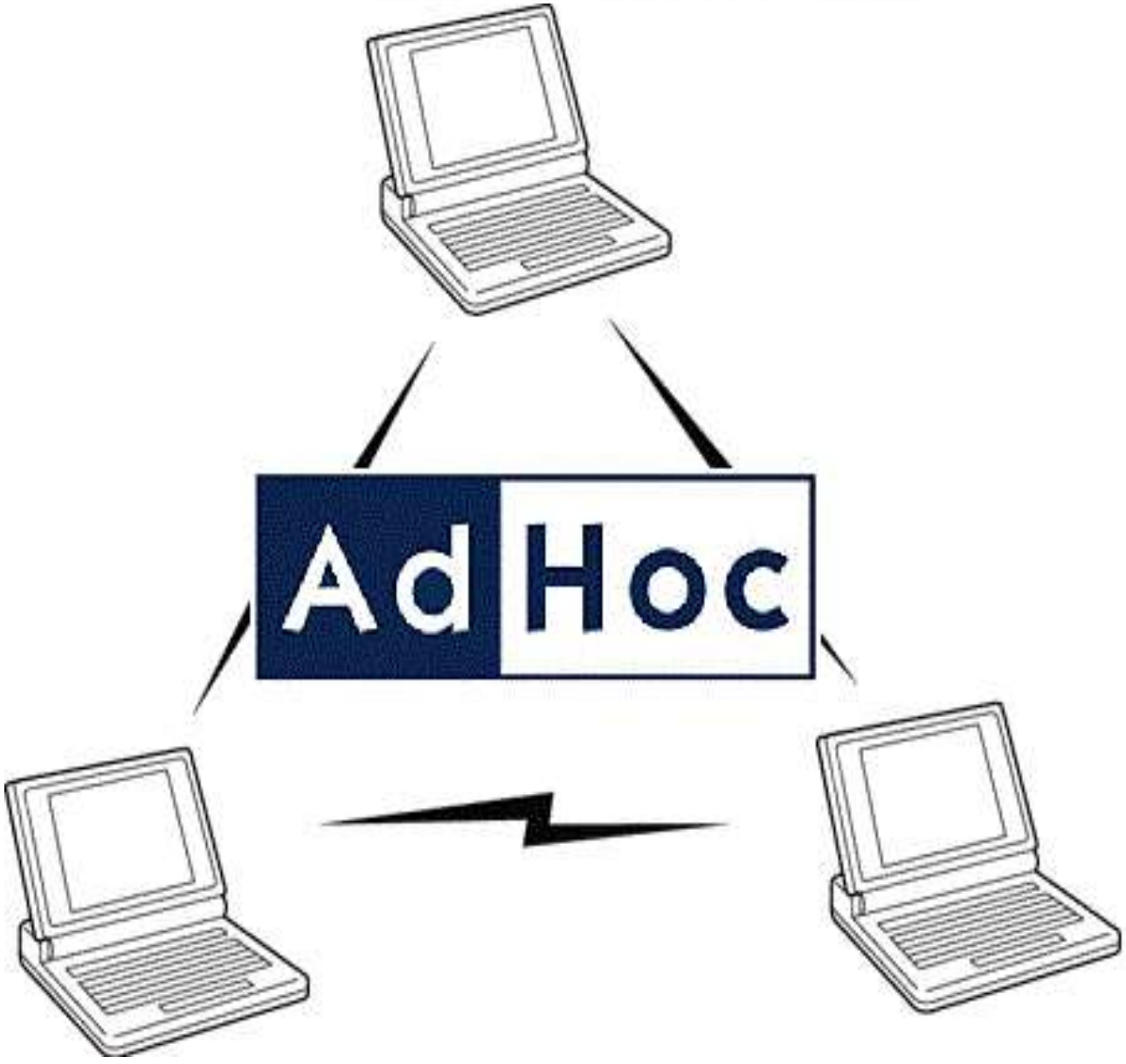
CHAPTER FIVE

MOBILE AD –HOC NETWORKING



Content of Lecture Five

5.1 INTRODUCTION

Wireless ad hoc networks are formed by devices that are able to communicate with each other using a wireless physical medium without having to resort to a pre-existing network infrastructure. These networks, also known as mobile ad hoc networks **(MANETs)**, can form stand-alone groups of wireless terminals, but (some of) these terminals could also be connected to a cellular system or to a fixed network. A fundamental characteristic of ad hoc networks is that they are able to configure themselves on-the-fly without the intervention of a centralized administration. Terminals in ad hoc networks can function not only as end systems **(executing applications, sending information as source nodes and receiving data as destination nodes), but also as intermediate systems (forwarding packets from other nodes).** Therefore, it is possible that two nodes communicate even when they are outside of each other's transmission ranges because intermediate nodes can function as routers. This is why wireless ad hoc networks are also known as multi-hop wireless networks.

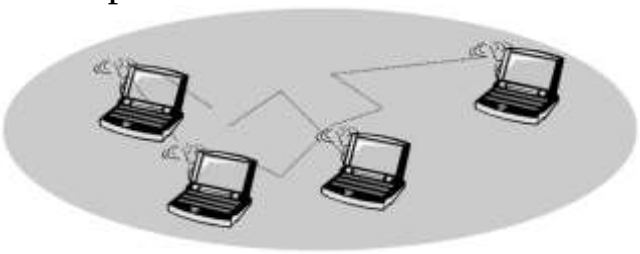


Fig (5.1) Ad-hoc networking

Ad hoc wireless networks inherit the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control, and transmission quality enhancement. In addition, the multi hop nature and the lack of fixed infrastructure generates new research problems such as configuration advertising, discovery, and maintenance, as well as ad hoc addressing and self-routing (see Figure 5.1).

5.2 Wireless Ad Hoc Networks

Wireless ad hoc networks are formed by devices that are able to communicate with each other using a wireless physical medium without having to resort to a pre-existing network infrastructure. Wireless networking paradigms can be categorized broadly into two classes: wireless ad hoc and cellular networking. The existence of a fixed infrastructure is the main difference between these two classes (Figure 5.2). In the ad hoc networking paradigm there is no fixed infrastructure and packets are delivered to their destinations through wireless multi hop connectivity. Nodes often act not only as hosts but also as routers, relaying the traffic by other nodes. The topology of an ad hoc network can change because nodes may not be fixed or, equally, they may fail. In the cellular networking paradigm, mobile terminals reach an access point via a single-hop wireless link. The basic characteristics of ad hoc and cellular networks are compared in Table 5.1.

