Paper

On-demand QoS and Stability Based Multicast Routing in Mobile Ad Hoc Networks

P. I. Basarkod and Sunilkumar S. Manvi

Department of Electronics and Communication Engineering, Reva Institute of Technology and Management, Bangalore, India

Abstract—Finding a connection path that remains stable for sufficiently longer period is critical in mobile ad hoc networks due to frequent link breaks. In this paper, an on-demand Quality of Service (QoS) and stability based multicast routing (OQSMR) scheme is proposed, which is an extension of ad hoc on-demand multicast routing protocol (ODMRP) to provide QoS support for real time applications. The scheme works as follows. Each node in the network periodically estimates the parameters, i.e., node and link stability factor, bandwidth availability, and delays. Next step is creation of neighbor stability and QoS database at every node by using estimated parameters. The last sequence is multicast path construction by using, route request and route reply packets, and QoS and stability information, i.e., link/node stability factor, bandwidth and delays in route information cache of nodes, and performing route maintenance in case of node mobility and route failures. The simulation results indicate that proposed OQSMR demonstrates reduction in packet overhead, improvement in Packet Delivery Ratio (PDR), and reduction in end-to-end delays as compared to ODMRP, and Enhanced ODMRP (E-ODMRP).

Keywords—mobile ad hoc network, mobility, multicast routing, QoS, stability.

1. Introduction

Mobile Ad hoc Networks (MANETs) are self-organizing networks consisting of mobile nodes which can be rapidly deployable in emergency situations like battlefields, earthquakes, tsunami, floods, or any major disaster areas. MANETs are deployed without base stations and do not have wired infrastructure. They must adapt to traffic and node mobility patterns. In MANET, a mobile node can act as a router as well as a host. Two nodes can communicate with each other eventhough they are outside their transmission range. The successful communication in such a situation depends upon the intermediate node mobility and failure probability [1].

Normally, MANETs are used for group communications, where multicast protocols are efficient compared to unicast protocols since they improve the efficiency of the wireless links in MANETs and when an application demands for sending multiple copies of messages from multiple sources to multiple receivers. Multicasting reduces the communication costs by sending the single copy of the data to multiple recipients rather than sending multiple copies by using multiple unicasts. Thus it minimizes the link bandwidth, processing, and transmission delay [2].

In broad sense, there are two types of multicast protocols: mesh and tree based. Tree based structures are not stable since they need to be reconstructed when topology is changing frequently [3]. Once the tree is established, a packet will be sent to all nodes in the tree. A packet traverses each node and link only once. It is not suited for MANETs since the tree could break any time due to changes in the topology. Therefore, focus of this work is on mesh based routing since it provides better service when a network is highly dynamic.

A mesh based structure can have multiple parents and a single mesh structure can connect all multicast group members with multiple links. When a primary link breaks away due to mobility of a node, alternate links are immediately available. For long duration connections, nodes/links on a path must be stable so that connection failures can be reduced. Stable connection facilitates data transfer without interruption. The probability of route failure can be reduced by lowering either the link failure rate or the number of links that compose the route. It is important to note that delay bounded route selection avoids larger delays.

Constructing and maintaining a multicast mesh should be simple so as to keep minimum control overheads. Most of the multicast routing protocols require periodic transmission of control packets in order to maintain multicast group membership; thus requires more bandwidth. The objective of presented work is to design and analyze a multicast mesh based on-demand routing scheme in MANET, which is enhanced version of On-Demand Multicast Routing Protocol (ODMRP), to provide bandwidth satisfied, reliable and robust route.

The rest of the paper is organized as follows. Section 2 presents an overview of existing MANET multicast protocols, Section 3 discusses the proposed work in detail. Simulation and result analysis are presented in Section 4, and conclusions and future works are given in Section 5.

2. Related Works

With the rapid development of multimedia applications in MANETs, there is an increasing need for QoS guarantee for a real time application. Therefore, protocols designed for MANETs should involve satisfying application requirements while optimizing network resources. In the design of routing protocols, finding the stability of nodes play an important role in establishing a stable and QoS path that offers better packet delivery ratio and low latency.

ODMRP is a protocol which makes use of group of forwarding nodes to establish a mesh of nodes for every multicasting group [4], [5]. The work on ODMRP in [6], considers node's energy in route selection from source to destination and results confirm that there is an improvement in stability of the route due to low energy consumption based routes.

In [7], E-ODMRP is presented which is an enhancement of ODMRP. It does not have the forwarder lifetime where as ODMRP's forwarder has a timeout which is 3 times the refresh interval. The route refresh rate is dynamically adapted to the environment rather than refreshing at fixed intervals as in ODMRP, which is a key parameter that has critical impact on the network performance.

In [8], the stable paths are found based on selection of forwarding nodes that have high stability of link connectivity. The work given in [9], proposes a QoS – aware Multicast Routing Protocol (QMRP) based on mesh architecture which offers bandwidth guarantees for applications in MANETs. QMRP takes an adaptive approach and starts with single path routing. When a single path routing fails, it switches to multipath routing by adding new searching.

In [10], a Source initiated Mesh based and Soft-state QoS Multicast Routing Protocol (SQMP) for MANETs is proposed. The ant colony optimization technique is used for finding best route to its destination through the cooperation with other nodes. In [11], a weighted multicast routing algorithm for MANET is proposed to find stable routes in which the mobility parameters are assumed to be random variables with an unknown distribution.

In [12], a stability-based unicast routing mechanism is discussed in which both link affinity and path stability are considered in order to find out a stable route from source to destination. It is then extended to support multicast routing where only local state information (at source) is utilized for constructing a multicast tree. The work given in [13], proposes a new algorithm for tree-based optimization. The algorithm optimizes the multicast tree directly, unlike the conventional solutions which find paths and integrating them to generate a multicast tree. The fuzzy logic modified Ad hoc On-demand Distance Vector (AODV) routing protocol for multicast routing in MANETs is discussed in [14]. The fuzzy weighted logic multi-criteria are based on the parameters like remaining battery power of the nodes, number of hop-counts and sent packets.

In [15], a multi-constrained QoS multicast routing scheme is presented using genetic algorithm. The scheme applies limited flooding using the available resources and minimum computation time in a dynamic environment. In [16], only the nodes that satisfy the delay requirements are used to flood the route request messages. The nodes are modeled as M/M/1 queuing systems, in which delay analysis is made based on random packet arrival, service process, and random channel access.

The Mesh-evolving Ad hoc QoS Multicast (MAQM) routing protocol presented in [17], achieves multicast efficiency by tracking the availability of resources for each node within its neighborhood. The QoS status is observed continuously and updated periodically to perform QoS provisioning. In [18], authors have evaluated the performance of mesh and tree-based multicast routing schemes relative to flooding, and also proposed two variations: flooding, scoped and hyper flooding, as a means to reduce overhead and increase reliability, respectively.

In [19], a multi-path QoS multicast routing (MQMR) protocol is proposed. The scheme offers dynamic time slot control using a multi-path tree. Work given in [20], proposes a novel Efficient Geographic Multicast Protocol (EGMP). EGMP uses a virtual-zone-based structure to implement scalable and efficient group membership management.

Effective transmission power control is a critical issue in the design and performance of wireless ad hoc networks. Current design of packet radios and protocols for wireless ad hoc networks are primarily based on common-range transmission control. The work given in [21], analyzes some of the widely used routing protocols with varying transmission range, mobility speed and number of nodes.

