4

Mobile Network Layer

This chapter introduces protocols and mechanisms developed for the network layer to support mobility. Mobile IP adds mobility support to the internet network layer protocol IP. IP is the common base for thousands of applications and runs over dozens of different networks. This is the reason for supporting mobility at the IP layer. To merge the world of mobile phones with the internet and to support mobility in the small more efficiently, so-called micro mobility protocols have been developed. Another kind of mobility, portability of equipment, is supported by the dynamic host configuration protocol (DHCP)

.

In former times, computers did not often change their location. Today, due to laptops or notebooks, students show up at a university with their computers, and want to plug them in or use wireless access. A network administrator does not want to configure dozens of computers every day or hand out lists of valid IP addresses, DNS servers, subnet prefixes, default routers etc. DHCP sets in at this point to support automatic configuration of computers. The chapter concludes with a look at ad-hoc networks in combination with the network layer. This is a fast-growing field of research with standards that are unclear as yet.

4.1Mobile IP

The following topic gives an overall view of Mobile IP, and the extensions needed for the internet to support the mobility of hosts. A good reference for the original standard is Perkins and Solomon which describe the development of mobile IP, all packet formats, mechanisms, discussions of the protocol and alternatives etc. in detail. The new version of Mobile IP does not involve major changes in the basic architecture but corrects some minor problems.

4.1.1 Goals, assumptions and requirement of mobile IP

The main goal of mobile IP is supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols. A host needs a topologically correct address to deliver a packet (mail boat). In a mobile state, the system will receive many packets. (i.e.) when the system leaves one network and joins another network, in transit the system receives many packets. All these packets need to be delivered correctly. A host sends an IP packet with the header and the message. The header contains a destination address. The role of the header is to determine,

1) The receiver.

2) Physical subnet of the receiver.

3) The packets come to the router.

4) The router routes the packet accordingly.

1. Solutions to deliver packets during mobility

1. One solution to address the mobility problem is to assign a new topologically (analysis sites) correct IP address to the moved system (i.e.,) when the system moves to a new location implies assigning a new IP address.

Disadvantages:

- This new address is not known to anybody.
- Identification of such mobile systems is difficult. This problem can be solved with the help of DNS.
- Higher layer protocols (Code of correct conduct) depend on the IP address.

DNS: Domain Name System

Domain Name System is a table which has logical name and its equivalent IP address. The main advantage is its quick reach ability. It has its own disadvantages. Such as The DNS needs some time to update the table. If the nodes move often the table cannot be updated quickly and it uses caching to improve scalability (quality).

2. When the IP address is changed while the TCP connection in open. It implies that the connection is broken. The TCP connection is identified by (Source IP address, source post, Destination IP address, Destination post). This is called socket pair. TCP cannot accept the address changes. The mobile node informs all its partners about the changes in the IP address.

3. While it is theoretically possible to change routing tables all over the world to create specific routes to a mobile node, this does not scale at all with the number of nodes in the internet. Routers are built for extremely fast forwarding, but not for fast updates of routing tables. Routers are the „brains" of the internet, holding the whole net together. No service provider or system administrator would allow changes to the routing tables, probably sacrificing stability, just to provide mobility for individual users.

4.1.2 Requirements

When the solutions did not work, a more general architecture had to be designed. Many field trials and proprietary systems finally led to mobile IP as a standard to enable mobility in the internet. Several requirements accompanied the development of the standard.

1. **Compatibility (**Capability of existing**):** The new standard cannot introduce changes. As there are millions of systems in the internet, they need to use the existing browser, operating system, routers and same addressing. The protocol mobile IP should be compatible with all the above. The other important format requirement is the ability of a mobile system to communicate with a fixed system.

2. **Transparency(**The quality of being clear and transparent**):** Mobility should remain invisible for higher layer protocols and applications (i.e.,) the higher layer should continue to work even if the computer has changed in point of attachment to a different network. When transparency not found the effect will be higher delay and lower bandwidth.

3. **Scalability** (quality**) and Efficiency (**ratio of the output**):** Of course the new mechanism should not have its effect on efficiency. The mobile IP should be scalable over a large number of participants in the internet, worldwide.

4. **Security:** All the messages should be authenticated in the minimum requirement. The IP layer must make sure that the destined receiver alone receives the packet.

4.1.3 Terminology used

1. **Mobile Node*:*** Mobile node is an end system (or) router that can change its point of attachment to the internet using mobile IP. The mobile node keeps its IP address and can continuously communicate with any other system in the internet.

2. **Correspondent Node:** This is another end for communication. This node can be a fixed node or mobile node.

3. **Home Network:** Home network is the subnet the mobile node belongs to with respect to the IP address.

4. **Foreign Network:** Foreign Network is the current subnet the mobile node visits which is not the home network.

5. **Foreign Agent*:*** The Foreign Agent provides services to the mobile node during its visit to the foreign network. The foreign agent can have a COA Care Of Address acting as a tunnel end point forwarding packets to the mobile node.

The Foreign Agent is the default router for the mobile network. The Foreign Agent also gives security service. Foreign Agent is implemented on a router for the subnet the mobile network attaches to **care of address.**

The COA defines the current location of the mobile node from the IP point of view. All the packets sent to the mobile network are delivered to the COA, not to the IP address of the mobile network.

The COA is the tunnel end point. The COA can be present in either of one location.

1. **Foreign Agent COA:** When the COA is present in FA, the COA is the IP address of FA. FA is the tunnel end point and forwards the packet to Mobile Network. Many mobile nodes using the FA can share this COA as common COA.

2. **Co-located COA:** The COA is co-located if the COA is present in the mobile node itself. Here the Mobile Network temporarily acquires an additional IP address which acts as COA. The tunnel end point is the Mobile Network itself. This method does not work well in IPV4 due to the scarcity of addresses.

6. **Home Agent :** Home Agent is present in the home network itself. The Home Agent provides services to the Mobile Network. Home Agent is the tunnel entry point. Home Agent has a location registry. This registry informs the current location of the Mobile Network with the help of current COA. The Home Agent can be present in

1. **Router of the home network**: This is the best position because all the packets for the MN have to go through the router.
2. **Arbitrary node in the subnet**: The disadvantage is the double crossing of the router by the packet, if the Mobile Network is in foreign networks. The packet comes via the router, the HA sends the packet through the tunnel which crosses the router.

3. **Router:** Acts as a manager for Mobile Network belonging to the virtual home network. Disadvantage is that all Mobile Network"s are always in a foreign network.

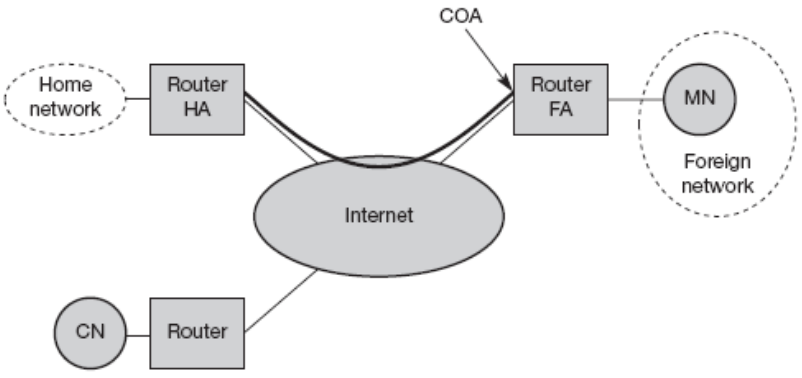

Fig 4.1: Mobile IP example network

The above figure shows a correspond node is connected via a router to the internet. There are home net work and foreign network. Foreign Agent is implemented on the router of the

Foreign Network. The tunnel for the packet starts at the HA and ends at the Foreign Agent. Foreign Agent has the COA for the Mobile Network.