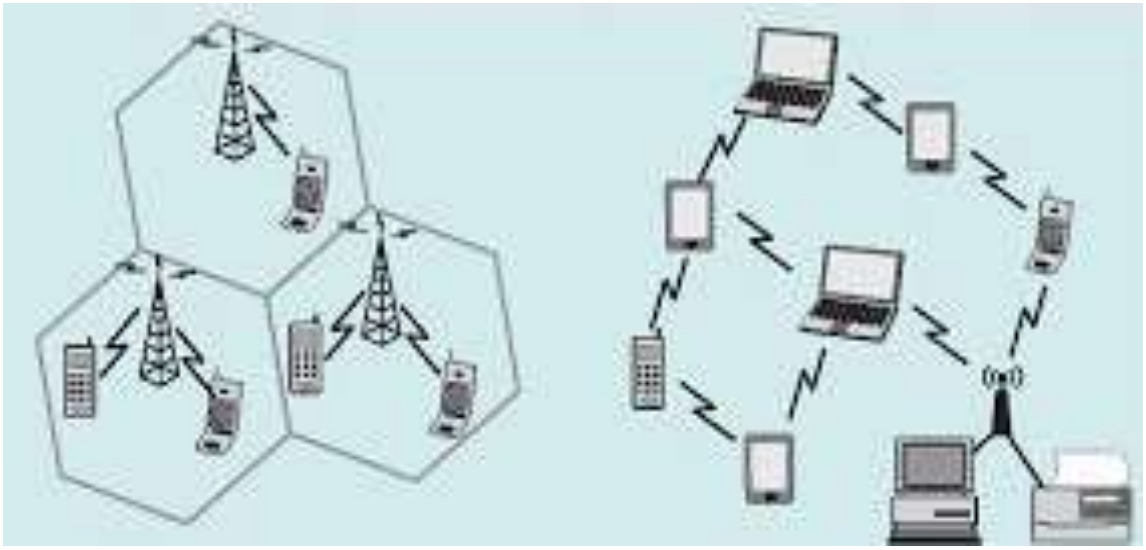


Fig (5.2) (a) Ad hoc and (b) cellular network

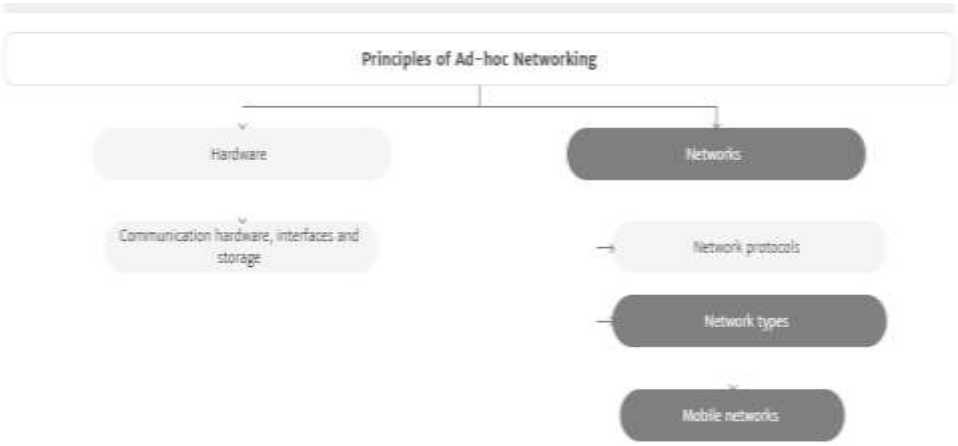
	Ad hoc networking	Cellular networking
Infrastructure	There is no infrastructure.	There is a fixed infrastructure.
Topology	The backbone nodes may be mobile. Topology may change, often due to mobility and/or node failures.	The nodes in the infrastructure are fixed. Terminals can be mobile. However, the topology of the infrastructure seldom changes.
Nodes	The terminal nodes used by the users can also relay the traffic of other nodes.	The nodes in the infrastructure convey data between the source and destination. Their usage as terminal stations or host computers is not mundane. The terminal nodes do not relay traffic from others.
Links	The links are mostly wireless. An end-to-end connection can be made through multiple wireless links, i.e. hops.	The terminal nodes access the infrastructure via a wireless link. The links in the infrastructure can be wireless or nonwireless.

Table (5.1) Ad hoc – Cellular networking

5.3 The principles of Ad-hoc networking

the basic principles of Ad-hoc networking are:

- Mobile device communicate in peer-to-peer fashion
- Self-organizing network without the need of fixed network infrastructure,,
- Multi-hop communication,,
- Decentralized, mobility-adaptive operation.



5.4 Applications of Ad-hoc networking

The most obvious application areas for ad hoc networks include the following:

1. **Temporary network deployment:** ad hoc networks can be deployed when it is not viable or cost effective to construct an infrastructure. For example, they can be used as a temporary solution in conferences, underdeveloped or sparsely populated areas and on terrain on which it is too difficult to install an infrastructure.
2. **Disaster relief operations:** the rapid deployment capability of ad hoc networks makes them an eminent technology to use for the management of relief operations after large-scale disasters such as earthquakes, tsunamis and floods.
3. **Smart buildings:** a large number of sensors and actuators can be deployed without installing any infrastructure to create smart surroundings and a sentient computing environment.
4. **Cooperative objects (COs):** COs are entities that are composed of sensors, actuators and COs capable of communicating and interacting with each other and with the environment in a smart and autonomous way to achieve a specific goal. Note that this is a recursive definition. A CO can be composed of other Co. COs are often mobile and sentient entities that react to real-time sensed data coming from a large number of sensors embedded in the environment as well as requests coming from other COs in the vicinity.
5. **Health care:** systems to monitor the health conditions and where about of patients and elderly people from another obvious application area for ad hoc networks.

5.5 The advantages of ad hoc networks

The advantages of an ad hoc network include:

1. Separation from central network administration.
2. Self-configuring nodes are also routers.
3. Self-healing through continuous re-configuration.
4. Scalability incorporates the addition of more nodes.
5. Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
6. Flexible ad hoc can be temporarily setup at any time, in any place.
7. Lower getting - started costs due to decentralized administration.
8. The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated.

