Dynamic Path Selection for Reliable Routing In Mobile Adhoc Network

T.Dhanalakshmi[1], P.Prema devi[2], Dr. T.Rajendran[3]

PG Scholar[1], Assistant Professor[2], Professor[3]

Department of Computer Science and Engineering

Angel College of Engineering and Technology

Mail-id: dhanaesec@gmail.com

***Abstract*- Objective is to deliver the packet in a reliable and timely manner in dynamic mobile environment. In this paper we propose an efficient Position-based Opportunistic Routing (POR) protocol which takes the stateless property of geographic routing and the broadcast nature of wireless medium. The additional delay incurred by local route recovery is greatly reduced and the duplicate relaying caused by packet reroute is also decreased. This paper addresses few related works done on trust evaluation and establishment in ad hoc networks. A new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate. If communication void occurs, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with POR. Both theoretical analysis and simulation results show that POR achieves excellent performance even under high node mobility with acceptable overhead with trust estimation and the new void handling scheme also works well.**

***Keywords*— Mobile Ad-hoc Network, Void handling, geographical routing, load balancing, Trust estimation**

I. INTRODUCTION

Ad-hoc networks are infrastructure less networks, made up of mobile nodes, which are using their neighbors as a mean of communication with other nodes in the network. 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. Ad-hoc networks change their topology, expressed by the node connectivity, over time, as the nodes change their position in space. Geographic routing (GR) [1] uses location information to forward data packets, in a hop-by-hop routing fashion. Greedy forwarding is used to select next hop forwarder with the largest positive progress toward the destination while void handling mechanism is triggered to route around communication voids [2].

Using greedy packet forwarding, the sender of a packet includes the approximate position of the recipient in the packet. This information is gathered by an appropriate location service. When an intermediate node receives a packet, it forwards the packet to a neighbor lying in the general direction of the recipient. Ideally, this process can be repeated until the recipient has been reached. Due to the broadcast nature of the wireless medium, a single packet transmission will lead to multiple receptions. If such transmission is used as backup, the robustness of the routing Protocol can be significantly enhanced. In order to acquire the inter node loss rates, periodic network-wide measurement is required, which is impractical for mobile environment. In this paper, a novel Position-based Opportunistic Routing (POR) protocol 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 multipath is exploited on the fly on a per packet basis, leading to POR's excellent robustness.

2. RELATED WORK

Most existing ad hoc routing systems distribute either topology information or queries to all nodes in the network. Some protocols such as DSDV, are proactive; they continuously maintain route entries

for all destinations. Other techniques are reactive, and construct routes to destinations as they are required.

A. Geographic Forwarding

The geographic forwarding layer uses a two hop distance vector protocol. This helps to improve the holes in the topology and ensures that each node knows the location of all nodes. Each node maintains a table of immediate neighbors as well as each neighbor's neighbors. Each entry in the table includes the node's ID, location, speed, and a timestamp. Each node periodically broadcasts a list of all neighbors it can reach in one hop, using a HELLO message. When a node receives a HELLO message, it updates its local routing table with the HELLO message information. Using this protocol, nodes may learn about two hop neighbors' nodes that cannot be reached directly, but can be reached in two hops via the neighbor that sent the HELLO message.

The routing table is also updated every time a node receives a packet, using the packet's preceding hop information. Each entry in the neighbor table expires after a fixed timeout. However, when an entry expires, the node estimates the neighbor's current position using its recorded speed. If it would likely still be in range, the entry may still be used for forwarding, but it is not reported as a neighbor in further HELLO messages. This special treatment is justified by two properties of the 802.11 MAC layer. First, broadcast packets are more likely to be lost in the face of congestion than unicast packets. Thus it is not unusual to miss HELLO messages from a node that is still nearby. Second, unicast transmissions are acknowledged. If the neighbor has actually moved away, the transmitting node will be notified when it attempts to forward packets through the missing node.