4.1.4 IP Packet delivery

Consider the following network. The following paragraph explains the packet delivery to and from the Mobile Network.

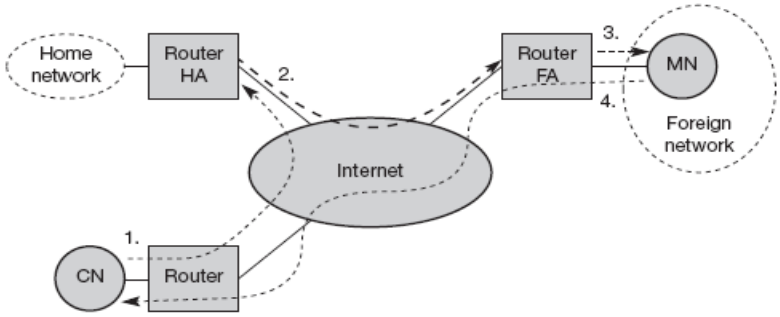

Fig 4.2: Packet delivery to and from the mobile node

When the correspondent node wants to send an IP packet to the MN. It transfers the packet to its Router (device) and it does not need to know about the current location of the Mobile Node.

Step 1: Correspondent Node sends the packet to the IP address of the Mobile Network, (i.e.,) Correspond Node sends a packet with MN as destination address, to the router(the HA). The Mobile IP is to support transparency to the packet in transferred to the home network of the Mobile Node.

Step2: Home Agent receives and intercepts the packet .It knows that the MN is not in the Home Network currently with the help of the registry .Hence the packet is not forwarded as usual. But the packet is encapsulated (reduce in volume) and travelled to the COA.A new header is attached which contains the Home Agent as the resource add and COA as the destination address

Step 3: The FA receives the packets, de -capsulate the packet and forwards the original packet to the destination Mobile Node.

Step 4: The Mobile Node sends the packet as usual with its own fixed IP address as source and Correspondent Node's address as destination.

The router with Foreign Agent acts as a default router and forwards the packet in the same way as is would do for any other node. If Correspondence Node is a fixed node the procedure is as usual. But if Correspondent Node is also a mobile node then the same procedure as that of Mobile Node to CN should be followed

4.1.5 Agent discovery

When the MN moves to a Foreign Network it needs the support of Foreign Agent. To identify the FA mobile IP suggests two methods.

1. Agent Advertisement.
2. Agent Solicitation.

4.1.5.1 Agent Advertisement

In this method the HA and Foreign Agent advertise periodically the "Agent advertisement messages". These messages are sent as **beacon broadcast** to the subnet. To advertise ICMP (Internet Control Message Protocol) are used.

The agent advertisement packet follows RFC 1256 standard plus mobility extension. The packets have the following structure in Figure 4.3.

The upper part represents the ICMP packet, the lower part is the extension needed for mobility. The TTL field of IP packet is =1 for all advertisements to avoid forwarding. IP destination address for advertisement is 224.0.0.1 the multicast address (or) 255.255.255.255 the broadcast address.

The description for the fields is as follows,

- **Type is set to 9 (Agent Advertisements)**
- **Code =0** if the agent also routes traffic from non-mobile mode.
- **Else Code=16** if the agent routes traffic only from mobile node.
- **Addresses:** The number of router's addresses advertised with this packet, while the addresses themselves follow as shown.
- **Lifetime:** Denotes the length of time this advertisement is valid.
- **Preference Levels** for each address help a node to choose the router that is most eager to get a new node.

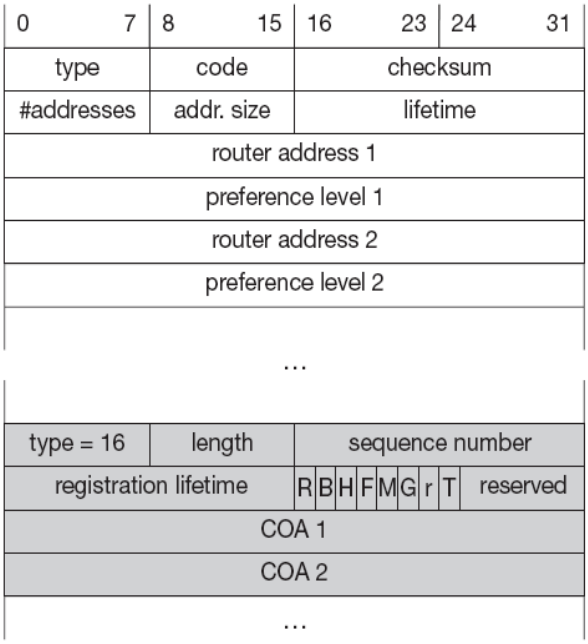

Fig 4.3: Packet structure

The extension for the mobility has the following.

- **Type:** Type is set to 16.
- **Length:** Depends upon the number of COA provided with the message and =6 +4*(Number of addresses).
- **Sequence Number:** The total number of advertisements sent since initialization.
- **Registration Life Time:** The agent can specify the maximum life time in seconds a node can request during registration. The Bits specify the character of an agent.

The following bits specify the characteristics of an agent in detail,

- **R:** Bit set if a registration with this agent in required even when using a co-located COA Mobile Node.
- **B:** Bit is set if agent is currently too busy to accept new registration.
- **H:** Bit is set if the agent is Home Agent.
- **F:** Bit is set if the agent in Foreign Agent.
- **M and G:** Specify the method of an encapsulation used for tunnel.
  - M stands for minimal encapsulation.
  - G stands for generic routing encapsulation field r is set he zero.
  - T field indicates that reverse tunneling is supported by the FA.

The following fields contain the COA advertised.

"A mobile node in a subnet can receive agent advertisement from its Home Agent or Foreign Agent".

4.1.5.2 Agent Solicitation (collection**):**

If no agent advertisements are present (or) Inter Arrival time is too high, and mobile Node has not received a COA by any other means, the Mobile Node must send "agent Solicitation".

- The Solicitations are based on RFC 1256.
- Care should be taken to ensure that solicitation messages should not flood the network.
- But the Mobile Node can search for an FA endlessly sending out solicitation messages.

A mobile Node can send out 3 solicitations, One-per second, as soon as it enters new networks. In highly dynamic networks, the Mobile Node's are moving, and the application receives continuous packets in one second interval between solicitation will be too long. Before the Mobile Node gets ends new address many packets will be lost. If the node does not receive an answer it must decrease the rate of solicitation exponentially to avoid flooding.

Mobile Node can discover a new agent.

1. When it is connected to a new network.
2. When the Mobile Node is looking for better connection.

After either advertisements (or) Solicitation the Mobile Node receives a COA. The next step is the registration with HA if Mobile Node is in foreign networks.

4.1.6 Registration

After receiving a COA the mobile node has to register with HA. The function of registration is to inform the HA the current location for forward of packets. Two ways of registration depending upon the location of the COA.

