INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

# DYNAMIC DATA ROUTING IN MANET USING POSITION BASED OPPORTUNISTIC ROUTING PROTOCOL

**P. Kalaivani[1], G. Sathya[2], N. Senthilnathan[3]**

[1]Assistant Professor, SNS College of Engineering. E-Mail: pkalai.ece@gmail.com
[2]Assistant Professor, SNS College of Engineering. E-Mail: sathya_g82@yahoo.co.in
[3]Architect, Robert Bosch Engineering India Limited. E-Mail:Senthilnathan.nagarajan@in.bosch.com

**ABSTRACT:**

MOBILE ad hoc networks (MANETs) have gained a great deal of attention because of its significant advantages brought about by multi-hop, infrastructure-less transmission. However, due to the error prone wireless channel and the dynamic network topology, reliable data delivery in MANETs, especially in challenged environments with high mobility remains an issue. A novel Position based Opportunistic Routing protocol (POR) is proposed, in which several forwarding candidates cache the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order. In this way, as long as one of the candidates succeeds in receiving and forwarding the packet, the data transmission will not be interrupted. Potential multi-paths are exploited on the- fly on a per-packet basis, leading to POR's excellent robustness. In case of communication hole, a Virtual Destination based Void Handling (VDVH) scheme is further proposed to work together with POR

## 1. INTRODUCTION:

Mobile Ad-Hoc Network (MANET) is a self configuring infrastructure less network of mobile devices connected by wireless links. The topology of the MANET may change uncertainly and rapidly due to high mobility of the independent mobile nodes, and because of the network decentralization, each node in the MANET will act as a router to discover the topology and maintain the network connectivity.

## 2. POSITION-BASED OPPORTUNISTIC ROUTING (POR) PROTOCOL

POR Protocol uses sseveral forwarding candidates cache the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order. In this way, as long as one of the candidates succeeds in receiving and

forwarding the packet, the data transmission will not be interrupted. Potential multipaths are exploited on the fly on a per packet basis, leading to POR's excellent robustness.

### 2.1. VIRTUAL DESTINATION BASED VOID HANDLING

To handle communication voids, almost all existing mechanisms try to find a route around. During the void handling process, the advantage of greedy forwarding cannot be achieved as the path that is used to go around the hole is usually not optimal. More importantly, the robustness of multicast-style routing cannot be exploited. In order to enable opportunistic forwarding in void handling virtual destination is introduced, as the temporary target that the packets are forwarded to.

## 3. MANET PROTOCOLS

### 3.1 Dynamic Source Routing

The Dynamic Source Routing (DSR) protocol is an on demand routing protocol that is based on the concept of Source Routing. Source Routing is a technique where by the sender of a packet can specify the route that a packet should take through the network. The DSR protocol is composed of two mechanisms of Route Discovery and Route maintenance, which works together to allow nodes to discover and maintain source routes to destination in the adhoc network. Route Discovery, by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery, is used only when S attempts to send a packet to D and does not already know a route to it. Route Maintenance indicates that a source route is broken, S can attempt to use any route to D or it can invoke Route discovery again to find a new route. Route Maintenance is used only when S is actually sending packets to D.

The Disadvantages of the DSR are:-

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network
- Potential collisions between route requests propagated by neighboring node

### 3.2. Adhoc on- Demand Routing Protocol (AODV):

The AODV Routing protocol uses an on-demand approach for finding routes, i.e., a route is established only when it is required by a source node for transmitting data packets. When a source node desires to send to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the destination.

Disadvantage of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also, multiple Route Reply packet in response to a single Route Request packet can lead to heavy control overhead. Another disadvantage of AODV is unnecessary bandwidth consumption due to periodic beaconing.

Routing discovery happens when a node wants to communicate with a destination while it obtains no proper route entry for that destination. In this situation, this source node (originator) will broadcast an RREQ (Routing REQuest) message to all its neighbors. Each neighbor who receives this RREQ will check in its own routing table if it contains the route entry for that destination. If not, it will set up a reverse path towards the originator of RREQ and rebroadcast this routing request.

Any node which receives this RREQ will generate a RREP (Routing Reply) message if it either has a fresh enough route to satisfy the request or is itself the destination. Then this intermediate or destination node will generate an RREP message and unicast it to the next hop toward the originator of the RREQ, as indicated by the routing entry for that originator. When a node receives an RREP message, it first updates some fields of the route table and the routing reply, and then forwards it to the next hop towards the originator. When a Source node receives a RERR (Routing Error) message, it shows that the packets are not reached the destination successfully.

