Comparative Study of Reactive Routing Protocols for MANETs

Sk. Munwar
Department of IT
Sree Vidyanikethan Engineering College
Tirupati-517 102, India

Dr. V.V.Rama Prasad
Department of IT
Sree Vidyanikethan Engineering College
Tirupati-517 102, India

***Abstract*—The mobile ad-hoc network (MANET) is an autonomous system of mobile routers connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. The infrastructureless and the dynamic nature of these networks demands new set of networking strategies to be implemented in order to provide efficient end-to-end communications in many different scenarios such as battlefield and disaster recovery. MANETs employs the traditional TCP/IP structure between the nodes to provide end-to-end communication. However, due to their mobility and limited resources in wireless networks, the TCP/IP model requires redefinition or modifications in each layer to function efficiently in MANETs. One interesting research area in MANET is routing. This has led to development of many different routing protocols for MANETs and each author of each proposed protocol argues that the strategy proposed provides an improvement over a number of different strategies consider in the literature for a given network scenarios. Therefore, it is quite different to determine which protocols may perform best under a number of different network scenarios, such as increasing node density and traffic. In this paper, we provide an overview of a wide range of reactive routing protocols proposed in the literature. We also provide a performance comparison of all reactive routing protocols and suggest which protocols may perform best in large networks.**

***Keywords*: Mobile ad-hoc networks, reactive routing protocols review.**

I. INTRODUCTION

Wireless mobile networks may be classified into two general categories:

Infrastructure-based Networks: Wireless networks often extended wired networks, and are referred to as infrastructure networks. It uses a hierarchy of wide area and local area wired networks as the backbone network. The wired backbone connects to special switching nodes called *base stations*. They are responsible for coordinating access to one or more transmission channel(s) for mobiles located within their coverage area. The end user nodes communicate via the base station using their respective wireless interfaces. Examples are Wireless LANs and WANs.

Mobile Ad hoc Networks (MANETs): A MANET is composed of a group of mobile wireless nodes that form a network independently of any centralized administration, while forwarding packets to each other in a multi-hop manner. Since the mobile devices are battery-powered, extending the network lifetime has become an important objective.

Existing protocols may be classified into two distinct categories. One category of protocols is based on minimum-power routing algorithms, which focus on minimizing the power requirements over end-to-end paths. A typical protocol in this category selects a routing path from a source to some destination so as to minimize the total energy consumption for transmitting a fixed number of packets over that path. Each link cost is set to the energy required for transmitting one packet of data across that link and Dijkstra's shortest path algorithm is used to find the path with the minimum total energy consumption. A key disadvantage of these protocols is that they repeatedly select the least-power cost routes between source-destination pairs. As a result, nodes along these least-power cost routes tend to "die" soon by rapidly exhausting their battery energy. This is doubly harmful since the nodes that die early are precisely the ones that are most needed to maintain the network connectivity (and hence increase the useful service life of the network.)

A second category of protocols is based on routing algorithms that attempt to increase the *network lifetime* by attempting to distribute the forwarding load over multiple different paths. This distribution is performed by either intelligently reducing the set of nodes needed to perform the forwarding duties, thereby, allowing a subset of nodes to sleep over different periods of time, or by using heuristics that consider the residual battery power at different nodes and route around nodes that have a low level of remaining battery energy. In this way, they balance the traffic load inside the MANET so as to increase the battery lifetime of the nodes and the overall useful life of an ad hoc network. These protocols indeed constitute the state of the art in power-aware network routing protocols. A number of different reactive routing protocols have been proposed to increase the performance of reactive routing. This section describes a

number of these strategies and makes a performance comparison between them. Table 1 provides the summary of the characteristic feature of each strategy and Table 2 provides a theoretical performance evaluation. Table 3 provides multicast reactive protocols comparison. Note that the performance metrics represent the worst case scenario for each routing protocol.

In this paper, we review and compare the performance of various reactive protocols. the rest of this paper is organized as follows: section II presents general classification of MANET routing protocols, section III basic reactive routing protocols, section IV Link stability based reactive protocols, section V Routing protocols using Locating Information, section VI Core-node based protocols, section VII luster-based protocols, section VIII Multicast reactive protocols. Section IX follows summary.

II.MANET ROUTING PROTOCOLS

Routing protocols in ad hoc networks may be classified into three groups (Fig. 1): *reactive* (on-demand), *proactive* (table-driven), and *hybrid*.

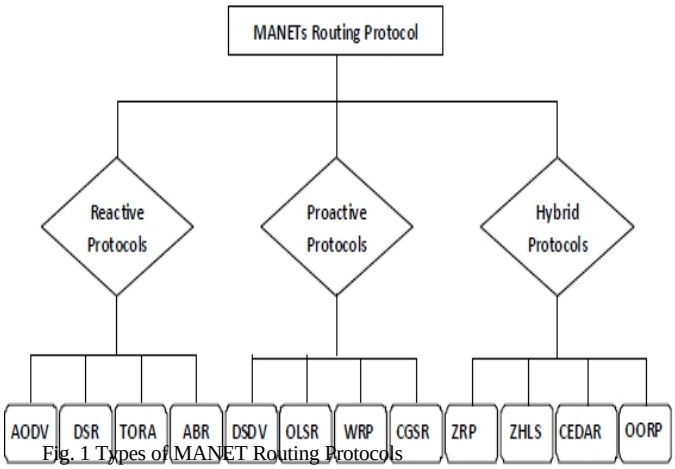

Fig. 1 Types of MANET Routing Protocols

Proactive (Table-Driven) Routing Protocols

These routing protocols are similar to and come as a natural extension of those for the wired networks. In proactive routing, each node has one or more tables that contain the latest information of the routes to any node in the network. Each row has the next hop for reaching to a node/subnet and the cost of this route. Various table-driven protocols differ in the way the information about change in topology is propagated through all nodes in the network.