4.1.6.1 COA at FA

- The mobile node sends the registration request to the Foreign Agent. The registration request message contains the CAO. The Foreign Agent will forward the request to the HA.
- The Home Agent sets up **mobility binding**. This contains the mobile node"s home IP address and the current COA.

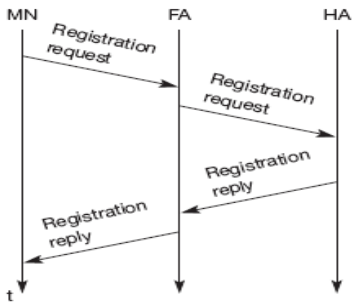

Fig 4.4: COA at FA

- The mobility binding also contains the life time of the registration.
- Registration expires after the life time and deleted.
- Registration should be renewed before expiration.
- After mobility binding, the Home Agent acknowledges by the Sending Registration Reply Message, to FA which in turn is forwarded to Mobile Node.

4.1.6.2 Co-located COA

- When the foreign agent is co-located the registration is simple.
- The Mobile Node directly sends the Registration Refined to Home Agent.
- The Home Agent acknowledges by Registration Reply to mobile node.

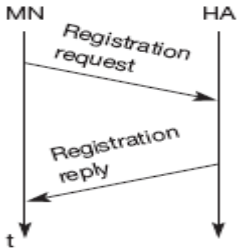

Fig 4.5: Co located COA

4.1.6.3 Format of Registration Request

UDP packets are used for registration request. The fields are defined as follows,

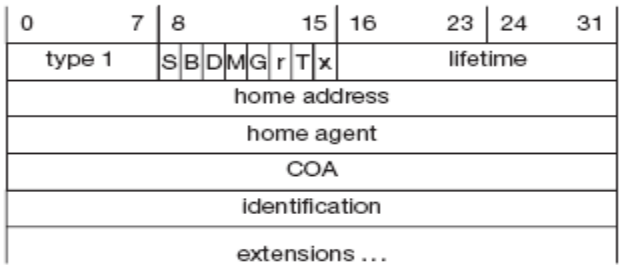

Fig 4.6: Registration Request

- **IP Source address:** It is the Interface address of MN.
- **IP destination address:** It is the FA or HA depending upon the location of COA.
- **Type:** This field is set to "1" for registration request.
- **S Bit:** Set when the MN wants the HA to retain prior mobility bindings.
- **B:** Set when the MN wants to receive the broadcast packets which have been received by the HA.
- **D Bit:** If the MN uses co-located COA it also takes care of decapsulation at the tunnel end point, and then the D-bit is set.
    - **M :** Minimal encapsulation.
    - **G :** Generic routing encapsulations.
    - **T :** Reverse Tunneling: r, x are set to zero.

- **Life Time:** It denotes the validity of the registration in seconds. When Life time = 0, It is called as deregistration. All bits set indicate Infinity.
- **Home Address:** Fixed IP address of the MN.
- **Home Agent:** IP address of the HA.
- **COA:** Tunnel end point.
- **Identification:** 64 Bits generated by the MN to identify a request and match in with registration replies.
- **Extension**: Contains the parameter to authentication.

Registration Reply

For registration reply also UDP packet is used. It contains a type field set to 3 and a code indicating the result of the registration request. Fig 4.8 gives some example codes.

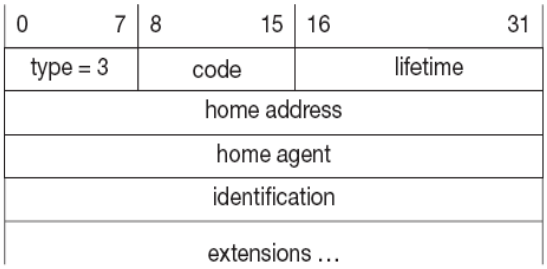

Fig 4.7: Registration Reply

The fields indicates,

- **Code:** Indicates the result of registration request.
- **Life Time:** Validity of registration in seconds
- **Home Address**: Home address of MN
- **Home Agent:** Address of HA
- **Identification:** 64 Bit, Match the Registration Request and Reply
- **Extension:** Contains the parameter for authentication

Registration	Code	Explanation
successful	0	registration accepted
	1	registration accepted, but simultaneous mobility bindings unsupported
denied by FA	65	administratively prohibited
	66	insufficient resources
	67	mobile node failed authentication
	68	home agent failed authentication
	69	requested lifetime too long
denied by HA	129	administratively prohibited
	130	insufficient resources
	131	mobile node failed authentication
	132	foreign agent failed authentication
	133	registration identification mismatch
	135	too many simultaneous mobility bindings

Fig 4.8: Example Registration Reply codes

4.1.7 Encapsulation

4.1.7.1 Tunneling and Encapsulation

- **Tunneling** describes the mechanism used to forward the packets between HA and COA. **Tunnel** is a virtual pipe to transfer data packets between the tunnel entry and end point. **Packets** entering the tunnel are forwarded and leave the tunnel unchanged. To send a packet through a tunnel it is encapsulated.

Encapsulation: Encapsulation is the mechanism of attaching a new header to the existing packet.

Decapsulation: The reverse operation where by the attached header is removed and the original packet are taken out.

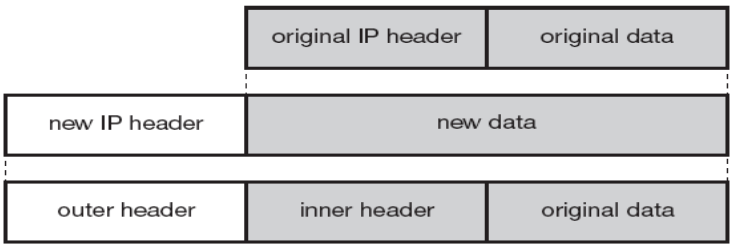

Fig 4.9: IP Encapsulation

- The above fig represents what happens at tunnel entry point.
- The Home agent takes the original packet, and attaches a new ip header which contains the destination address as the COA.
- The new header is called as outer header.
- The already existing header is called as inner header.

4.1.7.2 Methods of Encapsulation

Three methods of encapsulation are:

1. IP-in-IP Encapsulation

2. Minimal Encapsulation

3. Generic Routing Encapsulation.

4.1.7.2.1 IP-in-IP Encapsulation

This encapsulation is mandatory for mobile IP. The fig 4.9 shows the packet inside a tunnel.

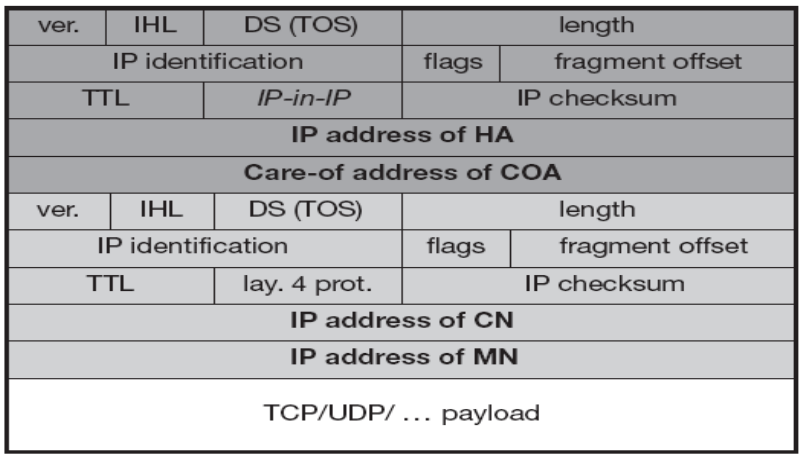

Fig 4.9: IP-IP Encapsulation

- **Ver:** version 4 when it is IPV4
- **IHL:** Internet header length denotes the length of the outer header in 32 bit words.
- **DS:** (TOS) is copied from inner header.
- **Length**: Length of the encapsulated packet.
- **TTL:** TTL must be set high so that the packet can reach the tunnel end point.
- **IP-in-IP:** Protocol type used in IP pay load. set to 4 if protocol type ,the protocol type for IPV4.
- **IP Checksum:** IP checksum is calculated.
- **IP address of HA:** Tunnel entry point address, which is the address of HA.
- **COA:** Tunnel exit point address, which is the address of COA.

