ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Management of Node Mobility in Mobile Ad Hoc Networks Using Multipath Routing Protocol

Jhunu Debbarma*
Asst. Professor, Deptt. of Computer Science & Engg.
Tripura Institute of Technology, Narsingarh
Agartala, India
jhunudb@gmail.com

Shimal Das
Asst. Professor, Deptt. of Computer Science & Engg.
Tripura Institute of Technology, Narsingarh
Agartala, India
Shimalcs.it@gmail.com

Rupanjal Debbarma
Asst. Professor, Deptt. of Electronics & Telecom.
Tripura Institute of Technology, Narsingarh
Agartala, India
rupanjal@ieee.org

Dr. Sudipta Roy
Associate Professor & HOD, Deptt. of IT,
School of Technology, Assam University
Silchar, India
sudipta.it@gmail.com

Abstract: Mobile Ad hoc networks are collections of wireless nodes that form temporary network without the aid of any infrastructure and central administration that gives the potential to every node to act as a router. The nature of ad hoc network is high mobility that results in ever changing topology and lower capacity of the shared wireless medium. To provide support for real-time applications there is requirement for stable routing considering the node mobility and signal strength of the nodes. There are several standard on-demand and pro-active routing protocols to support best traffic quality form source to destination. On-demand routing protocol like Ad hoc on demand distance vector (AODV) routing protocol is considered, due to the relative advantage when compared to pro-active routing protocols. To tackle the high mobility of nodes, each intermediate node on the path keeps three backup routes to solve route failure problem. The signal strengths from neighbouring nodes estimate relative stability of the link. In this paper we propose an on-demand AODV routing protocol that ensures stable route from the source to destination. Simulations were carried out in NS-2 that shows proper management of signal strength improves higher packet delivery ratio, increase in throughput and less end-to-end delay

Keywords: Mobile ad hoc networks, node mobility, signal strength, multi path, route stability, ad hoc on demand distance vector routing

I. INTRODUCTION

The standard AODV and DSR on-demand routing protocols are based on unipath routing protocols. The basic limitation in unipath routing protocol is that the packets are lost if the active route breaks due to link failure or quality of service (QoS) violation rules.[2,3] The different types of QoS parameters for real time traffic are - delay, delay jitter, reliability, throughput, etc. It is very challenging to meet the QoS factors in MANETs due to their dynamic nature. In the unipath routing, when an active route fails there is a procedure to reinvoke a route discovery to recover from the route failure. These types of frequent route failures result in delay, packet loss and are expensive too. Using multipath routing, a number of alternate paths can be made available at the source out of which one of the routes may be considered as the primary route and others as the alternate routes. Out of all the routes available the primary route is selected based on some stability criteria. In multipath routing, if the primary route breaks, then there is no need for initiating a route discovery or recovery procedure, but an alternate route may be selected from the already available alternate route lists. There is a need for path maintenance due to the high mobility of the nodes since the already available alternate routes may have become stale by the time the primary route failed. A new route discovery takes place only when all pre-computed path breaks. The usage of the stale nodes one after other results in an increased number of dropped packets. A periodic validation of alternate paths is essential in a multipath routing algorithm.

Our objective in this paper is to design a routing protocol that selects three node-disjoint paths with higher route stability values. For determining the stability of the three node disjoint paths, we consider the node mobility and signal strengths for computing the probability of link failure. It is difficult to predict the probability that a link may be broken in near future, but it is possible to determine the relative stability of the link based on the recent and current received signal strengths over the link. This paper is organized as follows. Section 2 provides an overview of the related work. Section 3 discusses the proposed stability model. In section 4 we present the proposed routing procedure, route validation and admission control. The performance of the proposed routing procedure is compared to the most widely accepted node-disjoint AODMV protocol. Section 5 concludes the paper and discusses the future work.

© 2010, IJARCS All Rights Reserved

II. RELETED WORKS

The idea of multipath routing is not new. It always has been a favorable alternative both for circuit switched and packet switched networks, as it provides an easy mechanism to distribute traffic and balance the network load, as well as provides fault tolerance. [1] A number of issues in QoS have been discussed to provide its services to multimedia applications such as digital video and audio. The paper has discussed about the problem in computing the best path based on multiple constraints and its implications on routing metric selection. The study was based on the basic problems QoS routing and proposal of path computation algorithms based on source routing and hop-by-hop routing [1-2] The motivation behind the on-demand protocols is that the routing overhead" (typically measured in terms of the number of routing packets transmitted, as opposed to data packets) is typically lower than the shortest path protocols, as only the actively used routes are maintained. However, as some recent performance evaluation work has shown [3], the routing overhead still approaches to that of the shortest path protocols, if a moderate to large number of routes needs to be actively maintained (when, for example, there is a moderate to large number of active peer-to-peer conversations). This is because the on-demand protocols discover routes via a *flooding* technique, where the source (or any node seeking the route) floods the entire network with a query packet in search of a route to the destination.[4] Flooding is also necessary for route maintenance activities, when a new route is needed, as the old one breaks because of node mobility.

