# An Analysis of Geographical location based Routing Protocol

V.Vallinayagi [1], Dr.G.M Nasira[2]
[1]Sri Sarada college for women,
[2]Chikkanna Government Arts college ,
Tamil Nadu
vallinayagimahesh@gmail.com

**Abstract**
Mobile Adhoc Networks indicate wirelessnodes that are freely and dynamically self organize into arbitrary and temporary network topologies. In recent years a lot of attention has been drawn on geographic routing portal. But in geographic routing there is a lack of holistic design to be more efficient and robust. We present an overview of ad-hoc routing protocol which select it's forwarded based on geographical position of a packet destinations. In this topology each node knows his one hop neighborhood in order to forward the packets. Maintenance of routes is not necessary. It is a position based Opportunistic routing protocol in which several forwarding candidate cache the packet that has been received and if the best forwarder does not forward the packet in a particular time slots, then suboptimal candidate will take turn to forward the packet... It is highly dynamic. The main request is the sender can obtain the current position of the destinations. Recently discovered protocols are discussed. We provide a qualitative comparison of the approaches in areas and investigate opportunities for fully research.

**KEYWORDS:**

**Aodv, Opportunistic routing, A20p, por, lpor, aodv, dsr, mfr, recent implementation**

## 1: INTRODUCTION:

A mobile ad-hoc network is a self configuring infrastructure less network of mobile devices connected by wireless. Ad-hoc networks consist of nodes that arranged to transport information. Ad-hoc network can be subdivided into two classes static and mobile. In static position of the nodes does not change. In dynamic the position of nodes always change there are two types of approaches which is based on topology and position based. They are further divided into

a) Proactive b) Reactive c) Hybrid

The proactive algorithm followed by ancient routes strategies link [OLSR] [TORA], they maintain route information about the valid path. The drawback is unused path which occupy more space and affect infrastructure of the two holes.

In reactive routing protocols we develop a path in on demand basis. Position based routing algorithm eliminate some of the limititation in topology based roting. The routing decision on each node is there by based on the destination position containing packet and position of forwarding nodes with neighboours. It's no need to establish or maintain the details about route. We apply some type of methodology

i. Find out the communications requirements of public service in terms of survive traffic and quality of service
ii. Research on current technology relating adhoc networks.

Therefore we design criteria which satisfy the new generation network by selecting new approaches from the literature that should provide good results against the needs of public safely. Now days we always go for minimum space and minimum time so locating the information is becoming economically available through the global positioning system. Nowadays Satellite based mobile communication

is available. In this article we prepare a list of protocols for mobile adhoc network. We discuss about the main problem to be carried out in class of routing protocols and their solution. Rest of the paper tells you about position based addressing and routing and give critical for a taxonomy of various proposed protocols. This paper tells us about various techniques used in position based routing protocol. Comparisons of the location service and forwarding strategies are also discussed.

Naursh Tabhan Khan[1] proposes Adaptive position update strategy for geographic Routing which dynamically adjust the frequency of position updated based on mobility dynamics of the node and forwarding pattern in the network . Greedy perimeter state less Routing shows that APU can significantly reduce the update cost and improve the routing performance in terms of packet delivery ratio and average end to end delay. Live and Bharagava[2] Introduces secure position service system that is necessary for privacy preservation in positioning adhoc routing algorithm only limited position information is revealed to the network to protect node a nomenclature Analysis and Simulation occur to evaluate the routing performance for the proposed Algorithm. Finally compare AO2P and GPSR Hop count is also compared, end to end through put in AO2P and RAOP is not significant. An identity is maintained for source node destination node and the forwarding node destinations. Node mobility is done by matching node if with a position moment. Ao2P is a self Adaptor protocol as it impedes a new date source to join heavers – loaded network through causing route discovery failure and prevents the network. Congestion large error may cause in efficient routing (ie) routes built up. Therefore Ao2P pressures communication privacy without significant routing performance degradation GPSR need much more position informed. Luciana pleura Mac coconut[3] proposes case studies related to opportunistic networking and organize taxonomy for the main routing and forwarding approaches in this challenging environment. Dissemination based algorithm are essentially forms of controlled flooding and differentiate themselves for the policy used to limit flooding. They gave no idea about Rooty algorithms which affect some form of infrastructure and which do not. They gave on multiple fully opportunities network. Kaizeg, Zhenyyang [4] proposes a protocol opportunistic effective onehop through to perform the message and hope in advance. A local rate adaption and candidate selection algorithm was used in this they examine the factors that affect the performance using multirate capability. Candidate selection, prioritizalion and co – ordination performance of MGOR, and, GR was compared. They study on MultiMate candidate selection. Prioritization and coordination and examine the impacts on the performance of GOR. A rate adaption and candidate selection algorithm to approach the local optimum of this metric. A heauistic algorithm was proposed. They applied heuristic candidate selection algorithm which finds the transmission rate and corresponding forwarding candidates approaching maximum OEOT. Zhengyyge [5] propose a deployment strategy that determines the positions and the rejections of these reliable nodes. A rotation was formed for reliable plan which is made up of multiple segments. Here we use minout algorithm . Failures of nodes are detected from source to destination computation and use of more disjoint routes could provide safety to node failures. A particular network with reliable nodes is used. A reliable path is to capture. It can with stand with dynamic topology changes. They propose a min's cut algorithm. Reliable path is set from source to destination. An efficient position based protocol [6] is proposed when data packed is sent out a for warder was find out and forward the packet. In the case of link break several forwarders explicitly selected and broken route was removed. In the case of changing node mobility they gave a reliable data delivery in mobile adhoc network using POR. Another scheme was proposed to virtual Destination scheme on packet delivery. Sahaya Rose Vijila,, [7] Proposed link Based Routing Protocol (POR) which the link instability can be a major factor for unreliable date delivery and chooses a forwarder based on the reception power of a node. Trigger nodes trigger a hole handing mechanism when routing holes are so encountered. L-Por guarantee reliability through best for warder selection based on the Khaled Ahmed [8] propose on routing algorithm for mobile adhoc network using most forward with in Radius. An analytic model to evaluate the performance of MFR Routing algorithm for mobile ad-hoc network. They used the probality of successful message delivery as performance metrics. The probability of successful message delivery decreases.

