Survey of Reactive Protocols in Ad-hoc Networks

Vishal S. Kore,
Computer Engineering Department,
Flora Institute of Technology, Khopi,
Pune, Maharashtra,
vshlkore@gmail.com

Shailendra A. Shete,
Computer Engineering Department,
Flora Institute of Technology, Khopi,
Pune, Maharashtra,
shailu8831@gmail.com

virendra Thoke.
Computer Engineering Department
Flora Institute of Technology, Khopi
Pune, Maharashtra
virendra.thoke@rediffmail.com

***Abstract*— Ad Hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration, in which individual nodes cooperate by forwarding packets to each other to allow nodes to communicate beyond direct wireless transmission range. Routing is a process of exchanging information from one station to other stations of the network. Routing protocols of mobile ad-hoc network tend to need different approaches from existing Internet protocols because of dynamic topology, mobile host, distributed environment, less bandwidth, less battery power.**

Ad Hoc routing protocols can be divided into two categories: table-driven (proactive schemes) and on-demand routing (reactive scheme) based on when and how the routes are discovered. In Table-driven routing protocols each node maintains one or more tables containing routing information about nodes in the network whereas in on-demand routing the routes are created as and when required. Some of the on-demand routing protocols like Ad Hoc on-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR) are discussed in this paper.

***Keywords*— AODV, Beacon, DSR, MANET, Link, Node. Proactive, Reactive, RREQ, Routing table, ZRP**

I. INTRODUCTION

There are currently two variations of mobile wireless networks infrastructured and Infrastructureless networks.

The infrastructured networks**,** also known as **Cellular network**, have fixed and wired gateways. They have fixed base stations that are connected to other base stations through wires. The transmission range of a base station constitutes a cell. All the mobile nodes lying within this cell connects to and communicates with the nearest bridge (base station). A hand off occurs as mobile host travels out of range of one Base Station and into the range of another and thus, mobile host is able to continue communication seamlessly throughout the network. Example of this type includes office wireless local area networks (WLANs).

The other type of network, Infrastructureless network, is known as **Mobile Ad-hoc NETwork (MANET).** These networks have no fixed routers. All nodes are capable of movement and can be connected dynamically in arbitrary manner. The responsibilities for organizing and controlling the network are distributed among the terminals themselves. The entire network is mobile, and the individual terminals are allowed to move at will relative to each other. In this type of network, some pairs of terminals may not be able to communicate directly to with each other and relaying of some messages is required so that they are delivered to their destinations. The nodes of these networks also function as routers, which discover and maintain routes to other nodes in the networks. The nodes may be located in or on airplanes, ships, trucks, cars, perhaps even on people or very small devices.

1.1Characteristics of MANET:

Dynamic Topologies: Since nodes are free to move arbitrarily, the network topology may change randomly and rapidly at unpredictable times. The links may be unidirectional bidirectional.

Bandwidth constrained, variable capacity links: Wireless links have significantly lower capacity than their hardwired counterparts. Also, due to multiple access, fading, noise, and interference conditions etc. the wireless links have low throughput.

Energy constrained operation: Some or all of the nodes in a MANET may rely on batteries. In this scenario, the most important system design criteria for optimization may be energy conservation.

Limited physical security: Mobile wireless networks are generally more prone to physical security threats than are fixed- cable nets. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered. Existing link security techniques are often applied within wireless networks to reduce security threats. As a benefit, the decentralized nature of network control in MANET provides additional robustness against the single points of failure of more centralized approaches.

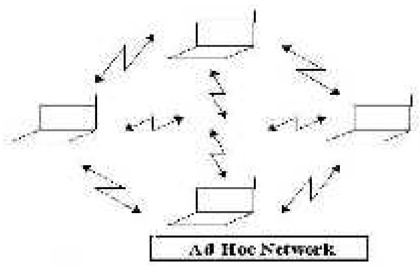

Figure: 1 Ad Hoc Network

The chief difference between ad hoc networks is the apparent lack of a centralized entity within an ad hoc network. There are no base stations or mobile switching centers in an ad hoc network.