The work given in [22], uses the mobility and link connectivity prediction to find routes and forwarding groups, and to reconstruct the path in anticipation of topology changes. The Associativity-based Ad hoc Multicast (ABAM) protocol given in [23], establishes multicast session on-demand and utilizes an association stability concept, which refers to spatial, temporal connection and power stability of node with respect to neighbors. The protocol improves throughput and has low communication overhead. In [24], Selfish Check Negotiation Protocol (SCNP) is presented which allows nodes to negotiate for collaboration. The impact of being selfish and unselfish used in network communication performance are discussed.

In [25], authors present the Multimedia Broadcast/Multicast Service (MBMS) extension, that allows multiple variants of the same content to be economically distributed to heterogeneous receivers, explicitly taking into account the possibility of using either dedicated or common radio channels. In [26], a novel analytical method for performance prediction estimation of single- and multi-layer Multistage Interconnection Networks (MINs) under multicast environments is presented. The "Cell Replication While Routing" is used as a packet routing technique, and the "full multicast" mode as transmission policy is employed in all the MINs under study. The work presented in [27], estimates and selects core for reducing multicast delay variation for delay sensitive applications in Delay Variation Bounded Multicast Tree (DVBMT).

Adaptive Demand-Driven Multicast Routing protocol (ADMR) presented in [28], supports source specific multicast joins and to route along shortest paths, and uses no periodic network-wide floods of control packets, periodic

neighbor sensing, or periodic routing table exchanges, and requires no core.
A reliable ODMRP is proposed in [29], for preferable throughput. It constructs multicast routing based on the cluster, and establishes a distributed mechanism of acknowledgment and recovery of packet delivery. A single forwarding path created in ODMRP is vulnerable to node failures, since a set of misbehaving or malicious nodes can create network partitions and mount Denial-of-Service (DoS) attacks. Resilient ODMRP (RODMRP) [30], offers more reliable forwarding paths in face of node and network failures and DoS attacks.

3. Proposed Work

This section presents node and link stability, bandwidth and delay estimation models, route discovery and maintenance phases.

3.1. QoS Metrics

The authors propose certain parameters to describe the Quality of Connectivity (QoC) for extracting the stable and QoS links connecting a pair of nodes over time. This is used as a criteria for route selection algorithm. Reliable network requires more stable nodes and high quality links which satisfy bandwidth and delay as QoS constraints. The set of forwarding nodes with higher stability can improve the routing performance. This section presents stability, bandwidth and delay estimation models used in presented scheme.

3.1.1. Node Stability

The stable nodes are necessary in forwarding group to provide better packet delivery services. Node stability in terms of movement around its current position gives an idea of stationary property of node. The authors use node stability metric from their previous work given in [31], to identify stable nodes in a path for forwarding packets from a source to multicast group.
Two metrics to represent node stability as the quality of connectivity is identified: *self stability*, and *neighbor nodes stability*. The steps in finding the stability of a node are as follows:

- all the nodes in MANET find the self stability, i.e., node movement relative to its previous position,
- find neighbors stability of all the nodes in MANET by considering the neighbors self stability. Each node in a MANET will compute the node stability factor based on self stability, and neighbor nodes stability.

Self stability. It can be defined as the node's movement with respect to its previous position. If a node is trying to move away from its position, the distance of the movement and transmission range decides the stability. A node is said to be stable if its movement is within given fraction of its transmission range. Consider the scenario as shown in Fig. 1, where a node with transmission range r moves from position (x_r, y_r) to (x_n, y_n) in a given time window by a distance d.

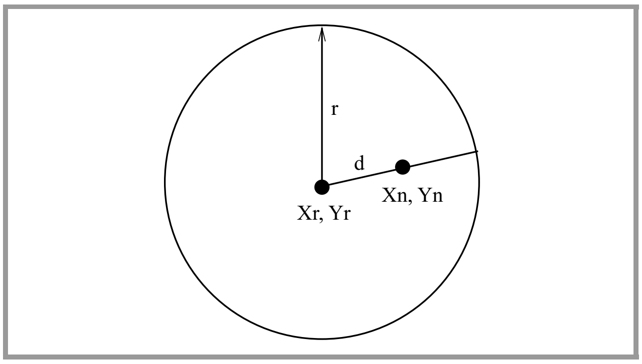

Fig. 1. Node movement.

When a node moves out from its previous position to the next position, its position stability keeps changing with respect to the distance moved. This change in distance (d_i^t) of a node i, in a time window t is estimated by using Eq. (1).

$$d_i^t = \sqrt{(x_n - x_r)^2 + (y_n - y_r)^2}\,. \qquad (1)$$

Based on the movement of the distance at every time window, the self stability metric $S_s(t)$ can be estimated as given in Eq. (2). $S_s(t)$ varies in the range 0 to 1. When the movement distance d_i^t of a node increases from its previous position, the self stability value will decrease. For the requirement of the higher degree of movement stability, $r/2$ can be replaced by $r/4$ or $r/8$.

$$S_s(t) = \begin{cases} 1 - \dfrac{d_i^t}{r/2} & \text{if } 0 \le d_i^t < r/2 \\ 0 & \text{otherwise} \end{cases}\,. \qquad (2)$$

There are some limitations in calculation of self stability due to influence of GPS accuracy and resolution. Better results can be estimated with higher accuracy and resolution in GPS. This work assumes that GPS accuracy and resolution is limited to 95% and 7.8 meters, respectively [32].

Neighbor node stability. It can be defined as how well a node is being connected by its neighbor in terms of their self stability. The nodes can exchange messages with each other, if they are within the transmission range. Each node accumulates connectivity information and signal stability of one hop neighbors, and maintains a neighbor list.
The degree of a node n is represented as number of links (or nodes) connected to it, and is denoted as ND. The neighbor node stability of a node $N_s(t)$ with respect to neighbors at time t can be expressed as in Eq. (3):

$$N_s(t) = \alpha \times \frac{1}{ND}\sum_{i=1}^{ND} {S_s}^i(t) + (1-\alpha) \times N_s(t-1)\,, \qquad (3)$$

where α is the weightage factor (lies between 0 and 1), and is distributed between 0.6 and 0.7, since they yield better results in simulation. $N_s(t-1)$ is the recent neighbor node stability, $S_s{}^i(t)$ is the self stability of neighbor node i. The authors are using the stability model to select nodes with higher self and neighbor stability values such that the selected path through such stable nodes stays for a longer duration.

3.1.2. Link Stability

Link stability between the nodes indicates quality and life time of the connection. The link stability estimated in the scheme is based on two parameters: received signal strength and life time of the link.
The Algorithm 1 represents a pseudocode for updating link stability status between the nodes. The different parameters used in the algorithm are as follows:

- lifetime – duration of continuous connectivity between the nodes,
- lifetime threshold – indicates the maximum limit of link lifetime that decides link stability,
- link stability status – is a boolean variable that defines link stability between the nodes,
- recent – indicates most recent response received for a Hello packet from a neighbor,
- P – number of Hello packets,
- received signal strength – is the strength of signal received from a neighbor,
- signal threshold – is an acceptable signal strength to be received from neighbors.