In this paper chapter 1 introduction about the ad-hoc network. In chapter 2 discuss about

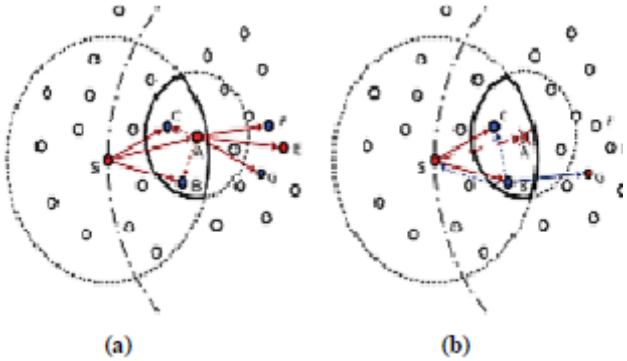
methods. Chapter3 discuss about POR. Chapter 4 discuss about MFR routing. In chapter 5 discuss about Opportunistic Routing/Forwarding Techniques. Chapter 6 Opportunistic Routing in MultiHop and MultiRate wireless networks. In chapter7 discuss about AOVDM routing. Chapter 8 ASDV and DSR are discussed. Chapter 9 discuss about the protocol AO2P. In 10th Chapter discuss about L-POR protocol.

## 2. METHODS:

In this paper we analyze the protocols used in mobile ad-hoc networks. In below each protocols are explained briefly.

### 2a] Position Based Opportunistic Petal routing:

POR design is based on geographic routing and opportunistic forwarding. The nodes are thought to be aware of their location and their direct neighbor's positions. Neighborhood location information is exchanged through a one-hop beacon or piggyback in the data packet header. Then the location registration and lookup service that maps node addresses to the locations is available for the destination position which can be realized through use of many types of location service. When a source node plans to transmit a packet, it first gets the destination location and after which it is attached with the packet header. As of the destination node's movement, a multi hop path may diverge from the final location's true location with a packet being dropped even if it has been delivered in the destination neighborhood. Additional destination node checks are introduced to handle such issues. The packet forwarding node checks the neighbor list at every hop to see whether destination is within its transmission range. If so, then the packet is directly forwarded to the destination, similar to destination location prediction scheme. Though such identification checks prior to greedy forwarding based on location information, path divergence effect can be alleviated.



(a) (b)

In Fig.1(a) In normal situation without link breakage, the packet is forwarded by the next hop node (e.g., nodes A, E) and the forwarding candidates (e.g., nodes B, C; nodes F, G) will be suppressed (i.e., the same packet in the Packet List will be dropped) by the next hop node's transmission. In case when node A fails to deliver the packet (e.g., node A has moved out and cannot receive the packet), then node B, the forwarding candidate with the highest priority, and will relay the packet and suppress the lower priority candidate's forwarding (e.g., node C) as well as node S.

### 2b] . MFR Routing:

Lifetime of a wireless link is defined as the amount of time (time interval) the link is available for transmission and its unit is seconds. We consider the lifetime of a wireless link between two nodes in the network as a continuous random variable. Further, we consider a route from a source node *S* to destination node *D* that contains a sequence of *m* wireless links for *m*-1 intermediate nodes. Let $X_{li}$ be the lifetime of the $i^{th}$ link in the route. We assume that the lifetimes are $X_{li}, i = 1,2..m-1$ exponentially, independently and identically distributed (iid) random variables, each with rate $\mu$ . When any link of the route breaks, then the route fails between the source *S* and destination *D*. Therefore the lifetime of this route *r* that consists of *m* links is a random variable expressed as follows:

$$X_r = \min(X_{l1}, X_{l2}, \ldots . X_{lm})$$

$$m \approx \frac{\ln(n)}{\ln(k)}$$

Where m is the distance between two nodes in terms of wireless links or hop counts, n is the number of the nodes in the network, and k is the

connectivity of the network (i.e. the average number of neighbors of a node in the network).

### 2c) Opportunistic Routing/Forwarding Techniques

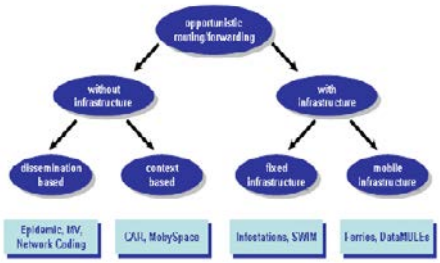



**Fig: 2 Opportunistic Routing/Forwarding Techniques**

3. ROUTINGWITHOUT INFRASTRUCTURE

### 1. Dissemination-based Routing

Some of the most distinguished features for these sub-division schemes are presented

- 1. Delivers a message to destination by diffusing it all over the network (flooding).
- 2. No knowledge of a possible path or appropriate to next-hop node.
- 3. Well performance in highly mobile networks with frequently contacts opportunities.
- 4. Tend to limit message delay.
- 5. Consume a lot of resources.
- 6. High contention and network congestion.
- 7. Increase the network capacity by limiting the number of hops of the spreading radius or by limiting the message copies present at the same time.
- 8. Network-coding-based-routing outperforms flooding as it is able to deliver the information with fewer messages in the network.

## 3 Context Based

Some of the most distinguished features for these sub-division schemes are presented:

- Exploits information about the context in which nodes are operating to identify next hops.
- More reduction of message's duplication compare to dissemination.
- Tend to increase message's delay in the delivery process.
- The computational cost is higher.
- Nodes need to maintain a state to keep track of the utility value.

### 4. Routing Schemes with Infrastructure

These are schemes that use some kind of infrastructure to deliver the message in an opportunistic form to its destination. A subdivision is made according to the type of infrastructure they rely on; in this case there are fixed infrastructure schemes and mobile infrastructure schemes. Special nodes of a fixed infrastructure are located at specific geographical points, whereas nodes of a mobile infrastructure move around in the network following either predetermined known paths or completely random paths, which will be collaborated in the forwarding of the message.

### 1. Fixed Infrastructure

Some of the most distinguished features for these sub-division schemes are presented:

- The message is sent only when a base station belonging to the sender node is reachable.
- Base stations are generally gateways towards less challenged networks.
- Two variations to the protocol are possible: one in which node-to-base-station communications is allowed. Another is in which node-to-base-station and node-to-node communication are allowed.
- Node-to-base-station communications experience high delay in delivery message.