The invalid neighbor entry is then removed immediately and a new forwarding path is chosen. To select a next hop, nodes first choose a set of nodes from all nodes in their neighbor table. This set consists of the best nodes to move the packet to, as defined by the shortest distance to the destination from the candidate nodes. All nodes whose distances to the destination are nearly equal are considered in this set. There are two main problems, named LLNK and LOOP that are caused by mobility-induced location errors. There are two mobility prediction schemes—Neighbor Location Prediction (NLP) and Destination Location Prediction (DLP) to mitigate these problems [3]. SOAR incorporates the following four major components to achieve high throughput and fairness[4]:

1) Adaptive forwarding path selection to leverage path diversity while minimizing duplicate transmissions.
2) Priority timer-based forwarding to let only the best forwarding node forward the packet.
3) Local loss recovery to efficiently detect and retransmit lost packets.
4) Adaptive rate control to determine an appropriate sending rate according to the current network conditions.

ExOR chooses each hop of a packet's route after the transmission for that hop, so that the choice can reflect which intermediate nodes actually received the transmission. This deferred choice gives each transmission multiple opportunities to make progress. As a result ExOR can use long radio links with high loss rates, which would be avoided by traditional routing. ExOR increases a connection's throughput while using no more network capacity than traditional routing. ExOR's design faces the following challenges. The nodes that receive each packet must agree on their identities and choose one forwarder. The agreement protocol must have low overhead, but must also be robust enough that it rarely forwards a packet zero times or more than once. Finally, ExOR must choose the forwarder with the lowest remaining cost to the ultimate destination. QOS parameters were considered in [13]. QOS attributes are response time and availability.

3. PROPOSED SYSTEM

A. Position-based Opportunistic Routing

The design of POR is based on geographic routing and opportunistic forwarding. The nodes are assumed to be aware of their own location and the positions of their direct neighbors. Neighborhood location information can be exchanged using one-hop beacon or piggyback in the data packet's header. While for the position of the destination, we assume that a location registration and lookup service which maps node addresses to locations is available just as in [5]. It could be realized using many kinds of location service ([6], [7]). In our scenario, some efficient and reliable way is also available. For example, the location of the destination could be transmitted by low bit rate but long range radios, which can be implemented as periodic beacon, as well as by replies when requested by the source.When a source node wants to transmit a packet, it gets the location of the destination first and then attaches it to the packet header. Due to the destination node's movement, the multihop path may diverge from the true location of

the final destination and a packet would be dropped even if it has already been delivered into the neighborhood of the destination. To deal with such issue, additional check for the destination node is introduced. At each hop, the node that forwards the packet will check its neighbor list to see whether the destination is within its transmission range. If yes, the packet will be directly forwarded to the destination, similar to the destination location prediction scheme described in [4]. By performing such identification check before greedy forwarding based on location information, the effect of the path divergence can be very much alleviated.

In POR, we use similar scheme as the MAC multicast mode described in [8]. The packet is transmitted as unicast (the best forwarder which makes the largest positive progress toward the destination is set as the next hop) in IP layer and multiple reception is achieved using MAC interception. The use of RTS/CTS/DATA/ACK significantly reduces the collision and all the nodes within the transmission range of the sender can eavesdrop on the packet successfully with higher probability due to medium reservation. As the data packets are transmitted in a multicast-like form, each of them is identified with a unique tuple (src_ip, seq_no) where src_ip is the IP address of the source node and seq_no is the corresponding sequence number.

Every node maintains a monotonically increasing sequence number, and an ID_Cache to record the ID (src_ip, seq_no) of the packets that have been recently received. If a packet with the same ID is received again, it will be discarded. Otherwise, it will be forwarded at once if the receiver is the next hop, or cached in a Packet List if it is received by a forwarding candidate, or dropped if the receiver is not specified. The packet in the Packet List will be sent out after waiting for a certain number of time slots or discarded if the same packet is received again during the waiting period (this implicitly means a better forwarder has already carried out the task).

