ISSN:2231-0711
www.ijcset.net

Classification of Routing Protocol in Mobile Ad Hoc Networks: A Review

Vishal Pahal,* Amit Verma, Payal Gupta
Department of Computer Science & Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.
Pahal7@gmail.com

***Abstract*— Mobile Ad-Hoc Network (MANET) is a wireless network without infrastructure. Self configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. Routing protocols used in wired network cannot be used for mobile ad-hoc networks because of node mobility. Efficient routing protocols will make MANETs reliable .Routing is a core issue in networks for delivering data from one node to another in ad hoc network. This Paper deals with number of ways of categorization of protocol and also present some specified protocols according to that classification. The emphasis of this paper is not to present protocol in detail but present main feature of wide variety of different protocols and discuss their suitability.**

Keywords- **Routing protocols, Mobile Ad hoc network, routing schemes Classification of protocols, Comparison of protocols.**

1. INTRODUCTION

Ad-hoc networks are wireless networks where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Each node itself acts as a router for forwarding and receiving packets to/from other nodes. MANET [1], [2], [3], is an autonomous system which consist of many mobile hosts that are connected by multi-hop wireless links [4]. The original idea of MANET started out in the early1970s. Some examples of the possible uses of ad hoc networking include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for situational awareness on the battlefield and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. The use of wired networks routing protocols in a dynamic network is not good because they place a heavy computational burden on mobile computers and they present convergence characteristics that don't suit well enough the needs of dynamic networks[15]. For instance, due to the dynamic nature of environment in ad hoc networks any routing scheme must consider that the network topology can change at the time of packet is being routed [15], and that the quality of the wireless links between nodes is highly variable. In wireless link failure is more common then as compare to wired network. Therefore, routes in MANET must be calculated much more frequently or time to time in order to keep up the same performance as of wired networks. Routing schemes in MANET are classified in four major groups, namely, Proactive routing, Reactive routing, and Hybrid routing ,Flooding. Flooding is used in MANET [1],[2],[3], to propagate control messages. Flooding is a distributed process in which a node transmits a message to all its neighbours and these transmit the message consecutively to their neighbours and so on until the message has been disseminated to the entire network. Although flooding is the simplest way to establish communication in MANET, it is not a efficient method and it generates big overhead on the network due to a big redundancy, wastage of bandwidth and increase in collisions in the network In proactive routing protocols maintain routes to all destinations, regardless of whether or not these routes are needed, valid routes are maintained to every node all the time. Updates are propagated throughout the network when a change in the network topology occurs. Proactive routing is only appropriate for small networks because as networks grow in size the overhead increases. Therefore, proactive routing protocols may waste bandwidth since control messages are sent out unnecessarily when there is no data traffic. In reactive routing the route evaluation is done only when it is necessary. When a node needs to find a route to destination for sending message, then it must begin a discovery process to find one that is appropriate. Paths are maintained only until they are needed. Hybrid routing use hierarchical approach [8], in which the network is organized into subsets of nodes, known as clusters and it also use best feature of both reactive and proactive protocol. This topology organization reduces network traffic because a node only needs to have knowledge of the routing information within its cluster and not of the entire network. Hybrid routing, also known as cluster-based routing is a convenient scheme for developing efficient routing algorithms in MANET. Apart from making a large network appear smaller, one significant attribute of cluster-based routing is that it can make a dynamic topology appear less dynamic. In order to implement a dynamic hybrid routing scheme, efficient clustering algorithms must be designed.

2. PROACTIVE (TABLE DRIVEN ROUTING) PROTOCOLS

In proactive or table-driven routing protocols, each node continuously maintains up-to-date routes to every other node in the network. Update is periodically and

also starts if there is some change in network topology. Routing information is periodically transmitted throughout the network in order to maintain routing table consistency. Thus, if a route has already existed before traffic arrives, transmission occurs without delay. Otherwise, traffic packets should wait in queue until the node receives routing information corresponding to its destination. The main disadvantage of a heavy control overhead during high mobility. So for highly dynamic network topology, the proactive schemes require a significant amount of resources to keep routing information up-to-date and reliable. Other proactive routing protocols are Destination- Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), Global State Routing (GSR) and Cluster head Gateway Switch Routing (CGSR).

3. ON-DEMAND ROUTING PROTOCOLS (REACTIVE)

In contrast to proactive approach, Protocols that fall under this category do not maintain the network topology information. They obtain the necessary path when it is required, by using a connection establishment process. in reactive or on demand protocols, a node initiates a route discovery throughout the network, only when it wants to send packets to its destination. For this purpose, a node initiates a route discovery process through the network. Hence these protocols do not exchange routing information periodically. This process is completed once a route is determined or all possible permutations have been examined. Once a route has been established, it is maintained by a route maintenance process until either the destination becomes inaccessible along every path from the source or until the route is no longer desired. In reactive schemes, nodes maintain the routes to active destinations. A route search is needed for every unknown destination. Therefore, theoretically the communication overhead is reduced at expense of delay due to route research. Some reactive protocols are Cluster Based Routing Protocol (CBRP), Ad hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA), Associatively-Based Routing (ABR), Signal Stability Routing (SSR) and Location Aided Routing (LAR).

4. HYBRID ROUTING PROTOCOLS [8]

Protocols belonging to this category combine the best features of the above two categories. Nodes within a certain distance from the node concerned, or within a particular geographical region, are said to be within the routing zone of the given node. For routing within this zone, a table-driven approach is used. For nodes that are located beyond this zone,an on-demand approach is used.Hybrid Routing, commonly referred to as balanced-hybrid routing, is a combination of distance-vector routing, which works by sharing its knowledge of the entire network with its neighbors and link-state routing which works by having the routers tell every router on the network about its closest neighbors. Hybrid Routing is a third classification of routing algorithm. Hybrid routing protocols use distance-vectors for more accurate metrics to determine the best paths to destination networks, and report routing information only when there is a change in the topology of the network. Hybrid routing allows for rapid convergence but requires less processing power and memory as compared to link-state routing. An example of a hybrid routing protocol is the Enhanced Interior Gateway Routing Protocol (EIGRP), developed by Cisco, ZRP protocol etc.