ISBN: 978-960-474-393-3

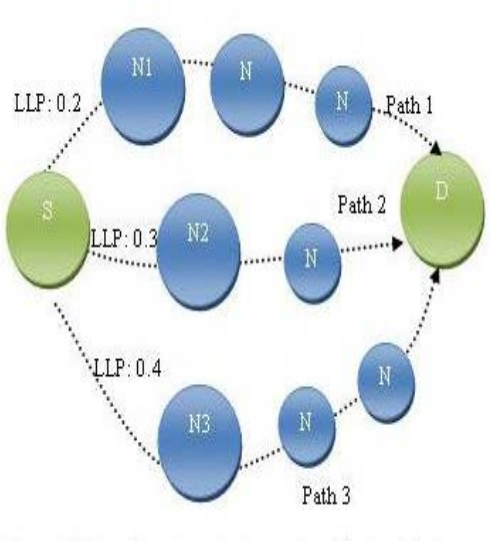
**2. Mobile Infrastructure**

Some of the most distinguished features for these sub-division schemes are presented

- Nodes of the infrastructure are mobile data collectors.
- The routes that the nodes follow can be predetermined or arbitrary.
- The nodes gather the messages from the nodes that pass by.
- In exclusive node-to-carrier communications, the special carrier-node is the only entities allow of delivering the messages.
- In exclusive node-to-carrier communications the carrier-node help to increase connectivity in sparse networks and also isolated node can be reached.
- In communications where is allow to nodes to communicate to carriers and ordinary nodes the delivery of the messages is accomplish by both.

**5. Opportunistic Routing in Multichip wireless networks**

Opportunistic routing is based on the broadcast transmissions of the data packets. This type of transmission is used in order to increase the probability that at least one potential relaying node receives the packet. Next figure illustrates the advantage of broadcast transmissions. The source (S) needs to send packets to the destination (D). It knows that its neighbors N1, N2 and N3 provide different paths to the destination (path1, path2 and path3). It has also estimated the loss probability in each link (LLP) to its neighbor. Specifically, the link to N1 has a loss probability of 0.2 while to N2 and to N3 the loss probability is 0.3 and 0.4 respectively.




Using traditional routing, the Source S should select one of these potential forwarders as the next hop. Then, it will end the packet to this neighbor by an uncast transmission. Taking into account the loss probability, the source will select N1 as the next hop and the probability that the packet is not retransmitted is 0.2. Alternatively, opportunistic routing will emit the packet in broadcast so the three neighbors (and some others too) will be able to receive it and to retransmit it. The probability that the packet will not be retransmitted is equivalent to the probability that no neighbors will receive the packet. This probability is 0.2•0.3•0.4, that is, 0.024. As we can see, the loss probability obtained with the opportunistic strategy is much lower than the resulting from the traditional routing. In order to better understand how opportunistic routing works, we will pay attention to the sequential phases that

Form part of an opportunistic routing protocol. These phases are:

• **Candidate Selection:** The protocol in the Layer-Three in the IP stack selects a set of nodes that allow the transmission of the packet from the source to the destination. This set of candidate relays is known as the forwarding candidates, the candidate forwarder set or the relay set. The nodes in the list may be ordered according to some criteria in the second phase. The source informs about its relay set including the IDs of the candidates belonging to the forwarding list in the packet header. In order to reduce the space required to store all the addresses of the relay set in the packet headers

• **Candidate Priority Assignment**: When the source informs about the forwarding candidates,

it orders them according to their convenience to act as relaying nodes. The appropriateness of a node is based on some metrics. For instance, the metrics could be derived at the MAC layer such as the loss probability. Nodes should periodically measure these parameters. The relay set plays an important role in opportunistic routing protocols. The candidate selection and its order are usually performed periodically so that the two first phases are not always executed in the emission of every data packet.

• **Data transmission**. The original opportunistic routing protocols are supported by the transmission of broadcast packets so that they can be received by multiple neighboring nodes. However, there are some opportunistic routing protocols where the data packets are uncast. In particular, the best forwarding node is specified in the next hop field of the packet. The other candidates receive the packet by eavesdropping.

• **Receiver coordination**: Among the forwarding candidates that receive the data packet, just one of them should be the relaying node for the current packet. The elected node will be also responsible for confirming the data reception at the MAC layer. The election is carried out by incorporating a distributed procedure in the nodes. The goal of the procedure is that the selected node should be the highest-priority relay that has successfully received the packet. In this sense, some proposals opt for modifying the MAC layer. For instance includes a list of four fields in the RTS (Ready to Send) messages. The list represents the forwarding set. The candidates reply with one CTS (Clear to Send) message sequentially. Then, the source decides about which node is going to act as the forwarding node and it sends the data to the elected node.

**MultiMate wireless Network**

In this section, we discuss the factors that affect the one-hop performance in terms of throughput and delay of OR. These factors include rate and forwarding strategy, which further includes candidate selection, prioritization and coordination.

## 6. One-hop Packet Forwarding Time of Opportunistic Routing

We define the one-hop packet forwarding time cost by the ith candidate as the period from the time when the sender is going to transmit the packet to the time when the ith candidate becomes the actual forwarder. Although the one-hop packet forwarding time varies for different MAC protocols, for any protocol, it can be divided into two parts. One part is introduced from the sender and the other part is introduced from the candidate coordination, which are defined as follows:

• Ts: the sender delay which can be further divided into three parts: channel contention delay (Tc), data transmission time (Td) and propagation delay (Tp):

$$Ts = Tc + Td + Tp$$

For a contention-based MAC protocol (like 802.11), Tc is the time needed for the sender to acquire the channel before it transmits the data packet, which includes the back-off time and Distributed Inter Frame Space (DIFS). Td is equal to protocol header transmission time (Th) plus data payload transmission time (Tpl), which is

$$Td = Th + Tpl$$

where $T_h$ is determined by physical layer preamble and MAC header transmitting time, and $T_{pl}$ is decided by the data payload length $L_{pl}$ and the data transmission rate. The payload may be transmitted at different rates. $T_p$ is the time for the signal propagating from the sender to the candidates, which can be ignored when electromagnetic wave is transmitted in the air.

• Tf (i): the ith forwarding candidate coordination delay which is the time needed for the ith candidate to acknowledge the sender and suppress other potential forwarders. Note that Tf (i) is an increasing function of i, since the lower-priority forwarding candidates always need to wait and confirm that no higher-priority candidates have relayed the packet before it takes its turn to relay the packet.

**Impact of Transmission Rate**

We examine the impact of transmission rate on the one-hop throughput of OR by using two examples. In one example, transmission at higher rate is better; while in the other example, lower rate achieves higher throughput. The one-hop throughput is defined as bit-meters successfully delivered per second with unit bumps. The one-hop delay per bit-meter is the inverse of the

ISBN: 978-960-474-393-3

throughput. So higher throughput implies lower delay in this context.

**Impact of Forwarding Strategy**

We have seen that multi-rate capability has an impact on throughput and delay. Other than this factor, for any given rate, different candidate prioritization also results in different throughput and delay in opportunistic routing. The one-hop throughput is 1.306G bmps, which is lower than that achieved by assigning higher priority to the candidate closer to the destination. Actually, it has been proved in [6] that giving candidates closer to the destination higher priorities achieves maximum expected packet advancement (EPA).