### 3.3. Greedy Perimeter Stateless Routing (GPSR)

Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet forwarding decisions. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology.

When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region. Greedy forwarding great advantage is its reliance only on knowledge of the forwarding node's immediate neighbors. The state required is negligible and dependent on the density of nodes in the wireless network, not the total number of destinations in the network. On networks where multi-hop routing is useful, the number of neighbors within a node's radio range must be substantially less than the total number of nodes in the network.

Assuming the wireless routers [nodes] know their own locations the Greedy forwarding algorithm will try to find the closest router which is also the closest to the final destination as seen in Fig.3.3.1

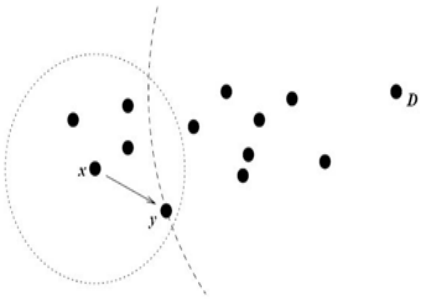



**Figure 3.3.1. Greedy Forwarding, y is the x's closest neighbor to D**

Node *x* wants to send information to node *D*, using the greedy forwarding algorithm, *x* calculates that the closest neighbor that is also the closest to *D* and that is in *x*'s radio range (the dotted circle surrounding *x*) is y. Even though there are other neighboring nodes with in *x*'s radio range closer to *x* than *y*, none of them are as close to *D* as *y* is and therefore *x* will send its information to *y*, which will use the greedy forwarding algorithm to send it to the next node until the information reaches the final destination *D*.

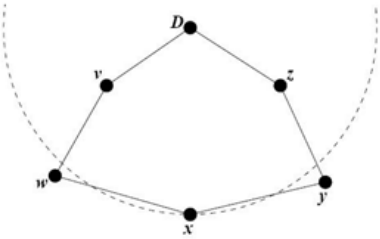



**Figure 3.3.2. Greedy Forwarding failure, x's is a local maximum in its geographic proximity to D, w and y are farther from D**

However, there is a drawback to the greedy forwarding algorithm which occurs when the network topology is like the one in fig 3.3.2. In this type of topology there is only one route possible and would cause *x* to send information to a neighbor that is farther away from *D* than *x* is. So in this case *x* is closer to *D* than its neighbors *w* and *y*. Therefore, *x* would be forced to send its information to *w* or *y* which is farther away in geometric distance from the destination *D* than *x* is. The greedy forwarding algorithm will not allow this to happen so a different mechanism must be used to forward the information in these situations like a perimeter forwarding algorithm.

## 4. PROPOSED SYSTEM

There are some disadvantages in the existing protocols, to overcoming that protocol by using new routing protocols namely,

- Position based Opportunistic Routing Protocol (POR)
- Virtual Destination based Void Handling Mechanism (VDVH)

### 4.1 Position based Opportunistic Routing Protocol (POR)

The design of POR is based on geographic routing and opportunistic forwarding. The nodes are assumed to be aware of its own location and the positions of its direct neighbors. Geographic Routing (GR) uses location information to forward data packets, in a hop-by-hop routing fashion. The concept of opportunistic forwarding is to select and prioritize the forwarding candidates. The forwarding candidates cache the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, suboptimal candidates will take turn to forward the packet according to a locally formed order.

On analyzing the effect of node mobility on packet delivery and explain the improvement brought about by the participation of forwarding candidates. Due to the selection of forwarding area and the properly designed duplication limitation scheme, POR's performance gain can be achieved at little overhead cost.

### 4.1.1 Selection and prioritization of forwarding Candidates

One of the key problems in POR is the selection and prioritization of forwarding Candidates. Only the nodes located in the forwarding area would get the chance to be backup nodes. The forwarding area is determined by sender and the next hop node. A node located in the forwarding area, satisfies following two conditions:

- It makes positive progress towards the destination.
- Its distance to the next hop node should not exceed half of their transmission range of a wireless node (i.e. R/2}.

The priority of a forwarding candidate is decided by its distance to the destination. The nearer it is to the destination, the higher priority it will get.