5.6 Challenges of Ad hoc network

There are many more application areas for ad hoc networks. These applications can be realized by tackling challenges specific to wireless ad hoc networking. Some of these challenges are briefly explained below:

5.6.1 The Wireless Medium

In ad hoc networks at least some of the communication links are established through the wireless medium.

5.6.2 Interference, Hidden Terminals and Exposed Terminals

Unconstrained transmission in broadcast media may lead to the time overlap of two or more packet receptions, called collision or interference. This is also possible in guided media, where the collisions can be detected. However, in the wireless medium the hidden terminal phenomenon hinders the detection of collisions. Another phenomenon that has an impact on the efficiency of ad hoc protocols, especially for medium access control, is called the exposed terminal. Source a may not start its transmission to Destination c in order to avoid colliding with the transmission of

Source b to Destination d, although in this case neither source interferes with the other's transmission at either destination. Here, Source a is an exposed terminal.

5.4.3 Mobility, Node Failures, Self-forming, Self-configuration, Topology Maintenance, Routing and Self-healing

The challenges introduced by the wireless medium are aggravated by the mobility of nodes, which act as both terminals and routers. when nodes change their location or fail, the topology of the network that they form changes. Most ad hoc networks are self-forming, self-configuring and self-healing, which means they can autonomously form a network and adapt to the changes in the network. The efficiency in these self-forming and self-healing schemes is closely related to the availability.

5.6.4 Node Localization and Time Synchronization

In a network where there is no fixed infrastructure, node localization and time synchronization become more challenging. Both of these topics can be very important for security and networking protocols in many applications.

5.6.5 End-to-end Reliability and Congestion Control

Since topology changes are always imminent in ad hoc networks and the wireless medium is error prone, the end-to-end connection-oriented transmission control protocol (TCP), which is based on the assumption that the packet losses during transfer are mostly due to congestion, does not fit well with ad hoc networks.

5.7 Mobile Ad hoc network (MANET)

Over the last few years' ad-hoc networking has attracted a lot of research interest. This has led to creation of a working group at the IETF that is focusing on mobile ad-hoc networking, called MANET.

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. MANETs are established and maintained on the fly and work without the support of any form of fixed infrastructure such as base station or an access point. Figure (6.3) shows the relation of MANET to mobile IP and DHCP. While mobile IP and DHCP handle the connection of mobile devices to a fixed infrastructure, MANET comprises mobile routers, too. Mobile devices can be connected either directly with an infrastructure using Mobile IP for mobility support and DHCP as a source of many parameters, such as an IP address. MANET research is responsible for developing protocols and components to enable ad-hoc networking between mobile devices. It should be noted that the separation of end system and router is only a logical separation. Typically, mobile nodes in an ad hoc scenario comprise routing and end system functionality.

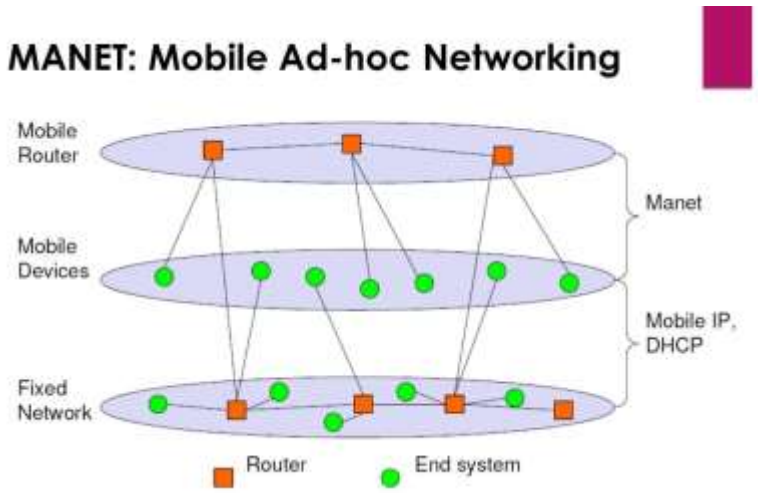


Fig (5.3) MANETs and Mobile IP

In mobile ad hoc networks, topology is highly dynamic and random. In addition, the distribution of nodes and, eventually, their capability of self-organizing play an important role. **The main characteristics can be summarized as follows:**

1. The topology is highly dynamic and frequent changes in the topology may be hard to predict.

2. Mobile ad hoc networks are based on wireless links, which will continue to have a significantly lower capacity than their wired counterparts.
3. Physical security is limited due to the wireless transmission.
4. Mobile ad hoc networks are affected by higher loss rates, and can experience higher delays and jitter than fixed networks due to the wireless transmission.
5. Mobile ad hoc network nodes rely on batteries or other exhaustible power supplies for their energy.

5.7.1 challenges of the MANET

1. Low Processing Capabilities & low bandwidth.
2. Computational & Communication overhead.
3. Mobility-induced route changes.
4. Battery Constraints.
5. Packet losses due to transmission errors.
6. Security Threats.
7. Dynamic Topology.

5.7.2 Applications of MANETs

Some of the typical applications include:

1. Communication among portable computers.
2. Environmental Monitoring.
3. Sensor Networks.
4. Military Sector.
5. Personal Area Network and Bluetooth.
6. Emergency Applications.

5.7.3 The advantages of MANET

the advantages of MANETs are:

1. They provide access to information and services regardless of geographic position.
2. Independence from central network administration.
3. Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.

4. Scalable-accommodates the addition of more nodes.
5. Improved Flexibility.
6. Robust due to decentralize administration.
7. The network can be set up at any place and time.

5.7.4 The disadvantages of MANET

the disadvantages of MANET are:

1. Limited Resource.
2. Limited Physical Security.
3. Vulnerable to attacks. Lack of authorization facilitates.
4. Variable network topology makes it hard to detect malicious nodes.
5. Security protocols for wired network cannot work for ad hoc network.
6. Battery constraints.
7. Frequent route changes leads to computational overhead.

5.8 Vehicular Ad hoc Network (VANET)

VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. Fixed equipment can belong to the government or private network operators or service providers.