**Impact of Candidate Coordination**

The coordination delay is another key factor affecting the packet forwarding time and one-hop throughput. When this delay is much larger than the sender delay, then it would be better to retransmit the packet instead of waiting for other forwarding candidates to relay the packet in order to save the packet forwarding time. While when this delay is negligible, we should involve all the available next-hop neighbors into opportunistic forwarding, because any extra candidates would help to improve the relay reliability but without introducing any extra delay. We should also give candidates closer to the destination higher relay priorities, since larger-advancement candidates should always try first in order to maximize the EPA. If they failed to relay the packet, the lower-priority candidates could instantaneously relay the correctly received packet without having to wait. Therefore, the coordination
Delay has a great impact on throughput. Since we use the compressed slotted acknowledgement, which introduces small coordination delay among candidates, it would be better to give candidates closer to the destination higher relay priorities. In the compressed slotted acknowledgement mechanism, ACK plays two roles: one is to acknowledge the sender of data reception; the other is to suppress other candidates from forwarding duplicated packets. We discuss the reliability of this mechanism according to these two ACK roles. Firstly, following the collision avoidance rule, each node should sense the channel to be clear for at least DIFS before transmission. Since the ıt-priority candidate broadcasts the ACK with a short delay after successful packet reception, the ACK is unlikely to collide with other transmissions at the sender side. Carrier sensing range is around double of the data transmission range. So any two forwarding candidates will be in the carrier sensing range of each other. Then lower prioritized candidates should be able to detect a transmission emerged in the channel if a higher prioritized candidate does send out an ACK. False positive could happen when a lower-priority candidate senses a transmission emergence but it is from other transmission source. In this case, lower-priority candidate would drop its received packet. If all the lower-priority candidates who have received the packet correctly believe there is a higher-priority candidate that has received the packet but actually there is not, no ACK would be sent back to the sender, then the sender would retransmit the packet. However, the probability of other transmissions emerging in the short coordination period (multiple SIFS) and suppressing all the potential forwarding
Candidates should be relatively low.

**7. Ad-Hoc On-Demand Distance Vector Multipath (Aodvm) Routing**

We propose modifications to the AODV protocol so as to enable the discovery of multiple node-disjoint paths from a source to a destination. Instead of discarding the duplicate RREQ packets, intermediate nodes are required to record the information contained in these packets in a table which we refer to as the RREQ table. For each received copy of an RREQ message, the receiving intermediate node records the source who generated the RREQ, the destination for which the RREQ is intended, the neighbor who transmitted the RREQ, and some additional information (as shown in Fig. 2(a)) in the RREQ table. Furthermore, intermediate relay nodes are precluded from sending an RREP message directly to the source.

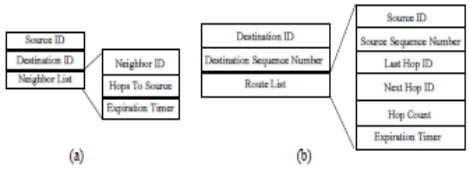



Fig. 2. (a) Structure of the each RREQ table entry in AODVM
(b) Structure of the each routing table entry in AODVM

When the destination receives the first RREQ packet from one of its neighbors, it updates its sequence number and generates an RREP packet. The RREP packet contains an additional field called "last hop -ID2" to indicate the neighbor from which the particular copy of RREQ packet was received. This RREP packet is sent back to the source via the path traversed by the RREQ copy, albeit in the reverse direction. When the destination receives duplicate copies of the RREQ packet from other neighbors, it updates its sequence number and generates RREP packets for each of them. Like the first RREP packet, these RREPpackets also contain their respective last hop nodes' IDs.

When an intermediate node receives an RREP packet from one of its neighbors, it deletes the entry corresponding to this neighbor from its RREQ table and adds a routing entry to its routing table (shown in Fig. 2(b)) to indicate the discovered route to the originator of the RREP packet (the destination). The node, then, identifies the neighbor in the RREQ table via which, the path to the source is the shortest, and forwards the RREP message to that neighbor. The entry corresponding to this neighbor is then deleted from the RREQ table. In order to ensure that a node does not participate in multiple paths, when nodes overhear any node broadcasting an RREP message, they delete the entry corresponding to the transmitting node from their RREQ table.

When an intermediate node that receives an RREP message cannot forward it further (its RREQ table is now empty), it generates an RDER or Route Discovery Error message and sends that message to the neighbor that actually forwarded the RREP to this node. The neighbor, upon receiving the RDER message will now attempt to forward the RREP to a different neighbor who can potentially forward it further towards the source.

## 8. AODV

When a node S needs a route to some destination D, it broadcasts a ROUTE REQUEST message to its neighbors, including the last known sequence number for that destination. The ROUTE REQUEST is flooded in a controlled manner through the network until it reaches a node that has a route to the destination. Each node that forwards the ROUTE REQUEST creates a reverse route for itself back to node S.

When the ROUTE REQUEST reaches a node with a route to D, that node generates a ROUTE REPLY that contains the number of hops necessary to reach D and the sequence number for D most recently seen by the node generating the REPLY. Each node that participates in forwarding this REPLY back toward the originator of the ROUTE REQUEST (node S), creates a forward route to D. The state created in each node along the path from S to D is hop-by-hop state; that is, each node remembers only the next hop and not the entire route, as would be done in source routing. In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbor is taken as an indication that the link to the neighbor in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbors.

When a link goes down, any upstream node that has recently forwarded packets to a destination using that link is notified via an UNSOLICITED ROUTE REPLY containing an infinite metric for that destination. Upon receipt of such a ROUTE REPLY, a node must acquire a new route to the destination using Route Discovery as described above.

## 10) DSR

The DSR protocol consists of two mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism by which a node S wishing to send a packet to a destination D obtains a source route to D. To perform a Route Discovery, the source node S broadcasts a ROUTE REQUEST packet that is flooded through the network in a controlled manner and is answered by a ROUTE REPLY packet from either the destination node or another node that knows a route to the destination. To reduce the cost of Route Discovery, each node maintains a cache of source routes it has learned or overheard, which it aggressively uses to limit the frequency and propagation of ROUTE REQUESTs. Route Maintenance is the mechanism by which a packet's sender S detects if the network topology has changed such that it can no longer use its route to the destination D

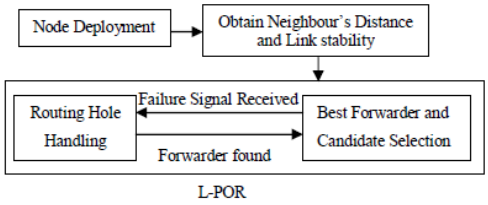
because two nodes listed in the route have moved out of range of each other. When Route Maintenance indicates a source route is broken, S is notified with a ROUTE ERROR packet. The sender S can then attempt to use any other route to D already in its cache or can invoke Route Discovery again to find a new route.