Algorithm 1: Link stability status between the nodes

```
P = No_of_Hello_Packets;
lifetime = 0;
link_stability_status = 0;
Recent = 0;
lifetime_threshold = P × Hello_Packet_Interval;
while P > 0 do
    if received_signal_strength ≥ signal_threshold then
        lifetime = lifetime + 1;
        Recent = 1;
        P = P − 1;
    else
        Recent = 0;
        P = P − 1;
    end if
end while
lifetime_sec = lifetime × Hello_Packet_Interval;
if (lifetime_sec > lifetime_threshold) and (Recent)
then
    link_stability_status = 1;
else
    link_stability_status = 0;
end if
```

Following parameter values are considered in Algorithm 1: the signal threshold = -8.9 dB [33], No. of Hello Packets = 4, Hello packet exchange interval = 60 s, and lifetime threshold is three times of the Hello packet exchange interval. A typical neighbor information for a node with neighbors A, B, C, etc., is given in Table 1. It comprises of neighbor Id and its related information such as neighbor stability factor, link stability factor, recent, lifetime, and link stability status. For every neighbor node, link and node stability factor will be estimated as discussed in Subsection 3.1.3.

3.1.3. Stability Factor

This section describes computation of stability factor by using node and link stability factor.

Node stability factor. First there is need to map the self stability, and neighbor nodes stability on to a single metric called node stability factor, Nsf. This can be expressed as in Eq. (4). The $Nsf(t)$ in time interval t represents the stability of node at a given time interval with respect to its neighbor movement from their respective positions. Higher the value of $Nsf(t)$ indicates better stability

$$Nsf(t) = f(S_s(t), N_s(t)) = \beta S_s(t) + (1-\beta) N_s(t) . \quad (4)$$

The weight factor β denotes the relative importance of the quantities $S_s(t)$ and $N_s(t)$. It is assumed the value of β to be distributed between 0.6 and 0.7, since they yield better results in simulation.
Stability factor of a node is computed only if self stability and neighbor stability is greater than zero. Thus this scheme extracts the highly stable nodes and adjusts the network topology, so as to reduce the probability of route failure.

Link stability factor. A node is capable of estimating its neighbor's time of connection called as life time of a node. The node is assumed to be aware of its direct (or immediate) neighbor's relative speed, called as v. The relative speed is calculated based on [34]. Let's denote the range of a node as r, and the distance moved by the node as d. The remaining distance is (r–d) for which connectivity may still exist. A relationship between these parameters when the link_stability_status = 1, is given in Eq. (5), called as link stable duration (Lsd):

$$Lsd = \frac{(r-d)}{v} . \quad (5)$$

Link stable duration can be normalized by using a lifetime_threshold (LTT), which has a higher value than any Lsd's may be observed. Normalized Lsd, denoted as link stability factor, Lsf at a given time interval t is given in Eq. (6):

$$Lsf(t) = \begin{cases} \dfrac{Lsd}{LTT} & \text{if } Lsd \leq LTT \\ 1 & \text{otherwise} \end{cases} . \quad (6)$$

Table 1
Neighbor information table

Neighbor Id	Neighbor stability factor	Link stability factor	Recent	Lifetime	link_stability_status
A	0.9	0.2	0	3	0
B	0.8	0.4	1	4	1
C	0.6	0.3	0	3	0
...	...	...	...	...	...
...	...	...	...	...	...

Stability-Factor-Between-Nodes. Proposed routing scheme makes use of node stability factor coupled with link stability factor called as Stability Factor Between Nodes (SFBN). SFBN is used for QoS based applications to find the route from a source to destination. SFBN (a normalized value) is given in Eq. (7), which helps in selecting stable nodes and links for routing in multihop networks which can stay together for a longer duration

$$SFBN(t) = \frac{1}{2}\big(Nsf(t) + Lsf(t)\big). \tag{7}$$

The path from source to multicast group will be forwarded through intermediate links, and the link with minimum SFBN is selected as PathSFBN at a given time interval t. This is given in Eq. (8), and is denoted by PathSFBN for N intermediate links

$$PathSFBN(t) = \min(SFBN_i(t)); \forall i = 1 \ldots N. \tag{8}$$

3.1.4. Delay Estimation

For delay estimation, an arbitrary node that contributes to traffic forwarding using the M/M/1 queuing system is modeled. This queue represents a single queuing station with a single server [35]. The authors assume that the contributing nodes are served by a single server with first come first serve queuing policy. Packets arrive according to a Poisson process with rate λ, and the probability distribution of the service rate is exponential, denoted by μ. The maximum size of the queue in every node is represented by K.

To satisfy delay requirements in multimedia real time applications, packets must be received by multicast receivers which satisfies the application delay constraints. When a packet is to be sent either by a source node or forwarding group of nodes; it experiences three types of delays: queuing, contention and transmission delay. The total delay considered over a link between two nodes is given by

$$d_{Total} = d_Q + d_C + d_T. \tag{9}$$

The queuing delay denoted by d_Q is the delay between the time the packet is assigned to a queue and the time it starts transmission. During this time, the packet waits while other packets in the transmission queue are transmitted. This is the amount of time a packet is spent in the interfacing queue. The average contention delay, denoted by d_C is the time interval between the time the packet is correctly received at the head node of the link and the time the packet is assigned to an outgoing link queue for transmission by the physical medium. The transmission delay denoted by d_T is the one between the times that the first and last bits of the packet are transmitted over the physical medium successfully. In proposed model, every node will estimate single hop delay with its neighbor nodes. The maximum value of d_{Q+C} is approximated as the ratio of maximum queue size over the service rate in a node, and is given by

$$d_{Q+C} \approx \frac{K}{\mu}. \tag{10}$$

Transmission delay. Transmission mechanism used for multicasting is different from unicast in random access wireless communications. To transmit data packets over a physical media, random access MAC model is employed. Source node uses carrier sense multiple access with collision avoidance protocol (CDMA/CA) to avoid packet collision.

When a node has data to send, it senses the physical medium. If the medium is idle, the packets are injected into the network. Otherwise, it waits until the medium gets idle and then it counts down a certain period of time called back-off time before sending a data packet. When backoff reaches zero, the packet is transmitted. When a collision is detected, the contention window size is doubled and the process is repeated. After a fixed number of retry attempts, the packet is dropped. The time for which channel is available for an arbitrary node with ϕ interfering nodes can be expressed as

$$d_{BussyChannel} = \frac{\phi \times m}{bw}, \tag{11}$$

where m represents the packet size and bw denotes the single hop bandwidth between two nodes. Therefore the time that the channel is available for data transmission in time unit (1 s) is

$$d_{FreeChannel} = 1 - d_{BussyChannel} = 1 - \frac{\phi \times m}{bw}. \tag{12}$$

The service time can be defined as

$$T_{serviceTime} = \varepsilon + \frac{m}{bw}, \tag{13}$$

where ε is the duration of the back-off time during which channel keeps sensing for idleness. The packet will be transmitted if the backoff window counts down to zero. In fact this time depends on the network load, since the process of countdown will be halted because the medium is found to be busy. The pausing period of a packet stops transmitting, which depends on the backoff interval and this in-turn depends on the network load. Finally, the mean transmission time required to transmit a packet is defined as the ratio of the service time over the fraction of time the channel is free. Hence, mean transmission delay is

$$d_T = \frac{\varepsilon + \frac{m}{bw}}{1 - \frac{\phi \times m}{bw}}. \quad (14)$$

