Efficient Two Hop Local Route Repair Mechanism Using Qos-Aware Routing for Mobile Ad Hoc Networks

S. Subburam*[1] and P. Sheik Abdul Khader[2]

[1] *Associate Professor, Department of Information Technology, B.S. Abdur Rahman University Vandalur,Chennai – 600 048, India, *Research Scholar, Satyabama University.*

[2]*Professor and Head, Department of Computer Applications, B.S.Abdur, Rahman University, Chennai –600 048, India*

subburam@bsauniv.ac.in, hodca@bsauniv.ac.in

Abstract

An important challenge to enable real-time applications for MANETs is incorporating support for quality of service (QoS), such as delay and bandwidth constraints. To provide quality of service, extensions can be added to the AODV routing protocol while finding the route. These extensions specify the service requirements which must be met by nodes rebroadcasting a route request (RREQ) or returning a route reply (RREP) for a destination. In this paper, we propose an on demand delay and bandwidth based quality of service (QoS) routing protocol (AODV-D) to ensure that delay does not exceed a maximum value and the minimum available bandwidth is required to send the packets. Moreover, our proposed routing protocol will follow the concept of unicast-type two hop local route repair protocol to recover the lost links efficiently while increasing network reliability, increasing utilization, minimizing the number of control messages and shortening the repair delay. The protocol is implemented and simulated using Ns-2 simulator. The simulation studies were carried out for AODV_D , AODV,QS-AODV with different input parameters viz. number of Nodes, Node Mobility Speed; in the output parameters of packet delivery ratio, end-to-end delay and route life time was considered for all the above three protocols. The results have shown that the proposed algorithm AODV-D performed well when compared with AODV and QS-AODV.

Keywords: Mobile Adhoc Networks(MANET), Two hop local route repair, Node traversal time, Minimum Available Bandwidth, QoS-aware routing

1. Introduction

A Mobile ad-hoc network is one of the types of wireless communication networks and their characters and topology are different from other types of networks. A Mobile ad-hoc network is a group of nodes such as Mobile, Laptop and PDA that can be dynamically connected by radio waves in the fly. The host is communicating together through the transmitter and receiver. The data transmissions between the nodes are without the help of Infrastructure, Central Controller, Access Point and Base Station. In Mobile ad-hoc network, if the source node wants to communicate with destination node, they directly communicate with destination when source and destination pair is close. Otherwise, intermediate node acts as a router that help the source node communicate with the destination node. For the reasons, Mobile ad-hoc network is also called multi-hop networks. The main character of mobile node is route discovery and maintenance in the network. The MANET is self- configure, self-organized network (Moorthy and Manoj 2004). The Mobile ad-hoc networks are mainly used for military, rescue operation, audio conferencing, video conferencing, e-commerce, educations, gaming and disaster. Most recent years, the wireless ad-hoc networks support multimedia files such as data, video and voice applications (van Der Schaar M and Sai Shankar N., 2005). The usage of the mobile users is growth, so the multimedia and commercial applications are increasing for mobile users in the world. So it is needed to provide Quality of Service for such networks.

The mobile ad-hoc network does not provide quality of service guaranteed comparatively other types of networks such as GSM, Wi-Fi, Wi-MAX, UMTS and CDMA. QoS provisioning is challenging problem due to unexpected node mobility, less signal strength, low memory and low power. The mobility in Mobile ad-hoc network and the shared nature of wireless medium, offering guaranteed Quality of Service (QoS), such as delay, jitter, throughput, bandwidth, Packet delivery ratio, Packet loss rate, etc. (Lei Chen and Heinzelman WB, 2007),(Bheemarjuna Reddy T, Karthigeyan I, Manoj BS and Siva Ram Murthy C. 2006). So, stable (long life time) route is needed to maintain continuity.

Stability of the route in mobile ad-hoc network is degraded due to node mobility, less signal strength, low memory, battery capacity and processing power. So, the node drops a packet and also it cannot forward the packet to the next hop of the route. The following metrics are considering the stability such as node stability, Link stability, path stability, etc. Node Stability mainly considers the following parameters. Such as, mobility, packet transmission, battery life, and memory. If the route is break, the node stability is less. If battery life is high, the node stability is high. If the memory is high, the node stability is high. If the number of neighbor is high, the node stability is less. Link Stability is mainly consider the following factors such as pocket loss rate, channel fading rate, error rate, bandwidth fluctuation rate. If the packet is loss, then the link will be failure and degrade the stability.

If channel fading rate, bit error rate and bandwidth fluctuation is increases, the link stability is decreases. Path Stability is mainly considered the source node, intermediate node and destination node. Path stability is product of all the link stability. If the link life time is decreases, then the stability is decreases.

This paper proposes an efficient QoS-aware routing protocol for provision of end-to-end delay guarantee in mobile ad hoc networks and evaluates the performance of the proposed algorithm by simulation taking different mobility and traffic patterns. The protocol modifies and extends QS-AODV (Lajos Hanzo, Rahim Tafazolli, 2011) to discover a route with least traffic and maintain the required QoS delay constraint throughout the communication process. This algorithm selects routes with least traffic and follows alternate route method for route maintenance. The protocol estimates node delay dynamically and destination nodes monitor the healthiness of the paths by piggybacking delay information and selects better route in advance of congestion. Earlier papers(Chen L, Heinzelman W. 2005) consider only minimum number of hops as route selection metric.

The rest of this paper is organized as follows.: An overview of the Previous Research, Proposed Qos Aware Routing Algorithm based on delay and bandwidth estimation, simulations, results and the final section of the paper provided with conclusion and future work.