The two kinds of table updating in proactive protocols are the periodic update and the triggered update [1]. In periodic update, each node periodically broadcasts its table in the network. In triggered update, as soon as a node detects a change in its neighborhood, it broadcasts entries in its routing table that have changed as a result. Examples of this class of adhoc routing protocols are the Destination- Sequenced Distance-Vector (DSDV) [2] and the Wireless Routing Protocol (WRP) [3]. Proactive routing tends to waste bandwidth and power in the network because of the need to broadcast the routing tables/updates. Furthermore, as the number of nodes in the MANET increases, the size of the table will increase; this can become a problem in and of itself.

Reactive (On-Demand) Protocols

Reactive routing protocols take a lazy approach to routing. They do not maintain or constantly update their route tables with the latest route topology. Instead, when a source node wants to transmit a message, it floods a query into the network to discover the route to the destination. This discovery packet is called the *Route Request (RREQ)* packet and the mechanism is called Route Discovery. The destination replies with a *Route Reply (RREP)* packet. As a result, the source dynamically finds the route to the destination. The discovered route is maintained until the destination node becomes inaccessible or until the route is no longer desired.

The protocols in this class differ in handling cache routes and in the way route discoveries and route replies are handled. Reactive protocols are generally considered efficient when the route discovery is employed rather infrequently in comparison to the data transfer. Although the network topology changes dynamically, the network traffic caused by the route discovery step is low compared to the total communication bandwidth. Examples of Reactive routing protocols are the *Dynamic Source Routing (DSR)* [1][4], the ad hoc on-demand Distance Vector Routing (AODV) [5] and the Temporally-Ordered Routing Algorithm (TORA)[6].

Hybrid Routing Protocols

Both the proactive and reactive protocols work well for networks with a small number of nodes. As the number of nodes increases, hybrid reactive/proactive protocols are used to achieve higher performance. Hybrid protocols attempt to assimilate the advantages of purely proactive and reactive protocols. The key idea is to use a reactive routing procedure at the global network level while employing a proactive routing procedure in a node's local neighborhood.

Zone Routing Protocol (ZRP), Zone-based hierarchical link state protocol (ZHLS)[1] is an example of the hybrid routing protocols.

III. REACTIVE (On-Demand) PROTOCOLS

On-demand routing protocols were designed to reduce the overheads in proactive protocols by maintaining information for active routes only. This means that routes are determined and maintained for nodes that require sending data to a particular destination. Route discovery usually occurs by flooding a route request packets

through the network. When a node with a route to the destination (or the destination itself) is reached a route reply is sent back to the source node using link reversal if the route request has travelled through bi- directional links or by piggy-backing the route in a route reply packet via flooding. Therefore, the route discovery overhead (in the worst case scenario) will grow by O(N+M) Here N=number of nodes in network, M=number of nodes in reply path. When link reversal is possible and O(2N) for unidirectional links.

Reactive protocols can be classified into two categories: source routing and hop-by-hop routing. In Source routed on-demand protocols [7, 8], each data packets carry the complete source to destination address. Therefore, each intermediate node forwards these packets according to the information kept in the header of each packet. This means that the intermediate nodes do not need to maintain up-to-date routing information for each active route in order to forward the packet towards the destination. Furthermore, nodes do not need to maintain neighbor connectivity through periodic beaconing messages. The major drawback with source routing proto-cols is that in large networks they do not perform well. This is due to two main reasons; firstly as the number of intermediate nodes in each route grows, then so does the probability of route failure. Secondly, as the number of intermediate nodes in each route grows, then the amount of overhead carried in each header of each data packet will grow as well. Therefore, in large networks with significant levels of multi-hoping and high levels of mobility, these protocols may not scale well. In hop- by-hop routing (also known as point-to-point routing) [9], each data packet only carries the destination address and the next hop address. Therefore, each intermediate node in the path to the destination uses its routing table to forward each data packet towards the destination. The advantage of this strategy is that routes are adaptable to the dynamically changing environment of MANETs, since each node can update its routing table when they receiver fresher topology information and hence forward the data packets over fresher and better routes. Using fresher routes also means that fewer route recalculations are required during data transmission. The disadvantage of this strategy is that each intermediate node must store and maintain routing information for each active route and each node may require being aware of their surrounding neighbors through the use of beaconing messages.

A. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) [10] is an Ad Hoc routing protocol which is based on the theory of source based routing rather than table-based. This protocol is source- initiated rather than hop-by-hop. This is particularly designed for use in multi hop wireless ad hoc networks of mobile nodes. Basically, DSR protocol does not need any existing network infrastructure or administration and this allows the Network to be completely self-organizing and self- configuring. This Protocol is composed of two essential parts of route discovery and route maintenance. Every node maintains a cache to store recently discovered paths. When a node desires to send a packet to some node, it first checks its entry in the cache. If it is there, then it uses that path to transmit the packet and also attach its source address on the packet. If it is not there in the cache or the entry in cache is expired (because of long time idle), the sender broadcasts a route request packet to all of its neighbors asking for a path to the destination. The sender will be waiting till the route is discovered. During waiting time, the sender can perform other tasks such as sending/forwarding other packets. As the route request packet arrives to any of the nodes, they check from their neighbor or from their caches whether the destination asked is known or unknown. If route information is known, they send back a route reply packet to the destination otherwise they broadcast the same route request packet. When the route is discovered, the required packets will be transmitted by the sender on the discovered route.