Inner Header:

The header remains almost unchanged during encapsulation. The only change is TTL is decremented by 1.Tunnel is considered as a single hop. At the end the pay load is present. Several fields are redundant.

4.1.7.2.2 Minimal Encapsulation

Here the redundant fields are removed.

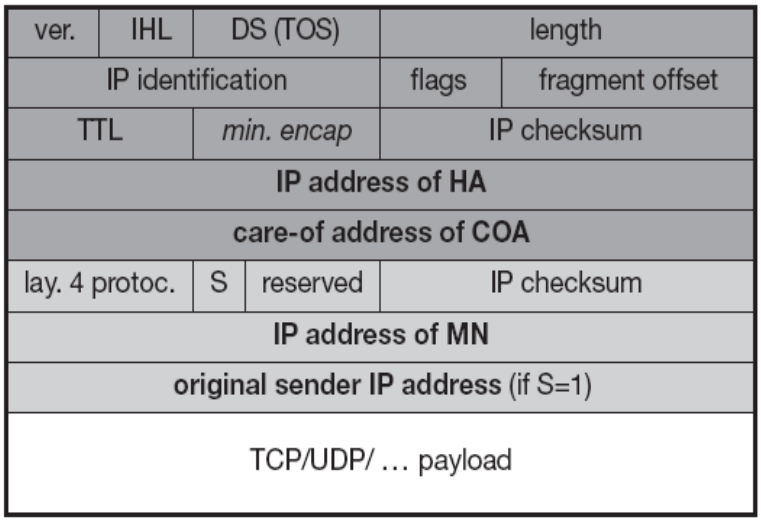

Fig 4.10: Minimal Encapsulation

- This encapsulation is an optional encapsulation method for mobile IP.
- The tunnel entry point and end point are specified.

4.1.7.2.3 Generic Routing Encapsulation

This encapsulation supports other network layer protocols.

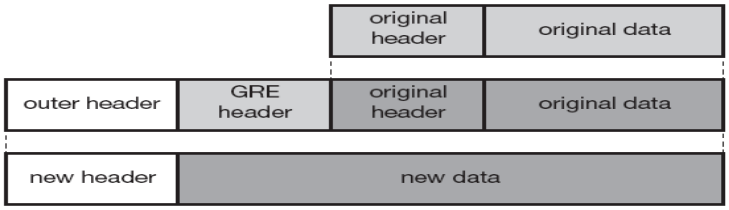

Fig 4.11: Generic routing encasulation

- The GRE header is pretended to the packet which contains the original header and data. (The packet is different protocol suite).To the above the new header is pretended. This header is the second protocol suite.

Fields:

- The figure 4.12 follows RFC 1701 format.
- **Outer Header** is the standard IP header HA is the sources and COA as destination address.
- **Protocol Type:** 47 for GRE. TTL is decremented by 1.

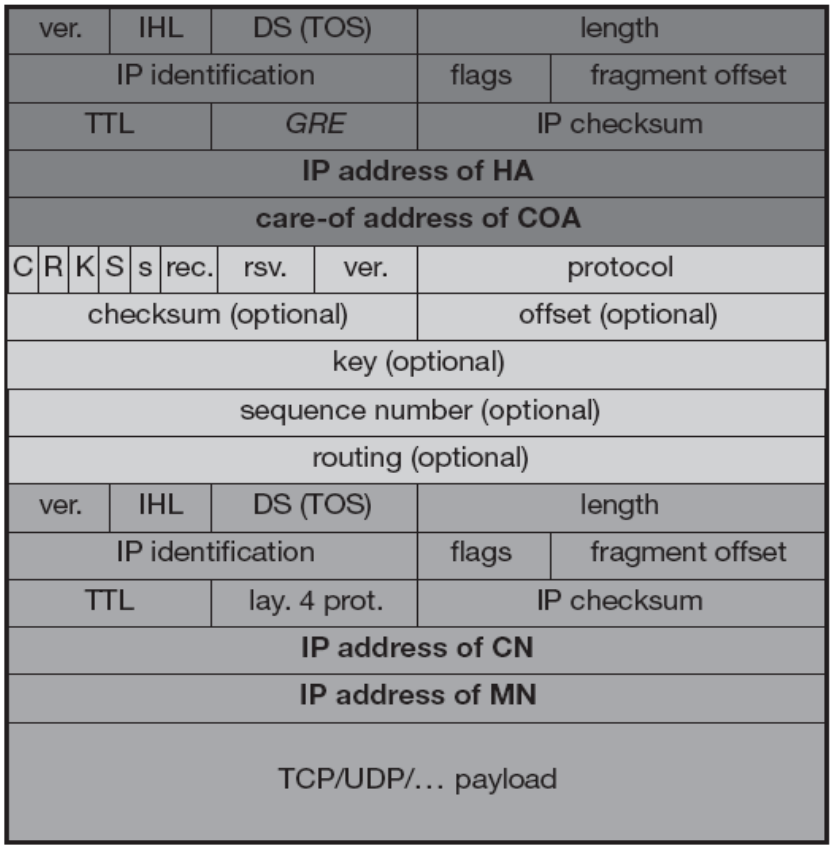

Fig 4.12: Protocol fields for GRE according to RFC1701

GRE Header:

- Minimal GRE header user 4 bytes.
- **Bits** C when set indicates check sum is present and the field contains a valid Checksum.
- **R Bit** when indicates the offset and routing fields are present and contain valid information.
- **Offset:** Represent offset in Bytes for the first source routing entry.
- **C Bit:** If the C Bit is set offset is also present.
- **R Bit Set:** Check sum must be present.
- **K Bit:** Key field used for authentication.

- **S Bit:** Sequence number field in set when sequence number is present .S in important for in order transmission of packets.
- **Rec:** Recursion control field. This field represents a counter that shows the number of allowed recursive encapsulation.
  - When the packet arrives at an encapsulation it checks whether the field=0.
  - If not Zero, additional encapsulation is allowed packet is encapsulated, field in by 1, decremented else packet is discarded.
  - Default value is 0; allows only one level of encapsulation.

Reserved Fields:

- Field=0 and are ignored at reception.
- **Version:** =0 For GRE version.

4.1.8 Optimization

Consider the example.Japanese and a German meet at a conference on Hawaii .Both use their laptops for exchanging data both run mobile IP for mobility support.

If the Japanese sends a packet to the German, his computer sends the data the Home Agent of the German. (i.e.) from Hawaii to German. The Home Agent in Germany encapsulates the packets and tunnels them to the COA of the German laptop on Hawaii.