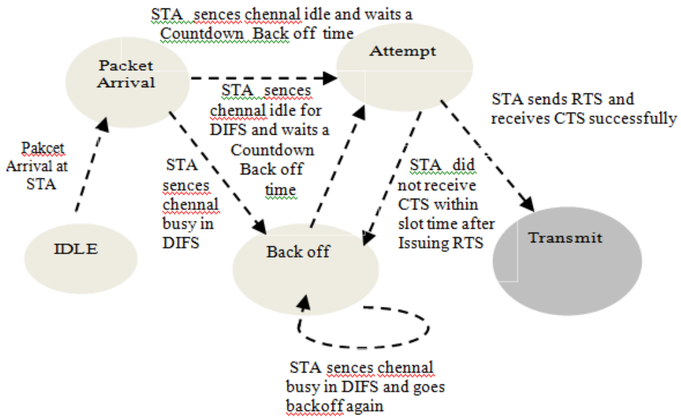
2. Previous Research

In on-demand routing algorithms such as AODV (Perkins, Royar and Das, 1999) and DSR (Johnson, Hu and Maltz, 2007), when a link is broken, the broken link drop the packet because the dropped packets are routed over the broken link and no alternate path to the destination is available. The proactive routing protocols such as DSDV (Perkins and Bhagwat, 1994) are periodically maintaining only single route per destination, each packet is unable to deliver because there is no alternate path. In (Neng-Chung and Chao-Yang, 2009), proposed a reliable QoS aware routing protocol with slot assignment for mobile ad hoc networks by constructing multiple QoS paths from source to destination node. This route must satisfy certain bandwidth requirements. In (Xue and Ganz, 2003; Chen and Nahrstedt, 1999; Chen and Heinzelman, 2005), Ad-hoc on-demand QoS routing algorithms in MANETs are used to end-to-end quality of service (QoS) in terms of bandwidth and end-to-end delay constraints. They allow estimating the available bandwidth and end-to-end delay in unsynchronized wireless environment. For mobility problems, due to the mobility of mobile nodes in MANETs, the wireless links may be easily broken. Many researchers addressed reliable routing protocols to enhance a network's stability (Chiu, Wu and Chen, 2005; Lim, Shin and Lee, 2002). Route recovery and maintenance procedures are executed, when a route is broken. However, these procedures use many resources. To minimize route breaking, it is important to find a route that endures a longer time. If a route discovery algorithm can find a stable route that endures a longer time and can reduce route discovery packets and route maintenance overheads. In (Shahram, Bita and Alimohammadi, 2011), proposed a stable QoS routing protocol which bases on the route life time that is obtained using mobility information, the residue energy and hop count. Suguna and subathra (2011) have shown that the route selection algorithm incorporates the Link Expiry Time which helps in selecting links for authentication and data communication. This enhances the stability of the certificate chain which in turn provides enhanced security. It has been found that the proposed scheme decreases the number of path changes and the time taken for authentication. Recently, many routing protocols have been proposed for MANETs that use global positioning system (Boukerche and Rogers, 2001). The coordinates of each node can be known by GPS. Further, the transmission routing protocols can complete the process of route discovery by mathematically calculating the routing. The Signal Strength Adaptive (SSA) protocol (Dube, Rais, Wang and Tripathi, 1997) uses the stability of individual links as the route selection criterion. Each node classifies its neighbors as strongly or weakly connected on the basis of link-layer beacons sent periodically. SSA ensures that the route established is strongly connected. Route Stability Based QoS Routing in Mobile ad hoc networks has been studied by Shrma and Nandi, (2010) using a simple model for computing link stability and route stability based on signal strength. Improving TCP performance in ad hoc networks using signal strength based link management (Fabius, Zhenqiang, et al, 2005), proposed a mechanisms that are based on signal strength measurements to alleviate such packet losses due to mobility and it is improve the TCP performance. QoS-Aware Routing and Admission Control in Shadow-Fading Environments for Multirate MANETs (Lajos and Rahim, 2011), proposed new solution for improving the performance of QAR and AC protocols in the face of mobility, shadowing, and varying link SINR. It is found that proactively maintaining backup routes for active sessions, adapting transmission rates, and routing around temporarily low SINR links can noticeably improve the reliability of assured throughput services.

3. Proposed Qos Aware Routing Algorithm based on delay and bandwidth estimation

For route selection, proposed algorithm considers not only those routes which have total path delay less than or equal to that specified in the route request but also it will consider the minimum bandwidth availability. For calculating path delay, it estimates current delay [Murthy CSR, Manoj BS, 2004] at each node. For calculating path bandwidth , it estimates minimum available bandwidth will be satisfied at each node. For route maintenance, each node in the path piggyback the delay information to data packets, so that destination node can initiate for finding alternate route in advance of congestion. In this section, we describe our proposed protocol which includes calculation of FORWARDING_DELAY or TRAVERSAL TIME and Bandwidth estimation at each mobile node, initiation of route discovery and route maintenance processes.

Fig.1. *State transistion diagram of a mobile node*



3.1 Calculation of the Node Traversal Time

Fig. 1 shows the simplified transition state diagram of STAi (node i) attempts to transmit packets in IEEE 802.11 standard. The Traversal time at a mobile node STAi is calculated as per the following equation given in (1).

$$D^{i}delay = P^{i}idle(DIFS) \text{ X } (DIFS + b + EA(i)) + (1-P^{i}idle(DIFS)) \text{ X } (DIFS + EB(i)) + T_{trans} \quad (1)$$

where

$$EA(i) = Pi_{idle}(slot) \text{ X } (RTS + 2.SIFS + CTs) + (1-Pi_{idle}(slot)) \text{ X } (RTS + 2.SIFS + EB(i)) \text{ and}$$

$$EB(i) = [1/ \{P^{i}idle(DIFS) \text{ X } (slot)\}] \text{ X } [P^{i}idle(DIFS) \text{ X } (DIFS + b + RTS + 2.SIFS + Piidle(slot) \text{ X } CTS) + (1-P^{i}idle(DIFS)) \text{ X } B]$$

The value obtained from equation (1) for node i is named as TRAVERSAL TIME. In wireless links, the propagation delays are very small and almost equal for each hop along the path because of limited length of link. So, here we assume that the propagation delay is negligible.