The interest in wireless ad hoc networks stems from of their well-known advantages for certain types of applications. Since, there is no fixed infrastructure; a wireless ad hoc network can be deployed quickly. Thus, such networks can be used in situations where either there is no other wireless communication infrastructure present or where such infrastructure cannot be used because of security, cost, or safety reasons.

Ad-hoc networks were mainly used for military applications. Since then, they have become increasingly more popular within the computing industry. Applications include emergency search and rescue operations, deployment of sensors, conferences, exhibitions, virtual classrooms and operations in environments where construction of infrastructure is difficult or expensive. Ad-hoc networks can be rapidly deployed because of the lack of infrastructure.

1.2 Problem Description

The objective of this paper is to discuss two of the proposed routing protocols namely, AODV and DSR, for wireless ad-hoc networks.

The goal of this report is to:

1. To explain general concept of ad -hoc networks.
2. To give knowledge about classification of routing protocols in Ad-hoc networks.
3. To discuss Reactive routing protocols i.e. AODV and DSR.

II. LITERATURE REVIEW

Mobile ad-hoc network is deployed in applications such as disaster recovery and distributed collaborative computing, where routes are mostly multi-hop and network hosts communicate via packet radios. Routing is one of the challenging issues in mobile ad-hoc network.

2.1Why Routing Protocols are the main issue In Ad Hoc networks?

Routing is an activity or a function that connects a call from origin to destination in Telecommunication networks and also plays an important role in architecture, design and Operation of networks. Wireless mobile ad-hoc networks are characterized as networks without any physical connections.

Routing support for mobile hosts is presently being formulated as mobile IP technology when the mobile agent moves from its home network to a foreign (visited) network, the mobile agent tells a home agent on the home network to which foreign agent their packets should be forwarded. In addition, the mobile agent registers itself with that foreign agent on the foreign network. Thus, the home agent forwards all packets intended for the mobile agent to the foreign agent, which sends them to the mobile agent on the foreign network. When the mobile agent returns to its original network, it informs both agents (home and foreign) that the original configuration has been restored. No one on the outside networks need to know that the mobile agent moved. But in Ad Hoc networks there is no concept of home agent as it itself may be moving.

Supporting Mobile IP form of host mobility requires address management, protocol inter operability enhancements and the like, but core network functions such as hop by hop routing still presently rely upon pre existing routing protocols operating within the fixed network. In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes, which may be combined routers and hosts, themselves form the network routing infrastructure in an ad hoc fashion. Hence, the need to study special routing algorithms to support this dynamic topology environment. Routing protocols for mobile ad-hoc networks have to face the challenge of frequently changing topology, low transmission power and asymmetric links.

In these networks there is no fixed topology due to the mobility of nodes, interference, multipath propagation and path loss. A good routing protocol for this network environment has to dynamically adapt to the changing network Topology. Second, the underlying wireless channel provides much lower and more variable bandwidth than wired networks. Hence a dynamic routing Protocol is needed for these networks to function properly [1].

*2.2 Ad Hoc Routing Protocols***:**

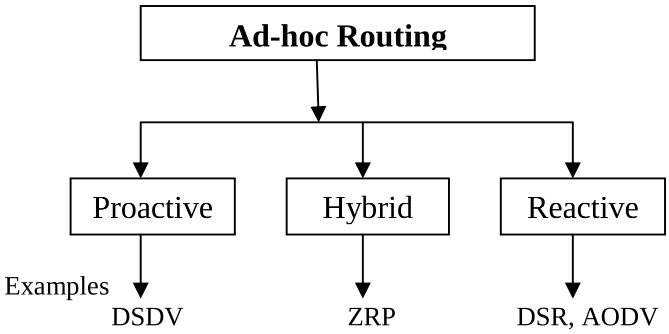

Figure 2: Categorization of Ad-Hoc Routing Protocols

We can also see the third type of protocols i.e. Hybrid (Both Proactive and Reactive) routing protocols in figure [2].