Flooding takes up a substantial amount of network bandwidth, which is at a premium in wireless networks. Efficient control of frequent network-wide flooding is thus important for the efficient performance of on-demand protocols. Some of our prior work was directed to limit the flood within a small region of the network [2,3,4] to reduce its impact on the network performance. The proposal given by Goff et al. [5] uses the concept of preemptive routing that recovers the route before the actual route fails. This type of proposal requires an accurate prediction of route failure which is not an easy task in case of MANETs. Earlier works on multipath routing in [6] show that the availability of multipath gives good support to dynamic networks towards lower control overhead, end-to-end delay and high packet delivery ratio. In [4,5] QoS aware multipath routing protocols are based on CDMA/TDMA based medium access layer. It shows that it is difficult to have a centralized MAC scheme in dynamic networks due to the rapid changing node positions. ADQR [6] finds disjoint paths that satisfy throughput requirements with longer live connectivity based on the available bandwidth information obtained during route recovery. The distribution of traffic in the different disjoint paths give rise to the packet reordering and it was not addressed in ADQR protocol. In IMRP protocol [4-6] there is proposal for QoS multipath routing protocol for the time sensitive traffic.

This protocol suggest the method to find out disjoint paths based on link stability and available bandwidth but the method to estimate the bandwidth and the link stability in the routes are not specified. The proposal in [7-9] combines with NDMR [ ] with DiffServ to support QoS in MANETs. NDMR protocol reduces the routing overhead and congestion control by the concept of load balancing on the various disjoint routes. SMORT [10,11,12] provides all the intermediate nodes on the primary path with multiple routes to the destination. [12] show that there is reasonable amount of power diminution problem in multipath routing protocols due to route request (RREQ) forwarding policy and the path selection procedure adopted at the intermediate nodes and destination. Nasipuri et al. [13-16] reveals that performance gain is marginal beyond a few number of routes. Our algorithm proposes to select at most three QoS- aware routes that have higher route stability value.

III. STANDARD AODV PROTOCOL

A. Route discovery procedure in AODV protocol:

In AODV protocol, routes are built only when the nodes intend to communicate with each other and so the relevant routing information are stored only in the source node, intermediate nodes and destination node. There are two important step: route discovery procedure and route maintenance procedure. To start the route discovery procedure, a source node broadcast the route request broadcast packets (RREQ) to the entire accessible neighbor node.[17]
The format of the RREQ packet is given as follows:

s_addr	**d_addr**	**d_seq**	**lifetime**	**Hop_count**
s_addr	**d_addr**	**Broad_id**	**s_seq**	**d_seq**	**hop_count**

The fields in the RREQ packet are :
s_addr : IP address of the source node and source node.
d_addr : IP address of the source node and destination node.
Broad_id : Broadcast Identification Number
s_seq, d_seq: Sequence number of the source and destination node
hop_count: The number of nodes the broadcast message has transferred from source to destination
On receiving the broadcast message from the source node to the intermediate node the route reply packet (RREP) is transmitted back to the source.
The format of the RREP is given below:
s_addr : IP address of the source node and source node.
d_addr : IP address of the source node and destination node.
d_seq : Sequence number of the destination node
Lifetime: The time for which nodes receiving the RREP consider the route to be valid.
hop_count: The number of hops from the source to the Destination.

When an intermediate node receives the RREQ packet it checks if it can act as the intermediate node from the source to destination node. In case, the intermediate node has no route to the destination node then the *hop_count* field is incremented by 1 and rebroadcast the RREQ packet to the neighbors and sets up a reverse path pointer to the source node from where it received the RREQ. When the destination node receives RREQ, the active route is found. Then it would unicast a Route Reply packet (RREP) along the reverse path back to the source node. The *hop_count* field is reset to zero and counted again.

