Unit – IV

Mobile Agents in Mobile Computing

In Mobile Computing, Mobile Agents are the composition of computer software and data that can autonomously move from one computer to another computer and continue its execution on the destination computer.

In other words, you can say that An Mobile Agent is an autonomous program that is capable of moving from host to host in a network and interact with resources and other agents. In this process, the chance of data loss is scarce because the state of the running program is saved and then transported to the new host. It allows the program to continue execution from where it left off before migration. The most significant advantage of mobile agents is the possibility of moving complex processing functions to the location where you have enormous amounts of data and that have to be processed.

Mobile Agents are also called as transportable agents. They are classified into two types:

- **Mobile Agents with pre-defined path:** They have a static migration path.
- **Mobile Agents with undefined path i.e., Roamer:** They have dynamic migration paths. The mobile agents choose their path according to the present network condition.

Features of Mobile Agents

The mobile agents are autonomous with intelligence, social ability, learning, and the most important feature is their mobility. They are independent in nature, self-driven and do not require a corresponding node for communication. They can work efficiently even after the user gets disconnected from the network.

Intelligence

Mobile Agents are capable of learning and searching for knowledge about their domain. That's why they are called intelligent agents because they possess a degree of domain knowledge. They can also transport their state from one environment to another without disturbing the previous holding data and be capable of performing appropriately in the new environment.

Autonomous

The Mobile Agents are Autonomous. It means the agents are not only motivated by the outside actions initiated by the users or system but also they have internal events that decided their performance and behaviour. The mobile agents can also take an autonomous decision while selecting a node.

Mobility

Mobile Agents contain some degree of mobility. The agent is not limited to its home node only. They can migrate from one node to another and can carry out tasks along with them. This feature distributes the processing and balancing of the load. Another benefit of this capability is that when the user goes offline, the agents will still keep functioning.

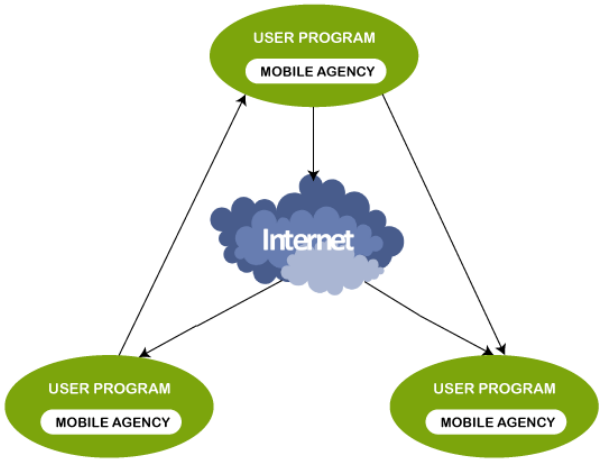
Communicative

Mobile Agents can communicate effectively with other agents, users and systems. The mobile agents use a communication language for inter-agent communication.

Life Cycle of Mobile Agents

The life cycle of mobile agents ensures the following conditions:

- They can adapt to the environment. For example, either home or foreign environment.
- They are capable of switching among the positions of one node to another.
- They are autonomous and focused on the final output.



Advantages of Mobile Agents

The following are some advantages of mobile agents over conventional agents:

- Mobile Agents are autonomous and self-driven in nature.
- They are maintenance-friendly or easily maintainable.
- They are Fault-tolerant. It means they are able to operate without an active connection between client and server.
- They reduce the compilation time.
- They provide less delay in the network.
- They provide fewer loads on the network.

- They facilitate parallel processing. It means they can be asynchronously executed on multiple heterogeneous network hosts.
- They provide dynamic adaptation in which their actions are dependent on the state of the host environment.