A Vehicular Ad hoc Network (VANET) is a special type of MANET in which moving automobiles form the nodes of the network. i.e., vehicles are connected to each other through an ad hoc formation that forms a wireless network.

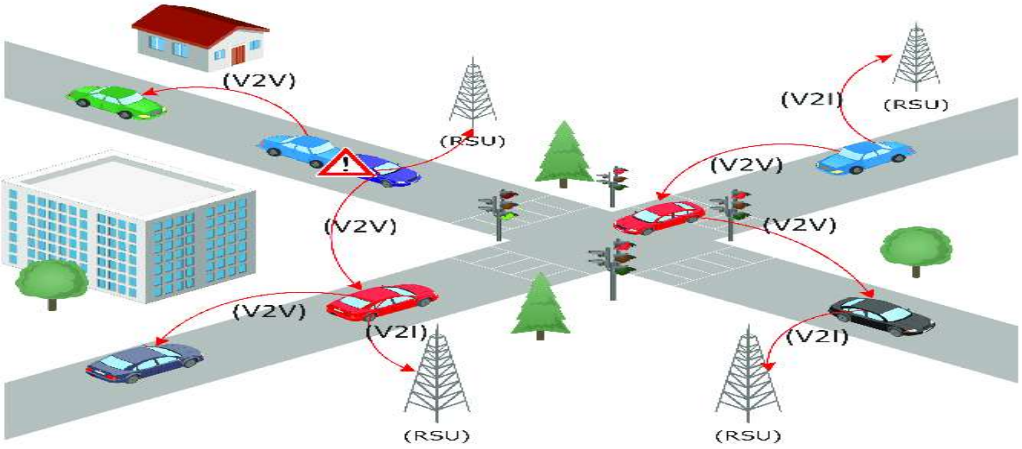


Fig (5.4) VANET

5.8.2 The goals of VANET

1. Improve traffic safety and comfort of driving
2. Minimize accidents, traffic intensity, locating vehicles
3. Up-to-date traffic information
4. Intersection collision warning
5. Weather information.

5.8.2 Special Characteristics of VANET

Though VANET could be treated as a subgroup of Mobile Ad Hoc Networks (MANETs) and it is still necessary to consider VANETs as a distinct research field, especially in the light of security provisioning. The unique characteristics of VANET include features:

1) High Dynamic Topology

The speed and choice of path defines the dynamic topology of VANET. If we assume two vehicles moving away from each other with a speed of 60 km/h (25 m/s) and if the transmission range is about 250m, the link between these two vehicles will last for only 5 seconds (250m). This defines its highly dynamic topology.

2) the Anonymous Addressee

Most applications in VANETs require identification of the vehicles in a certain region, instead of the specific vehicles. This may help protect node privacy in VANETs.

3) Mobility Modeling and Prediction:
The above features for connectivity therefore needed the knowledge of node positions and their movements which is as such very difficult to predict keeping in view the nature and pattern of movement of each vehicle.

4) Communication Environment
The mobility model highly varies from highways to that of city environment. The node prediction design and routing algorithm also therefore need to adapt for these changes. Highway mobility model is essentially a one-dimensional.

5) Unlimited Transmission Power
The node (vehicle) itself can provide continuous power to computing and communication devices.

6) Hard Delay Constraints
The safety aspect (such as accidents, brake event) of VANET application warrants on time delivery of message to relevant nodes. It simply cannot compromise with any hard data delay in this regard.

7) Interaction with onboard Sensors
These sensors help in providing node location and their movement nature that are used for effective communication link and routing purposes.

8) Higher Computational Capability
Indeed, operating vehicles can afford significant computing, Communication and sensing capabilities.

9) Rapidly Changing Network Topology
Due to high node mobility, the network topology in VANET tends to change frequently.

10) Potentially Unbounded Network Size
VANETs could involve the vehicles in one city, several cities or even a country. Thus, it is necessary to make any protocols for VANET is scalable in order to be practical.

11) Time-Sensitive Data Exchange
Any protocols and a scheme for VANET is better. Most safety related applications require data packet transmission in a timely

manner. Thus, any security schemes cannot harm the network performance of VANETs.

12) Abundant Resources

VANET nodes have abundant energy and computation resources. This allows schemes involving usage of resource demanding techniques such as ECDSA, RSA etc.

13) Better Physical Protection

VANET nodes are better protected than MANETs. Thus, Nodes are more difficult to compromise which is also good news for security provisioning in VANETs.

14) Partitioned Network

Vehicular networks will be frequently partitioned. The dynamic nature of traffic may result in large inter vehicle.

5.8.3 The uses of VANET

1) A VANET can help drivers to get advance information and warnings from a nearby environment via message exchanges.
2) A VANET can help disseminate geographical information to the driver as he continues to drive.
3) Drivers may have the opportunity to engage in other task.

5.8.4The applications of VANETs

1) Safety oriented
   a) Real-time traffic
   b) Cooperative message transfer
   c) Post-crash notification
   d) Road hazard control notification
   e) Traffic vigilance
2) Commercial oriented
   a) remote vehicle personalization
   b) internet access
   c) digital map downloading
   d) real time video relay

S.No		VANET – Vehicular Adhoc Network	MANE – Mobile Adhoc Network
1	**Basic Idea**	It is a collection of nodes(vehicles) that communicate with each other over bandwidth constrained wireless links with certain road side infrastructure or base station	It is a collection nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support
2	**Production Cost**	Costly	Inexpensive
3	**Network Topology Change**	Frequent and very fast	Sluggish / Slow
4	**Mobility**	High	Low
5	**Density in Node**	Frequent variable and dense	Sparse
6	**Bandwidth**	1000 kbps	100 kbps
7	**Range**	Up to 600 m	Up to 100 m
8	**Node lifetime**	It is depend on vehicle life time	It is depend on power source
9	**Reliability**	High	Medium
10	**Nodes moving Pattern**	Regular	Random

Table (5.2) compare MANET vs VANET

5.9 Routing in Ad- hoc network

While in wireless networks with infrastructure support a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network. A destination node might be out of range of a source node transmitting packets. Routing is needed to find a path between source and destination and to forward the packets appropriately.
In wireless networks using an infrastructure, cells have been defined. Within a cell, the base station can reach all mobile nodes without routing via a broadcast. In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates many additional problems that are discussed in the following paragraphs. Figure (5.5) gives a simple example of an ad-hoc network. At a certain time t1 the network topology might look as illustrated on the left side of the figure. Five nodes, N1 to N5, are connected depending on the current transmission characteristics between them. In this snapshot of the network, N4 can receive N1 over a good link, but N1 receives N4 only via a weak link. Links do not necessarily have the same characteristics in.