Now, the total single hop delay between two nodes is the sum of all the delays mentioned in Eq. (9), and it is

$$d_{Total} = d_{Q+C} + d_T = \frac{K}{\mu} + \frac{\varepsilon + \frac{m}{bw}}{1 - \frac{\phi \times m}{bw}}. \quad (15)$$

By using Eq. (15), each node will estimate the single hop delay. The path delay or end-to-end delay from source to destination is the delay through intermediate links and is additive in nature. It is given by Eq. (16), denoted by $Delay(P_i)$ where P_i is the i-th path, N is the number of intermediate links, and for each path:

$$Delay(P_i) = \sum_{j=1}^{N} d_{Total_j}. \quad (16)$$

3.1.5. Bandwidth Estimation

The bandwidth information is one of the important metric of choice for providing Quality of service (QoS). The authors considered their previous work presented in [36], to estimate the available bandwidth based on the channel status of the radio link to calculate the idle and busy periods of the shared wireless media. By observing the channel utility, the measure of the node activities can be taken as well as its surrounding neighbors and thus obtain good approximation of bandwidth usage.

In IEEE 802.11 MANETs, due to the contention based channel access, a node can only transmit data packets after it gains the channel access. Hence, a node first listens to the channel and estimates bandwidth by using the idle and busy times for a predefined interval. This is expressed in following equation

$$BW = \frac{T_{idle}}{T_{interval}} \times C, \quad (17)$$

where T_{idle} denotes the idle time in an interval $T_{interval}$, and C denotes the channel capacity. $T_{interval}$ comprises of the following time periods: idle time of the channel T_{idle}, time taken for actual transmission of the data T_{tx}, time taken for retransmission of packets T_{rtx}, and time taken for backoff $T_{backoff}$. Equation (17) can be rewritten as

$$BW = \frac{T_{idle}}{T_{idle} + T_{tx} + T_{rtx} + T_{backoff}} \times C. \quad (18)$$

The time periods are measured individually and are incorporated in estimating the bandwidth. The path from source to destination will be forwarded through many intermediate links, and the link which is having minimum bandwidth (bottleneck BW) will be selected as Path bandwidth as given in Eq. (19) denoted by PathBW for N intermediate links

$$PathBW = min(BW_i) \quad \forall i = 1 \ldots N. \quad (19)$$

3.2. Route Establishment

OQSMR is an enhancement of ODMRP, since it is designed to reduce repeated usage of control packets, so that bandwidth consumption can be reduced. There are incorporated changes in structure of ODMRP route request (Join Query) and route reply (Join Reply) packets along with forwarding mechanism of route request packets. The databases for routing include QoS and Stability factors. The request and reply packets include QoS and stability factors.

Route establishment process of OQSMR makes use of parameters like SFBN, delay estimation and available bandwidth information at each node. It considers a stability and QoS database at each node for route request propagation and path(s) finding between source to multicast receivers. The scheme also uses a routing information cache at each node that facilitates route finding by providing path information. This will reduce route request propagation overheads. This section presents stability and QoS database (NSQB), route request (RR) packets, route reply (RP) packets, route error (RE) packets, and routing information cache (RIC).

3.2.1. Neighbor Stability and QoS Database

When a node establishes connections with its one hop neighbors, it maintains a database. This database contains information regarding neighbors that include: id of neighbor, its SFBN, bandwidth and delay values.

To explain the fields of the NSQB, let's consider the network topology given in Fig. 2, where S, A, B, C, R1, and R2 are the nodes connected in the network. S is the source

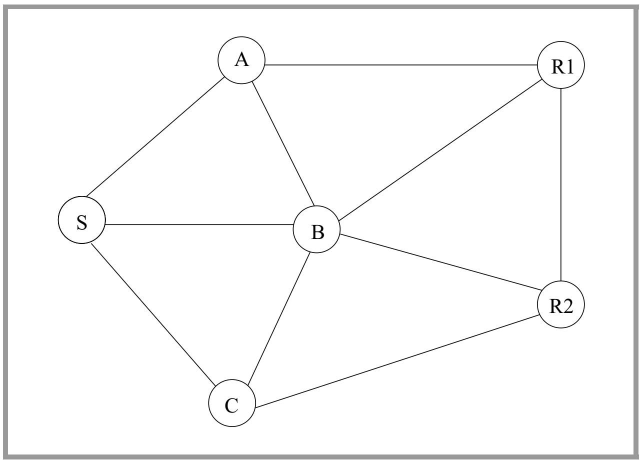

Fig. 2. Network topology.

Table 2
Neighbor Stability and QoS Database (NSQB) at source node S

Neighbor id	SFBN	BW [Mb/s]	d_{Total} [ms]
B	0.58	2.2	10
C	0.6	2.4	9.8
...	...	...	...
...	...	...	...

node, R1 and R2 are the receiver nodes and remaining are the intermediate nodes. The links between two nodes which are having SFBN below the SFTH will not be selected. The authors have found through simulation that SFTH with values between 0.5 to 0.9 and end-to-end delay threshold of 100 to 200 ms yield better PDR and reduced latency. Table 2 shows a typical neighbor information table for source node S. The information in the table are neighbor id, SFBN, available estimated bandwidth (BW), and single hop delay, d_{Total}.

3.2.2. Route Request, Route Reply and Route Error Packets

To create a multicast stable QoS route in a MANET from source to group of receivers, various control packets such as route request (RR), route reply (RP) and route error (RE) packets are used. In this section, some of the control packet components required for multicast stable QoS path creation are described, and handling link failure situations are shown. Some important fields of RR packet are:

- Source address – it is the address of the source from where the path has to be established to the multicast receivers. It originates the packet.
- Multicast receivers address – group of receivers address where packet has to be forwarded. It helps in accommodating the routes created by RR packets and RP packets.
- Time to live – it is the number of hops RR packet can travel. The value is decremented by one every hop.
- Next hop address – it is the address of the neighbor connected with in the transmission range for propagating RR and RP packet.
- Sequence number – the sequence number assigned to every packet delivered by the source that uniquely identify the packet. It is used to avoid multiple transmission of the same RR packet.
- Route record – it has the addresses of the visited previous nodes recorded in visiting sequence. This information will be used during the return journey to RR packet originator by corresponding RP packet.
- SFBN record – it has the values of SFBN associated with each link which are visited in sequence from the source to group of receivers. This will help in finding PathSFBN, which will be used by RP packet to update RIC.
- Available bandwidth record – it is the estimated available bandwidth value associated with each link visited in sequence from source to group of receivers. This will help in finding path available bandwidth, which will be used by RP packet to update RIC.
- Delay record – it is the estimated delay associated with each link visited in sequence from source to group of receivers. This will help in finding the total path delay, which will be used by RP packet to update RIC.
- Application bandwidth requirement – it is bandwidth required by an application at the source node.

RP packet format for multicast creation is almost similar to RR packet with few changes. The changes in RR packet to convert it into RP packet are as follows. When RR packet reaches any of the group receivers, source address and receiver address are interchanged, SFBN record will be replaced by PathSFBN, bandwidth record will be replaced by path available bandwidth, delay value will be replaced by the end-to-end delay and contents of route record will be reversed. RP packet from group of receivers will be sent to source on a route given in its route record.