3.2 Route Discovery Process

To provide quality of service (end-to-end delay), extensions are added to the RREQ (Fig. 4), RREP (Fig. 5) and RERR messages in addition to the extensions needed in the routing table structure of AODV protocol (Fig. 6). A node which receives a RREQ with a quality of service extension must agree to meet that service requirement (delay bound) in order to rebroadcast the RREQ. The RREQ includes a QoS object extension (Max_Delay) which specifies delay parameter. This Max_Delay extension is appended to a RREQ by a node requesting a QoS route in order to place a maximum bound on the acceptable time delay experienced on any acceptable path from the source to the destination. In order to enable the measurements to be accumulated for end-to-end delay, AODV also provides an Accumulated Value extension field (Acc_Delay) in the RREQ message. It provides information about the cumulative value that has been experienced by nodes along the path from the originating node to the node currently processing the RREQ. Route entries are created for every pair of source and destination i.e. for each session of communication since each session may have different delay requirement. Initially the value of Acc_Delay in a RREQ packet is set to zero. A node that agrees to satisfy delay constraints has to measure the average time it is currently requiring to forward a data packet. We call this average time the TRAVERSAL TIME, which is calculated as per equation (1) at every node. RREQ forward or drop is based on the delay demanded is illustrated in Fig. 2. When a route is required but no information to the destination is known, the source node floods the RREQ packet to discover a route . Maximum Delay, indicates the maximum number of seconds allowed for a transmission from a source to the destination. Every time a node receives a RREQ it subtracts the NODE TRAVERSAL TIME, which is the time required by this node to process the RREQ. If the NODE TRAVERSAL TIME is bigger than the delay time indicated in the RREQ the node will simply discard the RREQ. At every step the delay field in the RREQ message is reduced by the Traversal Time of the router. At the end egress D will reply a RREP message which will have a starting delay value of 0. This delay value will be added to the Traversal time of each node and registered (cached) in the Routing Table for future RREQs. The caching of the delay value will make the future discovery of that route a trivial task. So for example, when another RREQ is requested by Ingress node A , will be directly dropped by core node B since the demanded delay can't be met if the demanded delay is (10ms) because accumulated delay is (80ms). Of course in the future a node, such as core C, may have increased load which would change it NODE TRAVERSAL TIME from 50ms to 100ms. This change would affect all depending nodes such as B and A. For this reason node C will forward an ICMP QOS LOST message to all potentially nodes affected by the QoS parameter. This is also the reason why each node had initially stored a list of depending nodes, the "List of Sources Requesting Delay Guarantees". The ICMP QOS LOST message is quite short and it is sent recursively to all nodes affected. Then destination node selects an optimal route and a RREP packet is transmitted along the reverse route. RREQs received after generation of RREP are also buffered and used for route maintenance phase. In AODV, RREP packet can be created by the destination node or an intermediate node with a "fresh enough" route to the destination [4]. But, RREP packet can only be generated by the destination node in AODV-D, because it has to ensure that total path delay must satisfy the QoS delay requirements of a session.

Fig.2. *RREQ forward or drop is based on the delay demanded*

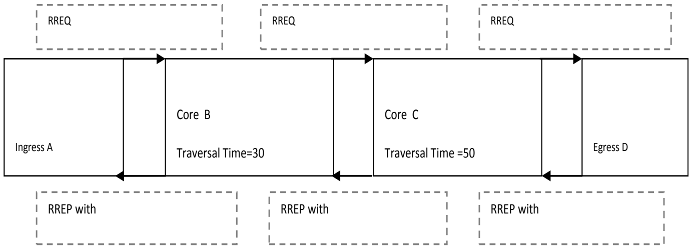


Fig.3. *RREQ forward or drop is based on the bandwidth demanded*

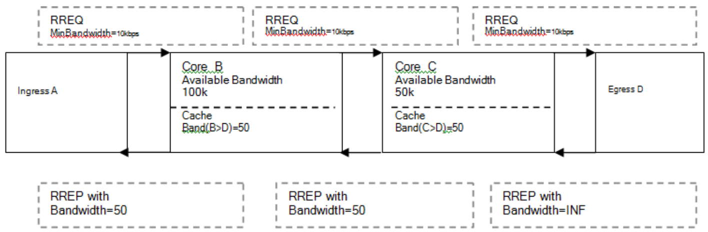


Fig.4. *Routing table entry structure in AODV and AODV-D*

(a) AODV

Dest address	Dest Seqno..	Session_ Id	No of Hop	Next hop	Time out	Active Neighbors of the route	Expira-tion Time

(b) AODV-D

Dest address	Dest Seqno..	Session _ Id	No of Hop	Next hop	Time out	Active Neighbors of the route	Expiration Time	Max_ Delay

Fig.5. *RREQ format for AODV and AODV-D*

(a) AODV

Source address	Dest address	Source Seq no.	Dest Seq no.	Broadcast_Id	Hop count

(b) AODV-D

Source address	Dest address	Source Seq no.	Dest Seq no.	Broadcast _Id	Session _ Id	Acc_ Delay	Max_ Delay

Fig.6. *RREP Format for AODV and AODV-D*

a) AODV

Source address	Dest address	Dest Seq no.	Session _ Id	hop count	Time out

(b) AODV-D

Source address	Dest address	Dest Seq no.	Session _ Id	hop count	Acc-Delay	Time out

Figure 3 is illustrated in RREQ forward or drop is based on the bandwidth demanded .Minimum Available Bandwidth, is a field which indicates the requested amount of bandwidth for a specific link (route). Every time a node receives a RREQ it must compare its available link capacity with the capacity of bandwidth requested in the RREQ. If the requested bandwidth is not available then the node will again, as the delay example, discard the RREQ and not process any further. If the bandwidth is available then the request will process until the egress router D is reached. At that point the egress router D, will respond with a RREP message which will be initialized with a bandwidth value equal to infinitive (a very large number). Each node forwarding the RREP compares the bandwidth field in the RREP and its own link capacity and maintains the minimum of the two in the Bandwidth field of the RREP before forwarding the RREP. This bandwidth value will be registered (cached) in the Routing Table bandwidth value for future RREQs. The caching of the bandwidth value will again make the future discovery of that route a trivial task. which makes the protocol handling violation of QoS parameters an a' posteriori approach instead of reserving the "promised" We can see again that another RREQ (which is route discovery message from A to D) request won't be satisfied because its request is 80Kbps exceeds the available 50Kbps which is now cached in nodes' B cache and hence be directly dropped by core node B.