2.2.1 Proactive Routing Protocols

Proactive protocols maintain unicast routes between all pairs of nodes regardless of whether all routes are actually used. Therefore, when the need arises (i.e., when a traffic source begins a session with a remote destination), the traffic source has a route readily available and does not have to incur any delay for route discovery. These protocols also can find optimal routes (shortest paths) given a model of link costs. Routing protocols on the Internet (i.e., distance vector-based RIP and link state-based OSPF) fall under this category. However, these protocols are not directly suitable for resource-poor and mobile ad hoc networks because of their high overheads and/or somewhat poor convergence behaviour.

Therefore, several optimized variations of these protocols have been proposed for use in ad hoc networks [3].

2.2.2 Reactive (on-demand) routing protocols

Main idea in on-demand routing is to find and maintain only needed routes. Recall that proactive routing protocols maintain all routes without regard to their ultimate use. The obvious advantage with discovering routes on-demand is to avoid incurring the cost of maintaining routes that are not used. This approach is attractive when the network traffic is sporadic, bursty and directed mostly toward a small subset of nodes. However, since routes are created when the need arises, data packets experience queuing delays at the source while the route is being found at session initiation and when route is being repaired later on after a failure. Another, not so obvious consequence of on-demand routing is that routes may become suboptimal, as time progresses since with a pure on-demand protocol a route is used until it fails.

2.2.3 Hybrid (Both Proactive and Reactive) routing protocol

A typical hybrid routing protocol is Zone Based Routing (ZBR). ZBR combines the Proactive and reactive routing approaches. Hybrid routing protocols are zone based; it means the number of nodes is divided into different zones to make route discovery and maintenance more reliable for MANET. The need of these protocols arises with the deficiencies of proactive and reactive routing and there is demand of such protocol that can resolve on demand route discovery with a limited number of route searches.

III. REACTIVE ROUTING PROTOCOLS

This paper is focused on AODV and DSR reactive routing protocols.

3.1 Dynamic Source Routing (DSR)

DSR is characterized by the use of source routing. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache. The data packets carry the source route in the packet header.

When a node in the ad hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Route discovery works by flooding the network with route request (also called query) packets. Each node receiving a request rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the request with a route reply packet that is routed back to the original source. Route request and reply packets are also source routed. The request builds up the path traversed so far. The reply routes itself back to the source by traversing this path backward. The route carried back by the reply packet is cached at the source for future use. If any link on a source route is broken (detected by the failure of an attempted data transmission over a link, for example), a route error packet is generated. Route error is sent back toward the source which erases all entries in the route caches along the path that contains the broken link. A new route discovery must be initiated by the source, if this route is still needed and no alternate route is found in the cache.

DSR makes aggressive use of source routing and route caching. With source routing, complete path information is available and routing loops can be easily detected and eliminated without requiring any special mechanism. Because route requests and replies are source routed, the source and destination, in addition to learning routes to each other, can also learn and cache routes to all intermediate nodes. Also, any forwarding node caches any source route in a packet it forwards for possible future use. DSR employs several optimizations including promiscuous listening which allows nodes that are not participating in forwarding to overhear on-going data transmissions nearby to learn different routes free of cost. To take full advantage of route caching, DSR replies to all requests reaching a destination from a single request cycle. Thus the source learns many alternate routes to the destination, which will be useful in the case that the primary (shortest) route fails. Having access to many alternate routes saves route discovery floods, which is often a performance bottleneck. This may, however, result in route reply flood unless care is taken. However, aggressive use of route caching comes with a penalty. Basic DSR protocol lacks effective mechanisms to purge stale routes. Use of stale routes not only wastes precious network bandwidth for packets that are eventually dropped, but also causes cache pollution at other nodes when they forward/overhear stale routes.