5. EXISTING ROUTING PROTOCOLS [15]

A communications protocol is a formal description of digital message formats and the rules for exchanging those messages in or between computing systems and in telecommunications. Protocols may include signaling, authentication and error detection and correction capabilities. A protocol describes the syntax, semantics, and synchronization of communication and may be implemented in hardware or software, or both. The protocols can be arranged on functionality in groups, for instance there is a group of transport protocols. The nature of the communication, the actual data exchanged and any state-dependent behaviors are defined by the specification. This approach is often taken for protocols in use by telecommunications. There are a lot of popularly used routing protocols. Some of them are explained below: -

5.1 AODV: Adhoc On–Demand Distance Vector

AODV [9],[12], is a distance vector routing algorithm which discovers route whenever it is needed via a route discovery process. It adopts a routing algorithm based on one entry per destination i.e., it records the address of the node which forwards the route request message. AODV possesses a significant feature that once the algorithm computes and establishes the route between source and destination, it does not require any overhead information with the data packets during routing. Moreover the route discovery process is initiated only when there is a free/available route to the destination. Route maintenance is also carried out to remove stale/unused routes. The algorithm has the ability to provide services to unicast, multicast and broadcast communication. AODV routing algorithm has two phases i.e. Route Discovery and Route Maintenance [9],[12]. The AODV routing protocol is a reactive routing protocol; therefore, routes are determined only when needed.

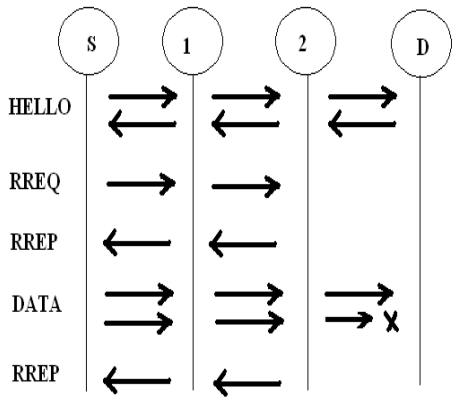

Fig. 1.1 AODV messages

fig. 1.1 shows various messages exchanges in the AODV protocol. The lists of these messages are:-

- HELLO
- RREQ
- RREP
- DATA
- RERR

Hello messages may be used to detect and monitor links to neighbors. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop by hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen. AODV uses the following fields with each route table entry:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Other state and routing flags (e.g., valid, invalid)
- Network Interface
- Hop Count (number of hops needed to destination)
- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

As data owns from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table. If data owns and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop by hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary [9].

5.2 DSR: Dynamic Source Routing

The major difference between this and other on demand routing protocol is that it is beacon-less and hence does not required any periodic Hello packet(beacon) transmissions, which are used by a node to inform its neighbors of its presence. The Dynamic Source Routing protocol (DSR) [4],[12], is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network [7]. Each node in the network maintains a route cache in which it caches the routes it has learned. To send data to another node, if a route is found in its route cache, the sender puts this route (a list of all intermediate nodes) in the packet header and transmits it to the next hop in the path. Each intermediate node examines the header and retransmits it to the node indicated after its id in the packet route. If no route is found, the sender buffers the packet and obtains a route using the route discovery process described below.

Route Discovery and Maintenance

To find a route to its destination, a source broadcasts a route request packet to all nodes within its radio transmission range. In addition to the addresses of the source and the destination nodes, a route request packet contains a route record, which is an accumulated record of nodes visited by the route request packet. When a node receives a route request, it does the following. If the destination address of the request matches its own address, then it is the destination. The route record in the packet contains the route by which the request reached this node from the source. This route is sent back to the source in a route reply packet by following the same route in reverse order. (It assumes bidirectional links. The alternative reply mechanism for unidirectional links is not considered here.) Otherwise, it is an intermediate node. If the node has not seen this request before and has a route to the destination in its cache table, it creates a route reply packet with the route from its cache, and sends it back to the source. Such replies are called Intermediate-Node replies; if it does not have a route; it appends its own address to the route record, an increment hop count by one, and rebroadcasts the request. When the source receives a route reply, it adds this route to its cache and sends any pending data packets. If any link on a source route is broken (detected by the MAC layer of the transmitting node) a route error packet is generated. The route error is unicasted back to the source using the part of the route traversed so far, erasing all entries that contain the broken link in the route caches along the way.

Optimization

By virtue of source routing, nodes have access to a large amount of routing information. For instance, the route indicated in a route request/reply or data packet can be used to learn routes to every other node on the route. DSR makes use of route caching aggressively. For example, a destination replies to every route request that it receives, and the source keeps the excess replies as alternate routes to the destination. Several optimizations to this basic protocol have been proposed and have been evaluated to be very effective by the authors of the protocol. Some of them are:

Gratuitous Replies

When a node overhears a packet addressed to another node, it checks to see if the packet could be routed via itself to gain a shorter route. If so, the node sends a

gratuitous reply to the source of the route with this new, better route.

Route Snooping

A node that overhears a data packet and does not have the packet route in its own cache, adds the new route to its cache for future use.

Data Salvaging

If an intermediate node encounters a broken link and has an alternate route to the destination in its cache, it can try to salvage the packet by sending it via the route from its cache.

Advantages and Disadvantages [17]:

It is reactive protocol, it eliminate need of periodically flooding the network, hence reduce the control overhead problem.The disadvantage is this protocol is that the route maintenance mechanism does not locally repair a broken link.

Security and Performance Issues

Certain features of DSR hurt its performance or make it vulnerable to security attacks. These are followings:-

No Expiration of Routes

Without an effective mechanism to remove excessively old (stale) entries, route caches may contain broken or non-minimum hop routes. Using stale routes causes loss of data packets (low delivery rate) and wastes network bandwidth. Route replies from intermediate nodes and snooping data packets exacerbate this problem by polluting caches with stale routes.

Intermediate-Node (IN) Replies

Intermediate-node replies make the route learning process faster because all route requests do not need to travel all the way to the destination. Without route freshness indication, however, it results in polluting caches with stale routes when node mobility is high and data transmissions are infrequent. When a source receives the bad route reply, it tries to send the waiting data packet along the route. Upon failure of one of the links along the route, a route error packet is propagated back to the source, which then issues a new route request, starting the process all over again.