Also an entry in the cache will be inserted for the future use. The node will also maintain the age information of the entry so as to know whether the cache is fresh or not. When a data packet is received by any intermediate node, it first checks whether the packet is meant for itself or not. If it is meant for itself (i.e. the intermediate node is the destination) the packet is received otherwise the same will be forwarded using the path attached on the data packet. Since in Ad hoc network, any link might fail anytime. Therefore, route maintenance process will constantly monitors and will also notify the nodes if there is any failure in the path. Consequently, the nodes will change the entries of their route cache.

BENEFITS OF DSR:

Route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

LIMITATIONS OF DSR:

1. Scalability, since the source need to add the IDs of all nodes along the path to the destination which increase the overhead in every data packet sent.
2. When a link is broken RouteError packets need to go all the way to the source to inform it about the problem.
3. Intermediate node can use outdated routes stored in their cache.
4. As mobility increases more links are broken hence more route reconstructions is needed.

B. Ad hoc On-demand Distance Vector (AODV)

AODV [11][5] routing algorithm is a reactive

routing protocol designed for ad hoc mobile networks. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the REQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the REQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ

which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its outing information for that destination and begin using the better route. When a link is broken due to movement of nodes or any other reason, the node that discover the failure link will send RouteError to the Source. When the source gets the RouteError Packet it will delete the path from the cache and will find another route in its cache, if it didn't find any route it will run RouteRequest again.

BENEFITS OF AODV:

1. In AODV routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is lower.

LIMITATIONS OF AODV:

1. In AODV the 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.
2. Multiple RouteReply packets in response to a single RouteRequest packet can lead to heavy control overhead.
3. Periodic beaconing leads to unnecessary bandwidth consumption.

C. Temporally Ordered Routing Algorithm (TORA)

TORA[6] is a distributed highly adaptive routing protocol designed to operate in a dynamic multihop network. TORA uses an arbitrary height parameter to determine the direction of link between any two nodes for a given destination. Consequently, multiple routes often exist for a given destination but none of them are necessarily the shortest route. To initiate a route, the node broadcasts a QUERY packet to its neighbors. This QUERY is rebroadcasted through the network until it reaches the destination or an intermediate node that has a route to the destination. The recipient of the QUERY packet then broadcasts the UPDATE packet which lists its height with respect to the destination. Then this packet propagates in the network, each node that receives the UPDATE packet sets its height to a value greater than the height of the neighbor from which the UPDATE was received. This has the effect of creating a series of directed links from the original sender of the QUERY packet to the node that initially generated the UPDATE packet. When it was discovered by a node that the route to a destination is no longer valid, it will adjust its height so that it will be a local maximum with respect to its neighbors and then transmits an UPDATE packet. If the node has no neighbors of finite height with respect to the destination, then the node will attempt to discover a new route as described above. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad hoc network.

BENEFITS OF TORA:

One of the benefits of TORA is that the multiple routes between any source destination pair are supported by this protocol. Therefore, failure or removal of any of the nodes is quickly resolved without source intervention by switching to an alternate route.

LIMITATIONS OF TORA:

The drawback of TORA is that it depends on synchronized clocks among nodes in the ad hoc network. The dependence of this protocol on intermediate lower layers for certain functionality presumes that the link status sensing, neighbor discovery, in order packet delivery and address resolution are all readily available. The solution is to run the Internet MANET Encapsulation Protocol at the layer immediately below TORA. This will make the overhead for this protocol difficult to separate from that imposed by the lower layer.

D. Light-weight Mobile Routing (LMR)

The LMR [12] protocol is based on the concept of link reversal algorithm. LMR addresses the issue of partitioned network by providing a link erasure mechanism. LMR requires two passes to re-establish and converge to an alternate route, if one exists. LMR can erase invalid routes and detect partition in a single pass. It is designed to reduce the control message propagation in highly dynamic mobile networking environment. Due to this shortest hop paths are given only secondary importance and this protocol fits under the stability criteria. The benefit of this protocol is that routes will be found rather quickly and broken links will have only

local affect. It has good performance if the network connectivity is high, i.e., in the case of dense network. Routes may be redundant. A higher level protocol could use redundant routes in a round-robin fashion to economically use local bandwidth. The limitation of this protocol is that in a rapidly changing network there may be many false RPY (reply) packets producing message overhead.

E. Routing On-demand Acyclic Multi-path (ROAM)

The ROAM [13] routing protocol uses intermodal coordination along directed acyclic sub-graphs, which is derived from the routers₃ distance to destination. This operation is referred to as a "di using computation". The advantage of this protocol is that it eliminates the search-to-infinity problem present in some of the on-demand routing protocols by stopping multiple flood searches when the required destination is no longer reach-able. Another advantage is that each router maintains entries (in a route table) for destinations, which flow data packets through them (i.e. the router is a node which completes/or connects a router to the destination). This reduces significant amount of storage space and bandwidth needed to maintain an up-to-date routing table. Another novelty of ROAM is that each time the distance of a router to a destination changes by more than a defined threshold, it broadcasts update messages to its neighboring nodes, as described earlier. Although this has the benefit of increasing the network connectivity, in highly dynamic networks it may prevent nodes entering sleep mode to con-serve power.