3.3 Route Maintenance

AODV-D tries to maintain the QoS delay constraint throughout the session by selecting alternate path(s). During data transmission, each mobile node appends the delay information to the data packets. Each packet header is time stamped when the mobile node receives a packet. Let ai and bi denote the arrival and successful transmission time of the ith packet respectively.After the ith packet's successful transmission at a node p, the estimated average total node delay qp which includes contention, queuing and transmission delays at node p is computed as per the following equation (2) [. H. Song, V. Wong, and V. C. M. Leung,2003].

$$QPI =(1-\alpha)\, Q^{P}_{I}-1+ \alpha(b_{i-1}-a_{i-1}) \qquad (2)$$

where i>1, 0 . . . 1 , and a_{i-1} and b_{i-1} are arrival and departure time stamps of previous packet i-1.

Thus, destination node monitors the route capacity to serve the QoS requirements of a session. If total path delay reaches the maximum limit the destination selects next better route from the buffered active routes, those routes whose ROUTE EXPIRARY [4] time are not expired. If buffer does not contain any fresh routes then it generates RERR packet in advance of congestion. When a link breaks, then AODV-D try to rebuild the broken link by doing Efficient local route repair mechanism. It will follow the concept of an unicast-type two hop local repair protocol to recovery the lost links efficiently while increasing network reliability, increasing utilization, minimizing the number of control messages and shortening the repair delay. Meanwhile, the optimal number of hops of neighbor table is also analyzed.

3.4 Data Structures Used

Each node of the ad hoc network keeps and maintains a neighbors table, a sessionID table, a route_buffer table, a route table and a reverse route table. The neighbors table is used to records neighborhood information. The sessionID table is used to record the current pair of source address, destination address and sessionID. The route_buffer table is used to store alternate routes available to each session while the route table is used to store routing information for every session.

3.5 Pseudocode of Delay Estimation

The steps of the proposed delay estimation algorithm are as under.

Route Discovery:

Step 1: **if** Ingress A has data packets to send Egress D
and no route is identified to the targeted node
then
{
initiate a RREQ with Maximum_Delay =x
Where x is the Maximum_delay in seconds and
set Cumulative_delay = 0
Also each node along the path calculates its
own traversal time as per equation (1) and records in
its routing table NODE TRAVERSAL TIME field.
}

Step 2: Difference = Maximum _delay – Cumulative_

Step 3: **if** (Difference > NODE TRAVERSAL TIME)
then
{
Update Cumulative_delay of RREQ as
Cumulative_delay =(Cumulative_delay +
NODE TRAVERSAL TIME);
Store Cumulative_delay of RREQ in Cumulative _delay field of routing table
Again broadcast the RREQ
}
else
Drop RREQ packet

Step 4: **if** destination node D that is Egress receives
RREQ message and if it satisfying the QoS delay parameter
then
buffer it.

Step 5: **if** buffer time expires
(NODE_TRAVERSAL X NETWORK_DIAMETER)
then
{
select a route with minimal travelsal time and
make routing table entry and unicast the
RREP in the backward direction towards the
Ingress.
}

Step 6: **if** egress node receives RERR message
with a RREPFAIL flag,
then
select a fresh route, next better route, from buffer
and unicast RREP to Ingress

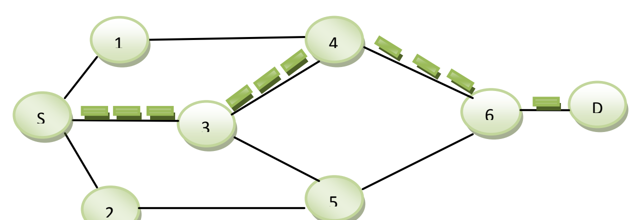
Step 7: **if** Ingress does not receive RREP in
RREP_WAIT_TIME from destination
then
restart route discovery with new session Id.

Step 8: **if** S receives a fresh RREP with same session Id
then
divert data transmission through new route.

4. Efficient Two Hop Local Route Repair Mechanism

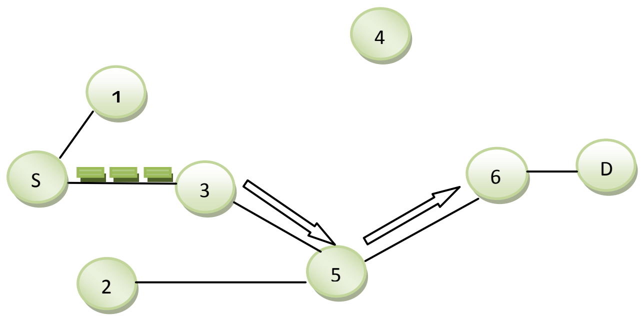
In MANETs, a set of nodes are used to route the data from source to destination and it is assumed that nodes are distributed over the entire region. Connectivity between any sources to destination pair in the network exists when they are in radio range of each other. The technique used to deal with the issues called Local route repair. It is an important issue in routing protocol which is needed for minimizing flooding and performance improvement. Local Repair is one of the major issues in the protocol; routes can be locally repaired by the node that detects the link break along the end to end path. Local Repair will increase the routing protocol performance. Although the local repair mechanism works with a specified TTL to limit the repair range of RREQ, large number of the broadcast RREQ messages result in extensive control messages and obvious power consumption for transmitting these broadcast messages . In our Proposed Local route repair AODV is extended with an Efficient two hop local route repair mechanism to minimizing the flooding.