**11 . AO2P**

In AO2P route discovery is done by using only the position of the destination. Other information such as forwarding nodes positions are hiding from the network. Real identities of source, destination and forwarding nodes are confidential. Date packet transmission uses the pseudo identifiers of the source, destination and forwarding nodes. Route is established by receiver contention scheme. In this protocol receivers (node receiving the rreq message) are included in different class. The receiver which is closer to the destination is in the higher priority class. Highest priority receiver is the destination node. A node in the network obtains its position through GPS. Every node has a region around a fixed center called virtual home region (VHR). Position information of the node is updated to the servers in the VHR. This distributed secure position service is named as DISPOSER which improves the position security. R-A02P is another method to provide more destination anonymity. In this position of a reference point is used for establishing the route instead of destination position.

**12 . Link and Position based Opportunistic Routing (L-POR)**

Link and Position based Opportunistic Routing (L-POR) protocol is designed to achieve maximum reliability in a mobile ad-hoc network. It combines geographic and opportunistic routing to achieve high packet delivery ratio. The protocol chooses the best forwarder based on the receptive power. When the best forwarder fails, a candidate node takes over the forwarding function. Trigger nodes trigger a hole handling mechanism when routing holes are encountered.




L-POR

Distance calculation between any two nodes, say node a and node b is based on Euclidean distance. Free-space propagation model can be used to predict the received strength when the transmitter and receiver have clear unobstructed line-of-sight path between them. When system losses are neglected, the free space power received by a receiver antenna separated from a transmitting antenna by a distance. Even if no matter exists between sender and receiver, the signal still experiences free space loss due to the distance traversed. As soon as there is matter between the sender and receiver, the situation becomes more complex.

**Forwarding Node Selection**

In below figure node S is the source and D is the destination node.R is the radius of the transmission range of node S. The transmission range of S is denoted by the dotted circle. The nodes in the area enclosed within the dashed arc make positive progress towards the destination. From these nodes, the one with maximum power for reception is chosen as the best forwarder, namely node B. R/2 denotes the radius of half the transmission range of node B. The intersection area of the transmission range of S and half of the transmission range of B is taken as the forwarding area. Nodes within the forwarding area, other than node B, become candidate nodes, namely nodes H, A and F.

ISBN: 978-960-474-393-3

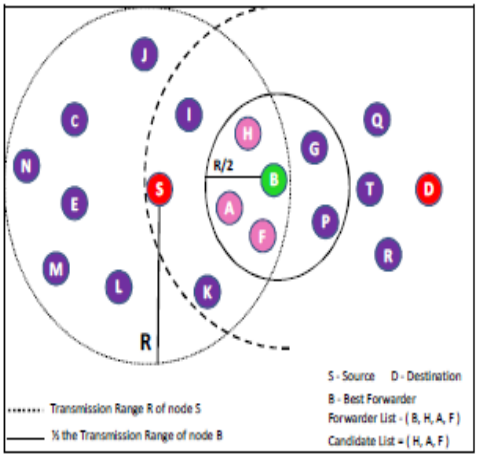



**Fig. Best forwarder and candidate selection**

**Routing Hole Handling**

Communication holes may exist since nodes are not uniformly distributed. When the best forwarder seeks the next hop node and finds none, a communication void is said to be encountered. The protocol then switches to a routing hole handling mechanism. When the best forwarder encounters a communication hole, it sends a void signal to the previous forwarder. The previous forwarder becomes the trigger node and the best forwarder becomes the void node. If the next hop is the destination, packets are forwarded and an acknowledgement is sent to the trigger node. If a neighbour that makes positive progress to the real destination and which is nearer to the destination than the current node is found, then the routing switches back to the normal L-POR routing algorithm. If no forwarders are found, then the routing fails and a disrupt message is sent to the trigger node.

Node A has chosen node B as the next forwarder. Node B finds no forwarders to forward the packets. In such a situation node B is said to encounter a routing hole. It sends a void warning signal to node A. Now, node B becomes the void node and node A becomes the trigger node. Node A switches to a whole handling algorithm. Node it may route around the void through C-H-G-T or L-OP- R. If destination is reached, then an acknowledgement is sent to the trigger node, else a disrupt signal is sent.

| NO | Method Name | Advantages | Disadvantages |
|---|---|---|---|
| 1 | OPR | It is scalable and applicable to large network. To improve the wireless network performance by exploiting the broadcost nature of the medium. It gives best performance and reliable solutions in the data transmission | .packet delivery ratio is minimum compared to other protocols. |
| 2 | MFR | Most Forward within Radius algorithm (MFR) is a greedy routing algorithm that used to minimize the Number of hops a message has to travel to reach the destination. | . The probability of successful message delivery increases as the lifetime of message delivery decreases. |
| 3 | Opportunistic Routing Technique | Routing with infrastructure Reliable and fast data transmission. Routing without infrastructure no path maintenance, energy-efficient. | some drawbacks to these schemes as additional delay in messages delivery and the error rate also increase |
| 4 | Opportunistic Routing in Multichip and MultiMate wireless Networks | The rate adaptation and candidate selection algorithm achieves the highest throughput and lowest delay among all the protocols. | The *opportunistic effective one hop throughput* (OEOT), to characterize the trade-off between the packet advancement and medium time cost under different data rates. |
| 5 | AODVM | It play a key role in maintaining freedom and disjointness properties. to provide robustness to both intermittent (or short term) and long term node failures in ad hoc networks. | These failures could be a result of either fading, battery failure or compromises. The computation and use of multiple node-disjoint routes could potentially provide some tolerance to node failures. |
| 6 | AODV, DSR | Faster operation. Quenches route request flood.It is simplicity. it is reactive, thus eliminating the need to flood the network . | The disadvantage of DSR is that the route-maintenance mechanism does not repair a broken link locally. |
| 7. | L-POR | Link and Position based Opportunistic Routing (L-POR) protocol is designed to achieve maximum reliability in a mobile adhoc network. It combines geographic and opportunistic routing to achieve high packet delivery ratio. The packet delivery ratio of L-POR is better than that of POR.L-POR guarantees reliability through best forwarder selection based on the | .<br>The hop count may not always be a minimal. This causes unpredictable end-to end delay. |

ISBN: 978-960-474-393-3

| | | | |
|---|---|---|---|
| | | node's link quality. | |

**Experimental results:**

To know the effectiveness of each surveyed protocol it compared with the various performance metrics like packet delivery ratio, end-to-end delay, shortest path, routing overhead and lifetime.