3.1.1 Example of Route Discovery in DSR

- When node 'S' wants to send a packet to node 'D', but does not know a route to 'D', node 'S' initiates a route discovery.
- Source node 'S 'floods Route Request (RREQ).
- Each node appends own identifier when forwarding RREQ.
- Destination 'D' on receiving the first RREQ sends a RREP as a response to RREQ to source node.
- RREP is sent on a route obtained by reversing the appended to receive RREQ.
- RREP includes the route from 'S' to 'D' on which RREQ was received by node 'D'.
- Node S on receiving RREP, caches the route included in the RREP.
- When node S sends a data packet to D, the entire route is included in the packet header.

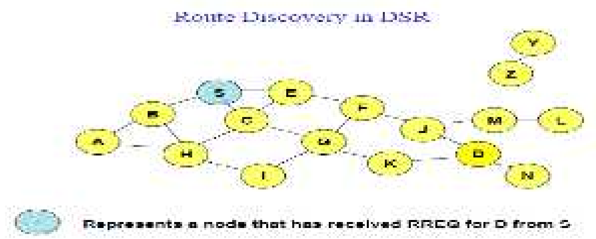

Figure 3 Route Discovery in DSR Source node 'S'

We can see the source node S who wants to send a packet to node 'D', but does not know a route to 'D' in figure 3.

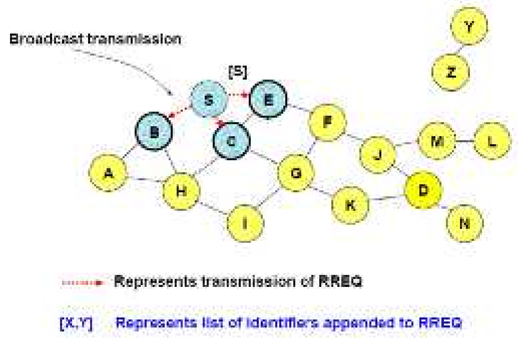

Figure 4 Source node 'S' Broadcasts RREQ message

We can observe that source node broadcasts RREQ message to find the way to reach at destination node i.e. node 'D' also we can see that node 'H' is getting RREQ packet from two neighbours i.e. from node 'C' and node 'B' which may cause collision of RREQ packet at node 'H'.

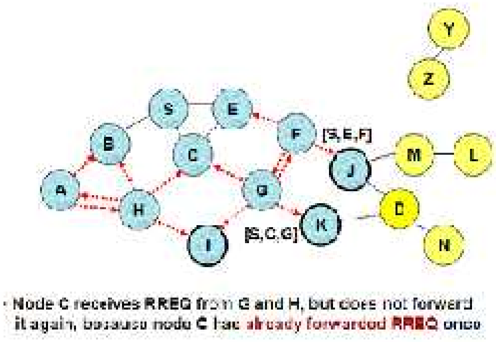

Figure 4 Route Discovery in DSR

The process of route discovery continues until RREQ packet is reaches to its destination, we can see that node 'C' got RREQ from node 'H' and node 'G' but it does not forward it again because node 'C' has already forwarded RREQ message which it got by node 'S'.

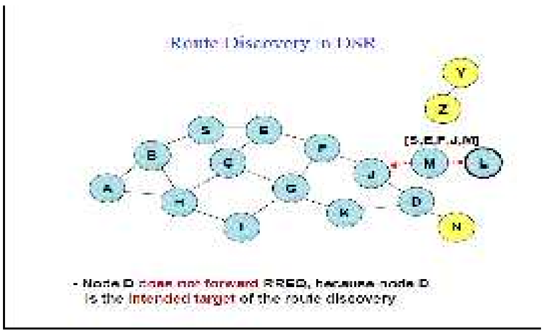

Figure 5 Destination node discovered i.e. node 'D'

Node 'D' is intended target or destination that's why it does not forward RREQ packet and the search of destination node comes to end.