5.3 ZRP: Zone Routing Protocols

In an ad-hoc network, it can be assumed that the largest art of the traffic is directed to nearby nodes. Therefore, ZRP reduces the proactive scope to a zone centered on each node. In a limited zone, the maintenance of routing Information is easier [18]. Zone Routing Protocol (ZRP) [5],[6], is a hybrid protocol which combines the advantages of both proactive and reactive schemes. It's taking advantage of pro-active discovery within a node's local neighborhood, and using a reactive protocol for communication between these neighborhoods. The Intrazone Routing Protocol must provide the possibility of direct neighbor discovery. This protocol is responsible for determining the routes to the peripheral nodes and is commonly a proactive protocol the Intrazone Routing Protocol or IARP. Communication between the different zones is guarded by the Interzone Routing Protocol, or IERP, and provides routing capabilities among peripheral nodes only. The Bordercast Resolution Protocol, or BRP, is used in the ZRP to direct the route requests initiated by the global reactive IERP to the peripheral nodes, thus removing redundant queries and maximizing efficiency [6]. The detailed description is given below: - It was designed to mitigate the problems of those two schemes. Proactive routing protocol uses excess bandwidth to maintain routing information, while reactive protocols suffers from long route request delays and inefficiently flooding the entire network for route determination. ZRP addresses these problems by combining the best properties of both approaches. Each node in ZRP, proactively maintains routes to destinations within a local neighborhood, which is referred as a routing zone.

However, size of a routing zone depends on a parameter known as zone radius. Fig. 1.2 (a) illustrates an example of routing zone (for node N1) of radius 2 hops. Nodes N1 through N11 are members of node N1's routing zone, whereas node N12 lies outside. Here, N8 through N11 are border nodes, whereas nodes N2 through N7 are interior nodes.

Component

The Zone Routing Protocol consists of several components, Fig. 1.2 (b) which only together provide the full routing

benefit to ZRP. Even though the hybrid nature of the ZRP seems to indicate that it is a hierarchical protocol, it is important to point out that the ZRP is in fact a flat protocol. ZRP is more efficiency for large networks.

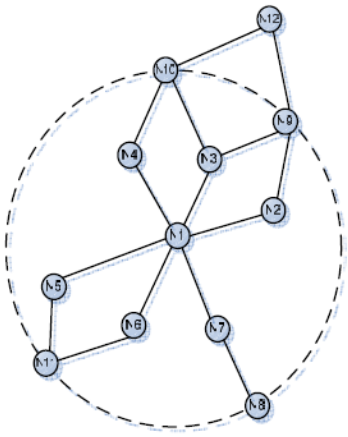

Fig.1.2 (a) Routing Zone of radius 2

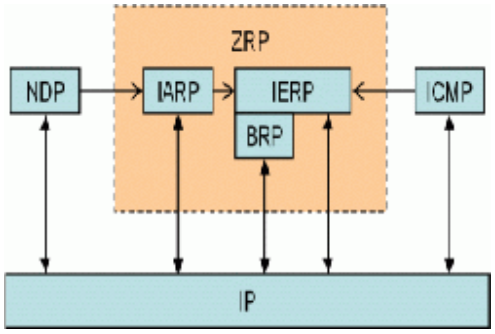

Fig 1.2 (b) Component of ZRP

5.4 Intrazone Routing Protocol (IARP)

In ZRP [5],[6], each node maintains the routing information of all nodes within its routing zone. Nodes learn the topology of its routing zone through a localized proactive scheme, referred as an Intrazone Routing Protocol (IARP). No protocol is defined to serve as an IARP and can include any proactive routing protocol, such as distance vector or link state routing. Different zone may operate with different proactive routing protocols as long as the protocols are restricted within the zone. A change in topology only affects the nodes inside the zone, even though the network is quite large.

5.5 Interzone Routing Protocol (IERP)

The Interzone Routing Protocol (IERP) is responsible for reactively discovering routes to the destination beyond a node's routing zone. This is used if the destination is not found within the routing zone. Fig.1.3

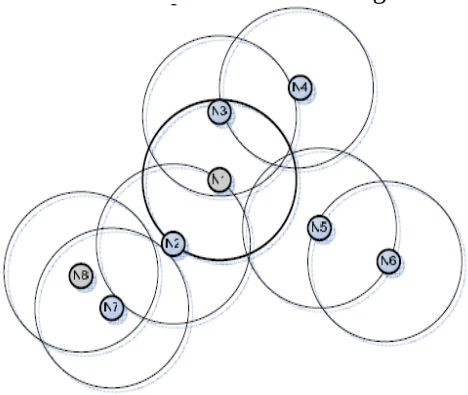

Fig. 1.3 An example of IERP operation

Bordercast Resolution Protocol (BRP)

The Bordercast Resolution Protocol, or BRP, is used in the ZRP to direct the route requests initiated by the global reactive IERP to the peripheral nodes, thus removing redundant queries and maximizing efficiency. Unlike IARP and IERP, it is not so much a routing protocol, as it is packet delivery service.

Advantage

Less control overhead as in a proactive protocol or an on demand protocol.

Disadvantage

Short latency for finding new routes.

5.6 OLSR: Optimized Link State Routing

The Optimized Link State Routing Protocol (OLSR)[20] is a proactive routing protocol. Every node sends periodically broadcast "Hello"-messages with information to specific nodes in the network to exchange neighbourhood information. The information includes the nodes IP, sequence number and a list of the distance information of the nodes neighbours. After receiving this information a node builds itself a routing table. Now the node can calculate with the shortest path algorithm the route to every node he wants to communicate. When a node receives an information packet with the same sequence number twice he is going to discard it. Developed for mobile ad hoc networks, the Optimized Link State Routing (OLSR) [13],[14],[20] is a table driven and proactive routing protocol. This type of algorithm maintains locally fresh information about the state of the network and periodically distributes this knowledge amid the other nodes participating in the routing environment. At the same time that proactive protocols are able to know a route before they need to use it, the constant exchange of messages to achieve this provokes bandwidth wastage [14]. The Optimized Link State Routing protocol inherits the stability of the pure link state algorithm and is an optimization over the classical link state protocol, adopted for mobile ad hoc networks. It is proactive in nature and has the advantage of having routes immediately available when needed. The key concept used in this protocol is that of multipoint relays (MPRs). MPRs are selected set of nodes in its neighbor, which forward broadcast messages during the flooding process. OLSR reduces the size of control packet by declaring only a subset of links with its neighbors who are its multipoint relay selectors and only the multipoint relays of a node retransmit its broadcast messages. Hence, the protocol does not generate extra control traffic in response to link failures and additions. The following section describes the functionality of OLSR in details.