F. Relative Distance Micro-discovery Ad hoc Routing (RDMAR)

RDMAR [14] attempts to minimize the routing overheads by calculating the distance between the source and the destination and therefore limiting each route request packet to certain number of hops (as described earlier). This means that the route discovery procedure can be confined to localized region. RDMAR also uses the same technique when link failures occurs (i.e. route maintenance). Thus conserving a significant amount of bandwidth and battery power. Another advantage of RDMR is that it does not require a location aided technology (such as a GPS) to determine the routing patterns. However, the relative-distance micro-discovery procedure can only be applied if the source and the destinations have communicated previously. If no previous communication record is available for a particular source and destination, then the protocol will behave in the same manner as the flooding algorithms.

G. Ant-Colony-based Routing Algorithm (ARA)

ARA [15] attempt to reduce routing overheads by adopting the food searching behavior of ants. When ants search for food they start from their nest and walk towards the food, while leaving behind a transient trail called pheromone. This indicated the path that has been taken by the ant and allows others to follow, until the pheromone disappears. Similar to AODV and DSR, ARA is also made up of two phases (route discovery and route maintenance). During route discovery a Forwarding ANT (FANT) is propagated through the network (similar to a RREQ). At each hop, each node calculates a pheromone value depending on how many number of hops the FANT has taken to reach them. The nodes then forward the FANT to their neighbors. Once the destination is reached, it creates a Backward ANT (BANT), and returns it to the source. When the source receives the BANT from the destination node, a path is determined and data packet dissemination begins. To maintain each route, each time a data packet travels between intermediate nodes the pheromone value is increased. Otherwise the pheromone value is decreased overtime until it expires. To repair a broken link, the nodes firstly check their routing table, if no route is found they inform their neighbors for an alternate route. If the neighbors do have a route they inform their neighbors by backtracking. If the source node is reached and no route is found, a new route discovery process is initiated. The advantage of this strategy is that the size of each FANT and BANT is small, which means the amount of overhead per control packet introduced in the network is minimized. However, the route discovery process it based on flooding, which means that the protocol may have scalability problems as the number of nodes and flows in the network grows

H. Flow Oriented Routing Protocol (FORP)

FORP [16] Attempt to reduce the effect of link failure due to mobility during data transmission by predicting when a route is going to be broken and therefore using an alternate link before route failure is experienced. To do this, when a node requires a route to a particular destination and a route is not already available, a Flow_REQ message is broadcasted through the network in a similar manner to a Route Request in DSR. How-ever, in FORP, each node that receives a Flow_ REQ calculates a Link Expiration Time (LET) with the previous hop (using a GPS) and appends this value to the Flow_REQ packet which is then rebroadcasted. When a Flow_REQ packet reaches the destination, a Route Expiration Time (RET) is calculated using the minimum of all the LETs for each node in the route and a Flow_SETUP packet is sent back toward the source. During data transmission, each intermediate node appends their LET to the data packet. This allows the destination to predict when a link failure could occur. When the destination determines that a route is about to expire, a Flow_HANDOFF message is generated and propagated via flooding (similar to a Flow_REQ). Therefore, when the source receives a Flow_HANDOFF message, it can determine the best route to handle the flow based on the given information (such as RET and hop count, etc) in

the Flow_HANDOFF packet. The source the sends a Flow_SETUP message along the newly chosen route. The advantage of this strategy com-pared to other on-demand routing protocols de-scribed so far is that it minimizes the disruptions of real time sessions due to mobility by attempting to maintain constant flow of data. However, since it is based on pure flooding, the protocol may experience scalability problems in large networks.

Table 1: Basic characteristics of reactive routing protocols

Protocol	RS	Multiple routes	Beacons	Route metric method	Route maintained in
AODV	F	No	Yes	Freshest & SP	RT
DSR	F	Yes	No	SP, or next available in RC	RC
ROAM	F	Yes	No	SP	RT
LMR	F	Yes	No	SP, or next available	RT
TORA	F	Yes	No	SP, or next available	RT
ABR	F	No	Yes	Strongest associativity & SP	RT
SSA	F	No	Yes	Strongest signal strength & stability	RT
RDMAR	F	No	No	Shortest relative distance or SP	RT
LAR	F	Yes	No	SP	RC
ARA	F	Yes	No	SP	RT
FORP	F	No	No	RET & stability	RT
CBRP	H	No	No	First available route	RT at cluster head

RS= routing structure, H=hierarchical, F=flat, RT=route table, RC=route cache, RET=route expiration time, SP= shortest path.

I. Dynamic MANET On-Demand (DYMO)

DYMO is a reactive routing protocol and its working is similar to AODV but in more enhanced way.DYMO has implemented the concept of path accumulation, removes gratuitous RREP and determines routes in a unicast way among DYMO nodes. In addition, the Internet connectivity is also defined in the DYMO Internet-Draft [17]. Each node maintains a routing table with information about nodes. Each entry in the routing table consists of a destination address, next hop address, hop count, sequence number, valid timeout, delete timeout and gateway flag. Valid timeout indicates the time at which route entry is no longer, the role of sequence number is same as in AODV, delete timeout shows time after which the entry will be deleted and gateway field shows if the destination node is internet gateway or not.

The DYMO protocol consists of two operation route discovery and route maintenance. In route discovery process, a source node broadcast a RREQ message in network. During this propagation process, each intermediate node records a route to the source node. Upon sending the RREQ, the originating node waits for a RREP message from the destination. In case no RREP is received within valid time the node may yet again strive to determine a route by issuing another RREQ. On getting RREP message source node starts sending message. Secondly, route maintenance is the process of responding to changes in topology due to node disassociation that happens after a route has been initially created. In such case a Route Error (RRER) message is sent to source node indicating the route is no longer valid. On receiving the RRER, source node re-initiate route discovery if still has packets to send.