The basic routing scenario of POR can be simply illustrated in Fig. 1. In normal situation without link break, 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 node A fails to deliver the packet (e.g.,node A has moved out and cannot receive the packet), node B, the forwarding candidate with the highest priority, will relay the packet and suppress the lower priority candidate's forwarding (e.g., node C) as well as node S. By using the feedback from MAC layer, node S will remove node A from the neighbor list and select a new next hop node for the subsequent packets. The packets in the interface queue The packets in the interface queue taking node A as the next hop will be given a second chance to reroute. For the packet pulled back from the MAC layer, it will not be rerouted as long as node S overhears node B's forwarding.

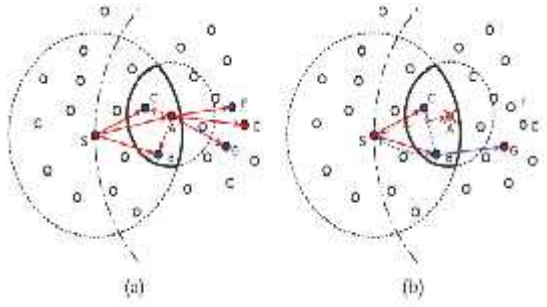


Fig.1. (a) The operation of POR in normal situation. (b) The operation of POR when the next hop fails to receive the packet.

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 [8] would get the chance to be backup nodes. The forwarding area is determined by the sender and the next hop node. A node located in the forwarding area satisfies the following two conditions: 1) it makes positive progress toward the destination; and 2) its distance to the next hop node should not exceed half of the transmission range of a wireless node (i.e., R=2) so that ideally all the forwarding candidates can hear from one another.In Fig. 1, the area enclosed by the bold curve is defined as the forwarding area. The nodes in this area, besides node A (i.e., nodes B, C), are potential candidates. According to the required number of backup nodes, some (maybe all) of them will be selected as forwarding candidates. 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. When a node sends or forwards a packet, it selects the next hop forwarder as well as the forwarding candidates among its neighbors. The next hop and the candidate list comprise the forwarder list. Algorithm 1 shows the procedure to select and prioritize the forwarder list. The candidate list will be attached to the packet

header and updated hop by hop. Only the nodes specified in the candidate list will act as forwarding candidates. The lower the index of the node in the candidate list, the higher priority it has.

Algorithm 1. Candidate Selection

```
ListN   : Neighbor List
ListC   : Candidate List, initialized as an
          empty list
ND      : Destination Node
Base    : Distance between current node and
          ND
if find(ListN,ND) then
   next hop ← ND
   return
end if
for i ← 0 to length(ListN) do
   ListN[i].dist ← dist(ListN[i],ND)
end for
ListN:sort()
Next_hop ← ListN[0]
for i ← 1 to length(ListN) do
if dist(ListN[i],ND)≥base or
   length(ListC)=N
   then
   break
else if dist(listN[i],listN[0]<R/2 then
ListC.add(ListN[i])
end if
end for
```

Every node maintains a forwarding table for the packets of each flow (identified as source-destination pair) that it has sent or forwarded. Before calculating a new forwarder list, it looks up the forwarding table, an example is illustrated in Table 1, to check if a valid item for that destination is still available. The forwarding table is constructed during data packet transmissions and its maintenance is much easier than a routing table. It can be seen as a trade-off between efficiency and scalability. As the establishment of the forwarding table only depends on local information, it takes much less time to be constructed. Therefore, we can set an expire time on the items maintained to keep the table relatively small. In other words, the table records only the current active flows, while in conventional protocols, a decrease in the route expire time would require far more resources to rebuild.

B. Virtual Destination-Based Void Handling

In order to enhance the robustness of POR in the network where nodes are not uniformly distributed and large holes may exist, a complementary void handling mechanism based on virtual destination is proposed.