Neighbors Sensing

For detecting the neighbor, each node periodically broadcasts its HELLO messages, which contains the information of the neighbors and their link status. The protocol only selects direct and bidirectional links, so that the problem of packet transfer over unidirectional links is avoided. HELLO messages are received by all one-hop neighbors, but they are not relayed further. These messages permit each node to learn the knowledge of its neighbors up to two hopes and help performing the selection of its multipoint relays.

Multipoint Relay Stations

Each node of the network selects its own set of multipoint relays from periodically broadcasted hello messages. The MPR set is selected by a node in a manner so that consists of a subset of one hop neighbors, which covers the entire two hop neighbors of the node. For example, in Fig. 1.4, node N2 selects nodes N1 and N6 to be the MPR nodes. Since these nodes cover all the nodes (N7, N8, N9 and N4), which are two hops away from it.

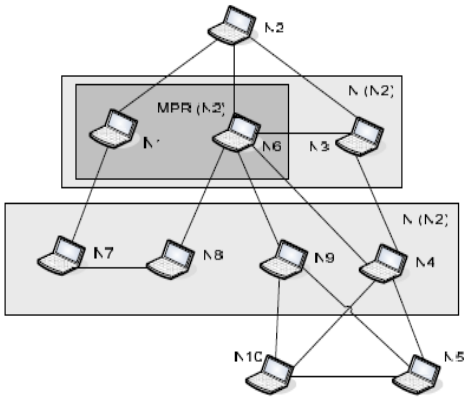

Fig. 1.4 An example of Multi Point Relay (MPR) selection

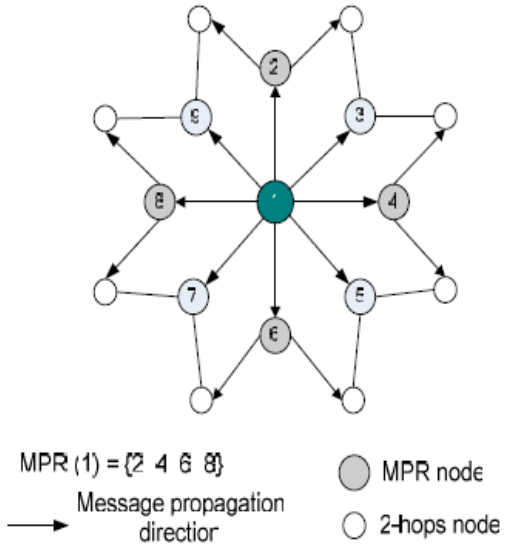

Fig. 1.5 An example of flooding using MPR nodes

Multipoint relays of a node are stated in its subsequent HELLO messages, so that the information reaches to the multipoint relays themselves. Multipoint relay set is recalculated when either a change in the neighborhood is detected or a change in the two hop neighbor set with bi-direction link is detected.

MPR Information Declarations

Each node in the network periodically broadcasts specific type of control messages called Topology Control (TC) message to build the intra-forwarding database needed for routing packets. Fig. 1.5 illustrates an example of flooding using MPR nodes throughout the network. A TC message is comprised of MPR selection set and with a sequence number, incremented when the MPR selector set changes. Information gained from TC messages is used to build the topology table in which it records the information about the topology of the network. A node records information about the multipoint Relays of other nodes in this table and then based on this information, the routing table is calculated.

Routing Table Calculation

Each node maintains a routing table which allows it to route the packets from source to destination. The routing table is calculated from the information it receives through TC messages. In these routing tables it stores the information of the route to each node in the network. The route entries in the routing table comprises of destination address, next-hop address and estimated distance to destination. The information is only updated when a change in the neighborhood is detected or a route to any destination is expired or a better route is detected for a destination [13].

Example Each node in the network, in our example node N2, Fig. 1.6 selected a few neighbour nodes in the network. These nodes will send node N2-packets. These selected nodes, N1 and N6 are called Multipoint Relays of node N2. Node N2 selects its MPR to cover all the nodes that are exactly two hops away from it. In our example: N7, N8, N9 and N4. A node which is not a Multipoint Relay can read the packet sent from N2 but cannot forward it.

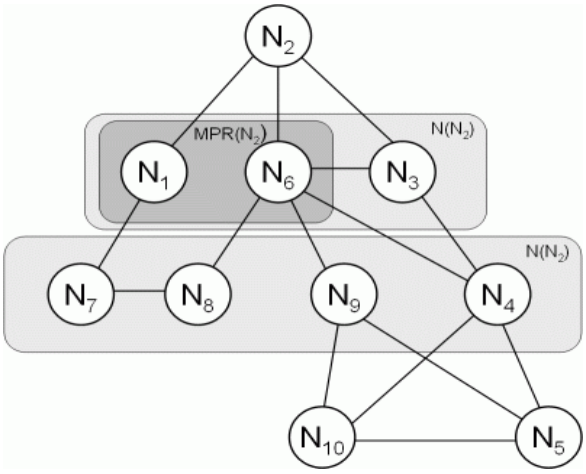

Fig 1.6 An example of OLSR

5.7 DSDV: Destination Sequenced Distance Vector Protocol

The destination sequenced distance vector routing protocol [11], is a proactive routing protocol which is a modification of conventional Bellman-Ford routing algorithm. This protocol adds a new attribute, sequence number, to each route table entry at each node. Routing table is maintained at each node and with this table; node transmits the packets to other nodes in the network. This protocol was motivated for the use of data exchange along changing and arbitrary paths of interconnection which may not be close to any base station. Each node in the network maintains routing table for the transmission of the packets and also for the connectivity to different stations in the network. These stations list for all the available destinations, and the number of hops required to reach each destination in the routing table. The routing entry is tagged with a sequence number which is originated by the destination station. In order to maintain the consistency, each station transmits and updates its routing table periodically. The packets being broadcasted between stations indicate which stations are accessible and how many hops are required to reach that particular station. The packets may be transmitted containing the layer 2 or layer 3 address Routing information is advertised by broadcasting or multicasting the packets which are transmitted periodically as when the nodes move within the network. The DSDV [11], protocol requires that each mobile station in the network must constantly; advertise to each of its neighbors, its own routing table. Since, the entries in the table my change very quickly, the advertisement should be made frequently to ensure that every node can locate its neighbors in the network. This agreement is placed, to ensure the shortest number of hops for a route to a destination; in this way the node can exchange its data even if there is no direct communication link. The data broadcast by each node will contain its new sequence number and the following information for each new route:

- The destination address.