Every intermediate node will increase the *hop_count* by 1 and relay it according to its Reverse Path Pointer. As soon as the source node receives the correct RREP, the data transmission begins. To speed-up the route discovery procedure, the AODV protocol allows the intermediate nodes

© 2010, IJARCS All Rights Reserved

that have the route to the destination node to generate the RREP packet and send it back to the source node. The nodes along the active route or Reverse Path store necessary information in their route tables and the other intermediate nodes will eliminate the routing information like Reverse Path pointer.

B. Route Maintenance Procedure:

In this procedure, the nodes keep an entry for each active route in their route table and periodically broadcast the *hello* message to its neighbor to get the most recent information about the neighboring nodes. [18-19]This would help to detect the link failure and in such case route error message is generated to inform all relative source nodes. The format of the RERR packet is given as

D_addr	**new d_addr**	**Hop_count** = ∞

new d_seq is bigger than the maximum *d_seq* of all the RREQ or RREP this node have received. *hop_count* is set to an infinite number which means the destination node is now unreachable.

Because nodes periodically send *hello* messages, if a node fails to receive several *hello* messages from a neighbor, a link break is detected.

C. IEEE 802.11 Standard:

The IEEE 802.11 Standard [20-21] is by far the most widely deployed wireless LAN protocol. This standard specifies the physical, MAC and link layer operation. Multiple physical layer encoding schemes are defined, each with a different data rate. Part of each transmission uses the lowest most reliable data rate, which is 1 Mbps. At the MAC layer IEEE 802.11 uses both carrier sensing and virtual carrier sensing prior to sending data to avoid collisions. Virtual carrier sensing is accomplished through the use of Request-To-Send (RTS) and Clear-To-Send (CTS) control packets.

When a node has a unicast data packet to send to its neighbor, it first broadcasts a short RTS control packet. If the neighbor receives this RTS packet, then it responds with a CTS packet. If the source node receives the CTS, it transmits the data packet. Other neighbors of the source and destination that receive the RTS or CTS packets defer packet transmissions to avoid collisions by updating their network allocation vector (NAV). The NAV is used to perform virtual channel sensing by indicating that the channel is busy, as shown in Figure 2. After a destination properly receives a data packet, it sends an acknowledgment (ACK) to the source. It states that the packet was correctly received. This procedure (RTS-CTS-Data-ACK) is called the distributed Coordination Function (DCF). For small data packets the RTS and CTS packets may not be used. If an ACK (or CTS) is not received by the source within a short time limit after it sends a data packet (or RTS), the source will attempt to retransmit the packet up to seven times. [21-23]. If no ACK (or CTS) is received after multiple retries, an error is issued by the hardware indicating that a failure to send has occurred. Broadcast data packets are handled differently than unicast data packets. Broadcast packets are sent without the RTS, CTS or ACK control packets. These control messages are not needed because the data is simultaneously transmitted to all neighboring nodes.

IV. MULTIPATH ROUTE STABILITY MODEL

The proposed multipath route stability model that is proposed takes care of the node mobility and signal strength to compute the probability of link failure. The proposed algorithm makes modification on the standard AODV protocol which is renamed as **modified AODV**. The received signal strength is MAC layer information used by routing layer through cross-layer interaction. [23-25] When a node *x* receives a signal from the previous hop node *y*, the MAC layer of node x can measure the signal strength of the route request packet ($SS^1_{x,y}$) and the **recent signal strength ($SS^2_{x,y}$)** is obtained from the neighbor information table(NIT) which is stored by all the neighboring nodes. The link stability is computed depending on whether the ($SS^2_{x,y)}$ is available for node y in NIT or not according to our proposed method. Two threshold values (*Thrhld1* and *Thrhld2*) are considered for admission control. Routing packets with signal strength ≤*Thrhld2* are dropped through the admission control. Routing packet with signal strength ≥ *Thrhld1* is assumed to have stability. The threshold values are under the condition that *Thrhld1* > *Thrhld2*. Link stability (LS_{xy}) between node x and y can take in only two values [0, 1].

The differentiated signal strength ($DiffSS_{xy}$) between nodes x and y indicates whether the signal strength is going stronger or weaker. U_1 is a threshold for Differentiated signal strength to handle small variations in signal strength due to temporary environmental factors like fading and interference. U_2 (>U_1) is used for detection of situations where two nodes go away from each other with high speed. Link Uncertainty (LU_{xy}) is a binary flag between nodes *x* and y, that means the link's stability cannot be determined due to lack of its recent signal strength value $SS^2_{x,y}$ in NIT. Link stability LS_{xy} is stated by the formula

$$\mathbf{LS_{xy} = (U_2 - DiffSS_{xy})/ (U_2-U_1)}$$

LS_{xy} : Link stability between node x and y can take in only two values [0, 1].