Fig.7. *Existing path*



In Figure 7 ,Source node send the data packet through the path S->3->4->6->D.In this path if link breakage occurred because of mobilty of node 4 means we follow the concept of two hop local route repair approach.This method will maintain the information of two hop neighbor nodes and to repair broken links.For example, in figure 8,node 3 will get the another neighboring node 5 from the two hop neighbor table. After determining the optimal substitute node from the extended routing table and the multihop neighbor table, a set of unicast-type repair messages are proposed instead of broadcast-based in AODV to repair broken links efficiently while reducing large control overhead significantly. The unicast-type multihop repair approach consists of four unicast-type repair messages, including FREQ (Fixed Request), FREP (Fixed Reply), FERR (Fixed Error) and FUPDATE (Fixed Update). The functions of FREQ, FREP and FERR are similar to the function of RREQ, RREP and RERR in AODV, respectively.So new path S->3->5->6->D will be formed.And the data packet will send through the alternate path.

Fig.8. *Alternate path*



5. Pseudocode of Route Maintenance

Step 1: **If** a node receives link break
Then
perform two hop local route repair
Step 2: **If** local repair successful
Then
{
update the route table **Else** send RERR to source and invalidate the associated route entry
}

Table 1. *Simulation Parameters*

Parameter	Value
Topology	1000mX 1000 m
No of Nodes	50
Mobility Model	Random way point
CBR sending rate (Packets/sec)	8 m/s
Pause Time	0
Transmission range	250 meters
Propagation model, Antenna type	Two-ray ground reflection, omni directional
Simulation Time	900s
Packet Size	512 bytes
Data Traffic	CBR
MAC Layer	IEEE 802.11 DCF
No of Flows	10

6. Simulations.

6.1 Simulation Setup

Fig.9. *Network Topology*

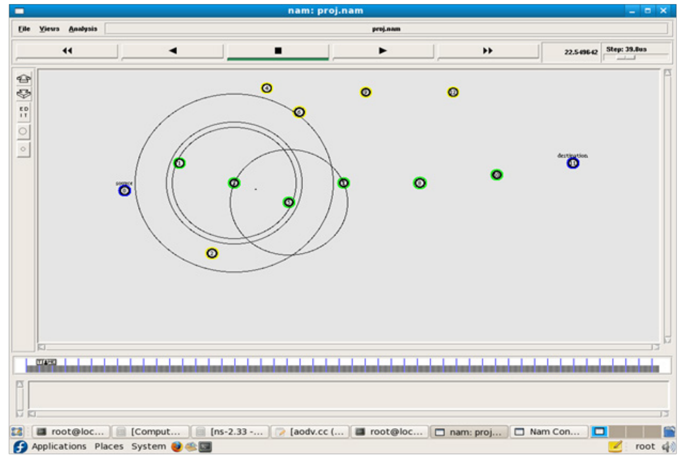


Fig.10. *Existing route*

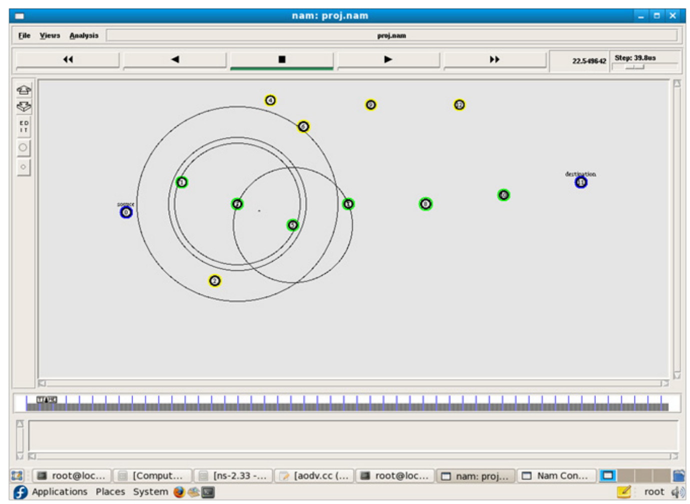
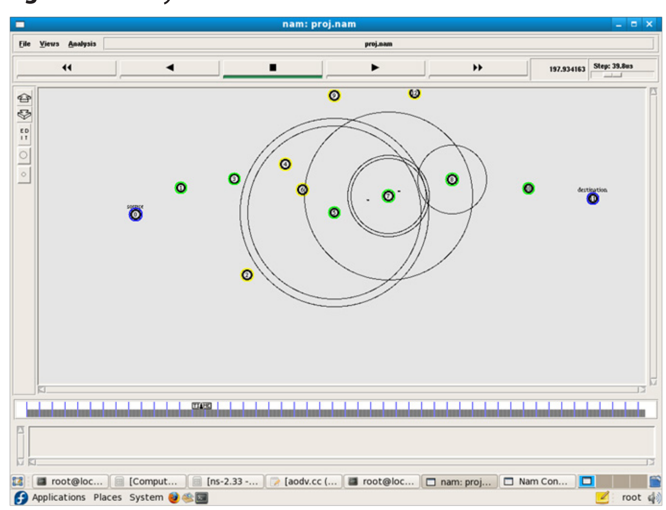


Fig.11. *Mobility of Nodes*



The performance of QoS-aware Routing protocol (AODV-D) has been compared with the QS-AODV (Perkins CE, Royar EM, Das S 1999) , DSR (Johnson D, and Hu Y, Maltz D 2007) protocols. The proposed simulations were conducted in the ns-2 simulator

[18,20]. The QS-AODV and AODV protocols simulations were implemented by ns-2 simulator. The network terrain area is 1000X1000 m2. This network is a homogeneous network. So the two-ray ground reflection channel with the radio transmission range per node is 250m assumed and is same for all nodes in the network. The data transmission rate is 2 Mbps, each run has been executed for 1000 sec of simulation time. Traffic source is based on Constant Bit Rate (CBR). The packet sending rate is 4 data packet per second. The packet size is 512 bytes long. It is assumed 50 nodes move over the network area. Mobiles nodes are assumed to move randomly according to the random waypoint model [24]. The pause time is zero seconds and the maximum speed of the mobile node is set to 0, 2, 4,8,10,12,14,16 and 18 m/s for different simulation runs. The metrics used to assess the performance of proposed QoS-aware Routing protocol against the QS-AODV and AODV are the packet delivery ratio and End-to-End delay. The detailed simulation parameters are summarized in Table 1.