1. Packet Delivery Ratio:

Packet delivery ratio is the ratio of the number of delivered data packet to the destination. The greater value of packet delivery ratio means the better performance of the protocol. The packet delivery ratio can be calculated as follows:

$$Packet\ Delivery\ Ratio = \frac{\sum Number\ of\ Packet\ Received}{\sum Number\ of\ Packet\ Sent}$$

2. End-to-End Delay:

End-to-End Delay is the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. The End-to-End Delay can be calculated as follows:

$$Packet\ Delivery\ Ratio = \frac{\sum(Arrival\ Time - Sent\ Time)}{\sum Number\ of\ Connections}$$

3. Throughput:

Throughput is the average data rate of successful data or message delivery over a specific communications link. Network throughput is measured in bits per second (bps). Throughput can be calculated as follows:

$$Throughput = \frac{File\ Size\ (sec)}{Transmission\ Time\ (bps)}$$

4. Lifetime:

Lifetime is the time (number of rounds) of network disconnection due to the failure of one or more sensor nodes. Lifetime can be calculated as follows:

$$Lifetime = \frac{File\ Size}{Bandwidth\ (sec)}$$

5. Routing Overhead:

Routing Overhead is the nodes that often change their location within network. so, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

The analysis of the performance metrics for various protocols is shown in the below table.

Table 1. Packet Delivery Ratio for Various Protocols

| No. of Nodes | MFR | ORT | MRWN | AODVM | AO2P | DSR | AODV | POR | L_POR |
|---|---|---|---|---|---|---|---|---|---|
| **50** | 0.8 | 0.85 | 0.9 | 0.89 | 0.89 | 0.85 | 0.9 | 0.93 | 0.95 |
| **100** | 0.78 | 0.84 | 0.87 | 0.85 | 0.88 | 0.83 | 0.88 | 0.9 | 0.92 |
| **150** | 0.77 | 0.83 | 0.85 | 0.83 | 0.85 | 0.81 | 0.87 | 0.85 | 0.9 |
| **200** | 0.75 | 0.81 | 0.83 | 0.81 | 0.84 | 0.8 | 0.85 | 0.82 | 0.88 |
| **250** | 0.69 | 0.8 | 0.81 | 0.8 | 0.81 | 0.78 | 0.83 | 0.8 | 0.85 |

Table 2. End-to-End Delay for Various Protocols

| No. of Nodes | MFR | ORT | MRWN | AODVM | AO2P | DSR | AODV | POR | L_POR |
|---|---|---|---|---|---|---|---|---|---|
| **50** | 2.4 | 2 | 1.8 | 2 | 2.2 | 1.9 | 1.2 | 0.9 | 0.5 |
| **100** | 2.6 | 2.2 | 2 | 2.1 | 2.4 | 2 | 1.5 | 1 | 0.7 |
| **150** | 2.7 | 2.3 | 2.1 | 2.2 | 2.5 | 2.2 | 1.6 | 1.2 | 0.8 |
| **200** | 2.9 | 2.4 | 2 | 2.6 | 2.7 | 2.4 | 1.7 | 1.3 | 0.9 |
| **250** | 3.2 | 2.2 | 1.9 | 2.5 | 2.8 | 2.5 | 1 | 1.4 | 1 |

Table 3. Throughput for Various Protocols

| No. of Nodes | MFR | ORT | MRWN | AODVM | AO2P | DSR | AODV | POR | L_POR |
|---|---|---|---|---|---|---|---|---|---|
| **50** | 55 | 59 | 65 | 79 | 74 | 67 | 75 | 88 | 94 |
| **100** | 54 | 60 | 64 | 80 | 72 | 65 | 77 | 85 | 92 |
| **150** | 56 | 61 | 62 | 78 | 73 | 64 | 74 | 86 | 93 |
| **200** | 52 | 62 | 63 | 79 | 71 | 66 | 73 | 87 | 94 |
| **250** | 53 | 60 | 61 | 81 | 74 | 65 | 71 | 85 | 91 |

ISBN: 978-960-474-393-3

Table 4. Lifetime for Various Protocols

| No. of Nodes | MFR | ORT | MRWN | AODVM | AO2P | DSR | AODV | POR | L_POR |
|---|---|---|---|---|---|---|---|---|---|
| **50** | 0.45 | 0.5 | 0.65 | 0.72 | 0.69 | 0.65 | 0.7 | 0.8 | 1 |
| **100** | 0.42 | 0.48 | 0.63 | 0.71 | 0.7 | 0.63 | 0.69 | 0.78 | 0.95 |
| **150** | 0.4 | 0.45 | 0.62 | 0.68 | 0.68 | 0.62 | 0.68 | 0.76 | 0.93 |
| **200** | 0.38 | 0.42 | 0.61 | 0.67 | 0.66 | 0.6 | 0.65 | 0.75 | 0.89 |
| **250** | 0.35 | 0.41 | 0.6 | 0.66 | 0.65 | 0.58 | 0.64 | 0.72 | 0.9 |

Table 5. Routing Overhead for Various Protocols

| No. of Nodes | MFR | ORT | MRWN | AODVM | AO2P | DSR | AODV | POR | L_POR |
|---|---|---|---|---|---|---|---|---|---|
| **50** | 0.08 | 0.06 | 0.075 | 0.08 | 0.075 | 0.07 | 0.05 | 0.04 | 0.02 |
| **100** | 0.085 | 0.07 | 0.08 | 0.085 | 0.08 | 0.075 | 0.055 | 0.045 | 0.03 |
| **150** | 0.09 | 0.08 | 0.085 | 0.09 | 0.07 | 0.08 | 0.07 | 0.059 | 0.05 |
| **200** | 0.1 | 0.09 | 0.09 | 0.085 | 0.08 | 0.085 | 0.075 | 0.072 | 0.06 |
| **250** | 0.11 | 0.095 | 0.075 | 0.086 | 0.085 | 0.09 | 0.08 | 0.09 | 0.065 |

To know the working of the various protocols, it is compared with various performance metrics. This is shown in the below graphs.