IV. LINK STABILITY BASED ROUTING PROTOCOLS

A. Associativity Based Routing (ABR)

In associativity-based routing ABR[18], protocol uses a different metrics than shortest path. It also uses the same mechanism as DSR which is aggregating the node IDs along the path to the final destination. The objective is to select a longer lived route which will help in reducing the cost of reconstructing routes. The metric used instead of the shortest hop count is the Location Stability or the Associativity between nodes. Moving nodes tend to break the associativity with their neighbors and hence they are not good candidates to carry routes. Nodes periodically broadcast beacons to signify their existence with their neighbors. Location Stability is determined by counting the periodic beacons that a node receives from its neighbors. Links between nodes are classified into Stable and Unstable links based on the count of beacons. Source Node broadcast RouteRequest packets. Each neighbor will check if it received this request before or if its ID is in the list. If yes it will drop the packet. If not it will append its ID and the status of the link weather it is stable or not to the packet and rebroadcast the packet again.

BENEFITS OF ABR:

1. Stable routes have a higher preference compared to shorter routes.
2. Fewer paths will break which reduces flooding.
3. A broken link is repaired locally, so the source node won't start a new path-finding-process when a broken link appears.

LIMITATIONS OF ABR:

1. Sometimes the chosen path may be longer than the shortest path, because of the preference given to stable paths.
2. Stability information is only used during the route selection process.
3. Local query broadcasts may result in high delays during the route repair.

B. Signal Stability Adaptive (SSA)

The SSA [19] routing protocol is a derivative of the ABR routing protocol. It selects routes based on the signal strength between nodes. Signal strength of the link with a neighboring node is determined using the periodic beacons received from that node. If the signal strength is beyond a threshold, the link is considered stable; otherwise, the link is designated to be weak. Preference is given to paths on the stronger stable channels, SSA fits under the stability category. Route discovery in SSA is through source-initiated broadcast request messages. A node forwards the request message to the next hop only if it is received over a stronger channel and has not been previously processed. The destination chooses the first arriving route-search packet and sends back a route-reply in the reverse direction of the selected route. In addition to choosing the path of strongest signal stability, it is most likely that first arriving route-search packet traversed over the shortest and/or the least congested path. If no route-reply message is received within a specific timeout period, the source initiates another route-search and also indicates its acceptability of weak channels in the search packet header.

The main advantage of SSA is that this protocol finds more stable routes to a destination the shortest path aren't necessary the best. With the beacons between the nodes, SSA classifies the link as stable or unstable to find the strongest path. The limitation of SSA is that there is more bandwidth consumption because it sends RouteRequest many times. Also the selected path may not be the shortest as the shortest path may have unstable link.

V. ROUTING PROTOCOLS USING LOCATION INFORMATION

A. Location Aided Routing (LAR)

LAR [20] is based on flooding algorithms (such as DSR). However, LAR attempts to reduce the routing overheads present in the traditional flooding algorithm by using location information. This protocol assumes that each node knows its location through a GPS. Two different LAR scheme were proposed in **[21],** the first scheme calculates a re-quest zone which defines a boundary where the route request packets can travel to reach the required destination. The second method stores the coordinates of the destination in the route request packets. These packets can only travel in the direction was the relative distance to the destination becomes smaller as they travel from one hop to another. Both methods limit the control over-head transmitted through the network and hence conserve bandwidth. They will also determine the shortest path (in most cases) to the destination, since the route request packets travel away from the source and towards the destination. The disadvantage of this protocol is that each node is required to carry a GPS. Another disadvantage is (especially for the first method), that protocols may behave similar to flooding protocols (e.g. DSR and AODV) in highly mobile networks.

VI. CORE – NODE BASED ROUTING PROTOCOLS

A. The Core-Extraction Distributed Ad Hoc Routing (CEDAR)

The Core-Extraction Distributed Ad Hoc Routing (CEDAR) [21] is a non-uniform routing protocol. In CEDAR, a subset of nodes in the network is identified as the "core". Core is determined according to a distributed algorithm and the number of core nodes is kept to be small. To select core odes, neighboring nodes periodically exchange link state messages. Every mobile node in the network must adjust to at least one core node and picks this core node as its dominator. The algorithm guarantees that there is a core node nearby using localized broadcasts. The link state information is propagated far only among core nodes. The propagation distance of a link state through the network is a function of its stability and bandwidth. Only the state of stable links with high band width is propagate far away and the link state information includes dominators of link endpoints. Hence, in CEDAR, a core node not only knows the state of local links but also the state of stable and high band width links far away. When source node wants to send packets to its destination, it informs its dominator core node. Then the dominator of the source finds a route in the core network to the dominator of the destination. This is done by means of a DSR- like route discovery process among core nodes. Then, core nodes involved in the previous step build a route from the source to the destination. Locally available link state information is used according to the QOS requirement such like band width. It is not necessary for the route to include core nodes.