$DiffSS_{xy}$: Differentiated signal strength between nodes x and y indicates whether the signal strength is going stronger or weaker

U_1 : Threshold value for differentiated signal strength to handle small variation in signal strength due to fading, interference, etc.

U_2 : Threshold value for differentiated signal strength to handle small variation in signal strength when two nodes go far apart.

The link stability between node x and y are said to be stable if the following conditions are satisfied

a. If $SS^1_{x,y} \geq$ *Thrhld1*, then link is sufficiently stable and they are very close nodes. $\mathbf{LS_{xy} = 1, LU_{xy}=0}$.
b. If $SS^1_{x,y} \geq$ *Thrhld2* and node y is a new neighbor of node x, (y was not the neighbor of x). $\boldsymbol{LU_{x,y}(t_1) = 1.}$

© 2010, IJARCS All Rights Reserved

c. If $SS^{1}_{x,y} \geq Thrhld2$ and $SS^{2}_{x,y} \geq RxThrhld2$ (reception threshold) then x and y are approaching to each other, stationary or leaving each other depending on the $DiffSS_{x,y} = SS^{2}_{x,y} - SS^{1}_{x,y}$.

In all the cases here $\mathbf{LU_{xy} = 0}$.

3 (a). If $DiffSS_{x,y} \leq U_1$ we set $LS_{xy} = 1$.

3 (b) If $DiffSS_{xy} > U_1$ and $DiffSS_{xy} > U_2$ then $LS_{xy} = 0$

3 (c) $DiffSS_{xy} > U_2$ set $\mathbf{LU_{xy} = 0}$.

So the route stability of the path PS_p is defined as $\mathbf{PS_p = \Pi_{e\ \varepsilon\ P}\ LS_e}$ where *e* is a link in the path *P*, and *P* is composed of the links connecting the source to the destination. Similarly, path uncertainty of *P*, PU_P, is defined as the number of uncertain links in the path *P* from the source to the destination. Hence, the route) stability of path *P*, PS_P, is defined as follows: $\mathbf{PS_p = \Pi_{e\ \varepsilon\ P}\ LS_e}$. So, the higher is the value of path stability, the higher is the possibility of selecting the path as the most stable path provided that the path has the smallest or admissible value for path uncertainty.The RREQ/RREP packet has been modified by the addition of two new fields that is the route stability field, throughput and delay. Some of the assumptions made in the proposed system are

i. Initial route discovery latency is tolerable in the supported applications.
ii. Commutative property- if node A can hear node B, this implies that node B also hears node A.
iii. MAC protocol is used for reliable unicast communication and it solves the hidden terminal problem with the help of RTS-CTS control packets.
iv. There is a close interaction between the MAC layer and the network layer.
v. Combinatorial stability of a network is assumed; it means topology changes occur sufficiently slowly to allow successful propagation of all topology updates as necessary.
vi. Hello intervals to update neighbor information are reasonable to capture the dynamics of the network.
vii. Transmission range and carrier sensing range are assumed to be same for available band width calculation at a node.

A. Different Tables:

These tables are used in managing nodes for the route stability: **Flow table** (forreserving the required bandwidth), **Route Request forward table** (store route stability information about RREQ packets received and forwarded by an intermediate node, per unique first hop neighbor of the source), **routing table** (set up and remember the forward path and reserve path entry after processing RREP and RREQ packets, respectively), route list table(store the sorted (according to route stability value) list of received QRREQ packets to be processed for computing node-disjoint paths at the destination), **neighbor information table** (stores information about neighbors).

B. Control Packets:

These packets are used in the proposed algorithms are: **RREQ** (route request), **RREP** (route reply), **RERR**(route error packet generated after detecting link lost), **HELLO** (neighborhood maintenance, refreshing signal strength value from neighbors, and providing bandwidth reservation information),**ROUTEM** (route maintenance packet sent from the source to the destination and vice versa, to keep the secondary paths active).Whenever a source needs to communicate with a destination node, a RREQ packet is issued to get the route if the destination is unknown or if the already available route is invalid or has expired. The d_seq number filed in the RREQ message is the last known d_seq number for this destination and copied from the d_seq number field in the routing table.