- The packets have to travel around the world.
- This inefficient behavior is called Triangular Routing.

Disadvantages

- Unnecessary Overheads.
- To optimize the route is to inform the correspondent node of the current location the mobile node
- Correspondent Node can learn the location by caching it in a binding cache.
- Binding Cache is a part of Routing Table.

To optimize needs four additional messages.

1. Binding Request:

Any Correspondent Node that wants to know the current location of a mobile Node can send a binding request to the Home Agent. The Home Agent can check if the Mobile Node has allowed dissemination of the current location.If the Home Agent is allowed to reveal the location it sends back a binding update.

2. Binding Update:

This message sent by Home Agent to Correspondent Node.This message tells the current location of network.This message can request an acknowledgement.

3. Binding Acknowledgement:

If requested Correspondent Node return this acknowledgement after receiving a binding update message.

4. Binding Warning:

A node decapsulates a packet for a Mobile Node, but the MN has moved to a new FA, the old FA sends binding warning. The warning contains Mobile Node"s HA and the target node address. Target node address in the address of the node that has tried sending packet to Mobile Node. The Home Agent receives this message, and the Home Agent sends a binding update to the node that has a wrong COA.

The following figure explains the four additional message .When the Mobile Node changes foreign Agent.

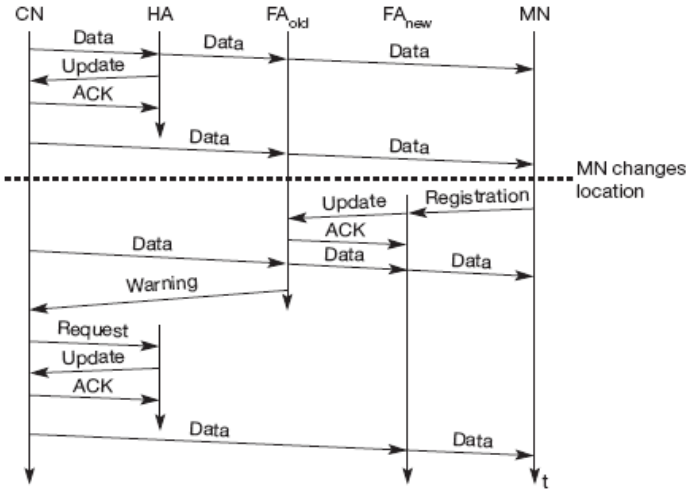

Fig 4.13: Change of the foreign agent with an optimized mobile IP

Explanation: (When the MN has moved)

The Mobile Node changes its location and register with FA.

- The registration is forwarded to Home Agent.
- The Home Agent updates the registry.
- FA informs FA about the change in location of Mobile Node.
- The new FA passes this old information via update message.
- This message is acknowledged by FA old.

- In case when the Correspondent does not know about the new changes of location, the Correspondent Node transmits packet to FA old.
- The FA old will notice that the Mobile Node is not attached to it. Hence it will forward the packets to FA new.
- This forwarding of packets is called smooth handover.
- In the absence of smooth handover the packets will be lost in the transit.
- To tell the CN that has a sate binding FA old sends warning message to CA.
- CN requests for binding update.
- The Home Agent sends an update to inform them to inform the CN about the new location.
    - This message is acknowledged. Hence after CN directly sends the packet to Foreign Agent new and avoids triangular routing.

Disadvantage:

Security Problems.

4.1.9 Reverse tunneling:

The return path from the Mobile Node to CN is not simple. The MN can directly send packets to CN but the problems faced are:

1. **Fire Walls:**

   The entire internal network is connected to Internet via firewall. The fire wall will filter the packets from malicious address. Here when the Mobile Node sends a packet with its fixed IP address fire walls will filter these packets because Mobile Node cannot send packets .To overcome this Network Address Translation is used by many companies. Reverse tunnel is used to resolve.

2. **Multi Cast:**

   Reverse Tunnels are needed for the Mobile Node to participate in a multicast group. For a Mobile Node in a foreign network to transmit multicast packets they need a reverse tunnel.

3. **TTL:**

   A Mobile Node sends a packet with a certain.TTL and still is in its home network. When the Mobile Node has removed to a foreign network this TTL is very low .Hence the packet will not reach the destination. This scenario reverse tunnel is needed whereby it considers the distance as 1 hop so that the packet reaches the destination within the specified TTL. RFC 2344 defines Reverse Tunneling as an extension to mobile IP.

Disadvantage:

- Reverse Tunneling creates a triangular routing in the reverse direction.
- Security issues need to be solved.

4.1.10 IPV6

Features of IPV6:

Several features that had to be separately specified for V4 come free in IPV6.

1) Security for authentication is a feature for IPV6.No special mechanisms needed for security.
2) Every node masters auto configuration (i.e.) the mechanisms to acquire COA is built in.
3) Neighbor discovery is mandatory for every node .For this no FA is needed to advertise.
4) Every IPV6 nodes can send binding update to another node. So the mobile node can send its current COA directly to COA and Home Agent.
5)A soft handover is possible .For this the Mobile Node sends in new COA to the old router and the old router encapsulates all incoming packets for the MN and forwards them to the new COA.
6) FA is not needed any more. The CN only has to be able to process binding updates .As no FA, the Mobile Node should be able to decapsulate packets to detect when needs a new COA and to determine when to send binding update to HA and CN.
7) IPV6 does not solve any firewall (or) privacy problem.

4.1.11Micro mobility

The mobile IP faces many problems in the duration of the handover and scalability of registration. Consider a larger number of nodes change the network frequently, a heavy load is present on the home agents and network for registration and binding update messages exists. To have fast seamless handover the “IP micro mobility protocols” comes as handy.

Concept:

To understand the concept of Micro mobility protocol considers the following example. A client arrives to the customer"s place with a laptop. The Home Agent needs to know only an entry point to the customer network .The entry point acts as the current location. When the client the location within the customer"s network it should be handle locally to avoid the traffic and to speed up the local handover.

Principle: The Home Agent needs to be informed only when the node changes a region. Three IP micro mobility approaches are

(1)Cellular IP
(2)Hawaii
(3)Hierarchical mobile IPV6

4.1.11.1 Cellular IP

- Cellular IP provides local handovers by installing a single cellular IP gateway for each Domain.
- This domain acts as a foreign agent to the outside world.
- Inside the domain, all nodes collect the routing information for accessing Mobile Node based on the origin of the packets.
- Soft handover is achieved by simultaneous forwarding of packets destined for a node along multiple paths.

A mobile moving between adjacent cells will temporarily receive the packets via old and new Base Stations.

Architecture:

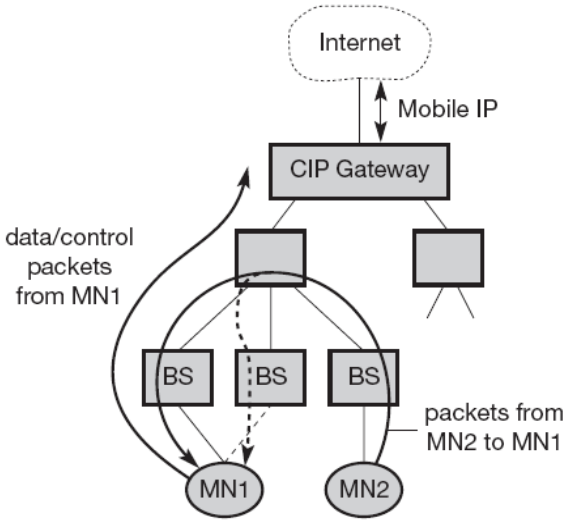

Fig 4.14: Basic Architecture of cellular IP

Advantages:

- Manageability
- Cellular IP is self configuring.
- Integration of CIPGW into a fire wall facilitates administration of mobility related functionality.