- The number of hops required to reach the destination.
- The new sequence number, originally stamped by the destination.

The transmitted routing tables will also contain the hardware address, network address of the mobile host transmitting them. The routing tables will contain the sequence number created by the transmitter and hence the most new destination sequence number is preferred as the basis for making forwarding decisions. This new sequence number is also updated to all the hosts in the network which may decide on how to maintain the routing entry for that originating mobile host. After receiving the route information, receiving node increments the metric and transmits information by broadcasting. Incrementing metric is done before transmission because, incoming packet will have to travel one more hop to reach its destination. Time between broadcasting the routing information packets is the other important factor to be considered. When the new information is received by the mobile host it will be retransmitted soon effecting the most rapid possible dissemination of routing information among all the cooperating mobile hosts. The mobile host cause broken links as they move from place to place within the network. The broken link may be detected by the layer2 protocol, which may be described as infinity. When the route is broken in a network, then immediately that metric is assigned an infinity metric there by determining that there is no hop and the sequence number is updated. Sequence numbers originating from the mobile hosts are defined to be even number and the sequence numbers generated to indicate infinity metrics are odd numbers. The broadcasting of the information in the DSDV protocol is of two types namely: -

- Full dump
- Incremental dump.

Full dump broadcasting will carry all the routing information while the incremental dump will carry only information that has changed since last full dump. Irrespective of the two types, broadcasting is done in network protocol data units (NPDU). Full dump requires multiple NPDU's while incremental requires only one NPDU to fit in all the information. When an information packet is received from another node, it compares the sequence number with the available sequence number for that entry. If the sequence number is larger, then it will update the routing information with the new sequence number else if the information arrives with the same sequence number it looks for the metric entry and if the number of hops is less than the previous entry the new information is updated (if information is same or metric is more then it will discard the information). While the nodes information is being updated the metric is increased by 1 and the sequence number is also increased by 2. Similarly, if a new node enters the network, it will announce itself in the network and the nodes in the network update their routing information with a new entry for the new node. During broadcasting, the mobile hosts will transmit their routing tables periodically but due to the frequent movements by the hosts in the networks, this will lead to continuous burst of new routes transmissions upon every new sequence number from that destination. The solution for this is to delay the advertisement of such routes until it shows up a better metric.

Advantages of DSDV

- DSDV protocol guarantees loop free paths.
- Count to infinity problem is reduced in DSDV.
- It can avoid extra traffic with incremental updates instead of full dump updates.
- Path Selection: - DSDV maintains only the best path instead of maintaining multiple paths to every destination. With this, the amount of space in routing table is reduced.

Limitations of DSDV

- Wastage of bandwidth due to unnecessary advertising of routing information even if there is no change in the network topology.
- DSDV doesn't support Multi path Routing.
- It is difficult to determine a time delay for the advertisement of routes.
- It is difficult to maintain the routing table's advertisement for larger network.
- Each and every host in the network should maintain a routing table for advertising. But for larger network this would lead to overhead, which consumes more bandwidth.

5.8 TORA: Temporary Ordered Routing Algorithm

The TORA attempts to achieve a high degree of scalability using a "flat", non-hierarchical routing algorithm. In its operation the algorithm attempts to suppress, to the greatest extent possible, the generation of far-reaching control message propagation. In order to achieve this, the TORA does not use a shortest path solution, an approach which is unusual for routing algorithms of this type. The Temporally Ordered Routing Algorithm (TORA) [10],[12], is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal. TORA is proposed for highly dynamic mobile, multi-hop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. TORA [10],[12], can suffer from unbounded worst-case convergence time for very stressful scenarios. TORA has a unique feature of maintaining multiple routes to the destination so that topological changes do not require any reaction at all. The protocol reacts only when all routes to the destination are lost. In the event of network partitions the protocol is able to detect the partition and erase all invalid routes [12]. It is a fairly complicated protocol but what makes it unique and prominent is its main feature of propagation of control messages only around the point of failure when a link failure occurs. On the contrary, other protocols need to re-initiate a route discovery when a link fails. TORA would be able to patch itself up around the point of failure. This feature allows TORA to scale up to larger networks but has

higher overhead for smaller networks. Moreover, in its enhanced version, it stores the time value since a link failure. The protocol has basic functions following: -

- Route creation
- Route maintenance

In route creation, routes are created mostly in reactive mode. Initially, all nodes are disconnected. The protocol then forms a DAG (Directed Acyclic Graph). The criterion of adding node is based on a metric called "height". The node j is added with the node i, which is already member of the DAG if hi > hj. The metric "height" consists of five arguments all of which define the "height" of the node. The source sends QRY packet indicating the destination node. The QRY packet propagates until it reaches a node whose neighbor is the specified destination which then transmits a UPD (update) packet. All is done locally. i.e. the nodes know only their neighbors and not all members of the network. In route maintenance, route is maintained only for nodes with non-null height. On link failure, if a node is not connected to any node with height smaller than its own, all of its links are reversed based on link reversal algorithm. This is how routes are adapted according to topological changes. This feature adds extra overhead even if that path is not required for data transmission. For this reason, TORA is also considered member of Table-Driven MANET protocols family. Route is erased on the reception of CLR packet from a source in route erasure phase. A node, on receiving CLR packet, sets its own height and heights of all its neighbors to NULL and broadcasts CLR packet. This way, route erasure is performed. Finally Fig.7 highlights the steps of route creation, maintenance and erasure in flowchart form. TORA create routes when required. In TORA, nodes can be aware of other nodes adopts local policy rule that's why TORA thus minimizing overhead during route creation. The performance of protocols is degraded with the increase in the number of nodes [12].