Disadvantages of Mobile Agents

The following are some disadvantages of mobile agents:

- The most significant disadvantage of mobile agents is their security. They are less secured

Applications of Mobile Agents

Mobile agents are used in the following applications:

- Mobile Agents are applied in a wide range of domains such as E-commerce, traffic control, network management, robotics, data-intensive applications etc.
- They are also used in grid computing, parallel computing, distributed computing and mobile computing etc.

Security Issues in Agent Systems

The autonomous and mobile nature of the agents introduces new complexities and security issues such as

- In E-Commerce scenario, Agent may be carrying sensitive information like Social Security Number or Bank Account details. Agents must be secure and tamper-proof, and must not reveal information inappropriately.
- The Host platform should provide a safe environment for the agent to execute.
- A malicious agent may attack the Host and access sensitive data or tie up inordinate amount of resources causing Denial of Service to other applications or agents.
- Since agents traverse multiple hosts trusted to different extents, implementing any security measure is complicated.

Classification of Security threats in an Agent System

- Agents attacking Hosts - Malicious agents can steal or modify the data on the host. Lack of sufficient authentication and access control mechanisms lead to these attacks. If

resource constraints are not set, they can also commit Denial of Service(DoS) attacks by exhausting computational resources and denying platform services to other agents.

- Hosts attacking the Agents – A malicious host can attack the agent, by stealing or modifying its data, corrupting or modifying its code or state, deny requested services, return false system call values, reinitialize the agent or even terminate it completely. It can also masquerade the agent by delaying the agent until the task is no more relevant. The Host may also analyze and reverse engineer the agent.
- Malicious Agent attacking another agent – A malicious agent may invoke public methods of another agent to interfere with its work.
- Attack by other entities – Some other entity in the network may manipulate or eavesdrop on agent communication.

Security Measures

Security in Agent System is based on the principle of trust. A set of security policies and protocols establish the trust relationship between the entities.

It is assumed that the agent trusts the Home platform that dispatches it.

Agent attacking the host environment

- Traditional methods such as authentication, access control, sand-boxing techniques, cryptography can be used to secure the Host.
- ***Authentication and access control mechanisms*** – This is the first line of defense against a malicious agent. If the Host can authenticate the agent and in turn the device that dispatched the agent, it can apply authorization and access control.
- ***Safe Code Interpretation*** – Due to the necessity for the agents to run on heterogeneous computer , interpreted scripting or programming languages are used. This produces intermediate code that is executed by a virtual machine that sits on top of the native processor and OS. This virtual machine can enforce additional security.
- ***Path Histories -*** An agent could reach the host by making a number of hops. During this transit a malicious host could have morphed the agent into a malicious agent. By storing the log of the travel of the agent, the current host can determine the route taken by the agent. . Each host platform to which the agent travels to, appends a signed entry to the path. This entry indicates the hosts identity as well as the identity of the next host the agent intends to visit. The platform has to judge by looking at the log if the previous platforms can be trusted.

- ***State Appraisal –*** The author of the agent supplies a state appraisal function called maximum function. This function calculates, depending on the state of the agent, the maximum set of permissions to be granted to the agent. This function is packaged together with the agent. The user/owner of the agent also supplies another state appraisal function called the request function. This calculates the permissions the user wants the agent to have during execution. The host platform uses these state functions to verify the correct state of the agent and hence determines the privileges to give to the agent depending on its state. This ensures that the agent has not turned malicious due to alterations of its states.

Host Platform attacking the Agents

- Providing security against the attacks by the host is difficult due to the fact that the host needs to have the full knowledge of the code and the state in order to execute the agent. Traditional mechanisms are not sufficient to protect an agent from the attack of malicious hosts.
- ***Mobile Cryptography*** – Cryptography is used to maintain code and data privacy and integrity. Both code and data can be encrypted.

Encrypted Functions – For the host to execute the agent, it has to have full control over the code. As prevention, the function of the agent is encrypted according to some conversion algorithm. This encrypted function is implemented as a cleartext program. Even though the host is able to read the program it won't understand what the program does i.e. the "program's function". The disadvantage of this technique is finding the encryption schemes to transform the arbitrary functions.