Figure 9,10,11,12,13 illustrated the sample screen shots of Network Topology, Existing route, Mobility of Nodes, Link Breakage and Alternate path respectively. The above simulation snapshot has one source and destination nodes. The packet transmission is between source and destination pairs.

Fig.12. *Link Breakage*

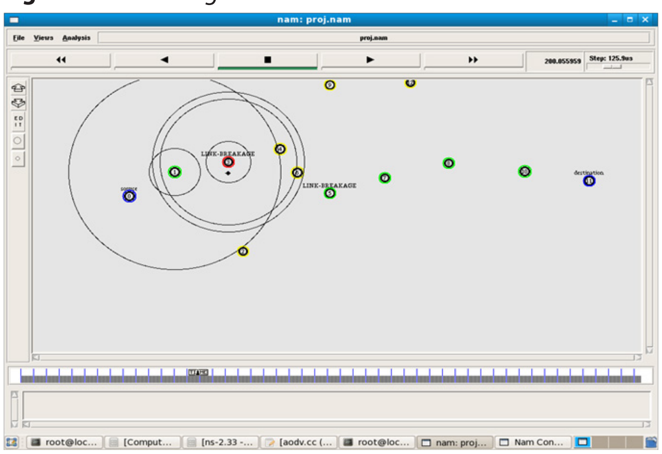
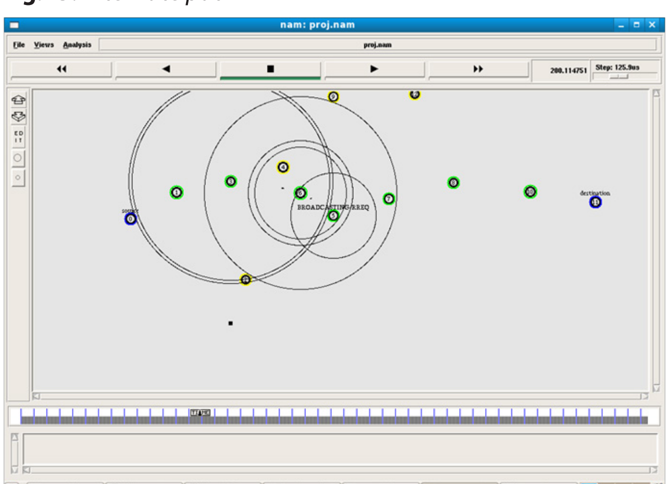


Fig.13. *Alternate path*



6.2 Performance Metrics

We use the following metrics to quantify the performance. Packet Delivery Ratio (PDR): The ratio between the number of packets originated by source and the number of packets received by the destination.

End-to-End delay: The average time between sending the packets at the source and receiving the packet at destination.

Route Life Time : It is the period of time taken during which the route remain connected.

7. Results

7.1 Analysis of packet delivery ratio (PDR)

Fig.14. shows the packet delivery ratio against the node mobility speed. In this experiment, maximum mobility speed from 10 km/h to 100 km/h with increment step of 10. It is observe that the packet delivery ratio of all routing protocols decreases as the node mobility speed increases. If node speed increases, the probability of link failure will more. As a result, AODV-D has highest packet delivery, QS-AODV is next level of packet delivery ratio and QS-AODV has the last packet delivery ratio. Because of the QS-AODV and AODV does not consider stability. So it has the packet drop rate is high.

Fig.14. *Packet Delivery Ratio vs. Node Mobility Speed (km/h) for 10 flows*

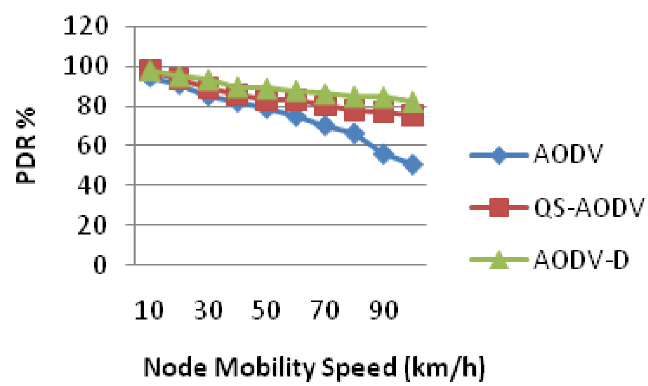


Fig.15. *Packet Delivery Ratio vs. Number of Nodes for 10 flows*

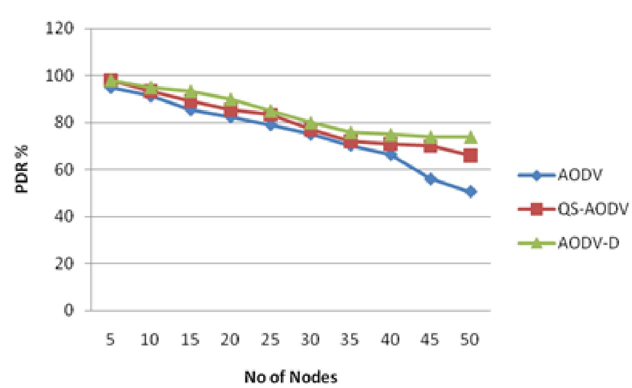


Fig. 15 shows the packet delivery ratio against the no of nodes. In this experiment, maximum node from 5 to 50 with increment step of 5. It is observe that the packet delivery ratio of all routing protocols decreases as the number of nodes increases. As a result, AODV-D has considerably better than QS-AODV, QS-AODV is better than AODV and AODV has the lowest packet delivery ratio. The numbers of nodes increases, the density will increases. So the packet delivery ratio decreases.