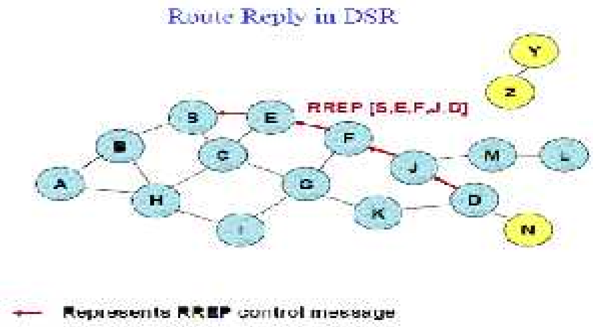

Figure 6 Route Reply by using reverse path

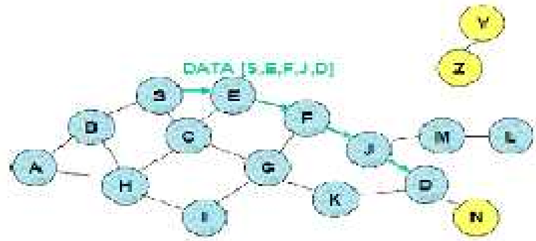

Figure 7 Data Delivery in DSR

We can see RREP packet is going towards source node 'S' by using reverse path as shown in figure 6 and data delivery takes place on receiving RREP, and after cacheing the route included in the RREP.

3.1.2 Advantages and Disadvantages of DSR

Advantages:

- ❖ Routes maintained only between nodes who need to communicate, reduces overhead of route maintenance.
- ❖ Route caching can further reduce route discovery overhead
- ❖ A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local Caches.

Disadvantages:

- ❖Packet header size grows with route length due to source routing.
- ❖Potential collisions between route requests propagated by neighboring nodes.
- ❖Increased contention if too many route replies come back at source node.
- ❖Stale caches will lead to increased overhead

3.2 Ad hoc On-demand Distance Vector (AODV)

AODV shares DSR's on-demand characteristics in that it also discovers routes on an "as needed" basis via a similar route discovery process. However, AODV adopts a very different mechanism to maintain routing information. It uses traditional routing tables, one entry per destination. This is in contrast to DSR, which can maintain multiple route cache entries for each destination. Without source routing, AODV relies on routing table entries to propagate a RREP back to the source and, subsequently, to route data packets to the destination. AODV uses destination sequence numbers to prevent routing loops and to determine freshness of routing information. These sequence numbers are carried by all routing packets.

The absence of source routing and promiscuous listening allows AODV to gather only a very limited amount of routing information with each route discovery. Besides, AODV is conservative in dealing with stale routes. It uses the sequence numbers to infer the freshness of routing information and nodes maintain only the route information for a destination corresponding to the latest known sequence number; routes with older sequence numbers are discarded even though they may still be valid. AODV also uses a timer-based route expiry mechanism to promptly purge stale routes. Again if a low value is chosen for the timeout, valid routes may be needlessly discarded. The AODV protocol is a loop free and avoids the counting to infinity problem.

3.2.1 Example of Route Discovery in AODV [5]

- When node 'S' wants to send a message to node 'D', 'S' searches its route table for a route to 'D'.
- If there is no route, 'S' initiates a RREQ message with the following components :
  - The IP addresses of 'S' and 'D'
  - The current sequence number of 'S' and the last known sequence number of 'D'
  - A broadcast ID from 'S'. This broadcast ID is incremented each time 'S' sends a RREQ message.
- Once a unicast route has been established between two nodes 'S' and 'D', it is maintained as long as 'S' (source node) needs the route.
- If 'S' moves during an active session, it can reinitiate route discovery to establish a new route to 'D'.
- When 'D' or an intermediate node moves, a route error (RERR) message is sent to' S'.