5.9 WRP: Wireless Routing Protocol

The Wireless Routing Protocol (WRP) [19] is a proactive unicast routing protocol for mobile adhoc networks (MANETs). WRP uses an enhanced version of the distance-vector routing protocol, which uses the Bellman-Ford algorithm to calculate paths. WRP belong to the class of path finding algorithms. The typical feature for these algorithms is that they utilize information about distance and second-to-last hop (predecessor) along the path to each destination. Path-finding algorithms eliminate the counting-to-infinity problem of distributed Bellman- Ford-algorithms by using that predecessor information, which can be used to infer an implicit path to a destination and thus detect routing loops.Because of the mobile nature of the nodes within the MANET, the protocol introduces mechanisms which reduce route loops and ensure reliable message exchange. The wireless routing protocol (WRP), similar to DSDV, inherits the properties of the distributed Bellman-Ford algorithm. To counter the count-to-infinity problem and to enable faster convergence, it employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and the penultimate hop node on the path to every destination node. Since WRP, like DSDV, maintains an up-to-date view of the network, every node has a readily available route to every destination node in the network. It differs from DSDV in table maintenance and in the update procedures. While DSDV [11], maintains only one topology table, WRP uses a set of tables to maintain more accurate information. The tables that are maintained by a node are the following: -

- Distance table (DT)
- Routing table (RT)
- Link cost table (LCT)
- Message retransmission list (MRL).

The DT contains the network view of the neighbors of a node. It contains a matrix where each element contains the distance and the penultimate node reported by a neighbor for a particular destination. The RT contains the up-to-date view of the network for all known destinations. It keeps the shortest distance, the predecessor node (penultimate node), the successor node (the next node to reach the destination), and a flag indicating the status of the path. The path status may be a simple path (correct), or a loop (error), or the destination node not marked (null). The LCT contains the cost (e.g., the number of hops to reach the destination) of relaying messages through each link. The cost of a broken link is infinity. It also contains the number of update periods (intervals between two successive periodic updates) passed since the last successful update was received from that link. This is done to detect links breaks. The MRL contains an entry for every update message that is to be retransmitted and maintains a counter for each entry. This counter is decremented after every retransmission of an update message. Each update message contains a list of updates. A node also marks each node in the RT that has to acknowledge the update message it transmitted. Once the counter reaches zero, the entries in the update message for which no acknowledgments have been received are to be retransmitted and the update message is deleted. Thus, a node detects a link break by the number of update periods missed since the last successful transmission. After receiving an update message, a node not only updates the distance for transmission neighbors but also checks the other neighbors' distance, hence convergence is much faster than DSDV. Each node implementing WRP keeps a table of routes and distances and link costs. It also maintains a message retransmission list (MRL). Routing table entries contain distance to a destination node the previous and next nodes along the route, and is tagged to identify the route's state: whether it is a simple path, loop or invalid route. (Storing the previous and successive nodes assists in detecting loops and avoiding the counting-to-infinity problem - a shortcoming of Distance Vector Routing.)The link cost table maintains the cost of the link to its nearest neighbors (nodes within direct transmission range), and the number of timeouts since successfully receiving a message from the neighbor. Nodes periodically exchange routing tables with their neighbors via update messages, or whenever the link state table changes. The MRL maintains a list of which neighbors are yet to

acknowledge an update message, so they can be retransmitted if necessary. Where no change in the routing table, a node is required to transmit a 'hello' message to confirm its connectivity. When an update message is received, a node updates its distance table and reassesses the best route paths. It also carries out a consistency check with its neighbors, to help eliminate loops and speed up convergence.

5.10 EIGRP: Enhanced Interior Gateway Routing Protocol

Balanced hybrid routing protocols combine aspects of both distance vector and link-state protocols. The balanced hybrid routing protocol uses distance vectors with more accurate metrics to determine the best paths to destination networks. However, the balanced hybrid routing protocol differs from most distance vector protocols in that it uses topology changes instead of automatic periodic updates to trigger the routing of database updates. The balanced hybrid routing protocol converges more rapidly than distance vector routing protocols, which is similar to link-state routing protocols. However, the balanced hybrid differs from distance vector and link-state routing protocols. Enhanced Interior Gateway Routing Protocol (EIGRP) is an example of a balanced hybrid routing protocol. EIGRP has several advantages over Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP), and even some advantages over Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS). EIGRP's enhancements come with many complexities that take place behind the scenes. Although configuring EIGRP is relatively simple, the underlying protocol and algorithm are not so simple.

EIGRP Features

In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. Some of the features of EIGRP are as follows: -

EIGRP has rapid convergence times for changes in the network topology. In some situations, convergence can be almost instantaneous. EIGRP uses DUAL to achieve rapid convergence. A router that runs EIGRP stores backup routes for destinations when they are available so that it can quickly adapt to alternate routes. If no appropriate route or backup route exists in the local routing table, EIGRP queries its neighbors to discover an alternate route. These queries are propagated until an alternate route is found.

EIGRP has low usage of network resources during normal operation; only hello packets are transmitted on a stable network. Like other link-state routing protocols, EIGRP uses EIGRP hello packets to establish relationships with neighboring EIGRP routers. Each router builds a neighbor table from the hello packets that it receives from adjacent EIGRP routers. EIGRP does not send periodic routing updates like IGRP does. When a change occurs, routing table changes are only propagated, not the entire routing table. When changes are only propagated, the bandwidth required for EIGRP packets is minimized, which reduces the load that the routing protocol itself places on the network.

EIGRP supports automatic (classful) route summarization at major network boundaries as the default. However, unlike other classful routing protocols, such as IGRP and RIP, manual route summarization can be configured on arbitrary network boundaries to reduce the size of the routing table.

EIGRP Terminology

EIGRP relies on various tables for its computations. These are followings: -

Neighbor table: - Each EIGRP router maintains a neighbor table that lists adjacent routers. This table is comparable to the adjacencies database that OSPF uses, and it serves the same purpose (to ensure bidirectional communication between each of the directly connected neighbors). There is a neighbor table for each protocol that EIGRP supports.

Topology table

Each EIGRP router maintains a topology table for each configured routed protocol. This table includes route entries for all destinations that the router has learned.

Routing table

EIGRP chooses the best (successor) routes to a destination from the topology table and places these routes in the routing table. The router maintains one routing table for each network protocol.

Successor

A route selected as the primary route to reach a destination. Successors (up to four) are the entries kept in the routing table.

Feasible successor

Considered a backup route. Backup routes are selected when the successors are identified; however, these routes are kept in a topology table. Multiple feasible successors for a destination can be retained.

The EIGRP is protocol independent, which means that it does not rely on Transmission Control Protocol/Internet Protocol (TCP/IP) to exchange routing information the way that RIP, IGRP, and OSPF do. To stay independent of IP, EIGRP uses RTP as its own proprietary transport layer protocol to guarantee delivery of routing information. EIGRP can call on RTP to provide reliable or unreliable service as the situation warrants. With RTP, EIGRP can simultaneously multicast and unicast to different peers, this allows for maximum efficiency.