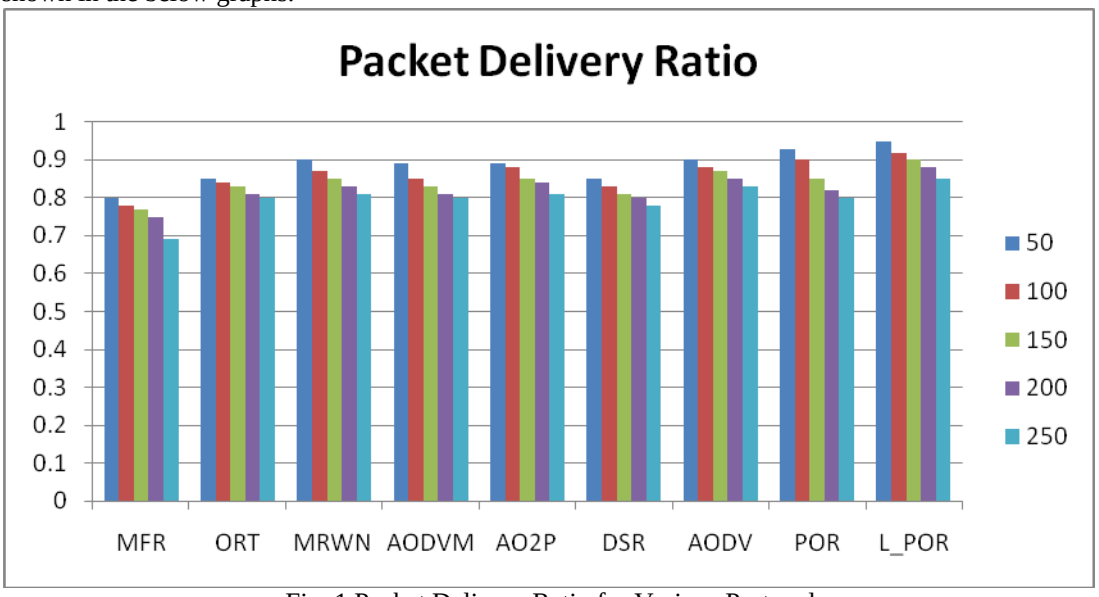



Fig. 1 Packet Delivery Ratio for Various Protocols

ISBN: 978-960-474-393-3

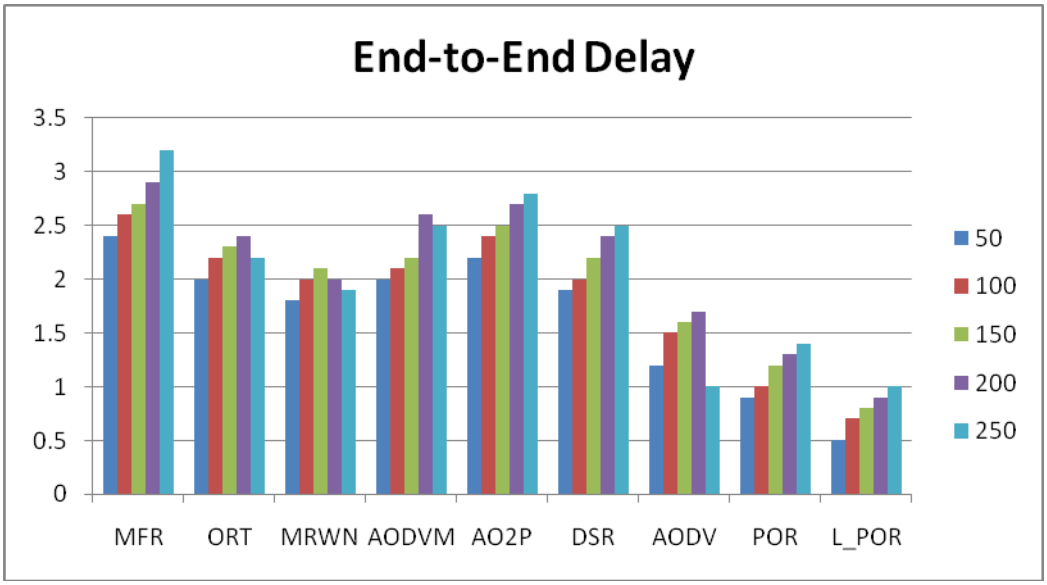



Fig. 2 End-to-End Delay for Various Protocols

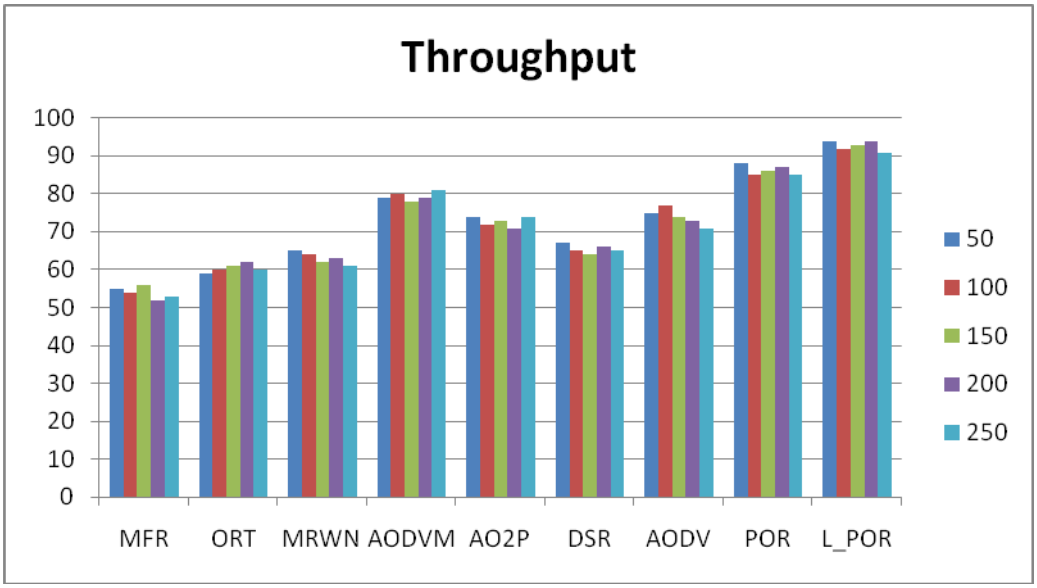



Fig. 3 Throughput for Various Protocols

ISBN: 978-960-474-393-3

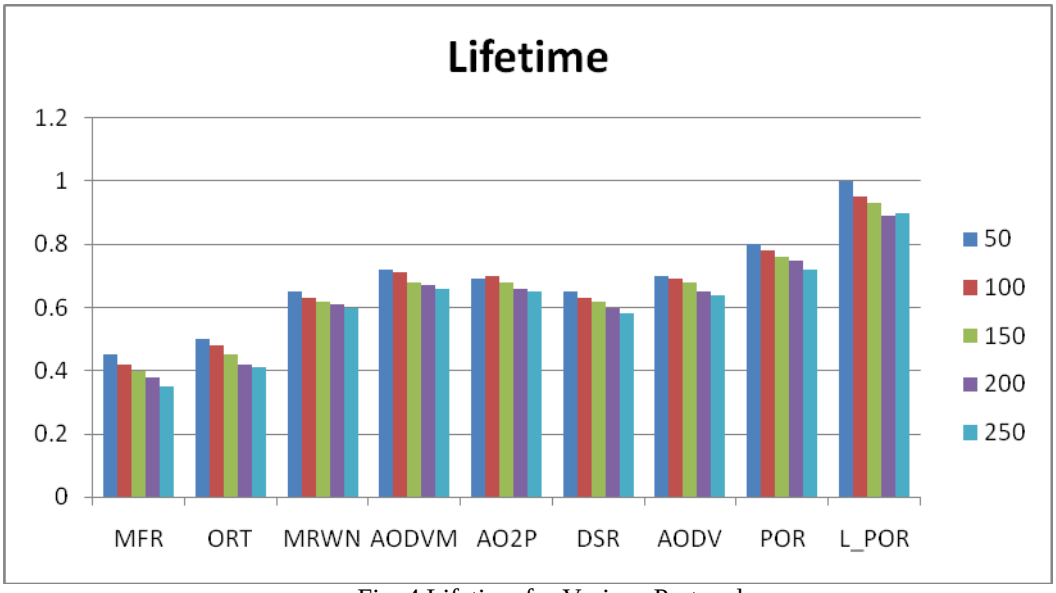



Fig. 4 Lifetime for Various Protocols

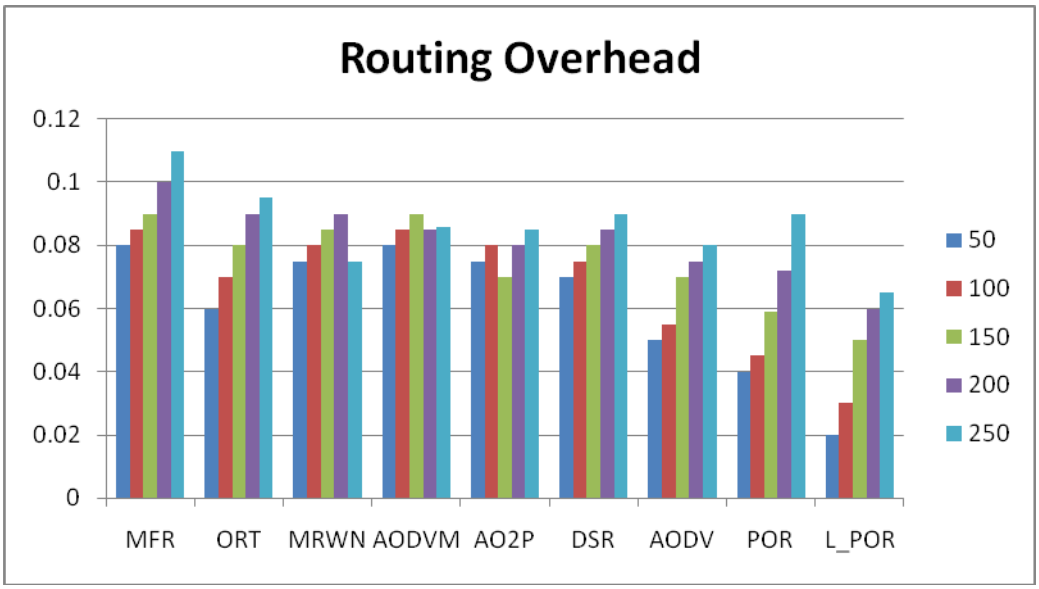



Fig. 5 Routing Overhead for Various Protocols

The above figures shows the various performance metrics, which is used to compare the surveyed protocols.

**CONCLUSION:**

In this paper we discussed about many types of routing protocols. Each routing techniques used in the wireless mobile ad-hoc network. Each protocols have merits and demerits. This chapter is discuss about the above table. The performance of DSR was very good at all mobility rates and movement speeds, although its use of source routing increases the number of routing overhead bytes required by the protocol. Finally, AODV performs almost as well as DSR at all mobility rates and movement speeds and accomplishes its goal of eliminating source routing overhead, but it still requires the transmission of many routing overhead packets and at high rates of node mobility is actually more expensive than DSR. The packet delivery ratio of L-POR is better than that of POR. L-POR guarantees reliability through best forwarder selection based on the node's link quality. Opportunistic routing schemes offer a significant improves in performance. These schemes use the broadcast

ISBN: 978-960-474-393-3

techniques of wireless communication to send data to several possible next hops in just one transmission and taking into account the current condition of the network situation, all of these help to avoid unnecessary retransmission and create robustness in the communication against disconnections. This also produces some drawbacks to these schemes as additional delay in messages delivery and the error rate also increase, therefore these schemes are to be applied in not real time application, which are delay-tolerant in nature and these drawbacks do not cause major trouble to the communication.