RE packet is generated when a node is unable to send the packets. Some of the fields of this packet are source address, receivers address, sequence number. Whenever a node identifies link failures, it generates RE packet to either source or nearest receiver. If link failure occurs in forward journey of a RR packet (from source to multicast receivers), RE packet is sent to the source. On the other hand if link failure occurs for reverse journey of the RP packet (from particular receiver to the source), RE packet is sent to that receiver. Nodes receiving RE packet updates their route information cache by removing paths having failed links and also examine its route cache for an alternate path. If an alternate path is found, it modifies the route, otherwise packet is dropped.

3.2.3. Routing Information Cache

Routing Information Cache (RIC) is used to store the latest routes to group of receivers learned through RR and RP packets. This avoids unnecessary route discovery operation each time when a data packet is to be transmitted. This reduces delay, bandwidth consumption, and route discovery overhead. A single route discovery may yield many routes to the group of receivers, due to intermediate nodes replying from local caches. When source node learns that a route to a particular identified receiver is broken, it can use another route from its local cache, if such a route to that receiver exists in its cache. Otherwise, source node

Table 3
Routing Information Cache at source node *S*

Receiver's address	Path information	PathSFBN	RPathBW [Mb/s]	Delay [ms]	Rec-Timestamp [H:Min:Sec]
R1	S-A-R1	0.6	1.8	100	0:0:0.4
	S-C-R2-R1	0.8	1.6	120	0:0:0.6
R2	S-C-R2	0.7	1.0	89	0:0:0.8
...	...	...	...	...	...
...	...	...	...	...	...

initiates route discovery by sending a route request. Use of RIC can speed up route discovery and it can reduce propagation of route requests. The contents of RIC will be removed at every periodic interval, if it is not updated for certain time (may be 180 to 360 s).
Each node in the network maintains its own RIC that aids in forwarding packets to neighbors. For every visited RP packet at a node, RIC is updated by using some of the fields in RP packet required for establishing stable QoS paths. Table 3 presents a typical RIC at node S for topology given in Fig. 2. Various Fields in the table are explained as follows:

- Receivers address – it is the address of the node where packet has to be forwarded (extracted from RP packet destination address and route record). It helps in accommodating the routes for RR packets.
- Path information – it represents a complete path (a sequence of links).
- PathSFBN – it is the combined stability factor of path as given in Eq. 8.
- Delay – it is the end-to-end delay to meet the total delay constraint of the application as given in Eq. 16, and it must be less than the threshold value.
- RPathBW – it is the remaining path bandwidth which is the difference of PathBW and application bandwidth.
- Recorded timestamp – it contains the time at which RIC is updated by using RP packet.

3.3. Route Discovery Process

Multicast stable QoS path creation involves two phases: a request and a reply phase. Request phase invokes route discovery process to find routes to group of receivers using stable and QoS intermediate nodes. Reply phase involves updating of RIC and conforming the routes found in request phase. Stable nodes are the one who satisfy stability criteria based on our module given in Subsection 3.1 as well as accommodate bandwidth and delay requirement of application. These stable and QoS nodes act as intermediate nodes that help to create multicast mesh from source to group of receivers.

3.3.1. Request Phase

This section presents the process of request phase, reply phase, and route maintenance that helps in discovering a path.
A source node finds the route to its group of receivers by using RR packets. The sequence of operations that occur are as follows:

1. Source node prepares a RR packet with application bandwidth and delay requirements.
2. Selective transmission of RR packet to neighbors who satisfy stability criteria, i.e., SFBN greater than SFTH, and bandwidth requirement, i.e., estimated bandwidth greater than twice the application requirements.
3. A node receiving RR packet will discard it, if it is already received (by using sequence number and source address).
4. If RR packet is not a duplicate, checks RIC for availability of route; if available, RP packet will be generated and start reply propagation to source.
5. If RR packet is a duplicate, then discard it and stop transmission of RR packet.
6. If not duplicate and no route available in RIC, transmit the RR packet by updating its fields (route record, SFBN record, bandwidth record, delay record, time to live, and nexthop address) to its neighbors as in step 2.
7. Perform steps 3 to 6 until destination is reached.
8. If receiver is not reached within certain hops, send RE packet to the source node.

Figure 3 illustrates the basic operation of route request phase for the network topology of Fig. 2:

- Source node S prepares a RR packet with application bandwidth and delay requirements.
- Broadcasts RR packet to discover the routes to multicast receivers R1 and R2.

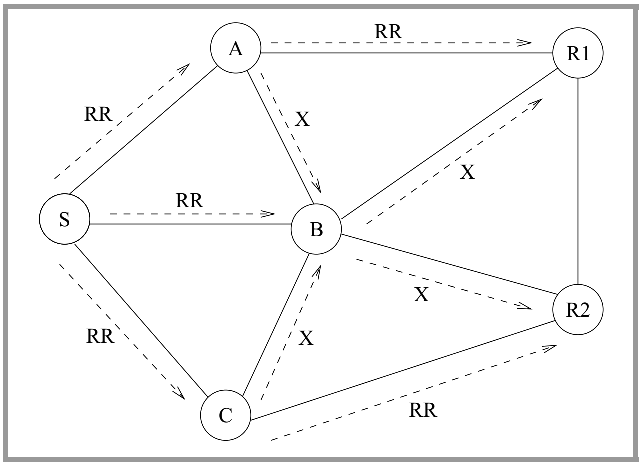

Fig. 3. Route request paths from S to R1 and R2.

- Nodes A, B and C receive RR packet from source S, with assumption that they satisfy the SFBN, BW and delay requirements.
- Check RIC for availability of route at A, B and C to R1 and R2.
- Node A broadcasts RR packet to R1 and B. Node C broadcasts to B and R2. Node B broadcasts to A, R2, R1 and C.
- Node B finds that the packets received through A and C are same as that received by S. Thus duplicate packets are eliminated, as indicated by cross mark in Fig. 3. Similar elimination of duplicated packets are done at nodes A and C which are being received by B.
- R1 and R2 eliminates duplicate packets from nodes B and C respectively.
- If A, B and C have no direct routes to R1 and R2, they update and modify the RR packet (for route record, SFBN record, BW record, end-to-end delay, Time to live and next-hop add) and transmit to next forwarding group of nodes.
- As R2 and R1 are the receiver nodes, they updates RIC and modify the RR packet.
- Finally now, R1 and R2 have paths to the source S: R1-A-S, R1-B-S, R2-C-S, and R2-B-S.

3.3.2. Reply Phase

Multicast receivers initiates the reply phase. When RR packet reaches the receiver node, following operations are performed in the reply phase.

1. RP packet is generated from RR packet by performing following changes in RR packet; receiver and source node addresses are interchanged, route record is reversed, update SFBN record with PathSFBN, update bandwidth record with PathBW and delay record with end-to-end delay.
2. Update RIC at receiver node with receiver id, path information, PathSFBN, PathBW, delay and time.
3. RP packet is forwarded to nexthop node as per the route record if PathBW, and end-to-end delay are satisfied.
4. Node receiving RP packet checks whether available PathBW is greater than application requirement, and end-to-end delay less than the delay threshold, if so, updates RIC by using contents of RP packet. Updates will happen only if current time is greater than the time recorded in RIC. If bandwidth is not available, and end-to-end delay not less than the threshold, send RE packet to receiver and visited intermediate nodes to stop RP packet propagation.
5. Perform steps 3 and 4 until source is reached.
6. If source is not found due to link breaks, send RE packet to the receiver.
7. The source node chooses one of the received paths with higher bandwidth availability and delay with lesser time and keeps other paths as backup paths.