Encrypted Data - The agent data is encrypted and sent to host for computation. The data that the agent needs for its computation may have to be decrypted again and again at the host platform. For this reason, the agent will have to carry the decryption key making it that much vulnerable.

- ***Obfuscated code*** – A "blackbox" agent is generated from the agent specification wherein the agent's code and data cannot be read or modified. Only its input and output can be observed. The algorithm that creates the agent is called "mess-up or obfuscating algorithm". To prevent dictionary attacks the algorithm, that converts the agent specs into an agent, uses some random parameters. These parameters allow creation of number of different agents out of the same specification. The agents differ in code and data representation but give the same results.

- ***Secure Routing*** - An agent can be programmed to have a routing policy such that it migrates only to certain servers. Since a malicious host can tamper with the agent's itinerary and also computation results, which can propagate, some fault tolerance is needed to ensure that the agent reaches its destination and perform its job correctly. Replication and voting can be used to achieve fault tolerance. The agent is replicated at each stage and run on hosts. The results from these computations are compared (i.e. voted). Then the correct result is sent out as output.
- ***Detecting attack using Dummy data*** –In this technique, dummy data items called *detection objects* are used. This dummy data is stored in the database of the agent and it will not be modified while the agent performs its functions. After the agents return, if the detection objects have not been modified, then one can have reasonable confidence that legitimate data also has not been corrupted. This technique requires that the dummy data should not adversely affect the results of the query.
- ***Using Trusted Hardware*** - This technique uses tamper proof trusted hardware to encapsulate the entire agent execution environment in which the agent executes, thus isolating the agent from the malicious host. The whole agent is not visible to the host environment. The agent in this system will interact with the Host environment through messages. Each Host in the Mobile Agent System is equipped with this hardware. The hardware can be in form of PC Cards, Smartcards, Integrated Circuits, etc. PC Cards are powerful and allow the whole agent code to be loaded into the card. Smartcards are limited in their capabilities. Only a part of agent code can be loaded on the card. The agent carries rest of the code along with it. The code that the agent carries is encrypted.

Fault tolerance through mobile agents

Errors may happen on the server, it may also happen during the network communication. The longer the path of the agent, the higher the possibility that it gets some troubles. Thus it is important to make a mobile agent fault-tolerant. That is to say, the errors can be detected and recovered.

Traditional Primary-Backup protocol

In the traditional Primary-Backup protocol, a fault-tolerant service is implemented through the use of multiple servers. The state information of the service is fully replicated at each server, one of the servers is designated as the primary and the others are designated as backups. Normally, a client sends its request to the primary, which processes the request and sends a response to the clients, In order to preserve the consistency of the replicated service, the

primary also sends to all the backups the database update that occur when each request is processed. When the primary fails, one of the backups takes over as the primary and notices the clients so that subsequent requests will be sent to new primary. In this model, the clients are driven by the servers in the system, they play no role in determining the next primary or in identifying faulty servers.

Active client's primary-backup model

The active client's primary-backup protocols extends the traditional primary-backup model, each client's maintains an ordered list of servers and uses it to detect faulty servers and elect new primary server. The AC model can tolerate three types of failures: crash failures, sendomission failures and receive-omission failures of servers and clients and using minimal replication.