**Algorithm Used: Candidate selection algorithm:**

1. First, initialize the candidate selection to select and prioritize the forwarder list.
2. Only the nodes specified in the candidate list will act as forwarding candidates.
3. The lower index of the node in the candidate list has higher priority.

Thus the candidate selection algorithm is used to select best forwarding candidates in the POR routing protocol.

### 4.1.2 Limitation on Possible Duplicate Relaying

Due to collision and nodes movement, some forwarding candidates may fail to receive the packet forwarded by the next hop node or higher-priority candidate, so that a certain amount of duplicate relaying would occur.

To limit such duplicate relaying, only the packet that has been forwarded by the source and the next hop node is transmitted in an opportunistic fashion and is allowed to be cached by multiple candidates.

### 4.1.3 MAC Modification and Complementary Techniques

#### 4.1.3.1 MAC Interception

The broadcast nature of 802.11 MAC was all nodes within the coverage of the sender would receive the signal. However, its RTS/CTS/DATA/ACK mechanism is only designed for unicast. It simply sends out data for all broadcast packets with CSMA. Therefore packet loss due to collisions would dominate the performance of multicast like routing protocols. Here, did some alteration on the packet transmission scenario.

In the network layer, just send the packet via unicast, to the best node which is elected by greedy forwarding as the next hop. In this way, make full utilization of the collision avoidance supported by 802.11 MAC .It is then further processed by POR. Hence the benefit of both broadcast and unicast (MAC support) can be achieved.

#### 4.1.3.2. MAC Call back

When the MAC layer fails to forward a packet, the function implemented in POR – Mac_ callback will be executed. The item in the forwarding table corresponding to that destination will be deleted and the next hop node in the neighbor list will also be removed. If the transmission of the same packet by a forwarding candidate is overheard, then the packet will be dropped without re-forwarding again, otherwise it will be given a second chance to reroute.

The packets with the same next hop in the interface queue which is located between the routing layer and MAC layer will also be pulled back for rerouting. As the location information of the neighbors is updated periodically, some items might become obsolete very quickly especially for nodes with high mobility. This scheme introduces a timely update which enables more packets to be delivered.

#### 4.1.3.3. Interface Queue Inspection

One of the key points of POR is that when an intermediate node receives a packet with the same ID (i.e. same source address and sequence number), it means a better forwarder has already taken over the function. Hence, it will drop that packet from its packet list.

Besides maintaining the packet list, check the interface queue. When the packet arrives at the routing layer, the same packet might have already been sent down to the lower layers by the current node. With additional inspection of the interface queue, it further decreases the duplicate packets appearing in the wireless channel.

### 4.2. Virtual Destination based Void Handling Mechanism (VDVH)

#### 4.2.1. Virtual Destination

In the case of communication hole, a Virtual Destination Void Handling (VDVH) scheme in which the advantages of greedy forwarding and opportunistic routing can still be achieved while handling communication voids.

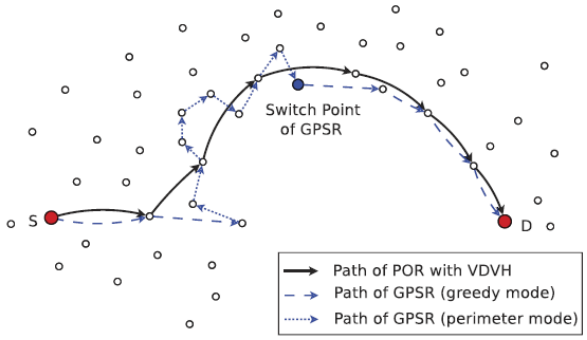



**Figure.4.2. The paths exploited by VDVH a GPSR**

To handle communication voids, almost all existing mechanisms try to find a route around. During the void handling process, the advantage of greedy forwarding cannot be achieved as the path that is used to go around the hole is usually not optimal (e.g. with more hops compared to the possible optimal path). More importantly, the robustness of multicast-style routing cannot be exploited. In order to enable opportunistic forwarding in void handling, which means even in dealing with voids, we can still transmit the packet in an opportunistic routing like fashion; virtual destination is introduced, as the temporary target that the packets are forwarded to.

The figure 4.2 shows an example in which VDVH achieves the optimal path of 7 hops while GPSR undergoes a much longer route of 15 hops. Thus, by using VDVH protocol the time is consumed.