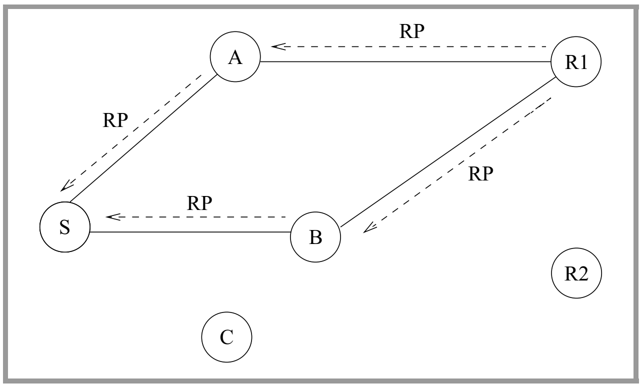

Fig. 4. Reply paths from R1 to S.

Figure 4 illustrates the basic operation of reply phase from receiver R1 to source S, for the network topology of Fig. 2.

- Receiver node R1 prepares RP packets for the RR packets in two directions R1-A-S and R1-B-S.
- Route for one RP packet is R1-A-S and for other RP packet is R1-B-S. PathSFBN, PathBW and delay in the RP packets are updated.
- Both the RP packets are assumed to flow through the paths and reach the source S. The visited intermediate nodes will update paths to node A and B in their RIC's.
- RIC at node S will be updated after receiving RP packets in both directions.

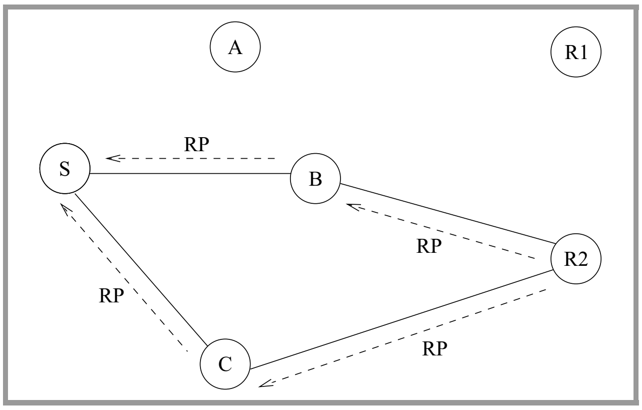

Fig. 5. Reply paths from R2 to S.

Figure 5 illustrates the basic operation of reply phase from receiver R2 to source S, for the network topology of Fig. 2.

- Receiver node R2 prepares RP packets for the RR packets in two directions R2-B-S and R2-C-S.
- Route for one RP packet is R2-B-S and for other RP packet is R2-C-S. PathSFBN, PathBW and delay in the RP packets are updated.
- Both the RP packets are assumed to flow through the paths and reach the source S. The visited intermediate nodes will update paths to node B and C in their RIC's.
- RIC at node S will be updated after receiving RP packets in both directions.

The mesh structure created between source S and group of receivers R1 and R2 in our example with A, B and C as forwarding nodes is given in Fig. 6. In OQSMR, selection of stable forwarding nodes plays an important role in creating mesh structure which satisfies stability, bandwidth and delay requirements. A forwarding node always checks for higher value of the stability factor, minimum bandwidth and less delay. Thus created mesh is the reliable and robust structure which can be used for multimedia real time application.

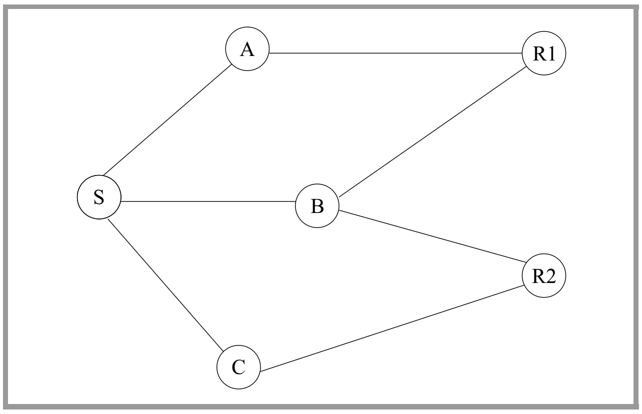

Fig. 6. Mesh created between source S and receivers R1 and R2.

3.4. Route Maintenance

Route maintenance is required in case of link failures. There are three cases: link failure between stable intermediate nodes, between source and stable intermediate node, and between receivers and stable intermediate node. The problem can be tackled in following ways. In case of link failure between two stable intermediate nodes, the node detecting failure condition will use RR and RP packets to find stable QoS path between itself and the receiver. The new path from intermediate node to destination will be informed to source. If a new path is not found, the node sends RE packet to source to rediscover the paths. In case of link failure between source and stable intermediate node, source node will probe backup path, if it is working, it will use backup path. Routes will be rediscovered if backup path does not exist. In case of link failure between receiver and stable intermediate node, the intermediate node will use RR and RP packets to discover paths to receiver from itself and informs the source about the path. If route is not discovered, the node sends RE packet to source to initiate route rediscovery. The source constructs a new path in all the cases for further routing of packets.

4. Simulation and Performance Evaluation

In this section, the performance of proposed protocol with ODMRP [4], and E-ODMRP [7] is compared, through extensive set of simulations. These protocols have been taken for comparison because both are mesh based. These protocols are compared in terms of packet delivery ratio, control overhead, and average end-to-end delay. Simulation considers the values of the performance parameters taken for several iterations, and the values are used for computing the mean. The values lying with in 95% of the confidence interval of the mean are used for computing the mean value, which are plotted in the graphs in result analysis section.

The various network scenarios have been simulated using discrete event simulation model developed by C programming language. Simulation environment consists of four models: Network, Channel, Mobility, and Traffic. In network model an ad hoc network is generated in an area of $l \times b$ square meters. It consists of N number of mobile nodes that are placed randomly within a given area. The coverage area around each node has a limited bandwidth that is shared among its neighbors. It is assumed that, the operating range of transmitted power and communication range r are constant.

Channel Model assumes free space propagation model and error free channel. To access the channel, ad hoc nodes use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) media access protocol to avoid possible collisions and subsequent packet drops is used. In mobility model: a random way-point (RWP) mobility model based upon three parameters: speed (Mob) of movement, direction for mobility and time of mobility. In RWP, each node picks a random destination uniformly within an underlying physical space, and nodes travel with a given speed. The node pauses for a time period Z, and the process repeats itself. The traffic model is a constant bit rate model that transmits certain number of fixed size packets at a given rate.

4.1. Performance Parameters

Following metrics have been used to analyze the performance:

- Packet Delivery Ratio (PDR) – it is the ratio of number of average data packets received at the multicast receivers to the number of data packets sent by the source;
- Packet Overhead – it measures the ratio of control packets sent to the network to the total number of average data packets delivered to the receivers;
- Average end-to-end Delay – it is the average delay experienced by the successfully delivered packets in reaching their receivers.