Agent execution model

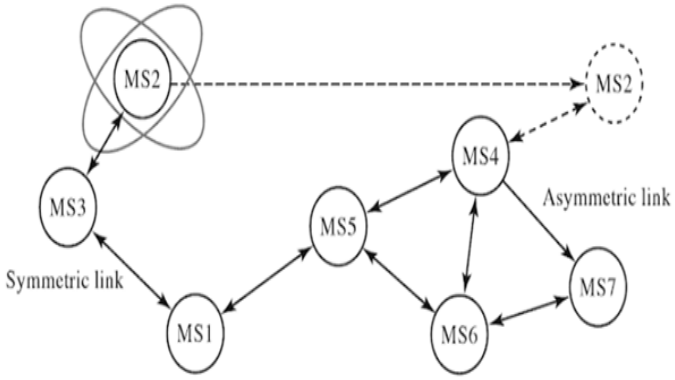
In their agent execution model, tasks are assigned to agents, which perform them autonomously. To execute its task a mobile agent may exploit the services provided by the various nodes of a computer network. Although there could be a couple of candidates, an agent moves to one node before accessing the node's resources, i.e., agents only interact with local services. Agent execution proceeds in steps, where a new step is initiated whenever an agent migrates to the next node in its itinerary. A step of an agent is defined to be the set of operations performed by the agent while it visits this node. In the execution model, resources are encapsulated in resource managers. So each step may change the agent's state as well as the state of the local resources.

The Mobile Transaction Processing

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.

- This is in contrast to the well-known single hop cellular network model that supports the needs of wireless communication between two mobile nodes relies on the wired backbone and fixed base stations.
- 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:



  - As nodes move, the connectivity may change based on relative locations of other nodes. The resulting change in the network topology known at the local level must be passed on to other nodes so that old topology information can be updated.
  - For example, as MS2 in the figure changes its point of attachment from MS3 to MS4, other nodes that are part of the network should use this new route to forward packets to MS2. In the figure, we assume that it is not possible to have all nodes within each other's radio range. In case all nodes are closed by within each other's radio range, there are no routing issues to be addressed.
  - In figures raise another issue, that of symmetric and asymmetric (bidirectional) and asymmetric (unidirectional) links. Consider symmetric links with associative radio range; for example, if MS1 is within radio range of MS3, then MS3 is also within radio range of MS1. The communication links are symmetric. This assumption is not always valid because of differences in transmitting power levels and the terrain. Routing in asymmetric networks is relatively hard task. In certain cases, it is possible to find routes that exclude asymmetric links, since it is cumbersome to find the return path. The issue of efficient is one of the several challenges encountered in a MANET.

- The other issue is varying the mobility patterns of different nodes. Some other nodes are highly mobile, while others are primarily stationary. It is difficult to predict a node's movement and direction of movement and numerous studies have been performed to evaluate their performance using different simulators.

Characteristics of MANET

Some characteristics of adhoc network are as follows:

- **Dynamic topologies:** nodes are free to move arbitrarily; thus the network topology may be changed randomly and unpredictably and primarily consists of bidirectional links. In some cases where the transmission power of two nodes is different, a unidirectional link may exist.
- **Bandwidth-constrained and variable capacity links:** wireless links continue to have significantly lower capacity than infrastructure networks.
- **Energy-constrained operation:** some or all of the MSs in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes or devices, the most important system design optimization criteria may be energy conservation.
- **Limited physical security:** MANETs are generally more prone to physical security threats than wire line networks. The increased possibility of eavesdropping, spoofing, and denial of services (DoS) attacks should be considered carefully. To reduce security threats, many existing link security techniques are often applied within wireless networks.

Applications of MANET

Some specific applications of ad hoc networks include industrial and commercial applications involving cooperative mobile data exchange. There are many existing and future military networking requirements for robust, IP-compliant data services within mobile wireless communication networks, with many of these networks consist of highly dynamic autonomous topology segments. Advanced features of Mobile ad hoc networks, including data rates compatible with multimedia applications global roaming capability, and coordination with other network structures are enabling new applications.

- **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.
- **Crisis management applications:** These arise, for example, as a result of natural disasters in which the entire communication infrastructure is in disarray. Restoring communications quickly is essential.

- **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.
- **Tele-geoprocessing application:** The combination of GPS, GIS (Geographical Information Systems), and high-capacity wireless mobile systems enables a new type of application referred to as tele- geo processing.
- **Virtual Navigation:** A remote database contains the graphical representation of building, streets, and physical characteristics of a large metropolis. They may also "virtually" see the internal layout of buildings, including an emergency rescue plan, or find possible points of interest.
- **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.