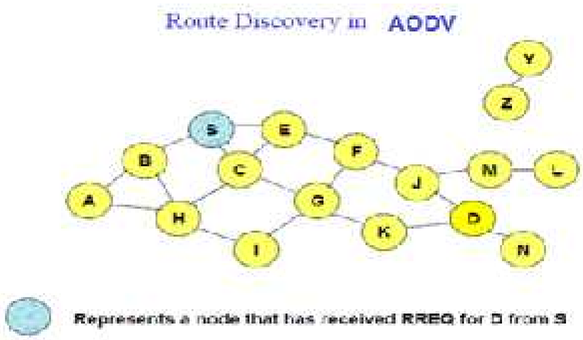

Figure 8 Route Discovery in AODV (Source node 'S')

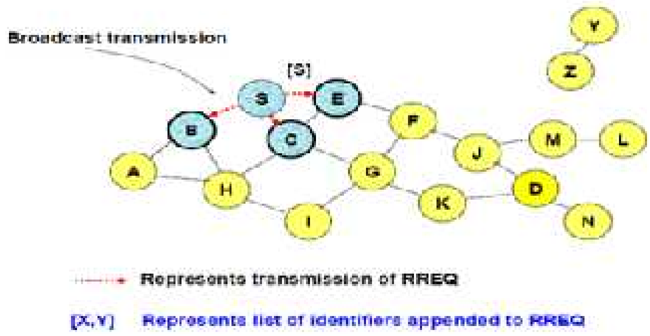

Figure 9 Route Request in AODV (Source node 'S')

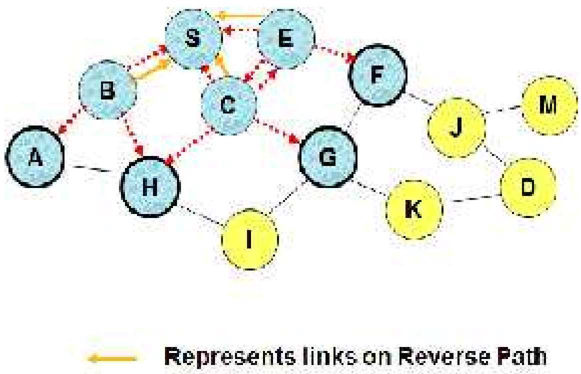

Figure 10 Reverse path maintained while forwarding RREQ in AODV

Route discovery by source node 'S' is shown in figure 8. The route discovery process consists of a route-request message (RREQ) which is broadcasted as shown in figure 9. If a node has a valid route to the destination, it replies to the route-request with a route-reply (RREP) message as shown in figure 10. Additionally, the replying node creates a so called reverse route entry in its routing table which contains the address of the source node, the number of hops to the source, and the next hop's address, i.e. the address of the node from which the message was received. A lifetime is associated with each reverse route entry, i.e. if the route entry is not used within the lifetime it will be removed [4].

The process of route discovery continues until RREQ packet is reaches to its destination, we can see that node 'C' got RREQ from node 'H' and node 'G' but it does not forward it again because node 'C' has already forwarded RREQ message which it got by node 'S'.

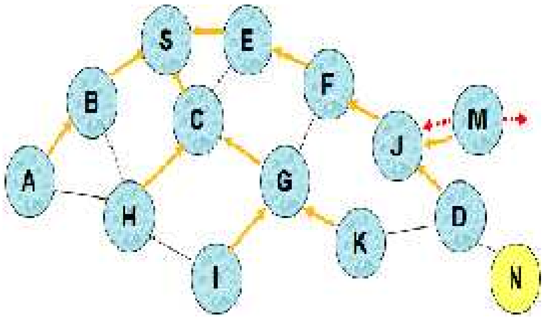

Figure 11 Destination node discovered i.e. node 'D'

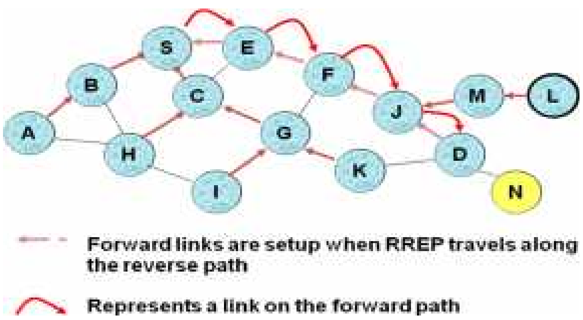

Figure 12 Forward Path Setup in AODV

Above figure indicates that when RREP message is being sent to source node at that time forward links are setup for data transmissions between source 'S' to destination 'D'. Once a unicast route has been established between two nodes S and D, it is maintained as long as S (source node) needs the route. If S moves during an active session, it can reinitiate route discovery to establish a new route to D.When D or an intermediate node moves, a route error (RERR) message is sent to S.