The reasons for this are, e.g. different antenna characteristics or transmit both directions power. N1 cannot receive N2 at all, N2 receives a signal from N1.

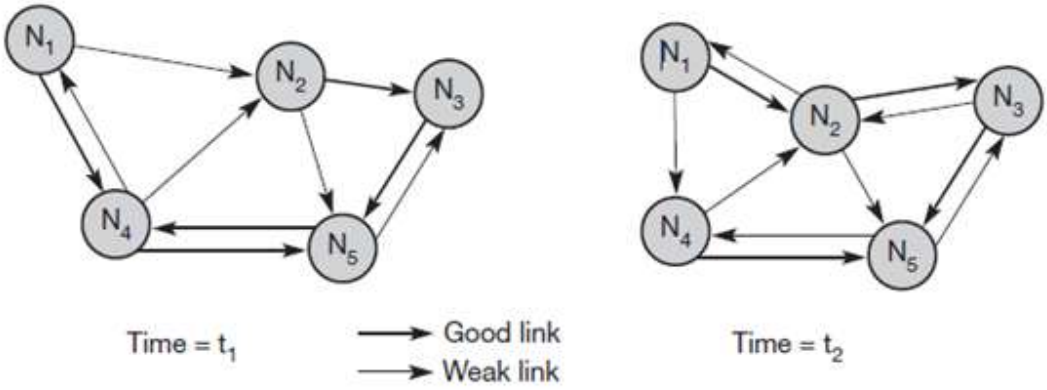


Fig (5.5) Example ad-hoc network

This situation can change quite fast as the snapshot at t2 shows. N1 cannot receive N4 any longer, N4 receives N1 only via a weak link. But now N1 has an asymmetric but bi-directional link to N2 that did not exist before. This very simple example already shows some fundamental differences Between wired networks and ad-hoc wireless networks related to routing.

- Asymmetric links

Node A receives a signal from node B. But this does not tell us anything about the quality of the connection in reverse. B might receive nothing, have a weak link, or even have a better link than the reverse direction. Routing information collected for one direction is of almost no use for the other direction. However, many routing algorithms for wired networks rely on a symmetric scenario.

- Redundant links

Wired networks, too, have redundant links to survive link failures. However, there is only some redundancy in wired networks, which, additionally, are controlled by a network administrator. In ad-hoc

networks nobody controls redundancy, so there might be many redundant links up to the extreme of a completely meshed topology.

Routing algorithms for wired networks can handle some redundancy, but a high redundancy can cause a large computational overhead for routing table updates.

- Interference

In wired networks links exist only where a wire exists, and connections are planned by network administrators. This is not the case for wireless ad-hoc networks. Links come and go depending on transmission characteristics, one transmission might interfere with another, and nodes might overhear the transmissions of other nodes. Interference creates new problems by 'unplanned' links between nodes: if two close-by nodes forward two transmissions, they might interfere and destroy each other. On the other hand, interference might also help routing. A node can learn the topology with the help of packets it has overheard.

- Dynamic topology

The greatest problem for routing arises from the highly dynamic topology. The mobile nodes might move as shown in Figure ٦.٦ or medium characteristics might change.

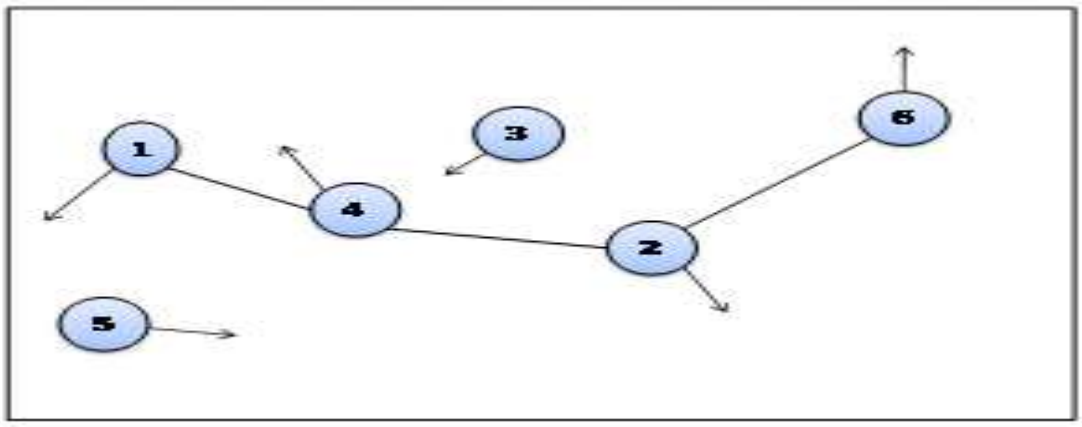


Fig (5.6) Dynamic Topology

This results in frequent changes in topology, so snapshots are valid only for a very short period of time. In ad hoc networks, routing tables must somehow reflect these frequent changes in topology, and routing algorithms have to be adapted. Routing algorithms used in

wired networks would either react much too slowly or generate too many updates to reflect all changes in topology.

Routing table updates in fixed networks, for example, take place every 30 seconds. This updating frequency might be too low to be useful for ad-hoc networks. Some algorithms rely on a complete picture of the whole network. While this works in wired networks where changes are rare, it fails completely in ad-hoc networks. The topology changes during the distribution of the 'current' snapshot of the network, rendering the snapshot useless. Ad-hoc networks using mobile nodes face additional problems due to hardware limitations. Using the standard routing protocols with periodic updates wastes battery power without sending any user data and disables sleep modes. Periodic updates waste bandwidth and these resources are already scarce for wireless links.