Disadvantages:

- **Efficiency**: Additional load is induced by forwarding packets on multiple paths.
- **Transparency**: Changes to Mobile Node"s are required.
- **Security**: Routing tables are changed based on messages sent by mobile nodes.

4.1.10.2 Hawaii (Hand-off Aware Wireless Access Internet Infrastructure).

- Tries to keep micro mobility support transparent to Home Agent and Mobile Node.
- Increase Performance and Reliability.
- Support QOS.

Concept:

Step1: When a mobile node enters a HAWAII domain, the mobile Node obtains a co-located COA.
Step 2: Registers with Home Agent.
Step 3: When moving to another cell inside the foreign domain, the MN sends a registration requests to the new base station as to foreign agent.
Step 4: The base station intercepts the registration request and sends out a handoff update message, which reconfigures all routers on paths from the old and new base station to the cross over routes.

Routing changes are a initiated by the foreign domain"s infrastructure and the message as are authenticated.

Architecture:

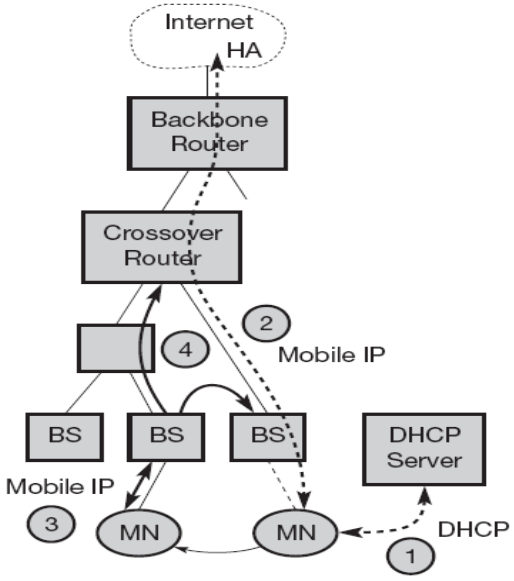

Fig 4.15: Basic architecture of Hawaii

Advantages:

- **Security:** Challenge response extensions are mandatory, initiated by foreign domains infra structure.
- **Transparency:** Transparent to middle nodes.

Disadvantages:

- **Security:** IP Sec Tunnel cannot be setup.
- **Implementation**: No private address support because of co-located COA.

4.1.11.3 Hierarchical Mobile IPV8.

- Micro mobility is supported by installing a mobility anchor pointer (MAP). This MAP is responsible for certain domains and act as a local HA with in this domain for visiting Mobile Node.
- MAP receives all packets on behalf of Mobile Node encapsulates and forwards to the Mobile Node"s current address.
- As long as Mobile Node stays within the domain of MAP, the global COA does not change. This Global COA is called as Regional COA (RCOA).
- The MAP"s boundaries are defined by access routers (AR). The MAP helps in local hand from RCOA to LCOA.
- The Mobile Node registers with the RCOA.
- When the Mobile Node moves locally, it should register with the new LCOA (Local COA) with its MAP.
- RCOA is unchanged.

Architecture:

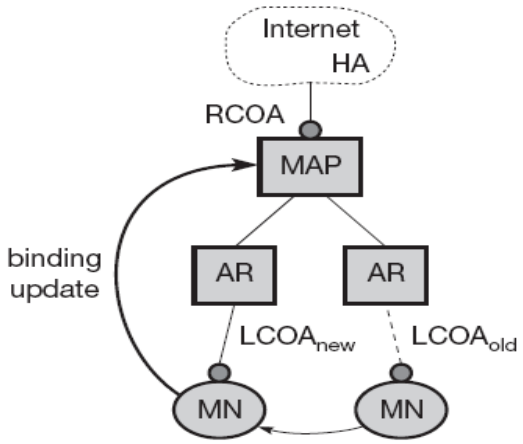

Fig 4.16: Basic architecture of hierarchical mobile IP

Advantages:

- **Security:** MN has little location privacy because L COA can be hidden.
- **Efficiency**: Direct routing is possible.

Disadvantages:

- **Transparency:** Additional component MAP is needed.
- **Security:** Routing table are changed based on messages sent by mobile nodes.
- Additional Security functions are needed in MAP.

4.2 Dynamic host configuration protocol (DHCP)

1) The aim of DHCP is to simplify the installation and maintenance of network computer.
2) When a new computer is added to the network, DHCP can provide with all necessary information for integration.
3) DHCP provides IP address.

Configuration/model

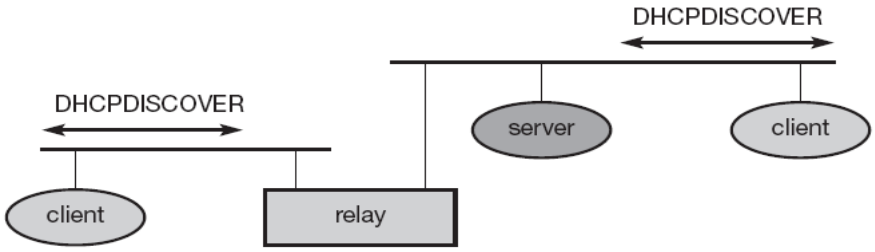

Fig 4.17: Basic DHCP configuration

- DHCP is based on client server model.
- DHCP client sends a request to the server using DHCP Discover, which is broadcasted.
- The server responds.
- The relay is needed to forward across the interworking units to a server.

Client Initialization via DHCP:

Initialization phase:

- The client broadcasts a DHCP discover to the subnet. There may be a relay to forward this broad.
- In the above figure two servers receive this broadcast and determine the configuration they can offer to the client.

- Server"s reply to the client"s request with DHCP OFFER and offers a list of configuration parameters.
- The client can choose one of the configurations offered.
- The client replies to the servers either accepting or rejecting using DHCP REQUEST for rejection the client sends DHCP REQUEST with a reject.
- The rejected server releases the reserved configuration.
- The accepted server sends back DHCP acknowledgement.