Trigger Node

In many existing geographic routing protocols, the mode change happens at the void node of packet forwarding switch from greedy mode to void handling mode, e.g., Node B in Fig. 3. Then, Path 1 (A-B-E-…..) and/or Path 2 (A-B-C-F-….) (in some cases, only Path 1 is available if Node C is outside Node B's transmission range) can be used to route around the communication hole. From Fig. 3, it is obvious that Path 3 (A-C-F-….)

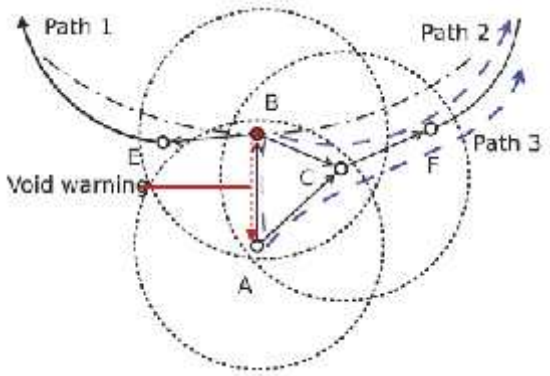


Fig.3. Potential paths around the void.

is better than Path 2. If the mode switch is done at Node A, Path 3 will be tried instead of Path 2 while Path 1 still gets the chance to be used. A message called void warning, which is actually the data packet returned from Node B to Node A with some flag set in the packet header, is introduced to trigger the void handling mode. As soon as the void warning is received, Node A (referred to as trigger node) will switch the packet delivery from greedy mode to void handling mode and rechoose better next hops to forward the packet. Of course, if the void node happens to be the source node, packet forwarding mode will be set as void handling at that node without other choice (i.e., in this case, the source node is the trigger node).

Virtual Destination

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. Virtual destinations are located at the circumference with the trigger node as center (Fig. 4), but the radius of the circle is set as a value that is large enough.

C. Load balancing

A novel load-balancing technique for ad hoc on demand routing protocols is presented. Currently, ad hoc routing protocols lack load-balancing capabilities, and thus, they often fail to provide good performance especially in the presence of a large volume of traffic. It present a simple but very effective method to achieve load balance and congestion alleviation. The new scheme is motivated by the observation that ad hoc on demand routing protocols flood route request (RREQ) messages to acquire routes, and only nodes that respond to those messages have a potential to serve as intermediate forwarding nodes [22]. If a node ignores RREQ messages within a specific period, it can completely be excluded from the additional communications that might have occurred for that period otherwise. Thus, a node can decide not to serve a traffic flow by dropping the RREQ for that flow.

In the new scheme, RREQ messages are forwarded selectively according to the load status of each node so that overloaded nodes can be excluded from the requested paths. Each node begins to allow additional traffic flows again whenever its overloaded status is dissolved. The new scheme utilizes interface queue occupancy and workload to control RREQ messages adaptively. Position-based Opportunistic Routing (POR) protocol, when a data packet sends out, some of the neighbors that have overheard the transmission will serve as forwarding candidates. Best forwarder will be chooses based on the load of that node which has low traffic in the network.

D. Minimum queue length

Position-based Opportunistic Routing (POR) protocol, when a data packet sends out, some of the neighbors that have overheard the transmission will serve as forwarding candidates. Best forwarder will be chooses based on the minimum queue length algorithm which will reduces error rate in network. It will make traffic flow among the path based the queue size of each node.

D. Trust Estimation

All the nodes in an ad hoc network are categorized as *Most trusted*, trusted or non trusted based on their relationships with their neighboring nodes. During network initiation all nodes will be non trusted to each other. A *trust estimator* is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into *friends* (most trusted), trusted and not trusted. In an ad hoc network, the relationship of a node *i* to its neighbor node *j* can be any of the following types

(i) Node i is a untrusted (U) to neighbor node j:
Node i have never sent/received messages to/from node j. Their trust levels between each other will be very low. Any new node entering ad hoc network will be a stranger to all its neighbors. There are high chances of malicious behavior from stranger nodes.