Routing

Routing is the process of finding the best path for traffic in a network, or across multiple networks. The role of routing is similar to the road map for a hotel. In both cases, we need to deliver messages at proper location and in an appropriate way.

Routing in a mobile ad-hoc network depends on many factors such as:

- Modeling of the topology,
- Selection of routers,
- Initiation of a route request,
- And specific underlying characteristics that could serve as heuristics in finding the path effectively.

In a MANET, each node or device is expected to serve as a router, and each router is indistinguishable from another in the sense that all routers execute the same routing algorithm to compute paths through the entire network.

Need for Routing

There are following needs for routing:

- Since centralized routing in a dynamic and even for small networks is impossible therefore routing computation must be distributed.
- Route computation should not add many more nodes.
- If any host demands for the route, they must have quick access.
- Maintenance of a global state should not involve in the route computation.
- Each node should care about their destination node to its route and should not be involved in frequent topology updates for those portions of the network that have no traffic.
- Since broadcast can be time consuming for MANETs, it must be avoided as much as possible.
- In routing there must have a backup route when the primary route has become stale.

Routing Classification

Routing protocol can be classified as:

1. Proactive Protocol
2. Reactive Protocol
3. Hybrid Protocol

1. Proactive Protocol

Proactive protocols attempt to evaluate continuously the routes within the network. It means proactive protocol continuously maintain the routing information, so that when a packet needs to be forwarded, the path is known already and can be immediately used. The family of distance vector protocols is an example of proactive scheme.

The advantage of the proactive schemes is that whenever a route is needed, there is negligible delay in determining the route.

Unfortunately, it is a big overhead to maintain routing tables in the MANET environment. Therefore, this type of protocol has following common disadvantages:

- Requires more amounts of data for maintaining routing information.
- Low reaction on re-structuring network and failures of individual nodes.

2. Reactive Protocols

Reactive protocols do not maintain routes but invoke a route determination procedure only on demand or we can say reactive protocols build the routes only on demand. Thus, when a route is required, some sort of global search procedure is initiated. The family of classical flooding algorithms belongs to the reactive protocol group. Examples of reactive ad-hoc network routing protocols include ad hoc on demand distance vector (AODV) and temporally ordered routing algorithm (TORA).

These protocols have the following advantages:

- No large overhead for global routing table maintenance as in proactive protocols.
- Reaction is quick for network restructure and node failure.
  Even though reactive protocols have become the main stream for MANET routing, they still have the following disadvantages:
- Latency time is high in route finding
- Excessive flooding can lead to network clogging.

3. Hybrid Protocols

Hybrid protocols attempt to take advantage of best of reactive and proactive schemes. The basic idea behind such protocols is to initiate route discovery on demand but at a limited search cost. One of the popular hybrid protocols is zone routing protocol (ZRP).

Routing protocols may also be categorized as follows:

1. Table-driven protocols
2. Source initiated on -demand protocols

1. Table-driven routing protocol

- These protocols are called table-driven because each node is required to maintain one or more tables containing routing information on every other node in the network.
- They are **proactive** in nature so that the routing information is always consistent and up to date.
- The protocols respond to changes in network topology by propagating the updates throughput the network so that every node has a consistent view of the network.

The table driven routing protocols are categorized as follows:

Destination - sequenced distance vector routing

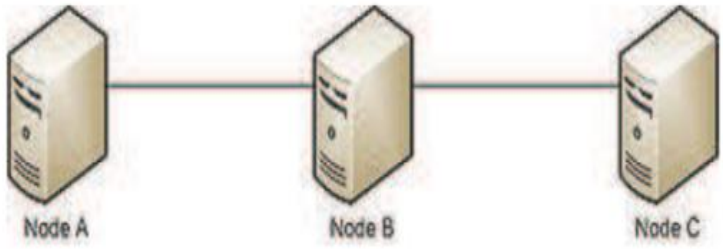
- Destination sequenced distance vector routing (DSDV) is a table driven routing protocol for MANET based on Bellman-Ford algorithm.