Fig.16. *Average End-to-End delay vs. Node Mobility Speed (km/h)*

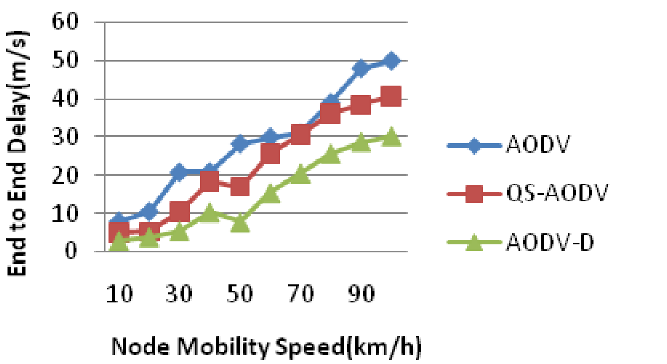


Fig.17. *Average End-to-End delay vs. Number of Nodes*

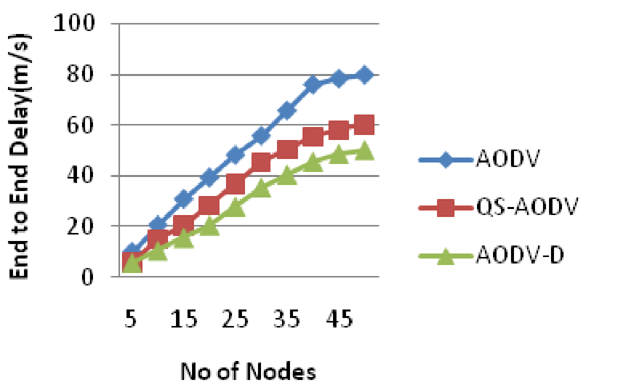
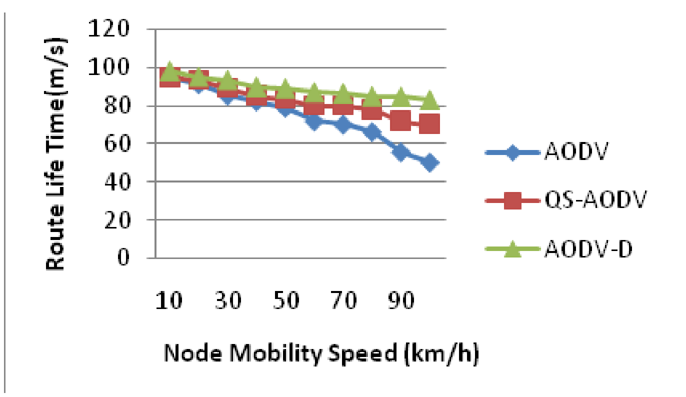


Fig.18. *Route Life Time vs. Mobility (m/s) for 10 flows*



7.2 Analysis of average end-to-end delay

Fig. 16 shows the average End-to-End delay of data packets vs. node mobility speed (km/h). If nodes mobility increases, the end-to-end delay of data packets also increases. This is because the paths frequently move between source and destination and path break. Comparing the result shown in this fig. 9, it can be seen that AODV-D has shortest end-to-end delay than QS-AODV and AODV. Route failure probability is reduced in AODV-D.

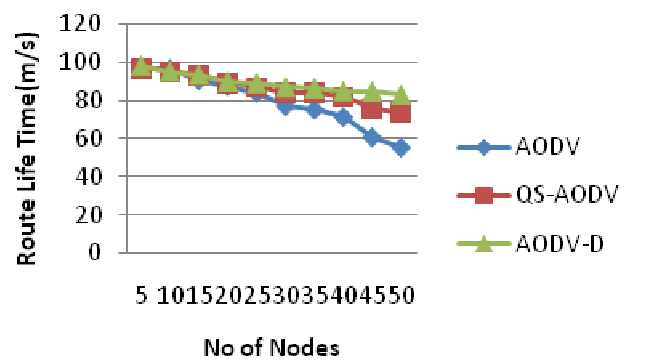
Fig. 17 shows the Average End-to-End delay of data packets vs. Number of Nodes. If the number nodes increase, the end-to-end delay of data packets also increases. Because of node density will increases. As a result, the AODV-D is better than QS-AODV and AODV.

7.3 Analysis of Route life time

Fig. 18 shows the Route Life Time vs. node mobility speed (km/h). If nodes mobility increases, the route life time is decreases. In mobility, the route is break continuously. But the AODV-D protocol design consider with signal stability and boundary level. So the route life time is increases better than QS-AODV and AODV.

Fig. 19 shows the simulation results of the route life time of AODV-D, QS-AODV and AODV in 1000 X 1000 m2 area. We observe that the route life time of our proposed routing protocol is longer than that of the other QS-AODV and AODV. The main reason is that we took into account the Efficient two hop Local Route repair mechanism using QoS-aware routing to design the protocol.

Fig.19. *Route Life Time vs. Number of Nodes for 10 flows*



8. Conclusion

In this paper, we review the current research on QoS routing algorithms in MANET. Although all of the research focuses on different problems, they are highly related to each other and have to deal with some common difficulties, which include mobility, limited bandwidth and power consumption, and broadcast characteristic of radio transmission. QoS in Manets is a new but rapidly growing area of interest. This great research and market interest is firstly because of the rising popularity and necessity of multimedia application and secondly because of the potential commercial usage of Manets. Thus QoS support in Manets has become an unavoidable task. QoS routing in Mobile Ad hoc network is a rather hot concept in computer communications. This means that there is much research going on and much issue that remains to be solved.Moreover we developed a efficient two hop local route repair mechanism using QoS-aware routing protocol(AODV-D) for mobile ad hoc networks . This routing protocol satisfies End-to-End delay, Packet Delivery Ratio and Route Life Time constraints. It is observed that the AODV-D algorithm achieves high performance with high packet delivery ratio, End-to-End delay and Route Life Time compared to the Ad-hoc On-demand Distance Vector (AODV) routing algorithm and QS-AODV.