### 4.2.3 Path Acknowledgement and Disrupt Message

In VDVH, if a trigger node finds that there are forwarding candidates in both directions, the data flow will be split into two where the two directions will be tried simultaneously for a possible route around the communication void.

In order to reduce unnecessary duplication, two control messages are introduced, namely, path acknowledgement and reverse suppression. If a forwarding candidate receives a packet that is being delivered or has been delivered in void handling mode, it will record a reverse entry. If a forwarding candidate receives a packet that is being delivered or has been delivered in void handling mode, it will record a reverse entry If a forwarding candidate receives a packet that is being delivered or has been delivered in void handling mode, it will record a reverse entry

Once the packet reaches the destination, a path acknowledgement will be sent along the reverse path to inform the trigger node. Then the trigger node will give up trying the other direction.

For the same flow, the path acknowledgement will be periodically sent. If a packet that is forwarded in void handling mode cannot go any further or the number of hops traversed exceeds a certain threshold but it is still being delivered in void handling mode, a DISRUPT control packet will be sent back to the trigger node as reverse suppression. Once the trigger node receives the message, it will stop trying that direction.

### Advantage:

- No end-to-end routes need to be maintained, leading to high efficiency and scalability in transfer
- The additional latency incurred by local route recovery is greatly reduced and the duplicate relaying caused by packet reroute is also decreased.
- No data loss
- Data can be forward through neighbor node to the destination node.

## 5. RESULTS AND DISCUSSION

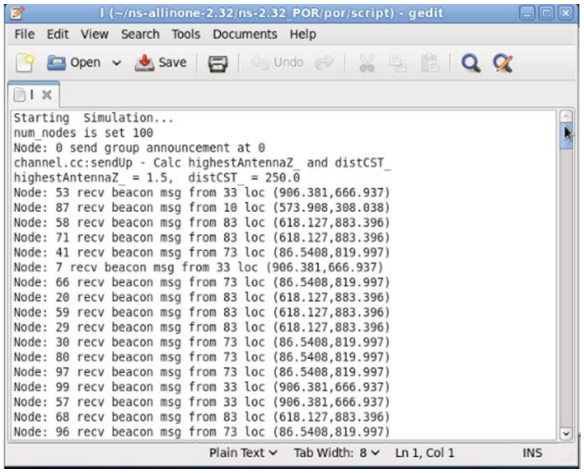
### 5.1. PERFORMANCE ANALYSIS

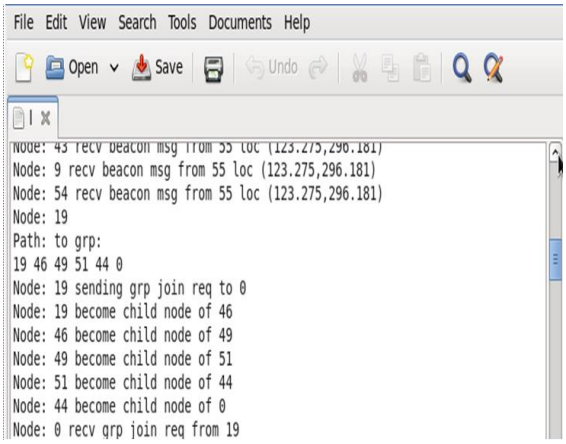
Performance will be analyzed for POR and GPSR based on following attributes:

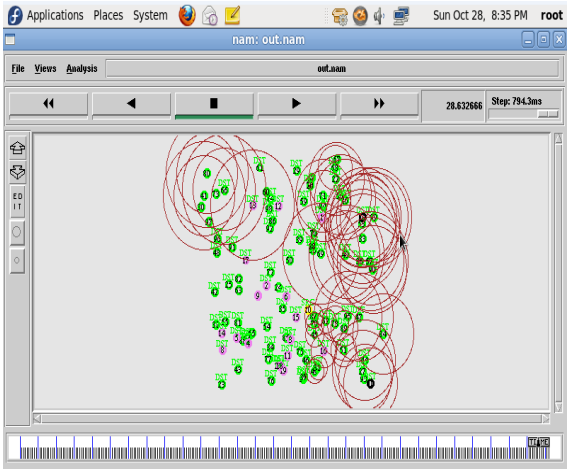
- **Packet delivery ratio:** The ratio of the number of data packets received at the destination to the number of data packets sent by the source.
- **End-to-end delay:** The average and the median end-to-end delay are evaluated, together with the cumulative distribution function (CDF) of the delay.
- **Path length:** The average end-to-end path length (number of hops) for successful packet delivery.
- **Packet forwarding times per hop (FTH):** The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet over each hop.
- **Packet forwarding times per packet (FTP):** The average number of times a packet is being forwarded from the perspective of routing layer to deliver a data packet from the source to the destination.