(ii) Node i is an trusted (T) to neighbor node j:
Node i have sent/received few messages from node j. Their mutual trust level is neither too low nor too high to be reliable. The chances of malicious behavior will have to be observed.
(iii) Node i is a *most trusted* (M) to neighbor node j:
Note i sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Probability of misbehaving nodes may be very less.
The above relationships are computed by each node and a friendship table is maintained for the neighbors. Fig. 1 shows the relationship of N4 with its neighbors. The corresponding friendship table maintained in N4 is given in Table I. The threshold trust level for a stranger node to become an acquaintance to its neighbor is represented by Tacq and the threshold trust level for an acquaintance node to become a friend of its neighbor is denoted by Tfri.
Fig. 1 Trust Relationship of a node in an ad hoc network. The relationships are represented as:
$R(ni \rightarrow nj) = M$ when $T \geq Tfri$
$R(ni \rightarrow nj) = T$ when $Tacq \leq T < Tfri$
$R(ni \rightarrow nj) = U$ when $0 < T < Tacq$
During route discovery phase of the POR protocol, the extended system also computes the aggregate trust along different paths to the destination by the

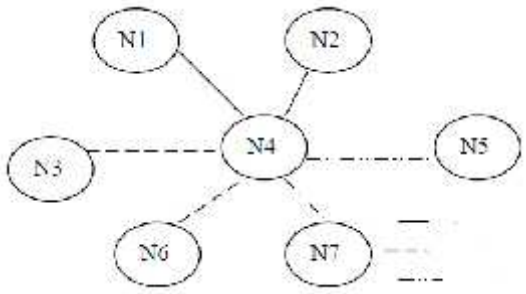


Fig. 4 Trust Relationship of a node in an ad hoc network

"path semiring" algorithm as proposed. From this, the most trusted path between the source and the destination is found out before establishing the data transfer. The segregation of the neighboring nodes into *most trusted*, trusted and untrusted is the outcome of the direct evaluation of trust.

Table I
Friendship table for node (n4) in fig. 4

Neighbors	Relationship
N1	M
N2	M
N3	T
N5	U
N6	T
N7	U

4. SIMULATION RESULTS

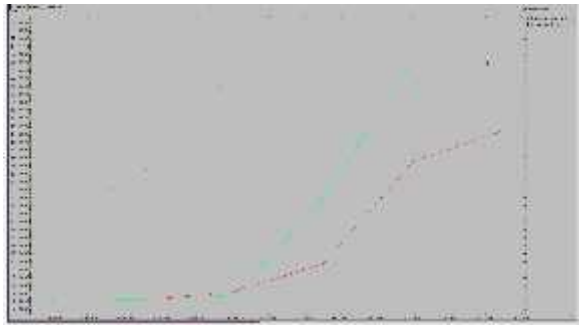
To evaluate the performance of POR, we simulate the algorithm in a variety of mobile network topologies in ns-2[14], together with the on demand routing protocol AODV. Performance metrics include packet delivery ratio, the 90th percentile and average of packet transmission delay.

A. Normal Situations

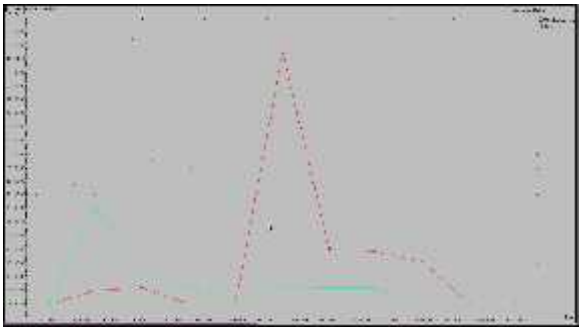
Nodes	Region	CBR flow	Max speed
20	500 m×500 m	10	10 m/s, 20 m/s
45	750 m×750 m	10	10 m/s, 20 m/s
80	1000 m×1000 m	10	
125	1250 m×1250 m	10	10 m/s, 20 m/s