9. References

1. Murthy C S R, Manoj B S, Ad Hoc Wireless Networks: Architecture and Protocols, Pearson Education: India, (2004), pp.213-214.
2. van Der Schaar M, Sai Shankar N, Cross-layer wireless multimedia transmission: challenges, principles, and new paradigms, Wireless Communications (2005), Vol.12, pp.50-58, DOI: 10.1109/MWC.2005.1497858.
3. Lei Chen, Heinzelman W B. A Survey of Routing Protocols that Support QoS in Mobile Ad Hoc Networks. Network (2007), Vol. 21, pp.30-38, DOI: 10.1109/MNET.2007.4395108.
4. Bheemarjuna Reddy T, Karthigeyan I, Manoj BS, Siva Ram Murthy C, Quality of service provisioning in ad hoc wireless networks: a survey of issues and solutions, J*ournal of Ad Hoc Networks (2006)*, Vol.4, pp.83-124, DOI: 10.1016/j.adhoc.2004.04.008.
5. Perkins C E, Royar E M, Das S, Ad-hoc On-Demand Distance Vector (AODV) Routing, Proceeding of the IEEE Workshop on Mobile Computing Systems and Applications (1999), pp.90-100. DOI: 10.1109/MCSA.1999.749281.
6. Johnson D, Hu Y, Maltz D. The Dynamic Source Routing Protocol (DSR), IETF mobile ad hoc networking Working Group INTERNET DRAFT (2007), RFC 4728.
7. Perkins C E, Bhagwat P, Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers. Computer Communication Review (1994), pp.234-244. DOI: 10.1145/190314.190336.
8. Neng-Chung Wang, Chao-Yang Lee, A reliable QoS aware routing protocol with slot assignment for mobile ad-hoc networks, *Journal of Network and Computer Applications (2009*), pp.1153-1166.
9. Xue Qi, Ganz Aura. Ad hoc QoS on-demand routing (AQOR) in mobile ad hoc networks, *Journal of Parallel Distributed Computing (2003)*, Vol.63, pp.154-165, DOI: 10.1016/S0743-7315(02)00061-8.
10. Chen S, Nahrstedt K. Distributed Quality-of-Service Routing in *Ad Hoc Networks. Communications (1999)*, Vol.17, pp.1488-1505, DOI: 10.1109/49.780354.
11. Chen L, Heinzelman W, QoS-aware routing based on bandwidth estimation for mobile ad hoc networks. *IEEE Journal on Communications (2005)*, Vol.23, pp.561-572, DOI: 10.1109/JSAC.2004.842560.
12. chiu C Y, Wu H K, Chen G H. Stability Aware Cluster Routing Protocol for Mobile Ad Hoc Networks, Proceeding of the 9th International Conference on Parallel and Distributed Systems (2002), pp.471-479. DOI: 10.1109/ICPADS.2002.1183441.
13. Lim G, shin K, Lee S, Ma JS. Link stability Route life time in Ad Hoc Wireless Networks. Proceeding of the International IEEE Conference on Parallel Processing Workshops (2002), pp.116-123. DOI: 10.1109/ICPPW.2002.1039720.
14. Suguna M, Subathra P. Establishment of Stable Certificate Chains for Authentication in Mobile Ad Hoc Networks. International IEEE Conference on Recent Trends in Information Technology (2011), pp.234-239. DOI: 10.1109/ICRTIT.2011.5972278.
15. Shahram Jamali, Bita Safarzadeh, Hamed Alimohammadi. A stable QOS-aware reliable on-demand distance vector routing protocol for mobile ad-hoc networks. Scientific Research and essays (2011), pp.3015-3026.
16. Boukerche A, Rogers S G P S Query Optimization in Mobile and wireless Networks. Proceedings of the sixth IEEE conference on symposium (2001), pp.198–203. DOI: 10.1109/ISCC.2001.935375.
17. Rappaport T S. Wireless Communications: Principles and Practice; Prentice-Hall: India, (1995), pp.110-120.
18. Fall K, Varadhan K. The ns Manual, (2001).
19. Dube R, Rais P C, Wang K, Tripathi S K, Signal Stability Based Adaptive Routing for Ad Hoc Mobile Networks, IEEE Personal Communication (1997), pp.36–45, DOI: 10.1109/98.575990.
20. The Network Simulator – ns-2 available at http:/www.isi.edu/nsnam/ns/.
21. Sarma N, Nandi S, Route Stability Based QoS Routing in Mobile ad hoc networks. *Journal of Wireless Press Communication (*2010), Vol.54, pp.203-224, DOI: 10.1007/s11277-009-9718.
22. Fabius Klemm, Zhenqiang Ye, Srikanth V. Krishnamurthy, Satish K, Tripathi. Improving TCP performance in ad hoc networks using signal strength based link management, Ad hoc Networks (2005), Vol.3, pp.175-191.
23. Lajos Hanzo, Rahim Tafazolli. QoS-Aware Routing and Admission Control in Shadow-Fading Environments for Multirate MANETs. *IEEE Transactions on Mobile Computing (2011)*, Vol.10, pp.622-637.
24. Bettstetter C, Hartenstein H, PereZ-Costa X. Stochastic Properties of the Random-Way Point Mobility Model. *Wireless Networks 2004*, Vol.10, pp.555-567.
25. J H Song, V Wong, and V C M. Leung, "Load-Aware On-Demand Routing (LAOR) Protocol for Mobile Ad Hoc Networks", roc. of IEEE Vehicular Technology Conference, Jeju, Korea, April 2003.