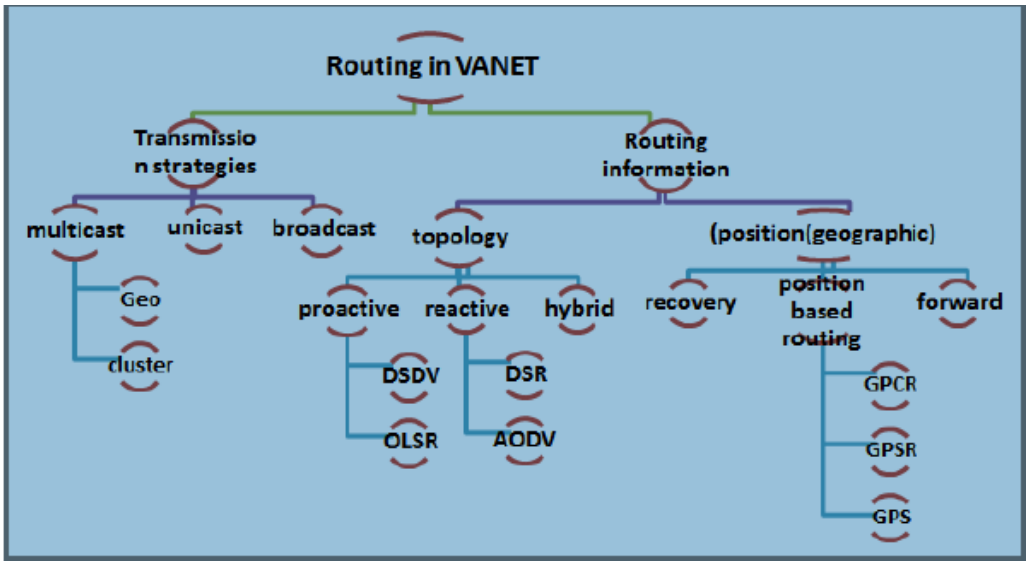


Fig (5.7) Routing protocols

5.9.1 Proactive protocols (Table- Driven)

Set up tables required for routing regardless of any traffic that would require routing functionality. DSDV, as presented is a classic

member of this group. Many protocols belonging to this group are based on a link-state algorithm as known from fixed networks. Link-state algorithms flood their information about neighbors periodically or event triggered.

In mobile ad-hoc environments this method exhibits severe drawbacks: either updating takes place often enough to reflect the actual configuration of the network or it tries to minimize network load. Both goals cannot be achieved at the same time without additional mechanisms and fuzzy sighted link-state attack this problem by making the update period dependent on the distance to a certain hop. Routing entries corresponding to a faraway destination are propagated with lower frequency than those corresponding to nearby destinations. The result is routing tables that reflect the proximity of a node very precisely, while imprecise entries may exist for nodes further away. Other link-state protocols that try to reduce the traffic caused by link-state information dissemination are topology broadcast based on reverse path forwarding.

A general advantage of proactive protocols is that they can give QoS guarantees related to connection set-up, latency or other real time requirements. As long as the topology does not change too fast, the routing tables reflect the current topology with a certain precision. The propagation characteristics (delay, bandwidth etc.) of a certain path between a sender and a receiver are already known before a data packet is sent.

A big disadvantage proactive schemes are their overheads in lightly loaded networks. Independent of any real communication the algorithm continuously updates the routing tables. This generates a lot of unnecessary traffic and drains the batteries of mobile devices.

5.9.1.1Destination sequence distance vector(DSDV)

Destination sequence distance vector (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks. DSDV can be considered historically. Each node exchanges its neighbor table periodically with its neighbors. Changes at one node in the

network propagate slowly through the network (step-by-step with every exchange). The strategies to avoid this problem which are used in fixed networks. This might create loops or unreachable regions within the network.

DSDV now adds two things to the distance vector algorithm:

- Sequence numbers: Each routing advertisement comes with a sequence number. Within ad-hoc networks, advertisements may propagate along many paths. Sequence numbers help to apply the advertisements in correct order. This avoids the loops that are likely with the unchanged distance vector algorithm.
- Damping: Transient changes in topology that are of short duration should not destabilize the routing mechanisms. Advertisements containing changes in the topology currently stored are therefore not disseminated further. A node waits with dissemination if these changes are probably unstable. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.

The routing table for N1 in Figure (5.٨) would be as shown in Table (5.3)

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

Table (5.3) part of Routing table for DSDV

For each node N1 stores the next hop toward this node, the metric (here number of hops), the sequence number of the last advertisement for this node, and the time at which the path has been installed first. The table contains flags and a settling time helping to decide when the path can be assumed stable. Router advertisements

from N1 now contain data from the first, third, and fourth column: destination address, metric, and sequence number.

Besides being loop-free at all times, DSDV has low memory requirements and a quick convergence via triggered updates.

5.9.2 Reactive protocols (ON-demand)

Try to avoid this problem by setting up a path between sender and receiver only if a communication is waiting. The two most prominent members of this group are dynamic source routing (DSR) and ad-hoc on-demand distance vector (AODV) an on-demand version of DSDV. AODV acquires and maintains routes only on demand like DSR does. Both protocols, DSR and AODV, are the leading candidates for standardization in the IETF.

A clear advantage of on-demand protocols is scalability as long as there is only light traffic and low mobility. Mobile devices can utilize longer low-power periods as they only have to wake up for data transmission or route discovery. However, these protocols also exhibit disadvantages.

The initial search latency may degrade the performance of interactive applications and the quality of a path is not known a priori. Route caching, a mechanism typically employed by on-demand protocols, proves useless in high mobility situations as routes change.

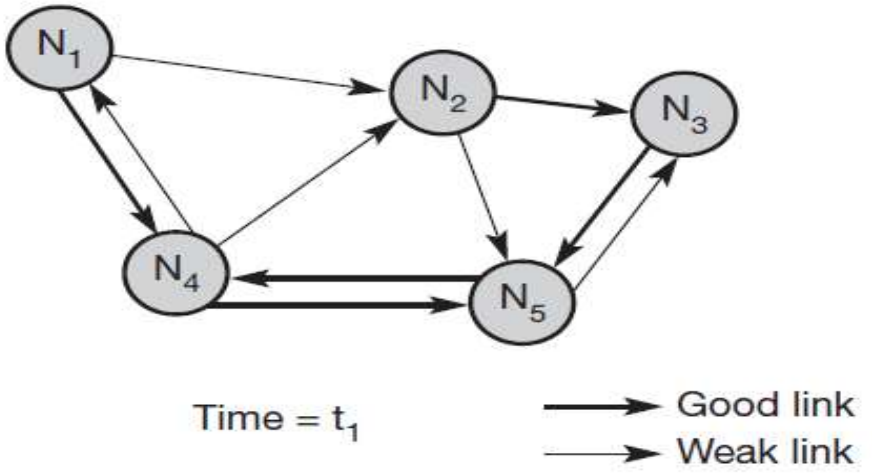
5.9.2.1 Dynamic source routing (DSR)