TABLE II
SIMULATED TOPOLOGY CHARACTERISTICS

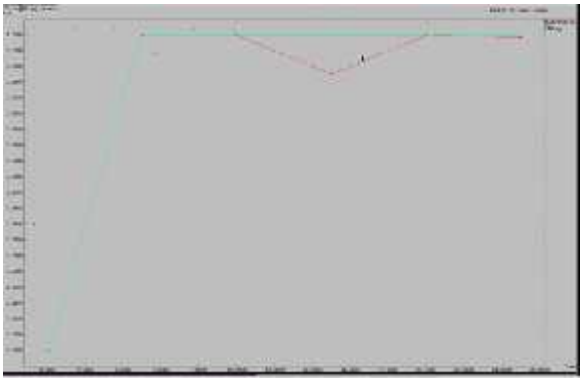
From Fig. 4 we can see that the delivery ratio of POR outperforms the other protocols, especially when the network is large and the mobility of the nodes increases.



Throughput



Average delay



Packet delivery ratio

B. Performance Evaluation

To evaluate the performance of POR, we simulate the algorithm in a variety of mobile network topologies in NS-2[14] and compare it with AODV [20].The improved random way point [8] without

pausing is used to model nodes' mobility. The minimum node speed is set to 1 m/s and we vary the maximum speed to change the mobility degree of the network. The following metrics are used for performance comparison:

1. **Packet delivery ratio**. The ratio of the number of data packets received at the destination(s) to the number of data packets sent by the source(s).
2. **End-to-end delay.** The average and the median end-to-end delay are evaluated, together with the cumulative distribution function of the delay.

IV CONCLUSIONS

In this paper, the issue of reliable data delivery in highly dynamic mobile ad hoc networks is handled by novel MANET routing protocol POR which takes full advantage of the wireless channel's broadcast nature. Through the introduction of a certain degree of redundancy and randomness in data delivery, the protocol is very robust as well as efficient. It performs well in normal situations and maintains high packet delivery ratio in critical environments. Constantly changing network topology makes conventional ad hoc routing protocols incapable of providing satisfactory performance. In case of frequent link break due to node mobility, substantial data packets would get lost. Besides selecting the next hop, several forwarding candidates are also explicitly specified in case of link break. It considers trust estimation and load balancing. Leveraging on such natural backup in the air, broken route can be recovered in a timely manner. The efficiency of the involvement of forwarding candidates against node mobility, as well as the overhead due to opportunistic forwarding is analyzed. On the other hand, inherited from geographic routing, the problem of communication void is also examined.

To work with the multicast forwarding style, a virtual destination-based void handling scheme is proposed. By provisionally adjusting the direction of data flow, the advantage of greedy forwarding as well as the robustness brought about by opportunistic routing can still be achieved when handling communication voids. In future work, more extended analysis and simulation will be carried out, including the consideration of packet duplication and buffer consumption. The selection of time slot and the maximum number of forwarders will also be evaluated and more comparisons with other protocols will be conducted. In future work best forwarder will be selected based on the functionality of Quality of Service (QoS) requirements as a secondary criterion for node selection.

REFERENCES

[1] M. Mauve, A. Widmer, and H. Hartenstein, "A Survey on Position-Based Routing in Mobile AdHoc Networks," IEEE Network, vol. 15, no. 6, pp.30-39, Nov./Dec. 2001.

[2] D. Chen and P. Varshney, "A Survey of Void Handling Techniques for Geographic Routing in Wireless Networks," IEEE Comm. Surveys and Tutorials, vol. 9, no. 1, pp. 50-67, Jan.-Mar.2007.

[3] D. Son,A. Helmy, and B.rishnamachari, "The Effect of Mobility Induced Location Errors on Geographic Routing in Mobile AdHoc Sensor Networks: Analysis and Improvement Using Mobility Prediction," IEEE Trans. Mobile Computing, vol. 3, no. 3, pp. 233-245,July/Aug.2004.