VII. CLUSTER- BASED ROUTING PROTOCOLS

A. Cluster Based Routing Protocol (CBRP)

Unlike the on-demand routing protocols de-scribed so far. In CBRP [22] the nodes are organized in a hierarchy. As most hierarchical protocols described in the previous section, the nodes in CBRP or grouped into clusters. Each cluster has a cluster-head, which coordinates the data transmission within the cluster and to other clusters. The advantage of CBRP is that only cluster heads exchange routing information, therefore the number of control overhead trans-mitted through the network is far less than the traditional flooding methods. However, as in any other hierarchical routing protocol, there are overheads associated with cluster formation and maintenance. The protocol also suffers from temporary routing loops. This is because some nodes may carry inconsistent topology information due to long propagation delay.

Table 2: complexity comparison of reactive routing protocols.

Protocol	TC[RD]	TC[RM]	CC[RD]	CC[RM]

AODV	O(2D)	O(2D)	O(2N)	O(2N)
DSR	O(2D)	O(2D)	O(2N)	O(2N)
ROAM	O(D)	O(A)	O(|E|)	$O(6G_A)$
LMR	O(2D)	O(2D)	O(2N)	O(2A)
TORA	O(2D)	O(2D)	O(2N)	O(2A)
ABR	O(D+P)	O(B+P)	O(N+R)	O(A+R)
SSA	O(D+P)	O(B+P)	O(N+R)	O(A+R)
RDMAR	O(2S)	O(2S)	O(2M)	O(2M)
LAR	O(2S)	O(2S)	O(2M)	O(2M)
ARA	O(D+P)	O(D+P)	O(N+R)	O(A+R)
FORP	O(D+P)	O(D+P)	O(N+R)	O(N+R)
CBRP	O(2D)	O(2B)	O(2X)	O(2A)

TC=time complexity, CC=communication complexity, RD= route discovery RM= route maintenance, D= diameter of the network N=number of nodes in the network, A=Number of affected nodes, B= diameter of the effected area, S=diameter of the nodes in localized region, M= Number of nodes in the localized region X= Number of clusters, R=Number of nodes forming the route reply path, RREP, BANT or Flow_SETUP. P= diameter of the directed path of the RREP, BANT or Flow_SETUP, |E|=number of edges in the network.

VIII. TYPICAL MULTICAST ROUTING ROTOCOLS

A. The On-Demand Multicast Routing Protocol (ODMRP)

The On-Demand Multicast Routing Protocol (ODMRP)[23] is a reactive mesh based multicast routing protocol. ODMRP uses a forwarding group concept for multicast packet transmission, in which each multicast group G is associated with a forwarding group FG. Nodes in FG are in charge of forwarding multicast packets of group G. In a multicast group of ODMRP, the source manages the group membership, establishes and updates the multicast routes on demand.

ODMRP comprises two main phases: the request phase and the reply phase. When the multicast source has a packet to send but it has no routing and group membership information, it floods a Join Request packet to the entire network. Join Request packets are member advertising packets with piggybacked data payload. When node receives a non duplicate Join Request, it stores the upstream node ID in its routing tale and rebroadcasts the packet. When the Join Request packet reaches a multicast receiver, the receiver refreshes or creates an entry for the source in Member Table and broadcasts JOIN TABLE packets periodically to its neighbors. When a node receives a JOIN TABLE packet, it checks each entry of the table to find out if there is an entry in the table whose next node ID field matches its ID. If there is match, the node recognizes that it is on the path to the source, thus it is part of the forwarding group. Then it sets the FG_FLAG and broadcasts its own JOIN TABLE built upon matched entries. Consequently, each member of a forwarding group propagates the JOIN TABLE packets until the multicast source is reached via the shortest path. This process constructs (or updates) the routes from sources to receivers and builds a mesh of nodes, the forwarding group.

Multicast senders refresh the membership information and update the routes by sending Join Request periodically. It uses a soft state approach for group maintenance. Member nodes are refreshed when needed and do not send explicit leave messages.

B. Multicast Ad Hoc On-Demand Distance Vector (MAODV) Routing Protocol

The MAODV [24] routing protocol discovers multicast routes on demand using a broadcast route-discovery mechanism. A mobile node originates an RREQ message when it wishes to join a multicast group, or when it has data to send to a multicast group but it does not have a route to that group. Only a member of the desired multicast group may respond to a join RREQ.

If the RREQ is not a Join Request, any node with a fresh enough route (based on a group sequence number) to the multicast group may respond. If an intermediate node receives a join RREQ for a multicast group of which it is not a member, or if it receives an RREQ and it does not have a route to that group, it rebroadcasts the RREQ to its neighbors.

As the RREQ is broadcast across the network, nodes set up pointers to establish the reverse route in their route tables. A node receiving an RREQ first updates its route table to record the sequence number and the next-hop information for the source node. This reverse route entry may later be used to relay a response back to the source. For join RREQs, an additional entry is added to the multicast route table. This entry is not activated unless the route is selected to be part of the multicast tree. If a node receives a join RREQ for a multicast group, it may reply if it is a member of the multicast group's tree and its recorded sequence number for the multicast group is at least as great as that contained in the RREQ. The responding node updates its route and multicast route tables by placing the requesting node's next-hop information in the tables, and then unicasts an RREP back to the source node. As nodes along the path to the source node receive the RREP, they add both a route table and a multicast route table entry for the node from which they received the RREP, thereby creating the forward path; see **Figure 2** for a non duplicate Join Request. It stores the upstream node ID (i.e., backward learning) and rebroadcasts the packet.