Destination	Next Hop	No. of Hops	Sequence no.	Install time
A	A	0	A46	001000
B	B	1	B36	001200
C	B	2	C28	001500

- 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.



For example the routing table of Node A from the above network is:

Basically the table stores description of all possible paths reachable by node A, along with the hop, number of hops, sequence number and install time.

Advantages

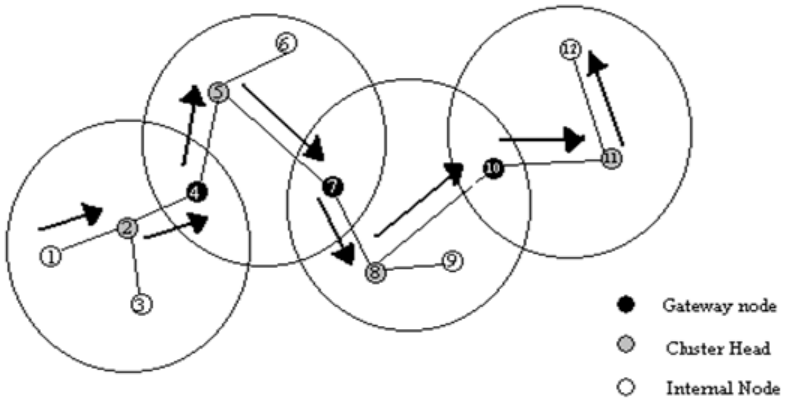
- Destination sequenced distance vector routing was one of the early algorithms available. It is suitable for creating ad-hoc networks with small no. of nodes.

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.

Cluster Head gateway switch Routing

- The cluster head (CH) gateway switch routing (CGSR) protocol is different from the destination sequenced distance vector routing in the type of addressing and the network organization scheme employed.
- Instead of a flat network, CGSR uses cluster heads, which control a group of ad hoc nodes and hence achieve a hierarchical framework for code separation among clusters, routing, channel access, and bandwidth allocation.
- Identification of appropriate clusters and selection of cluster heads is quite complex. Once clusters have been defined, it is desirable to use a distributed algorithm within the cluster to elect a node as the cluster head.
- The disadvantage of using a cluster head scheme is that frequent changes adversely affect performance as nodes spend more time selecting a cluster head rather than relaying packets. Hence, the least cluster change (LCC) clustering algorithm is used rather than CH selection every time the cluster membership changes. Using LCC, CHs change only when two CHs come into contact, or when a node moves out of contact with all other CHs.



- In this scheme, each node must maintain a cluster member table (CMT), which stores the destination CH for each node in the network. The cluster member tables are broadcast periodically by the nodes using the DSDV algorithm.
- When a node receives such a table from a neighbor, it can update its own information. As expected, each node also maintains a routing table to determine the next hop required to reach any destination.

Wireless routing protocol (WRP)

The wireless routing protocol is a proactive unicast routing protocol for MANETs. It uses an enhanced version of the distance vector routing protocol, which uses the Bellman - Ford algorithm to calculate paths.

For the wireless routing protocol (WRP) each node maintains 4 tables:

- Distance table
- Routing table
- Link cost table
- Message retransmission list (MRL) table

Each entry in the message retransmission list has a sequence number of the update message, a retransmission counter, an acknowledgment required flag vector with one entry per neighbor, and a list of updates sent in the update message. When any node receives a hello message from a new node, it adds the new node to its routing table and sends the new node a copy of its routing table. A node must send a message to its neighbors within a certain time to ensure connectivity.

Advantages

- The advantage of WRP is similar to DSDV. In addition, it has faster convergence and adds fewer table updates.