The source node's s_seq number in the RREQ is the source node's own sequence number. This number is incremented prior to insertion in the RREQ. Before broadcasting the RREQ, the originating node buffers the RREQ ID and the Originator IP address (its own address) of the RREQ for PATH_DISCOVERY_TIME.

V. ROUTE DISCOVERY PROCESS

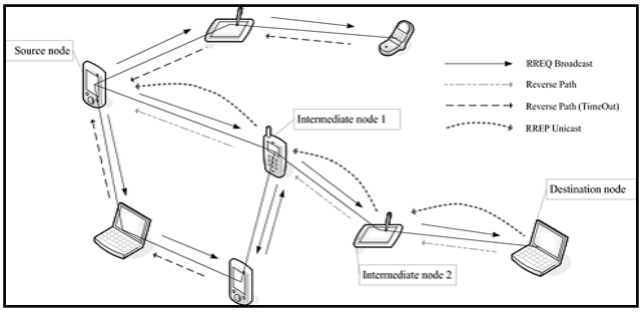

Figure 1. Route Discovery process

The control packet RREQ is modified to have extra parameters as shown

s_addr	d_addr	Broad_id	s_seq	d_seq	hop_count	Min_throughput	Max_delay	Acc_delay	APS/APU

S_addr, d_addr, s_seq, d_seq, hop_count: These fields hold the same meaning to the original AODV RREQ packet. **Sequence numbers:** these numbers are monotonically increasing numbers maintained by the source and destination node to determine the freshness of the information contained from the source node. **Min_throughput:** The throughput is set to minimum for assuring QoS requirements. **Max_delay:** This field is set to the maximum delay permissible for the packet to be routed. **Acc_delay**: stores the end-to-end delay of the explored path. **APS/APU**: store route stability of the explored path. RREQ packets are sending from the source to the neighboring nodes.

When the nodes receive with signal strength less than a threshold, $Thrhld_2$, are rejected to avoid the possibility of selecting paths with very weak links. Admission control for throughput and delay is performed on a hop-by-hop basis during forwarding of RREQ/RREP packets for QoS assurance to applications. To control the amount of broadcast of RREQ packets selective broadcast of duplicate copies of the RREQ packet is used. To eliminate formation of routing loops and prevent RREP packets to travel in the reverse direction, advertised hop count is used where each reverse routing table entry is stored with timeout period of 3 x D_{max}. After this timeout period, if no RREP packet comes, the reverse routing

© 2010, IJARCS All Rights Reserved

table entry along with any temporary entries created in the RFT for the route request is removed. The reason for setting timeout period as 3 x D_{max} is to allow the possible maximum time to receive the corresponding RREP packet. This maximum time includes the round trip time from the node to the destination, which is 2 x D_{max} and the extra processing/waiting time used in the destination, which we set in the order of D_{max}. Any duplicate QRREQ packets with a hop count less than or equal to the advertised hop count and coming through a distinct first hop neighbor of the source or through the same first hop neighbors of the source with a better route stability are forwarded by the intermediate node.

The RFT maintained in each node remembers the first hop neighbor and corresponding route stability values for the already forwarded QRREQ packets for each route request. Therefore, any QRREQ packet that arrived at an intermediate node will be dropped, if it does not pass the admission control check or cannot be forwarded due to the forwarding policy adopted as discussed above.

A. Route discovery algorithm:

Step 1:

If (no route is known in advance) t**hen**
initiate a RREQ with hop_count=0, max_hop=n, TOT_Delay = 0 Max_Delay = d.
End if

Step 2:

If (**Max_Delay** – **TOT_Delay** > LOCAL_DELAY) t**hen**

a. (Update) TOT_Delay=(TOT_Delay+ LOCAL_DELAY);
b. Record TOT_Delay of RREQ in TOT_Delay field of routing table.
c. hop_count=hop_count + 1.
d. broadcast the RREQ.