When the Join Request packet reaches a multicast receiver, the receiver creates or updates the source entry on its member. When a source node broadcasts an RREQ for a multicast group, it often receives more than one reply. The source node keeps the received route with the greatest sequence number and shortest hop count to the nearest member of the multicast tree for a specified period of time and disregards other routes. At the end of this period, it enables the selected next hop in its multicast route table, and unicasts an Activation Message (MACT) to this selected

next hop. The next hop, on receiving this message, enables the entry for the source node in its multicast route table. If this node is a member of the multicast tree, it does not propagate the message any further. However, if this node is not a member of the multicast tree, it will have received one or more RREPs from its neighbors. It keeps the best next hop for its route to the multicast group, unicasts a MACT to that next hop, and enables the corresponding entry in its multicast route table. This process continues until the node that originated the RREP (member of the tree) is reached. The activation message ensures that the multicast tree does not have multiple paths to any tree node. Nodes only forward data packets along activated routes in their multicast route tables.

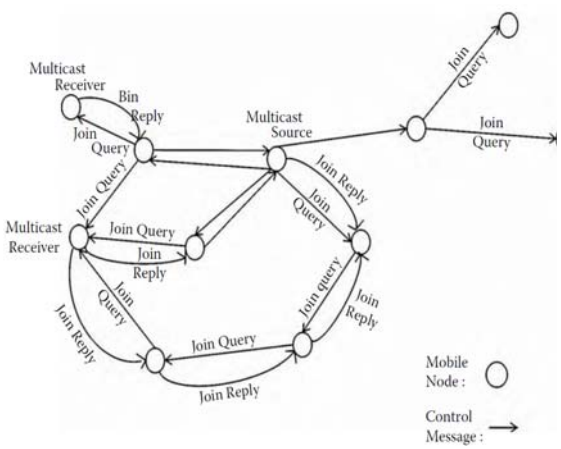

Figure 2: MAODV path discovery.

The first member of the multicast group becomes the leader for that group. The multicast group leader is responsible for maintaining the multicast group sequence number and broadcasting this number to the multicast group. This is done through a "Group Hello" message. The Group Hello contains extensions that indicate the multicast group's IP address and the sequence numbers (incremented with every Group Hello) of all multicast groups for which the node is the group leader. Nodes use the Group Hello information to update their request table.

Because AODV keeps hard state in its routing table, the protocol has to actively track and react to changes in this tree. If a member terminates its membership with the group, the multicast tree requires pruning. Links in the tree are monitored to detect link breakages. When a link breakage is detected, the node that is further from the multicast group leader (downstream of the break) is responsible for repairing the broken link. If the tree cannot be reconnected, a new leader for the disconnected downstream node is chosen as follows. If the node that initiated the route rebuilding is a multicast group member, it becomes the new multicast group leader. On the other hand, if it was not a group member and has only one next hop for the tree, it prunes itself from the tree by sending its next hop a prune message. This continues until a group member is reached.

Once separate partitions reconnect, a node eventually receives a Group Hello for the multicast group that contains group leader information that differs from the information it already has. If this node is a member of the multicast group, and if it is a member of the partition whose group leader has the lower IP address, it can initiate reconnection of the multicast tree.

MAODV uses a shared bidirectional multicast tree based on hard state, and any link breakages force actions to repair the tree. A multicast group leader maintains up-to-date multicast tree information by sending periodic Group Hello messages. Because MAODV unicasts the reply back to the source, if an intermediate node on the path moves away, the reply is lost and the route is lost. However, a broadcasted reply requires intermediate nodes not interested in the multicast group to drop the control packets, resulting in extra processing overhead. In MAODV, a potential multicast receiver must wait for a specified time, allowing for multiple replies to be received before sending an activation message along the multicast route that it selects.

IX. Conclusions

In this paper we tried to analyze the reactive unicast and multicast routing protocols. The on- demand routing protocols determine routes when they needed. Periodic updates are not required. However, some nodes may require periodic beacons. E.g. ABR. The routing structures of reactive protocols are mostly flat except CBRP. Control traffic volume is lower than global routing and further improved using GPS. E.g. LAR. To handle the effects of mobility ABR introduces LBQ. ROAM employs threshold updates. AODV uses local route discovery. A storage requirement of reactive protocols depends on the number of routes kept or required. Usually lower than proactive protocols, but the delay levels are higher than proactive protocols. Finally scalability level is upto few hundred nodes for source routing protocols. Also depends on the level of traffic and the levels of multihoping.

Protocol	Multicast delivery structure	Routing info acquirement / maintenance	Loop free	Dependency on unicast routing protocols	Control packet flooding	Periodic messages requirement	Routing hierarchy	scalability
ODMRP	Mesh	Proactive /Reactive	Yes	No	Yes	Yes	Flat	Fair
MAODV	Core based tree	Reactive	Yes	Yes	Yes	No	Flat	Fair

Table 3: Comparison of multicast protocols.

REFERENCES

[1] C. E. Perkins, "Ad Hoc Networking," Addison Wesley, 2001.

[2] C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing DSDV) for Mobile Computers," *Proc. of ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications*, pp. 234-244 Oct. 1994.

[3] Murthy and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," *ACM Mobile Networks and Applications Journal, Special issue on Routing in Mobile Communication Networks*, vol. 1, no. 2, pp. 183-197, 1996.

[4] D. B. Johnson, D. A. Maltz, Yih-Chun Hu and Jorje tag. Jetcheva, "The Dynamic Source Routing for Mobile AdHoc Wireless Networks," http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt, *IETF Internet draft*, Nov. 2001.

[5] C. E. Perkins, E. M. Belding-Royer, and S. Das, "Ad Hoc on demand Distance Vector (AODV) Routing," *IETFInternet draft*, draft-ietf-manet-aodv-12.txt, Nov.2002.