Simulation parameters used are summarized in Table 4.

Table 4
Simulation parameters description

Parameter name	Value
Topology	1000 m × 1000 m flat-grid area
Number of nodes	50
Multicast group size	10–50
Number of sources	1–6
Node placement	Random
Mobility model	Random way-point
MAC layer	IEEE 802.11 DCF
Channel capacity	2 Mb/s
Transmission range [m]	250
Carrier-sense range [m]	500
Antenna type	Omnidirectional
Node speed [m/s]	1–50 m/s
Traffic type	CBR
Packet size [bytes]	512
Traffic rate [packets/s]	4 to 32
Minimum bandwidth [Kb/s]	40
Maximum delay [s]	0.1
SFTH [Min.]	0.5
SFTH [Max.]	0.9
Simulation time [s]	500

4.2. Simulation Procedure

Simulation procedure for the proposed scheme is as follows:

1. Generate ad hoc network with given number of nodes.
2. Estimate stability factor based on self node stability and neighbor node stability.
3. Compute link stability factor using Table 1 and Lsd.
4. Compute bandwidth at each node to satisfy application requirement.
5. Update NSQB at each node considering their neighbors.
6. Initiate Route Discovery Process using RR, RP and RE, and accordingly update RIC.
7. Establish the path(s) from source to receivers, and send the data packets,
8. Compute performance parameters of the system.

4.3. Result Analysis

Effect of multicast group size. OQSMR performs better than ODMRP, and E-ODMRP in terms of PDR for the multicast group size (10 to 50) as shown in Fig. 7. The reasons for achieving high PDR (around 95%) in OQSMR are, use of high stable nodes, avoiding nodes with higher delays, and long duration links, and maintaining route cache at every node which avoids unnecessary route discovery. The performance analysis of packet overhead against number of multicast group size is shown in Fig. 8. The overhead is

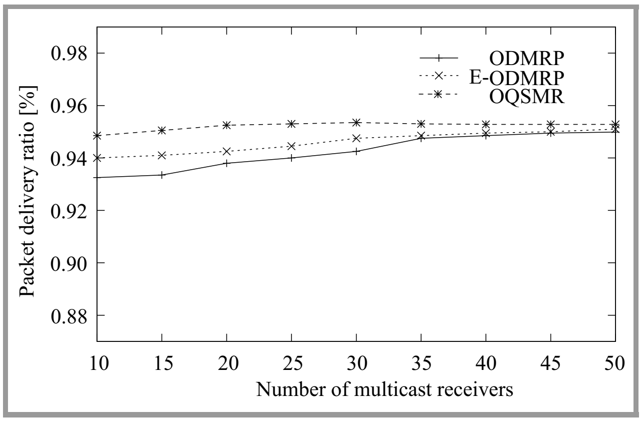

Fig. 7. Packet delivery ratio vs. multicast group size (1 multicast group, 1 source, and 20 m/s maximum speed).

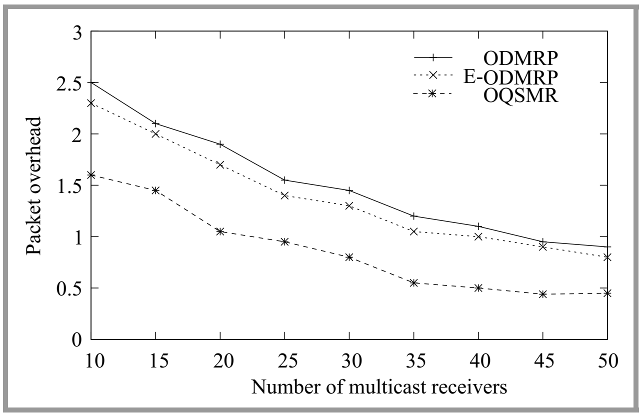

Fig. 8. Packet overhead vs. multicast group size (1 multicast group, 1 source, and 20 m/s maximum speed).

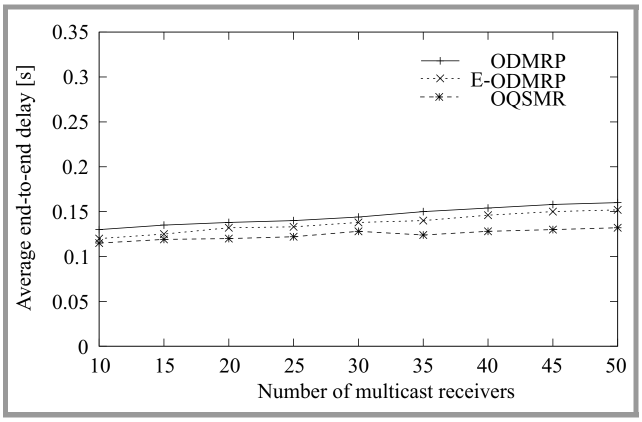

Fig. 9. Average end-to-end delay vs. multicast group size (1 multicast group, 1 source, and 20 m/s maximum speed)

reduced in OQSMR compared to ODMRP and E-ODMRP. The following reasons are given to claim the reduced overhead: strong mesh creation through stable nodes and longer lifetime of links, maintenance of route cache to store the latest routes to group of receivers, avoids unnecessary route discovery, and more efficient forwarding mechanism is created when multicat group size increases. From Fig. 9, OQSMR exhibits lower average end-to-end delay can be observed that compared to ODMRP and E-ODMRP because the multicast traffic is initiated through the nodes those come in non-congested areas, and links established through such stable nodes will have higher link lifetime.

Effect of multicast traffic load. Figures 10–12 exhibit the effect of increase in traffic load on network performance. The sending packet rate varies from 4 to 32 per second with a fixed packet size of 512 bytes, for one multicast source and 20 receivers in the multicast group. The maximum node movement is considered as 20 m/s.

Figure 10 depicts degradation in performance when packet sending rate is increased. High packet sending rate causes higher congestion and packet loss in the network. Results reveal that OQSMR outperforms compared to ODMRP and E-ODMRP. This is because, in OQSMR, nodes avoid intensive flooding of query messages. The direct implication

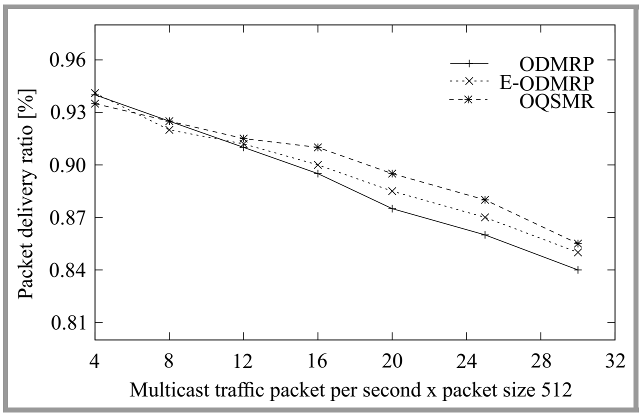

Fig. 10. Packet delivery ratio vs. multicast traffic (1 source, 20 multicast receivers and 20 m/s maximum speed).

is that more bandwidth is allocated to the nodes, and hence packet loss can be reduced. Furthermore, it improves the end-to-end delay as packet sending rate increases.