### 5.2. RESULTS:

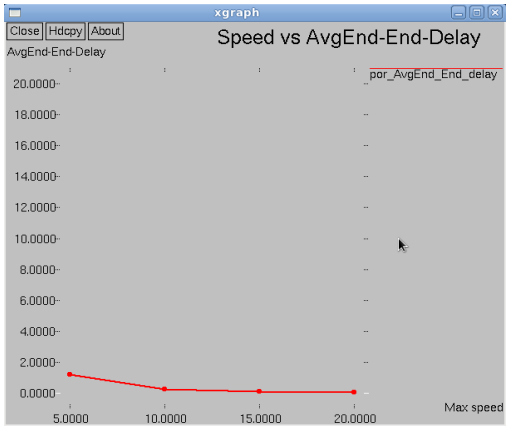
**SENDING BEACON MESSAGES FOR FIINDING THE NEAREST NEIGHBOUR**



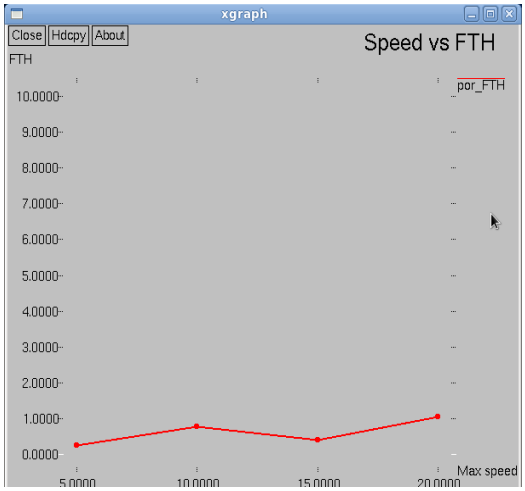



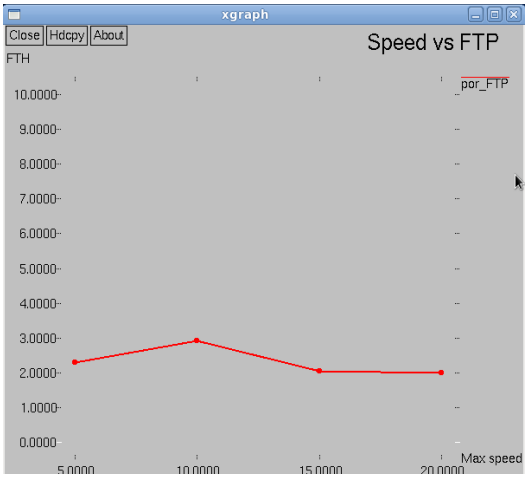
### 1. SPEED VS AVG END DELAY




### 2. SPEED VS FTH

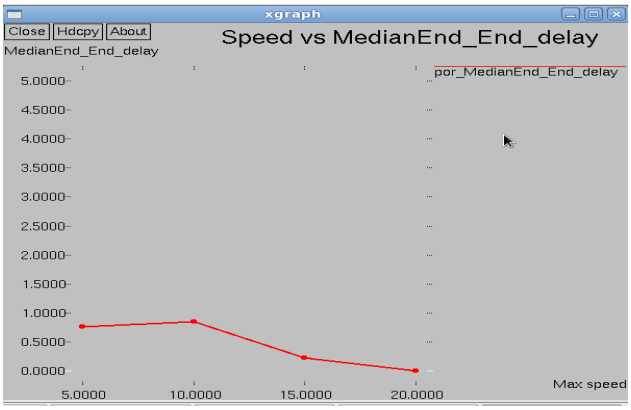



### 3. SPEED VS FTP

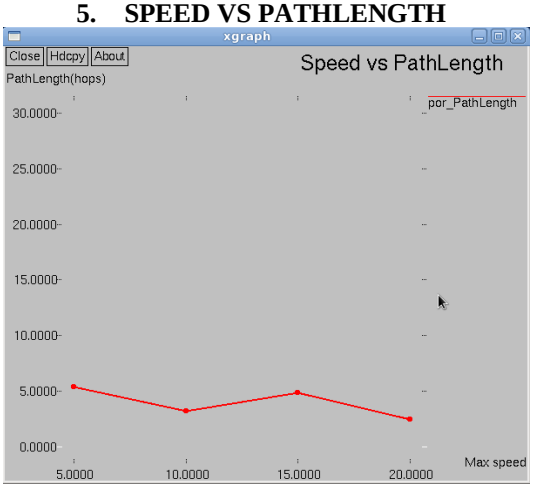


Vol.2 Issue.12, Pg.: 1-10
December 2014

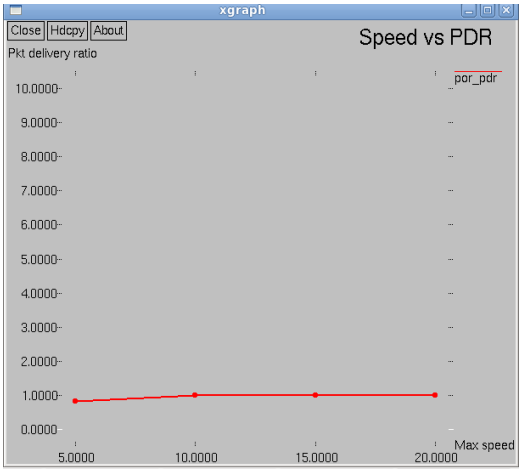
## 4. SPEED VS MEDIAN END DELAY




## 5. SPEED VS PATHLENGTH




## 6. SPEED VS PDR



## 6. CONCLUSION AND FUTURE WORK

In this paper, the problem of reliable data delivery in highly dynamic mobile ad hoc networks. Constantly changing network topology makes conventional ad hoc routing protocols incapable of providing satisfactory performance. In the face of frequent link break due to node mobility, substantial data packets would either get lost, or experience long latency before restoration of connectivity.

Inspired by opportunistic routing, a novel MANET routing protocol POR which takes advantage of the stateless property of geographic routing and broadcast nature of wireless medium is proposed. Besides selecting the next hop, several forwarding candidates are also explicitly specified in case of link break.

On changing the basic parameters of POR protocol can make efficient ad hoc routing protocol for dynamic packet delivery. On comparing these protocols the efficiency of delivering the packets in Mobile ad hoc networks is studied.