Imagine what happens in an ad-hoc network where nodes exchange packets from time to time, i.e., the network is only lightly loaded, and DSDV or one of the traditional distance vector or link state algorithms is used for updating routing tables. Although only some user data has to be transmitted, the nodes exchange routing information to keep track of the topology. These algorithms maintain routes between all nodes, although there may currently be no data exchange at all. This causes unnecessary traffic and prevents nodes from saving battery power. Dynamic source routing (DSR), therefore, divides the task of routing into two separate problems:

- Route discovery: A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- Route maintenance: If a node is continuously sending packets via a route, it has to make sure that the route is held upright. As soon as a node detects problems with the current route, it has to find an alternative. The basic principle of source routing is also used in fixed networks, e.g. token rings. Dynamic source routing eliminates all periodic routing updates and works as follows. If a node needs to discover a route, it broadcasts a route request with a unique identifier and the destination address as parameters. Any node that receives a route request does the following.
- If the node has already received the request (which is identified using the unique identifier), it drops the request packet.
- If the node recognizes its own address as the destination, the request has reached its target.
- Otherwise, the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.

Using this approach, the route request collects a list of addresses representing a possible path on its way towards the destination. As soon as the request reaches the destination, it can return the request packet containing the list to the receiver using this list in reverse order. One condition for this is that the links work bi-directionally. If this is not the case, and the destination node does not currently maintain a route back to the initiator of the request, it has to start a route discovery by itself. The destination may receive several lists containing different paths from the initiator. It could return the best path, the first path, or several paths to offer the initiator a choice.

Applying route discovery to the example in Figure (5.8) for a route from N1 to N3 at time t1 results in the following.



- N1 broadcasts the request ((N1), id = 42, target = N3), N2 and
- N2 then broadcasts ((N1, N2), id = 42, target = N3), N4 broadcasts ((N1, N4), id = 42, target = N3). N3 and N5 receive N2's broadcast, N1, N2, and N5 receive N4's broadcast.
- N3 recognizes itself as target, N5 broadcasts ((N1, N2, N5), id = 42, target =N3). N3 and N4 receive N5's broadcast. N1, N2, and N5 drop N4's broadcast packet, because they all recognize an already received route request (andN2's broadcast reached N5 before N4's did).
- N4 drops N5's broadcast, N3 recognizes (N1, N2, N5) as an alternate, but longer route.
- N3 now has to return the path (N1, N2, N3) to N1. This is simple assuming symmetric links working in both directions.

5.9.2.2 Ad-hoc On-Demand Distance Vector Routing Protocol (AODV)

AODV is a distance vector routing protocol that is included in the classification of the reactive routing protocol, which is just to Request a service when needed. This routing protocol determine the route to destination if there is node that wants to transmit data using Route request(RREQ)packet that sent by source.

If there is active route to the destination, receiver will reply the messages with route reply(RREP) packet. AODV is flat routing protocol that does not require central administrative system in routing process.

The advantage in AODV routing is providing the change in link situation very easily. It can undergo the large delays during route manipulation and consume more bandwidth when the network size increases. AODV have several characteristics among other routing protocols such as:

1. find routes only as needed.
2. Use of Sequence numbers to track accuracy of information.
3. Keeps only track of next hop for a route instead of the entire route.
4. Use of periodic HELLO messages to track Neighbors.
5. Using RERR message react to fast changing in network
6. Topology and updating affected host.
7. Loop free by using sequence number.

5.9.2.2.1 AODV Message Classes (control messages)

There following four classes represent the AODV messages consists of:

1- Route Request Message (RREQ): Source node that needs to Communicate with another node in the network transmits RREQ message, AODV floods RREQ message, using expanding ring technique there is a time to live (TTL)value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted. While communication routes between nodes are valid, AODV does not play any role.

2-Route Reply Message (RREP): When a RREQ reaches a destination node, the destination route is made available by unicasting a RREP back to the source route. Anode generates a RREP if it is itself the destination or it has an active route to the destination, an intermediate node may also respond with an RREP if it has afresh enough route to the destination.

3- Route Error Message(RERR): Every node in the network keeps monitoring the links tat us to its neighbor's nodes during active

routes. When the node detects a link crack in an active route, RERR message is generated by the node in order to notify other nodes that the link is down.

4- Hello messages: AODV is a reactive protocol it uses the Hello messages periodically to inform its neighbors that the link to the host is alive. The Hello messages are broad casted with TTL equals to1, so that the message will not be for warded further. When the host receives the Hello message it will update the life time of the host in formation in the routing table. If the host does not get information from the hosts neighbor for a specified amount of time, then the routing information in the routing table is marked as lost.

This action generates needed RRER message to inform other hosts of the link breakage .and figure (5.7) show basic AODV control packets.

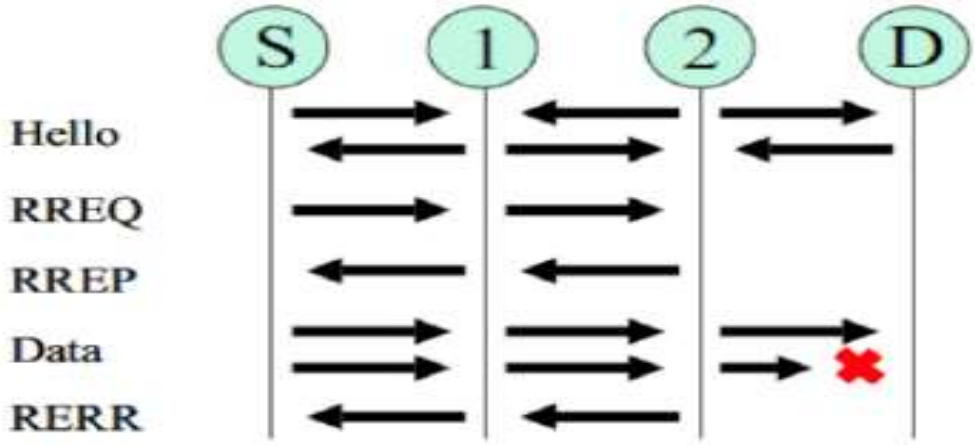


Fig (5.9) basic AODV control packets

5.9.2.2.2 Route Discovery Mechanism in AODV

The route discovery is done by using the steps of AODV routing algorithm on the basis of ROUTE-REQUEST, ROUTE REPLY, ROUTE-ACK and ROUTE-ERR messages. For path discovery source node broadcast a RREQ packet to all its neighbor nodes. The header of the RREQ packet contains the Sequence number and ROUTE-ID fields. The neighbor nodes then again rebroadcast the