Else
Drop RREQ packet.
End if

Step 3:

If (receiving_node=R) and (TOT_Delay<Max_delay) **then**
buffer RREQ Packet.
Else
Drop RREQ packet.
End if

Step 4:

If (buffer time expires) **then**
Select two best routes with minimal delay and maximum available bandwidth respectively and make routing table entry (two routes per destination node) and unicast two RREPs in the reverse direction (for both the route).
End if

Step 5:

If (R receives RERR message and RREPFAIL=true) **then**
Select other two better routes, from buffer and unicast RREP to source.
End if

Step 6:

If (A does not receive RREP with in RREP_WAIT_TIME) **then**
Sess_id=Sess_id +1
Restart route discovery with this new sess_id.
End if

Step 7:

If (A receives a fresh RREP with same sess_id) **then**
A stores this route in its routing table as the alternate route.
End if

Step 8: END

To reduce **path diminution extra forwarding rule** is adopted. S starts a multipath discovery for D and the RREQ packet from S following the path S-A-B-I reaches node I before the RREQ packet which follows the path S-F-G-H-I. Without this special RREQ forwarding rule, node I will drop the copy of RREQ packet received from H, which will eliminate the possibility of detecting two disjoint paths. By adopting the special forwarding rule, node I will forward the second copy of RREQ, which will result in the detection of a multipath with two node-disjoint paths (S-A-B-C-D and S-F-G-H-I-D) or (S-E-B-C-D and S-F-G-H-I-D) at the destination D.

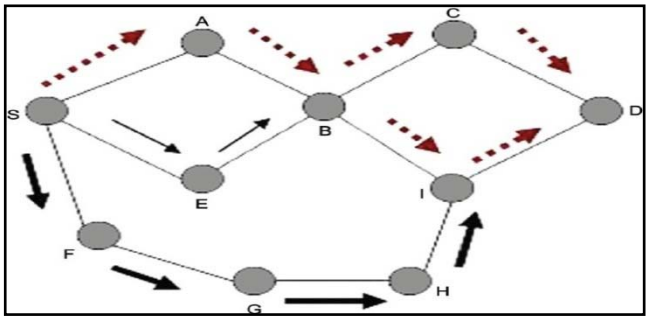

Figure 2. Multi path disjoint paths.

The **route maintenance** of the primary path as well as the secondary paths is very important. Accordingly, we have two types of route maintenance: One is due to the QoS violation on the active primary path and the other is continuous maintenance of alternate paths to ensure that only valid paths are maintained. Both of these methods reduce QoS disruptions.

VI. RESULTS

The proposed algorithm to manage the node mobility using multipath routing show better performance than the standard AODV protocol based on packet delivery ratio by 97 % in all mobility case for 10 flows. This is due to the following reasons: (i) the proposed algorithm always selects the most stable QoS path out of the selected node-disjoint paths for data transport; (ii) it performs admission control before admitting a flow in the network, thereby avoiding congested network paths; and (iii) in most of the cases, the primary route is switched before it breaks or becomes unstable due to node movements. These give rise to reduction in data packet loss during data communication. The average end-to-end delay of data packets includes (a) the waiting time in buffer during route discovery due to a route failure or recovery from QoS

© 2010, IJARCS All Rights Reserved

violation, (b) waiting time in nodes' interface queue, and (c) delays at the MAC layer during transmission/retransmission.

The selection of a QoS-aware stable node-disjoint path together with the use of stability-based route switching, admission control mechanism, and delay violation detection and recovery techniques in the algorithm significantly reduces and controls the end-to-end delay of the data packets. In our protocol, network control overhead includes both control packets generated during route discovery/recovery and due to periodic maintenance of alternate paths through *RouteM* messages. The amount of control overhead due to route discovery is more compared to the amount of control overhead due to alternate route maintenance, the first one using network-wide flooding and the second one using unicast communication. Though the overhead due to alternate route maintenance is not present in AODV, but due to its route selection procedure, most of the selected routes fail after a short period of their discovery which leads to frequent route recoveries to be initiated by the source. Due to the selection of the highly stable paths and careful selection of the alternate route maintenance period in the algorithm, its network control overhead remains lower in all mobility and traffic load scenarios.

The simulation parameters are given below

	Parameter Name	value
1.	Topology	1000 X 500 flat grid area
2.	Mobility Model	Random waypoint
3.	Channel capacity (Mb/s)	2
4.	Antenna type	Omni directional
5.	Pause Time	0
6.	No of flows	10
7.	Min B/W (Kbps)	40
8.	Max Delay(s)	0.1
9.	No of Nodes	50
10.	No of disjoint paths	(<= 3)
11.	u1, u2	0.05 X RxThr, 0.3XRxthr
12.	MAC layer	IEEE 802.11
13.	Traffic rate(packets/s)	10
14.	RouteM sending time(s)	1.0
15.	Thr1, Thr2	1.5 X RxThr, 1.2XRxThr