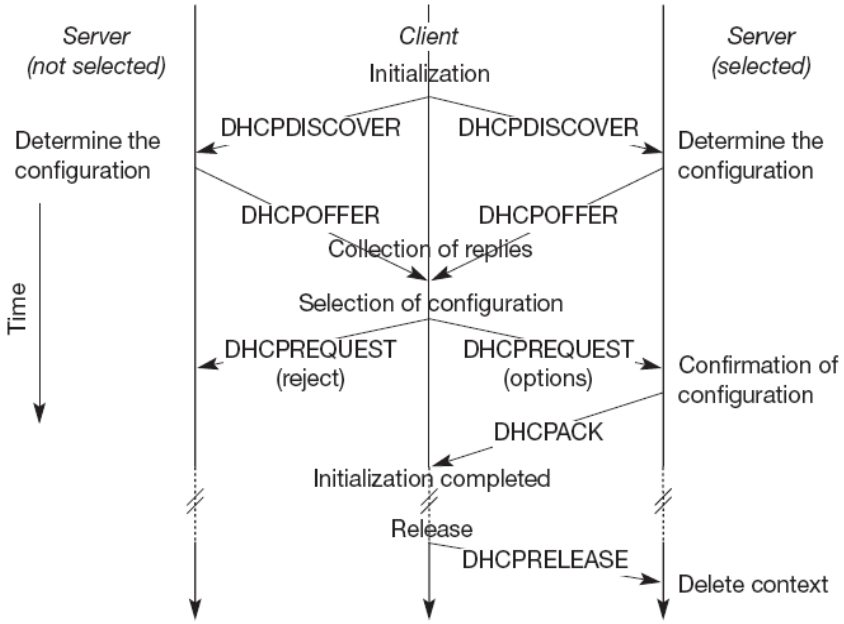

Fig 4.18: Client initialization via DHCP

Release:

- When the client leaves the subnet it should release the configuration received from the server.
- It does using the DHCP RELEASE.
- The period of service is fixed.
- If the client dose not reconfirm within that duration the server will free the configuration. Thus the DHCP supports the acquisition of COA for the mobile modes.

4.2.1 Mobile and adhoc networks

Adhoc Networks:

The networks devices which are mobile and use wireless communication are called as Adhoc Networks.

Examples:

1. **Instant Infrastructure:** Unplanned events cannot rely on infrastructure. Infrastructure takes a longer time. Hence adhoc is used.

2. **Disaster Relief**: During the time of hurricanes, flood the infrastructure break down. In military activities the Adhoc networks can be used.

3. **Remote Areas**: Setting up of infrastructure is costly in remote areas where the Adhoc Networks can be used.

4. **Effectiveness**: Services will be too expensive for certain applications where adhoc network can be used.

4.2.1.1 Concepts and terminologies of adhoc network

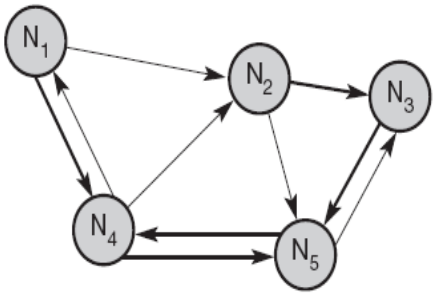

Fig 4.19: Example of adhoc network

- At a certain time t_1 the topology looks as at the left side. Nodes N_1 to N_5 are connected.
- N_1 can receive info over a weak link from N_4, but N_4 can receive over a strong link from N_1.
- The links can be strong or weak depending upon the antenna characteristics or transmit power. N_1 cannot receive from N_2.
- After some time at time t_2 the topology looks as at the right side.
- N_1 cannot receive from N_4, etc.
- Hence in adhoc wireless the topology changes.

4.2.2 Differences between wired and wireless network related to routing

1. **Asymmetric Links**: Routing information for one direction is not the same in the other direction in wireless (i.e.) Node A can receive signal from B. This does not tell about the reverse connection between B to A (i.e.,) B to A link can be either strong/weak or No link routing also for the wired depends upon symmetric scenario.

2. **Redundant Links:** There is no control for the redundant link in the wireless. But the network admin controls the redundancy in wired. High redundancy leads to heavy computational overhead for routing tables.

3. **Interference:** In adhoc the links come and go depending upon the transmission char. (i.e.) one transmission can interfere with other or overhear.

Interference has a disadvantage. If two close by nodes and forward, transmissions they might interfere and destroy each other.

Advantage:

- Node can learn the topology with the help of overhearing.

Dynamic Topology:

- The greatest problem for routing is due to dynamic topology.
- Frequent changes in the topology.
- Routing algorithm face many problems because they rely upon the topology.

4.2.2.1 Routing:

Routing is to find a path between source and destination and to forward the packets appropriately.

Due to the above discussed difficulties in adhoc networks, the following observations are made.

1. In adhoc environment the traditional routing algorithms cannot work because these algorithms cater to symmetric and static network topology.
2. Routing cannot rely on layer three knowledge alone.
3. Centralized approach will not work, because the network in dynamic.
4. Algorithms need to consider the limited battery power of the nodes.
5. Nodes need to make local decision to forward the packets.
6. Flooding is to done forward the packets. This mechanisms works when the load is low.

4.3 Routing Algorithm

The routing algorithms discussed are

1. Destination Sequence Distance Vector.
2. Dynamic Source Routing.
3. Other Routing Algorithm.

4.3.1 Destination Sequence Distance Vector (DSDV)

This DSDV is an enhancement to Distance Vector Routing.

Distance Vector Concept: Each node exchanges with its neighbor , the adjacency information (i.e.) hop count changes at one node in the network

To the existing also DSDV adds two concepts:

1. **Sequence Number:** Each routing advertisements comes with a sequence number. The advertisement travel in many paths. The sequence number is used to see the order of advertisements.
2. **Damping Advantage:** Avoid loops; when the topology remains the same.

Damping (breaking**):**

- Changes in the topology which is of short duration should not destabilize the routing.
- Advertisements containing such transient changes are not disseminated further.
- A node waits with destination if these changes are unstable.
- Waiting time depends on the time between the first and best announcements of a path to a destination.

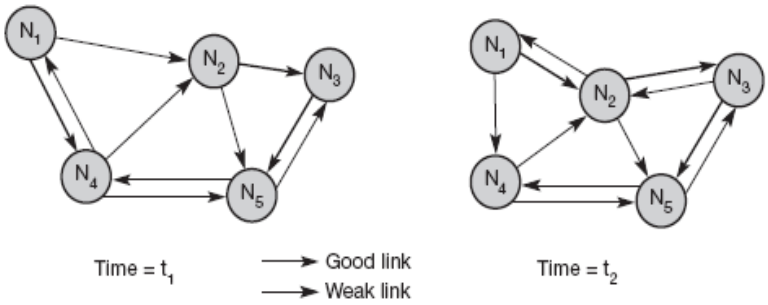

Fig 4.20: Example ad-hoc

The routing table is for N_1 is

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

The Destination is the other nodes in the network.

- **Next hop:** From starting node to which node, it will move in the next hop to reach the destination path to reach the destination is the next hop.
- **Metric:** Metric is the hop count.
- **Sequence No:** Sequence number of the last advertisement for this node.
- **Install Time:** The time at which path was installed first.

Advantages:

- Low memory needed.
- Quick convergence.
- Maintain routes between all nodes**.**

4.3.2 Dynamic Source Routing (DSR)

- In the DSDV, all nodes maintain path to all the other nodes.
- Due to this there is heavy traffic.
- To save the battery power DSR is considered.
- This DSV divides the routing into 2 sub problems.

1.Route Discovery:

Here a node tries to discover a route to a node (i) Only if there is information to send (ii) and no routes are known.

2.Route Maintenance:

If a node is continuously using this route to transmit a packet, then the route should be without problems. But if the node detects that the route is with problem, then it has to determine alternate route.

Working Principle:

If a node reads a route to a destination, it broadcasts a route request with a unique identifier band the destination address

The node which receives the (Route Request Message) does the following:

1. If the node has already received the request, it drops the request packet.
2. If the node recognizes own address as the destination, the request has reached the target.
3. Otherwise the node appends its own address in the route, and broadcasts this updated route request.