RREQ packet to their neighbor nodes. So, a reverse path is generated between the source and the neighbor node. The nodes which already get a ROUTE-ID will discard all then next coming ROUTE-IDs in order to prevent the loop formation in the route. So, the RREQ Packets propagate in the network until the destination is found.

When the destination is reached by the RREQ packet, the destination node sends a unicast RREP message towards the source.

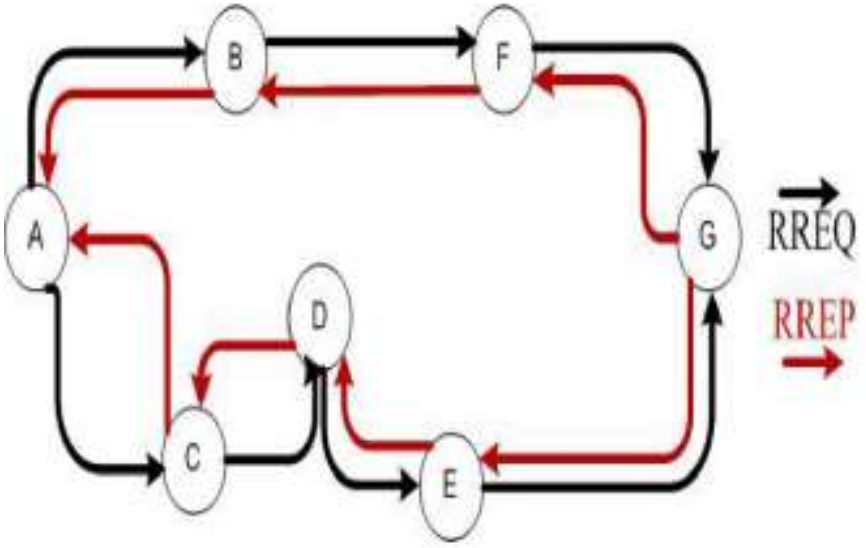


Fig (5.10) The Route Discovery Mechanism.

5.9.2.2.3 Route Maintenance in AODV

After the route discovery process, Path Maintenance begin, in This process when anode detects a path failure it broadcast a message to all other nodes exist in that network. It also provides a nearly recognition of node or link break down since wireless networks make use of hop-to-hop acknowledgement.

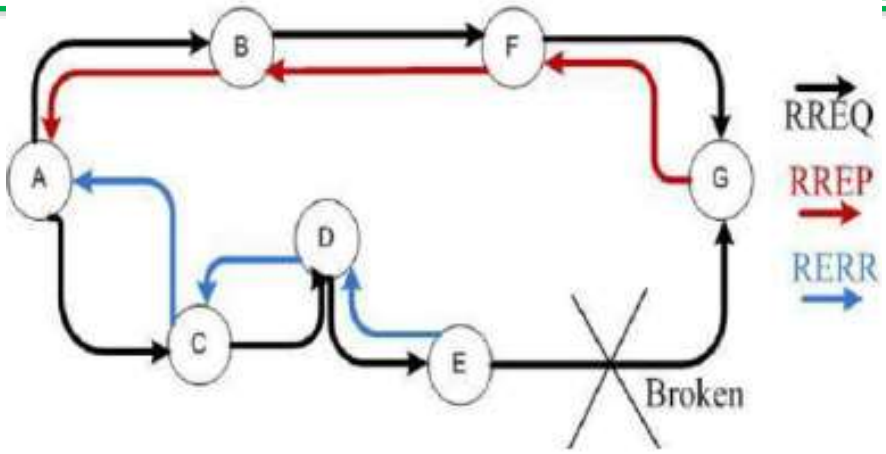


Fig (5.11) **Route Maintenance in AODV**

Table (5.4) compare Reactive VS Proactive

Parameters	Reactive Protocols (On-demand)	Proactive Protocols (table-driven)
Routes availability	Discovers route whenever it needed (on-demand basis)	Routes are always available to particular source to particular destination
Route maintenance	Effective route maintenance and routing cache is only updated when there are changes in network. **AODV**: It needs periodic updates(limited)	Periodic updates are required to maintain the active routes and nodes in a routing table. Routes in routing table may be wrong in highly dynamic network.
Bandwidth consumption	Less bandwidth is used for to maintain and exchange the routing information	It takes large bandwidth to share the routing information in large scale network. This large routing information exchange may cause broadcast storm when the mobility is high.
Energy consumption	Energy consumption is depends of the nodes mobility	Generally energy consumption is high than reactive protocol.

References

[1] D. Kouvatsos (Ed.): Next Generation Internet, LNCS 5233, pp. 746–766, 2011. c Springer-Verlag Berlin Heidelberg 2011

[2] Eng., EPSC, Tech. Univ. of Catalonia, Avda. del Canal Olimpic s/n, 08860 Castelldefels, Barcelona, Spain Wireless Ad Hoc Networks: An Overview 2011

[3] T. S. Rappaport, *Wireless communications: principles and practice* vol. 2: prentice hall PTR New Jersey, 1996.

[4] Principles of Ad-hoc NetworkingJune 2007 Go to Guide books homepage June 2007 Read More Authors: Michel Barbeau profile imageMichel Barbeau, Evangelos Kranakis profile imageEvangelos Kranakis Publisher: Wiley Publishing ISBN:978-0-470-03290-9.

[5] W. C. Lee, *Mobile cellular telecommunications: analog and digital systems*: McGraw-Hill Professional, 1995.

[6] Cayirci, E., & Rong, C. (2008). Security in wireless ad hoc and sensor networks. John Wiley & Sons.