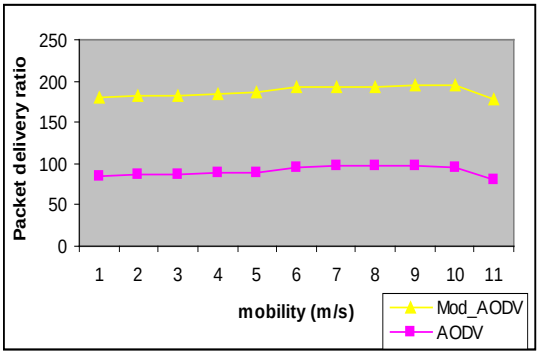

Figure. 3. Packet delivery ratio vs. node mobility (for 10 flows.)

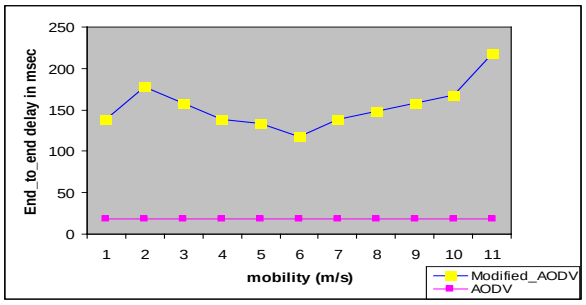

Figure 4. End to end delay vs node mobility (for 10 flows)

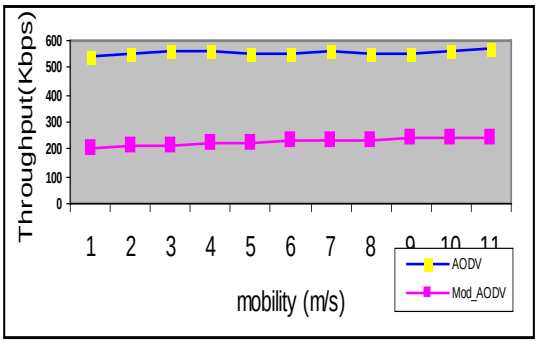

Figure. 5. Average throughput Vs Node mobility

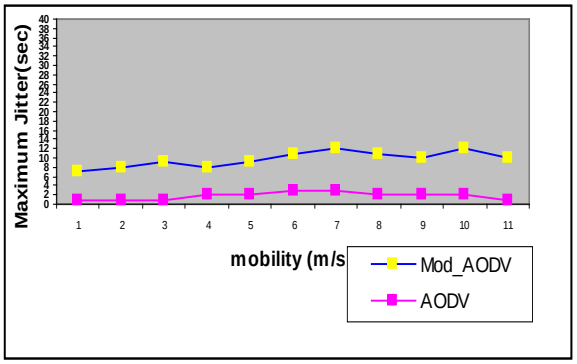

Figure 6. Maximum Jitter Vs Node mobility

VII. CONCLUSION

The methodology proposed in this paper provide throughput and delay assurance to real-time traffic in mobile ad hoc networks. The number or route recoveries required reduces by using the multipath disjoint routing where the mobility of the nodes are administered through different admission rules. Several simulation results show low end-to-end delay, high packet delivery ratio, and maximum delay jitter, especially in highly mobile scenarios without degrading network throughput. Extending the use node-disjoint paths in parallel, where the discovered node-disjoint paths will together fulfill QoS requirements of a flow while improving the network utilization, is left as our future work. It can result in admission of some flows, which otherwise are not possible due to unavailability of a single QoS capable path. The use of multiple paths in parallel needs the development of an effective packet scheduling scheme to perform load balancing and at the same time reducing packet reordering problem.

© 2010, IJARCS All Rights Reserved

VIII.REFERENCES

[1]. S. R. Das, C. E. Perkins and E. M. Royer. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. INFOCOM 2000, Tel Aviv, March 26 -30, 2000. [20] C. E. Perkins

[2]. D. B. Johnson, D. A. Maltz, and J. Broch. DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.

[3]. Dr.Yogesh Chaba and Naresh Kumar Medishetti, Routing Protocols in mobile Ad hoc Networks- A simualtion Study, Journal of Computer Science, JCS Vol.1 No.1,pp 83-88, August 2005.

