requires pair bands, one of the uplink and one for the downlink. It is also important that there is sufficient spacing between the top of the lower band and the bottom of the upper band to allow sufficient filtering. Also the uplink to downlink channel spacing must be sufficient to allow sufficient filtering to prevent the transmitted signal from entering he receiver and desensitizing it.

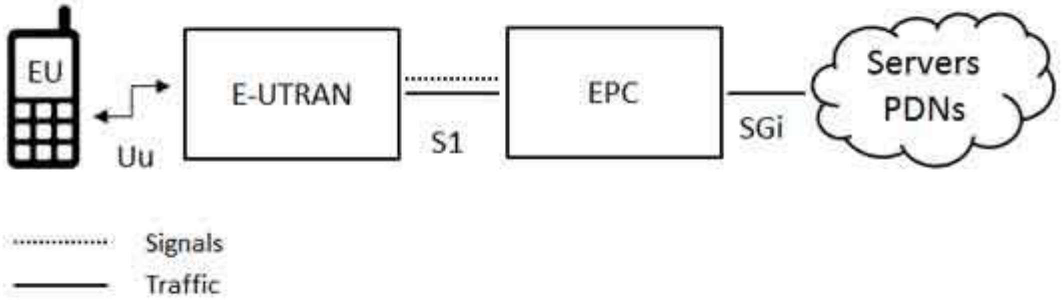
  TDD LTE bands : TDD transmissions only require a single band and in this way paired spectrum is not needed.

The different LTE frequency allocations or LTE frequency bands are allocated numbers. Currently the LTE bands between 1 & 22 are for paired spectrum, i.e. FDD, and LTE bands between 33 & 41 are for unpaired spectrum, i.e. TDD.

The high-level network architecture of LTE is comprised of following three main components:

- The User Equipment (UE).
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
- The Evolved Packet Core (EPC).

The evolved packet core communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia subsystem. The interfaces between the different parts of the system are denoted Uu, S1 and SGi as shown below:



The User Equipment (UE)

The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment (ME). The mobile equipment comprised of the following important modules:

- **Mobile Termination (MT)** : This handles all the communication functions.
- **Terminal Equipment (TE)** : This terminates the data streams.
- **Universal Integrated Circuit Card (UICC)** : This is also known as the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module (USIM).

A **USIM** stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

SAE

System Architecture Evolution (**SAE**) is a new network architecture designed to simplify **LTE** networks and establish a flat architecture similar to other IP based communications networks.

The Long Term Evolution System Architecture Evolution (LTE/SAE) of UMTS is one of the latest steps in an advancing series of mobile telecommunication systems. For secure communication, authentication service is one of the most essential services in these networks and guarantee that he/she is authorized for particular services.

LTE SON

A self-organizing network (**SON**) is an automation technology designed to make the planning, configuration, management, optimization and healing of mobile radio access networks simpler and faster.

VOLTE

voice over LTE

VoLTE stands for voice over LTE and it's more or less exactly what it says on the tin. It's voice calls over a 4G LTE network, rather than the 2G or 3G connections which are usually used.

Voice over LTE is what happens when your carrier allows you to place a **phone call** over your **LTE** connection instead of the older legacy voice networks.

Verizon Wireless, for example, traditionally used 1XRTT for all of your voice calls, relying on **LTE** for data.

VoLTE is an improved, more refined version of **4G** LTE. The disadvantage with **4G** LTE is that when you're travelling to remote places, you will not be able to make calls since there will be no 2G/3G network to fa**VoLTE** is relatively faster and has multitasked capabilities, unlike **Wi-Fi Calling**.

With new data and mobile networks altogether, it is easier to multitask with apps and phone **calls** at the fastest speed. Navigation and other partly features become much faster **than** those of Wi-Fi **Calling**.

SRVCC

Single Radio Voice Call Continuity (**SRVCC**) provides an interim solution for handing over VoLTE (Voice over **LTE**) to 2G/3G networks. The voice calls on **LTE** network are meant to be packet switched calls which use IMS system to be made. ... QoS is ensured by **SRVCC** operators for calls made.

SRVCC stands for Single Radio Voice Call Continuity. Putting it simple, it is a Handover technology between "VoIP over IMS in LTE" and Voice Call (CS) in a legacy system (e.g, WCDMA). It means it is for Handover between a Packet call in LTE and a Circuit Call in a legacy system (WCDMA).

SECURITY

Unlike previous 2G/3G technologies, **VoLTE** offers the possibility to use the end-to-end IP networks to handle voice communications. ... We will present vulnerabilities, both passive and active, and attacks that can be done using **VoLTE** Android smartphones to attack subscribers and operators' infrastructures.

By default, the **VoLTE** standard supports encrypted calls. For each call, mobile operators must select an encryption key (called a stream cipher) to **secure** the call.

References:-

Mobile communications by Jochen Schiller – second edition

.http://www.radio-electronics.com/info/cellulartelecomms/lte-long-term-evolution/3g-lte-basics.php.