Principle:

- The route request collects the list of address representing a possible path on its way towards the destination.When the request reaches the destination, it can return the request packet to the source.
- When the link is bi-directional the route list is sent in the reverse order to the destination.
- When the link is unidirectional the destination does not maintain the route. It needs to discover the route.

Example to find a route from N_1 to N_3 at t_1.

1. N_1 broadcasts the Request (N_1 id=42, target=N_3). N_2 and N_4 receive the packet.
2. N_2 broadcasts (N_1, N_2, id=42, target=N_3).N_4 broadcasts (N_1, N4,id=42,target=N_3).N_3 and N_5 receive N_2's broadcasts. N_1, N_2,N_5 receives N_4's broadcasts.
3. N_3 itself is the target.
4. N_5 broadcasts (N_1, N_2, N_5, id=45, target=N_3). N_3, N_4 receive this broadcast.
5. N_1, N_2, N_5 drop this because it has already received.
6. N_4 drops N_5's broadcast.
7. N_4 finds (N_1, N_2, and N_5) as an alternate route but a longer route.
8. N_3 has to return the path (N_1, N2, and N3) to N_1. N_3 can do the reverse forwarding because symmetric link is assumed.
9. When the links are uni-directional the algorithm needs to be applied again with N_3 as source and N_1 as destination.

Optimization:

1. To avoid too many broad cast route requests should contain a counter. For every rebroad cast the counter is incremented. When the counter exceeds the number of nodes in the network, the nodes can drop the request.
2. Node can Cache the path fragments from recent requests. This fragments can be used to find other route.
3. A node can update the Cache while forwarding the packets.
4. The node can update the Cache when it overhears the transmission from other nodes.

Maintenance of the Route:

When the routes are discovered they need to be maintained. Approaches to maintain the route are as follows

1. If the link layer uses acknowledgement this ack can be considered as an intact route.
2. The node can overhear the next hop which is passive acknowledgement.
3. A node can ask for explicit acknowledge.

When the links are bi-directional , no problem for maintenance. If not the situation is complicated. If there is connectivity problem, detected by a node, it has to inform the sender, to find a new route from the sender.

4.3.3 Other Routing Protocols

4.3.3.1 Flat ad hoc Routing

- This protocol does not set up in any hierarchies with nodes,
- All the nodes have an equal role in routing
- Addressing Scheme is flat.
- Protocols is of two types:
    1. Proactive protocols
    2. Reactive protocols.

1.Proactive Protocols

Sets up tables for routing (e.g.,) DSDV. The Algorithm is based on link state algorithm.

Link State Algorithm:

Such algorithm floods the information to the neighbors periodically. This algorithm cannot be used in mobile ad hoc environment due to too much of updates/too few updates the reduces the traffic.

To achieve both (i.e.) update without traffic.

1. Fisheye State Routing
2. Fuzzy Sighted Link State is used.

The concept is to transmit for away destination at a lower frequency.Some algorithms attacks,

1. Topology Broadcast based on reverse path forwarding.
2. Optimized link state routing.

Advantage of Proactive Protocol

- QOS guarantees
- Routing table reflect the current topology with certain precision.

Disadvantage

- Overhead in lightly loaded networks.

2.Reactive Protocols

A path between source and destination is set only if there is a necessity (e.g.) DSR, AODV (Ad hoc on Demand Distance Vector) on demand.

Advantages:

- Scalability
- Devices can use longer low power periods because they wakeup only when needed.

Disadvantages:

- Initial search latency.
- Route casting is useful only when there is high mobility.

4.3.3.2 Hierarchical Ad hoc Routing

For larger networks, clustering of rodes needs to be done. This algorithm is scalable.

Concept : Locality property. (i.e.)if a cluster can be established nodes remain in the cluster (grouping) with minor changes. When the topology changes only the cluster is to be informed. Nodes of other cluster needs to know how to reach the cluster.

Advantage:

- Lesser number of message transfers.
- Cluster can be combined to form super cluster.
- One node can act as cluster head.
- This cluster head is used as router for Inter Cluster Communication.

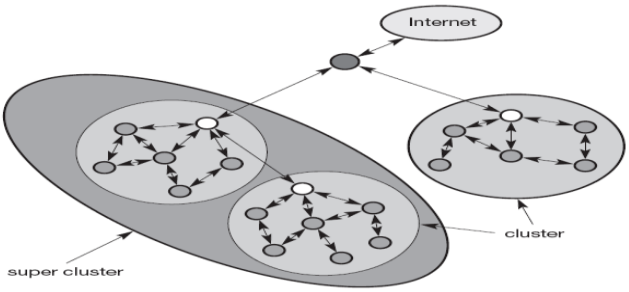

Fig 4.21: Building hierarchies in ad-hoc networks

Three protocols based on this concept are:

1. Cluster Head Gateways Switch Routing.
2. Hierarchical State Routing.
3. Zone Routing Protocol.

4.3.3.3 Geographic Position Assisted Ad hoc Routing

Here the mobile modes should know their geographical position. To get the position we can use Global Positioning System (GPS). Geocast allows the messages to be sent to all nodes in a specific region. This is done based on the address of (geographic information).The location aided routing protocol similar to DSR, can be used. But it is restricted to use in certain geographic only.

4.3.3.4 Greedy Perimeter Stateless Routing:

This method uses the location of neighbors that are exchanged via a periodic beacon messages or in a piggy banking. This follows the greedy method where by the packets are forwarded to the geographically closest neighbor via which the destination can be reached. Once when it reaches a dead end hash tracking should be done.

Metrics

1. Traditionally hop count is considered as Metrics. This hop count is best choice for fixed network.
2. Other metric can be Bandwidth.
3. Least Interference Routing can be considered as other metric.

Consider the topology

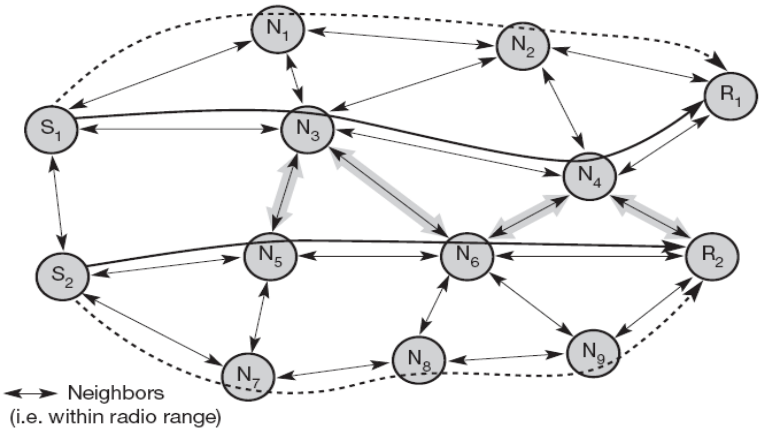

Fig 4.22: Example for least interference routing

S1 is the sources and R1 is the receiver. Possible paths are,

1. S1, N3, N4, R1=No. of hops =4 I=16
2. S1, N3, N2, R1=No. of hops =4 I=15
3. S1, N1, N2, R1=No. of hops =4 I=12
4. S1, N1, N2, N3, N4, R1, committed due to no. of hops =6 (I is the Inference).

This method calculates the Interference of a path. Interference is defined as number of neighbours that can over hear a transmission. Hence the route S1, N1, N2, R1 is selected.