[4]. Arun Kumar B. R., Lokanatha C. Reddy, Prakash.S.Hiremath, MOBILE AD HOC NETWORKS: ISSUES, RESEARCH TRENDS AND EXPERIMENTS, International Engineering & Technology (IETECH) Journal of Communication Techniques, Vol. 2, No. 2, 057-063, 2008.

[5]. Arun Kumar B. R., Lokanatha C. Reddy, Prakash.S.Hiremath, A Survey of Mobile Ad Hoc Network Routing Protocols, Journal of Intelligent System Research, 1(1) January-June 2008; pp. 49-64, Serials Publications, New Delhi, 2008.

[6]. Perkins, C.E., and E.M. Royer, 1999. Ad-hoc on demand distance vector routing, in: Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100.

[7]. Park, V.D., and M.S. Corson, 1997. A highly adaptive distributed routing algorithm for mobile wireless networks, in: Proceedings of INFOCOM-97 Volume: 3, pp. 1405-1413.

[8]. Dube. R., et. al., 1997. Signal Stability based Adaptive Routing (SSA) for Ad Hoc Mobile Networks, IEEE Pers., Communication, pp. 36-45.

[9]. Goldsmith, A.J., and S.B. Wicker, 2002. Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communications 9 (4) pp.8-27.

[10]. Acharya, A., A.Misra, and S.Bensal, 2002. A label switching packet forwarding architecture for multihop wireless LANs, in: M.Conti, D.Raychaudhuri(Eds), Proceedings of the ACM Workshop on Mobile Multimedia (WoWMoM 2002), Atlanta, GA.

[11]. C.E. Perkins, and E.M. Belding-Royer. Quality of Service for adaptive routing protocol for mobile ad hoc On-demand Distance Vector Routing", Inter Draft,)ct 2003.

[12]. N.Sharma and S. Nandi. Route stability based QoS Routing, Proc of the 10th International Symposium on wireless Personal Multimedia Communication (WPMC-2007) pp 770-3, Dec 2007.

[13]. A. Nasipuri, R Castaneda and SR Das. Performance of multipath routing on-demand protocols in Mobile Adhoc Networks, Mobile Networks and Applications vol. 6, pp 339-49, 2001.

[14]. Stojmenovic, I., and J. Wu, 2003. Broadcasting and activity-scheduling in ad hoc networks, in: S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Eds.), Ad Hoc Networking, IEEE Press Wiley, New York.

[15]. Belding-Royer, E.M., and C.-K. Toh, 1999. A review of current routing protocols for ad-hoc mobile wireless networks, IEEE Personal Communications Magazine, 46–55.

[16]. Freebersyser, J.A., and Barry Leiner, 2001. A DoD perspective on mobile ad hoc networks, in: Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, pp. 29–51.

[17]. Corson, M.S., J.P. Maker, and J.H. Cernicione, 1999. Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) pp. 63–70.

[18]. Chlamtac, I and A. Lerner, 1986. Link allocation in mobile radio networks with noisy channel, in: IEEE INFOCOM, Bar Harbour, FL.

[19]. Chlamtac, I, and A. Lerner, 1987. Fair algorithms for maximal link activation in multi-hop radio networks, IEEE Transactions on Communications COM-35 (7) pp 739-746.

[20]. Perkins, C.E., and P. Bhagwat, 1994. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers, Computer Communications Review pp. 234–244.

[21]. Chiang, C.C., H.K. Wu, W. Liu, and M. Gerla, 1997. Routing in clustered multihop, mobile wireless networks with fading channel, in: Proceedings of IEEE SICON-97, pp. 197–211.

[22]. Murthy, S., and J.J. Garcia-Luna-Aceves, 1996. An efficient routing protocol for wireless networks, ACM Mobile Networks and Applications (MONET) Journal, Special Issue on Routing in Mobile Communication Networks, pp. 183–197.

[23]. Jacquet, P, P. Muhlethaler, and A. Qayyum, 1998. Optimized Link State Routing Protocol, Internet Draft, draft-ietf-manetolsr- 00.txt.

[24]. Pei, G., M. Gerla, and T.-W. Chen, 2000. Fisheye state routing in mobile ad hoc networks, in: Proceedings of the 2000 ICDCS Workshops, Taipei, Taiwan, pp. D71–D78.

[25]. Pei, G., M. Gerla, and X. Hong, 2000. LANMAR: landmark routing for large scale wireless ad hoc networks with group mobility, in: Proceedings of IEEE/ACM MobiHOC 2000, Boston, MA, pp. 11– 18.

© 2010, IJARCS All Rights Reserved