Disadvantage

- The complexity of maintenance of multiple tables demands a large amount of memory and greater processing power from nodes in the MANET.
- Since it suffers from limited scalability therefore WRP is not suitable for highly dynamic and for a very large ad hoc wireless network.

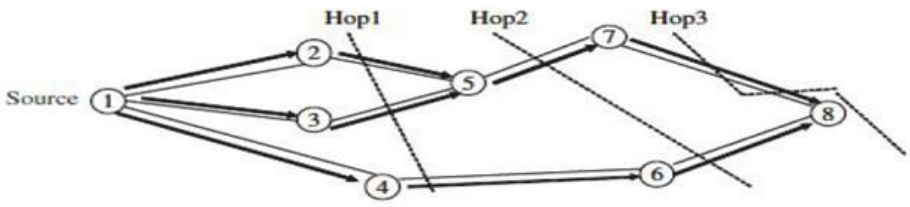
2. Source initiated on -demand protocols

- Source - initiated on demand routing is **reactive** in nature, unlike table driven routing. This type of protocols generates routes only when a source demands it.
- In other words, when a source node requires a route to a destination, the source initiates a route discovery process in the network. This process finishes when a route to the destination has been discovered or all possible routes have been examined without any success.
- The discovered route is maintained by a route maintenance procedure, until it is no longer desired or the destination becomes inaccessible.

The source initiated on demand routing is categorized as follows:

Adhoc on demand distance vector routing (AODV)

- AODV is a routing protocol for MANETs (mobile ad hoc networks) and other wireless ad hoc networks.
- It is a reactive routing protocol; it means it establishes a route to a destination only on demand.
- AODV routing is built over the DSDV algorithm. It is a significant improvement over DSDV.
- The devices that are not on a particular path do not maintain routing information, nor do they participate in the routing table exchanges.
- When a source requires sending a message to a destination and does not have a valid route to the latter, the source initiates a route discovery process.
- Source sends a route request (RREQ) packet to all its neighbors, the latter forward the request to all their neighbors, and so on, until either the destination or an intermediate mobile (node) with a "fresh enough" route to the destination is reached.

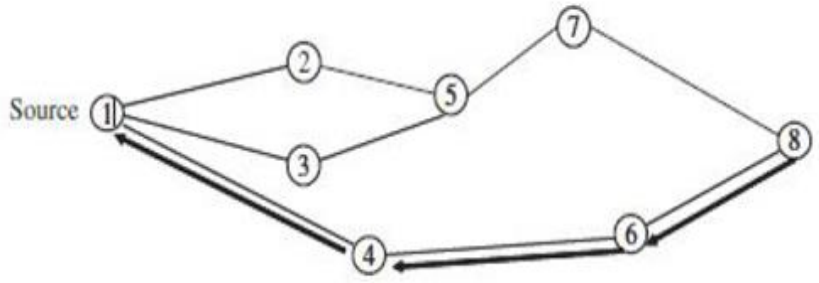


(a) Propagation of route request (RREQ) packet

The above figure illustrates the propagation of the broadcast request (RREQs) across the network. Since in DSDV, destination sequence numbers are used to ensure that all routes are loop free and contain the most recent route information. Each node has a unique sequence number and a broadcast ID, which is incremented each time the node, initiates RREQ.

The broadcast ID, together with the IP address of node, uniquely identifies every RREQ.

Intermediate mobile reply only if they have a route to the destination with a sequence number greater than or at least equal to that contained in the RREQ. To optimize the route performance, intermediate nodes record the address.



(b) Path taken by the route reply (RREP) packet

From the above figure, since RREP (route reply packet) travels back on the reverse path, the nodes on this path set up their forward route entries to point to the node from which RREP had just been received. These forward route records indicate the active forward route. The RREP continues traveling back along the reverse path till it reaches the initiator of the route discovery. Thus, AODV can support only the use of symmetric links.

Dynamic Source Routing (DSR)

- 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.