[4] E. Rozner, J. Seshadri, Y. Mehta, and L. Qiu, "SOAR: Simple Opportunistic Adaptive Routing Protocol for Wireless Mesh Networks," IEEE Trans. Mobile Computing, vol. 8, no. 12, pp.622-1635, Dec. 2009.

[5] K. Zeng, Z. Yang, and W. Lou, "Location-Aided Opportunistic Forwarding in Multirate and Multihop Wireless Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 6, pp. 3032- 3040, July 2009.

[6] D. Chen, J. Deng, and P. Varshney, "Selection of Forwarding Area for Contention-Based Geographic Forwarding in Wireless Multi-Hop Networks," IEEE Trans. Vehicular Technology, vol. 56, no. 5, pp. 3111-3122, Sept. 2007.

[7] A. Valera, W. Seah, and S. Rao, "Improving Protocol Robustness in Ad Hoc Networks through Cooperative Packet Caching and Shortest Multipath Routing," IEEE Trans. Mobile Computing, vol. 4, no. 5, pp. 443-457, Sept./Oct. 2005.

[8] J. Yoon, M. Liu, and B. Noble, "Random Waypoint Considered Harmful," Proc. IEEE INFOCOM, pp. 1312-1321, 2003.

[9] M. Marina and S. Das, "On-Demand Multipath Distance Vector Routing in Ad Hoc Networks," Proc. Ninth Int'l Conf. Network Protocols (ICNP '01), pp. 14-23, Nov. 2001.

[10] B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, pp. 243-254, 2000.

[11] N. Arad and Y. Shavitt, "Minimizing Recovery State in Geographic AdHoc Routing," IEEE Trans. Mobile Computing, vol. 8, no. 2, pp. 203-217, Feb. 2009.

[12] A. Tsirigos and Z. Haas, "Analysis of Multipath Routing-Part I: The Effect on the Packet Delivery Ratio," IEEE Trans. Wireless Comm., vol. 3, no. 1, pp. 138-146, Jan. 2004.

[13] Rajendran.T and Balasubramanie.P.2010, "An efficient architecture for agent-based dynamic web service discovery with qos", Journal of Theoretical and Applied Information Technology, Vol 15. No. 2, pp 86-95.

[14] Rajendran.T and Balasubramanie.P.2010, "An Optimal Broker-Based Architecture for Web Service Discovery with

QoS Characteristics", International Journal of Web Services Practices, Vol. 5, No.1, pp. 32-40.

AUTHOR'S PROFILE

Ms. T. Dhanalakshmi doing her Master of Engineering in Computer Science at Angel College of Engineering and Technology, Tiruppur and completed her Bachelor pf Engineering degree in Computer Scence from Erode Sengunthar Engineering College, Perundurai. She is a life member of IAENG. She has published 3 articles in International Journals. She has presented 5 papers in National and International Conferences.

Ms. P.Prema Devi completed her M.Tech., degree in 2010 at Anna University Of Technology, Chennai in the Department of Information and Communication Engineering. Now she is working as a Assistant Professor in Department of CSE at Angel College of Engineering and Technology, Tirupur, Tamilnadu, India. Her research interest includes Software Engineering, Networks and DBMS. She is a life member of ISTE. She has published 3 articles in International/ National Journals/Conferences.

Dr.T.Rajendran completed his PhD degree in 2012 at Anna University, Chennai in the Department of Information and Communication Engineering. Now he is working as a Dean for Department of CSE & IT at Angel College of Engineering and Technology, Tirupur, Tamilnadu, India. His research interest includes Distributed Systems, Web Services, Network Security and Web Technology. He is a life member of ISTE & CSI. He has published more than 51 articles in International/ National Journals/Conferences. He has visited Dhurakij Pundit University in Thailand for presenting his research paper in International conference. He was honored with Best Professor Award 2012 by ASDF Global Awards 2012, Pondicherry.