This work can be improved by estimating the quality parameters of the POR routing network for improving the reliability of the network.

## REFERENCES:

1. J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. Jetcheva (1998), “A performance comparison of multi-hop wireless ad hoc network routing protocols,” in MobiCom., pp.85-97.
2. M. Mauve, A. Widmer, and H. Hartenstein (2001), “A survey on position-based routing inmobile ad hoc networks,” Network, IEEE, vol. 15, no. 6. , pp. 30 – 39.
3. B. Karp and H. T. Kung (2000), “Gprs: greedy perimeter stateless routing for wireless networks,” in MobiCom, pp. 243–254.
4. D.Chen and P. Varshney (2007), “A survey of void handling techniques for geographic routing in wireless networks,” Communications Surveys & Tutorials, IEEE, vol. no.9, pp.50-67.
5. S. Biswas and R. Morris, “Exor: opportunistic multi-hop routing for wireless networks,” in SIGCOMM ’05, 2005, pp. 133–144.
6. S. Chachulski, M. Jennings, S. Katti, and D. Katabi, “Trading structure for randomness in wireless opportunistic routing,” in SIGCOMM ’07, 2007, pp. 169–180
7. S. Mueller, R. Tsang, and D. Ghosal, “Multipath routing in mobile ad hoc networks: Issues and challenges,” Lecture Notes in Computer Science, vol. 2965, pp. 209–234, 2004
8. B. Deb, S. Bhatnagar, and B. Nath, “Reinform: reliable information forwarding using multiple paths in sensor networks,” in Local Computer Networks, 2003. LCN ’03, Oct. 2003, pp. 406–415.
9. Tsirigos and Z. Haas, “Analysis of multipath routing-part I: the effect on the packet delivery ratio,” Wireless Communications, IEEE Transactions on, vol. 3, no. 1, pp. 138–146, Jan. 20