3.2.2 Advantages and Disadvantages of AODV

Advantages

- Sequence numbers are applied to find latest route to destination.
- Quick response to link breakage.
- The connection setup delay is lower.

Disadvantages

- Intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries
- Multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.
- Unnecessary bandwidth consumption due to periodic beaconing.

IV OBESERVATIONS

After doing lot of survey and explaining AODV and DSR briefly we have reached to point where we can compare them this comparison is shown in Table 1.

Factors	Protocol	
	DSR	AODV
Protocol Type	Source Routing	Distance Vector
Supports unicasting	Yes	Yes
Supports Multicasting	No	Yes
Multiple routes	Yes	No
Message Overhead	High	High
Periodic broadcast	No	Yes
Required sequence	No	Yes
Summary	Route Discovery, Snooping	Route Discovery, Expanding Ring Search ,Setting forward path
Route cacheing	High	Low
Beaconing	No	Yes
Response to link breakage	Low	High

Table 1 shows a comparison between the AODV and DSR routing protocols

DSR doesn't have proper mechanism to expire the stale routes and therefore the jitter and the average end-to-end delay is also very high in comparison to AODV [4].

DSR with the help of caching is more effective at low mobility and low loads. AODV performs well in more stressful scenarios of high mobility and high loads. These relative performance differentials are attributed to DSR's lack of effective mechanisms to purge stale routes and AODV's need for resorting to route discovery often because of its single path nature [3].

On-demand routing is naturally adaptive to traffic diversity and therefore its overhead proportionately increases with increase in traffic diversity. On-demand routing can also significantly benefit by caching multiple paths when node mobility is low.

V CONCLUSION

Due to the dynamically changing topology and infrastructure less, decentralized characteristics, of mobile ad hoc networks, designing routing protocols is always challengeable. Lots of research have been done by many researchers in Ad-hoc routing protocols but still there is a large scope for development.

We have studied ADDV and DSR briefly both use the reactive On-demand routing strategy DSR and AODV both use on-demand route discovery, but with different routing mechanics. In particular, DSR uses source routing and route caches, and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively and maintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes.

Reactive routing protocols are more efficient than table driven routing protocols. In reactive protocols a route is built only when required, Control information is not propagated unless there is a change in the topology.

V REFERENCES

[1] Krishna Gorantala," Routing Protocols in Mobile Ad-hoc Networks", Umea University Department of Computing Science, 2006

[2] Sat veer Kaur, **"**Performance Comparison of DSR and AODV Routing Protocols with Efficient Mobility Model in Mobile Ad-Hoc Network", International Journal of Computer Science and Technology, June 2011.

[3] P. Mohapatraa, S. Krishnamurthy," AD HOC NETWORKS Technologies and Protocols*"*, Springer, 2005

[4] Parma Nand and Dr. S.C. Sharma, IIT, Roorkee India," Traffic Load based Performance Analysis of DSR, STAR & AODV Adhoc Routing Protocol ", International Journal of Advanced Computer Science and Applications (IJACSA), October 2010.

[5] Dr. R. B. Patel," Ad hoc Network Routing Protocols", http://esjournals.org/journaloftechnology/archive/vol1no6/vol1no6_3.pdf

[6] Vijay Kumar," Analytical Evaluation of Protocols AODV and DSR", JMAcademy of IT & Management (JMIJIT**)**, January 2011.