EIGRP Packet Types

Like OSPF, EIGRP relies on different packet types to maintain its tables and establish relationships with neighbor routers. EIGRP uses the following five types of packets: -

- Hello
- Acknowledgment
- Update
- Query
- Reply

EIGRP relies on hello packets to discover, verify, and rediscover neighbor routers. Rediscovery occurs if EIGRP routers do not receive hellos from each other for a hold time interval but then reestablish communication. Hello packets are always unreliably sent. This means that no acknowledgment is transmitted. EIGRP routers send hello packets at a fixed interval called the hello interval. The default hello interval depends on the

interface's bandwidth. On low-speed networks, hello packets are sent every 60 seconds; for all other networks, the hello interval is 5 seconds. The neighbor table includes the Sequence Number field to record the number of the last received EIGRP packet that each neighbor sent. The neighbor table also includes a Hold Time field, which records the time the last packet was received. Packets must be received within the hold time interval period to maintain a passive state, which is a reachable and operational status. If EIGRP does not receive a packet from a neighbor within the hold time, EIGRP considers that neighbor down. By default, the hold time is three times the hello interval, but an administrator can configure both timers as desired. OSPF requires neighbor routers to have the same hello and dead intervals to communicate. EIGRP has no such restriction. Neighbor routers learn about each of the other respective timers through the exchange of hello packets. They then use that information to forge a stable relationship regardless of unlike timers. EIGRP routers use acknowledgment packets to indicate receipt of any EIGRP packet during a reliable exchange. RTP provides reliable communication between EIGRP hosts. The recipient must acknowledge a message that is received to make it reliable. Acknowledgment packets, which are hello packets without data, are used for this purpose. Unlike multicast hello packets, acknowledgment packets are unicast. Acknowledgments can be attached to other kinds of EIGRP packets, such as reply packets. Update packets are used when a router discovers a new neighbor. EIGRP routers send unicast update packets to that new neighbor so that the neighbor can add to its topology table. More than one update packet can be needed to convey all the topology information to the newly discovered neighbor. Update packets are also used when a router detects a topology change. In this case, the EIGRP router sends a multicast update packet to all neighbors, which alerts them to the change. All update packets are reliably sent. An EIGRP router uses query packets whenever it needs specific information from one or all of its neighbors. A reply packet is used to respond to a query. If an EIGRP router loses its successor and cannot find a feasible successor for a route, DUAL places the route in the active state. A query is then multicast to all neighbors in an attempt to locate a successor to the destination network. Neighbors must send replies that either provide information on successors or indicate that no information is available. Queries can be multicast or unicast, while replies are always unicast. Both packet types are reliably sent.

5.11 STAR: Source Tree Adaptive Routing (STAR) protocol [17]

The Source Tree Adaptive Routing protocol was the first proactive routing protocol that works with link-state information and was faster then on-demand protocols. It was also the first proactive routing protocol where LORA [17] principle was implemented. STAR [17] doesn't take shortest paths for keeping control messages low. STAR identifies every node with a fix address. Big advantage is that no periodically updates are needed. After the start procedure a source tree contains links to every neighbor. Next step, means first update step, STAR sends his own source tree immediately as update to all other neighbors. So every router can built with his own source tree and the received ones, a topology graph containing the whole network. Those updates consist of one or more LSU (Link-State Update Unit). All update information is broadcast information. If an update has to be sent differs of ORA or LORA has been implemented. At ORA updates are only needed when the routers own source tree changes. In the STAR protocol LORA is implemented and updates are send out, when:--

- the receiver is unreachable
- a new receiver is detected
- when it seems that loops where built

the metric of link exceed the limit All of these cases are discovered by comparing the received with the own source tree.

5.12 ZHLS: Zone Based Hierarchical Link State Protocol [17]

The Zone-Based Hierarchical Link State Protocol[17] is based on the GPS (Global Positioning System). ZHLS is similar to the Zone Routing Protocol. It is a hybrid routing protocol acting similar like ZRP. The protocol is proactive when the destination node is in the same zone as the node which sent the request (Intrazone Clustering). On the other hand, the protocol is reactive when the destination node isn't within the zone from the source node (Interzone Clustering). But in ZHLS the network is divided in non overlapping zones. There are two types of Link State Packets (LSP) as well: node LSP and zone LSP. A node LSP of a node contains its neighbor node information and is propagated within the zone whereas a zone LSP contains the zone information and is propagated globally. Each node only knows the node connectivity within its zone and the zone connectivity of the whole network. So given the zone id and the node id of a destination, the packet is routed based on the zone id till it reaches the correct zone. Then in that zone, it is routed based on node id. A <zone id, node id> of the destination is sufficient for routing so it is adaptable to changing topologies.

Properties

ZHLS can be adjusted of its operation to the current network operational conditions (ie. change the routing zone radius). However this is not done dynamically, but instead the zone radius is set by the administrator of the network. The performance of this protocol depends greatly on this parameter ZHLS also limits the propagation of information about topological changes to the zone of the change (as opposed to flooding the entire network). This causes a reduction of overhead control traffic, however, at an expense of creating no optimal routes (routes between zones are not necessarily minimum cost paths). In the hierarchical approach, ZHLS mitigates traffic bottleneck and avoids single point failures by avoiding cluster heads. However, because of this, a node has to keep track of its physical location continuously in order to determine its affiliate zone. This requires some a complicated geo-location algorithm and device for each node.

Unlike other hierarchical protocol, there is no zone head. The zone size depend on node mobility, network density, transmission power and propagation characteristics. Each node only knows the connectivity within its zone and the zone connectivity of the whole network. The node knows its position and zone ID because of the Global positioning system. It can determine its zone ID by mapping its physical location to a zone map. This zone map has to be worked out at the design stage.

Advantage:

- No overlapping zones
- The zone-level topology information is distributed to all nodes reduces the traffic and avoids single point of failure

Disadvantage:

Additional traffic produced by the creation and maintaining of the zone-level topology

6. Comparison

The routing protocols can be generally categorized into two groups: Table-Driven and On-Demand. DSDV, WRP, CGSR, and ZHLS utilize Table-Driven routing. AODV, TORA, DSR, On-Demand routing.DSDV routing is essentially a modification of the basic Bellman-Ford routing algorithm. DSDV provides one path to any given destination and selects the shortest path based on the number of hops to the destination. However, DSDV is inefficient because of the requirement of periodic update transmissions, regardless of the number of changes in the network topology.