**Reference**

[1] Josh Broch David A. Maltz David B. Johnson Yih-Chun Hu Jorjeta Jetcheva "A Performance Comparison of Multi-HopWireless Ad Hoc Network Routing Protocols" ACM/IEEE International Conference on Mobile Computing and Networking

[2] Anupriya Augustine , Jubin Sebastian E "A Study of Efficient Anonymous Routing Protocols in MANET" International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014 1

[3] Luciana Pelusi, Andrea Passarella, and Marco Conti "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad hoc Networks"

[4] Kai Zeng, , Zhenyu Yang, Member, "Location-Aided Opportunistic Forwarding in Multi-Rate and Multi-Hop Wireless Networks" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. , NO. , 200X

[5] Zhenqiang Ye "A Frame work for Reliable Rouling in Mobile Adhoc Network"

[6] J.JOHNSI, G.ABIJA "RELIABLE DATA DELIVERY FOR HIGHLY DYNAMIC MOBILE AD HOC NETWORKS USING OPR " International Journal of Emerging Technology and Advanced Engineering

[7] Sahaya Rose Vigita.E, Golden Julie.E "Reliable Link-Based Routing Protocol for Highly Dynamic Mobile Adhoc Networks" International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue5-May 2013

[8] Khaled Ahmed Abood Omer "Analytical Study of MFR Routing Algorithm for Mobile Ad hoc Networks" J. King Saud University, Vol. 22, Comp. & Info. Sci., pp. 29-35,Riyadh (1431H./2010)

[9] P.Revathi1, G.Kalpana "A Study on Timely and Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Network" International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

[10] A. Triviño-Cabrera, S. Cañadas-Hurtado "Survey on Opportunistic Routing in Multihop Wireless Networks" International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 2, August 2011.

[11] Deepti Singh, Birendra Kumar Sharma, Arvind Kumar "A Survey on challenges in Multipath Routing for Adhoc Networks " International Journal of Emerging Technology and Advanced Engineering Volume 4, Special Issue 1, February 2014)