[6] V. Park and S. Corson, "Temporally Ordered RoutingAlgorithm (TORA) Version 1", Functional specification IETF Internet draft.1999

[7] D. Johnson, D. Maltz, J. Jetcheva, "The dynamic source routing protocol for mobile ad hoc networks, InternetDraft, draft-ietf-manet- dsr-07.txt", 2002.

[8] C. Toh, "A novel distributed routing protocol to support ad-hoc mobile computing", in: IEEE 15th Annual International Phoenix Conf., 1996, pp. 480-486.

[9] S. Das, C. Perkins, E. Royer, "Ad hoc on demand distance vector (AODV) routing", Internet Draft, draft-ietf-manetaodv-11.txt, work in progress, 2002.

[10] D. B. Johnson and D. A. Maltz, "Dynamic SourceRouting in AdHoc Networks", Mobile Computing, T.Imielinskiand H. Korth, Eds., Kulwer Publ., 1996,pp. 152-81.

[11] C. E. Perkins and E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA,1999, pp. 90-100.

[12] M.S. Corson and A. Ephremides "A Distributed Routing Algorithm for Mobile Wireless Networks".[13] J. Raju, J. Garcia-Luna-Aceves, "A new approach to on demand loop-free multipath routing", in: Proceedings of the 8th Annual IEEE International Conference on Computer Communications and Networks (ICCCN), Boston, MA, October 1999, pp. 522-527.

[13] J. Raju, J. Garcia-Luna-Aceves, "A new approach to on demand loop-free multipath routing", in: Proceedings of the 8th Annual IEEE International Conference on Computer Communications and Networks (ICCCN), Boston, MA, October 1999, pp. 522-527.

[14] G. Aggelou, R. Tafazolli, RDMAR: a bandwidth-efficient routing protocol for mobile ad hoc networks, in: ACM International Workshop on Wireless Mobile Multimedia (WoWMoM), 1999, pp. 26-33.

[15] M. Gunes, U. Sorges, I. Bouazizi, Ara "the ant-colony based routing algorithm for manets", in: ICPP workshopon Ad Hoc Networks (IWAHN 2002), August 2002, pp. 79-85.

[16] W. Su, M. Gerla, "Ipv6 flow handoff in ad-hoc wireless networks using mobility prediction", in: IEEE Global Communications Conference, Rio de Janeiro, Brazil, December 1999, pp. 271-275.

[17] Chakeres, I. Perkins, C. "Dynamic MANET On-Demand (DYMO) Routing", IETF Internet-Draft, draft-ietf-manetdymo- 17.txt. 2010

[18] M. Kummakasikit, S.Thipchaksurat " Performance Improvement of Associativity-Based Routing for Ad-Hoc Mobile Networks" presented in International conference of Information, Communications and Signal Processing, 2006.

[19]Rrohit dube, Cynthia D. Rais , Kuang-Yeh-Wang ,and Satish K. Tripathi "Signal stability-based adaptive routing for adhoc mobile network" at University of Maryland.1996

[20] Y.-B. Ko, N.H. Vaidya, "Location-aided routing (LAR) in mobile ad hoc networks", in: Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom_98) , Dallas, TX,1998.

[21] P. Sinha, R.Sivakumar and V. Bharghaven, " CEDAR: a Core-Extraction Distributed Ad hoc Routing algorithm" IEEE INFOCOM, March 1999.

[22] M. Jiang, J. Ji, Y.C. Tay, "Cluster based routing protocol", Internet Draft, draft-ietf-manet-cbrp-spec-01.txt, work in progress, 1999.

[23] S.J.Lee, M. Gerla, C.C. Chiang, "On Demand Multicast Routing protocol" Proceedings of IEEE WCNC‟99, New Orleans, pages 1298-1302, Sept 1999.

[24] E. Royer and C. Perkins, "Multicast Ad hoc On-Demand Distance Vector (MAODV) Routing," *IETF Internet Draft*,draft-ietf-manet-maodv-00.txt.2004

Authors Biography

Sk. Munwar received the B.Tech degree in Information Technology from JNT University; He is currently working as Assistant Professor in the Department of Information Technology at Sree Vidyanikethan Engineering College, Tirupati, India since 2004. His current research interests include Computer Networks, Wireless Networks and Information Security and Algorithms. He is a member of ISTE.

Dr. V. V. Rama Prasad received the M.Sc (Tech.) degree in Electronic Instrumentation from Sri Venkateswara University, Tirupati in 1986 and M.E degree in Information Systems from BITS, Pilani, India in 1991. During the period 1989-1992 he worked as Assistant Lecturer in BITS, Pilani. From 1992 to 1995, he worked as Lecturer in Computer Science and Engineering and as Associate Professor from 1995 to 1998 at RVR & JC College of Engineering, Guntur, India. Since 1998, he is working as Professor and Head of Information Technology department at Sree Vidyanikethan Engineering College, Tirupati, India. He was awarded the Ph.D. degree in Computer Science by J.N.T. University, Hyderabad, during 2007 for the thesis in *Fractal Image Compression*. He has also worked as a Research Assistant at Indian Institute of Science, Bangalore during the year 1986. He has published about 10 papers in national and international journals and presented several papers in National and International conferences. He has edited books, and refereed conferences. He is also a reviewer for 06 International Journals. His current areas of research interest include Computer Graphics, Image Processing, Computer Networks, Computer Architecture and Neural Networks. He is a member of IEEE, IACSIT, IAENG, ISTE and CSI.