In CGSR, DSDV is used as the underlying routing protocol. Routing in CGSR occurs over cluster heads and gateways. One advantage of CGSR is that several heuristic methods can be employed to improve the protocol's performance. These methods include priority token scheduling, gateway code scheduling, and path reservation. However, CGSR is vulnerable to point failures and cluster head assignment is difficult to do.ZHLS is a very interesting proposal that divides the network into several zones. This approach is probably a very good solution for large networks as it reduces overhead control traffic by limiting topology updates within each zone. However, it produces no optimal (routes that are not shortest hop) for nodes between zones. In addition, there is overhead in maintaining the status of the zone a node is in. WRP protocol avoids the problem of creating temporary routing loops through the verification of predecessor information. This requires each node to maintain four routing tables, which can lead to substantial memory requirements, especially when number of nodes in the network is large. In addition, the use of HELLO packets whenever there are no recent packet transmissions from a given node consumes bandwidth. Of the reactive on-demand protocols, AODV and DSR are similar in that they have a route discovery mode that uses request messages to find new routes. The difference is that DSR is based on source routing and will learn more routes than AODV. DSR also has the advantage that it supports unidirectional links. DSR has the major drawback that the source route must be carried in each packet. The can be quite costly, especially with network size becomes very large. TORA uses a link-reversal algorithm to minimize reaction to topological changes. However, it suffers slow route convergence due to oscillations.

7. Conclusion

In this article we have discussed all the routing protocols [15], by studying the properties ,advantages and disadvantages of protocol used for route discovery and the root mantinance in wireless mobile adhoc network [7] a good understanding of tradeoffs in routing in ad hoc mobile networks is achieved .As it can be seen, there is vast number of different kinds of protocols. Only minority of the presented protocols will attain a technical or commercial success, one would forecast. Each of these protocols has some common goals. Every protocol has the ability of distributed routing calculations and every protocol try to manage the consequences caused by mobility of nodes. There are still many challenges facing wireless ad hoc networks. However because of there advantages, wireless ad hoc networks are becoming more and more prevalent in the world.

References

[1] A. Ephremides, J. E. Wieselthier and D. J. Baker, "A design concept for reliable mobile radio networks with frequency hopping signaling," Proc. IEEE, vol. 75, no. 1, Jan. 1987, pp. 56-73

[2] A. Bhatnagar and T. G. Robertazzi, "Layer Net: a new self-organizing network protocols," Proc. IEEE MILCOM '90, pp. 845-849.

[3] A. Alwan, R. Bagrodia, N. Bambos et al.,"Adaptive mobile multimedia networks," IEEE Personal Commun., Apr. 1996, pp. 34-51.

[4] D. B. Johnson, D. A. Maltz, J. Broch, "The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Proc. **Ad hoc networking,** Pub. Addison-Wesley Longman Publishing Co., Inc., (ISBN: 0-201-30976-9), pp. 139 - 172 (2010).

[5] J. Schaumann, "Analysis of the Zone Routing Protocol" pp. 1-21 (2002).

[6] N. Beijar, "Zone Routing Protocol (ZRP)" Networking Laboratory, Helsinki University of Technology, Finland, (2005).

[7] K. Gorantala, "Routing Protocols in Mobile Adhoc Networks", Master's Thesis in Computing Science, pp. 19-20 (2006).

[8] I. Chatzigiannakis and S. Nikoletseas, "Design and analysis of an efficient communication strategy for hierarchical and highly changing ad-hoc mobile networks," Mob. Netw. Appl., vol. 9, no. 4, pp. 319– 332, 2004.

[9] I. D. Chakeres, M. Belding-Royer "AODV Routing Protocol Implementation Design", Distributed Computing Systems Workshops, 2004 and proceedings 24th International Conference, (ISBN: 0-7695-2087-1), pp. 698 – 703 (2004).

[10] V. D. Park and M. S. Corson. Temporally-Ordered Routing Algorithm (TORA) version 1: Functional specification. Internet-Draft, draft-ietf-manet-tora-spec-00.txt, November 1997.

[11] C. E. Perkins and P. Bhagwat. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers.

[12] A. K. Gupta, H. Sadawarti, A. K. VermaI, "Performance analysis of AODV, DSR & TORA Routing Protocols", ACSIT International Journal of Engineering and Technology, (ISSN: 1793-8236), Vol.2, No.2, pp. 226-231 (2010).

[13] V. Pacheco and R. Puttini, "An Administration Structure for the OLSR Protocol**",** Proceedings of the 2007 International Conference on Computational science and Its Applications**,** (ISSN: 0302-9743), Vol. 4706, pp. 790 – 803 (2007).

[14] A. Huhtonen,"Comparing AODV and OLSR Routing Protocols", Seminar on Internetworking, pp. 1 - 9 (2004).

[15] E. M. Royer, Chai-Keong Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”, IEEE Personal Communications, (ISSN: 1070-9916), Vol. 6, Issue. 2, pp. 46-55 (1999).

[16] M. H. Mamoun, “Important Characteristic of Differences between DSR and AODV Routing Protocol”, MCN 2007 Conference, pp. 7-13 (2007).

[17] C.S.R Murthy and B.S. Manoj “ **Ad Hoc Wireless Networks** and protocosl “Architectures, Pub.Pearson Education, (ISBN: 81-297-0945-7,),pp.342(2005)

[18] Pearlman, Marc R., Haas, Zygmunt J.: Determining the Optimal Configuration for the Zone Routing Protocol, August 1999, IEEE Journal on Selected Areas in Communications, Vol. 17, No. 8.

[19] S. Murphy, J.J. Garcia-Luna-Aceves, “An EfficientRouting Protocol for Wireless Networks”, ACMMobile Networks and Applications Journal pp 183-197 Nov 1996. http://citeseer.nj.nec.com/10238. html

P. Jaquet, P. Muhlethaler and A. Qayyum, “Optimized Link State Routing Protocol”, IETF Draft, 2001. http://www.ietf.org/internetdrafts/ draft-ietf-manet-olsr-06.txt