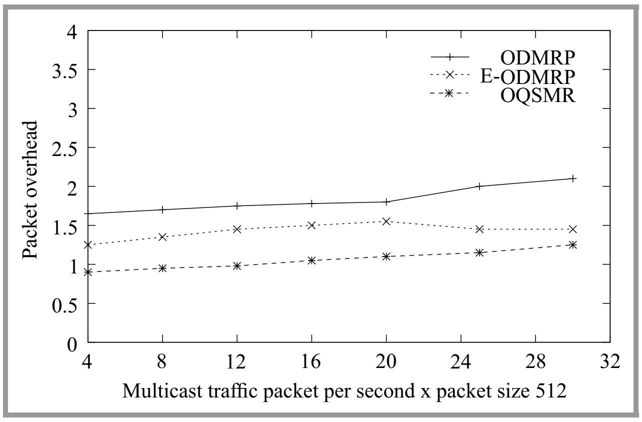

Fig. 11. Packet overhead vs. multicast traffic (1 source, 20 multicast receivers and 20 m/s maximum speed).

As depicted in Fig. 11, packet overhead in OQSMR remains lower than that of ODMRP and E-ODMRP, because it greatly reduces the cost of discovery mechanism due to the mesh architecture created among stable nodes. Figure 12 of the result analysis shows average end-to-end

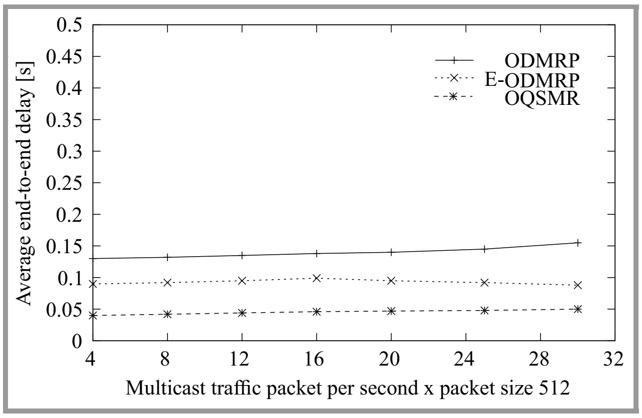

Fig. 12. Average end-to-end delay vs. multicast traffic (1 source, 20 multicast receivers and 20 m/s maximum speed).

delay against multicast traffic. As the sending traffic rate increases from 4 to 32 packets per second (for a fixed packet size of 512 bytes), ODMRP progresses slightly in upward direction which indicates increase in average end-to-end delay. This is because of extensive increase in the query messages at higher traffic load and service time delay among contributing nodes. It is relatively less in E-ODMRP and OQSMR. Presented protocol shows reduced end-to-end delay compared to other two protocols, since the query messages and their service time is reduced at high traffic load.

Effect of number of multicast sources. Figure 13 illustrates the effects of multicast sources on packet delivery ratio when a single multicast group is considered. The number of multicast source nodes from 1 to 6 is varied and keeping the number of receiver nodes as 20. Although mesh structure of routing protocols provides good delivery ratio, it suffers from poor packet delivery ratio in scenarios where multiple sources generate multicast traffic.

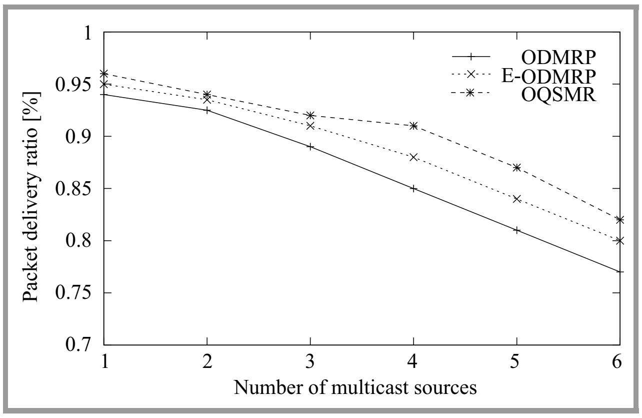

Fig. 13. Packet delivery ratio vs. multicast sources (1 multicast group, 1–6 sources, 20 multicast receivers and 20 m/s maximum speed).

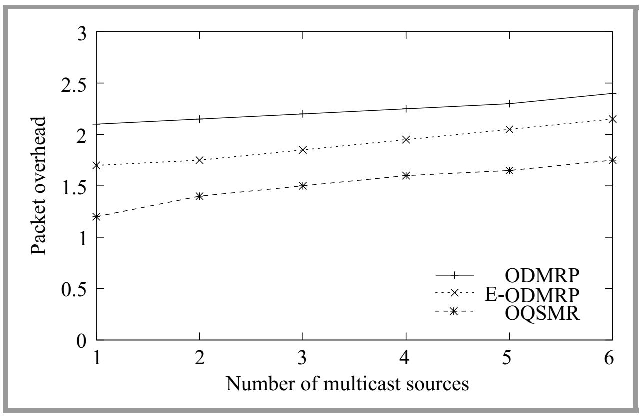

Fig. 14. Packet overhead vs. multicast sources (1 multicast group, 1–6 sources, 20 multicast receivers and 20 m/s maximum speed).

This will create congestion and packet loss within the network. It is observed that OQSMR has relatively higher PDR compared to ODMRP and E-ODMRP when number of sources are increased. Results in Fig. 14 reveal that presented method induces relatively lower packet overhead as the number of traffic sources increase compared to ODMRP and E-ODMRP. High packet overheads under high traffic loads are observed in ODMRP and E-ODMRP. This is because in scenarios where the number of multicast sources increase, a large number of request messages are injected into the network by non-active forwarding nodes resulting in higher network congestion and packet overhead.

Effect of node speed. Figures 15 to 17 show the effect of mobility on the performance of routing protocols. The maximum node speed varies from 1 to 50 m/s for 20 multicast receivers. The speed of 30 to 50 m/s can be applicable to class of MANETs such as VANETs (Vehicle Ad hoc Networks). Basically, the mesh nature and path redundancy in multicast based routing protocols compromise frequent link breakage. This is true in scenarios where the nodes move with high speed. The fault tolerance capabilities keep packet delivery ratio high by creating multiple forwarding routes and avoiding high packet loss rate due to link breakage. Figure 15, shows that OQSMR performs relatively better than ODMRP and E-ODMRP in

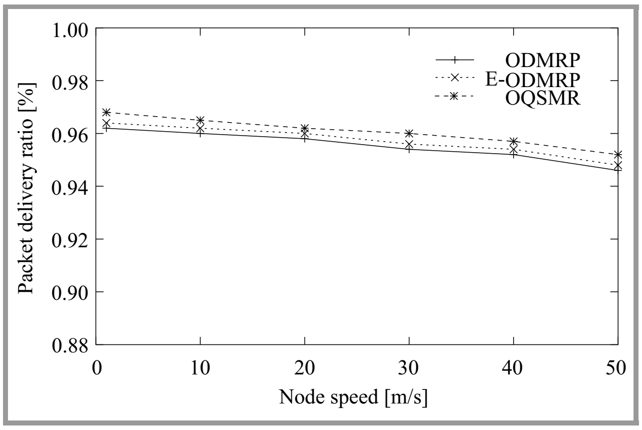

Fig. 15. Packet delivery ratio vs. node speed (1 group, 1 source, 20 multicast receivers).

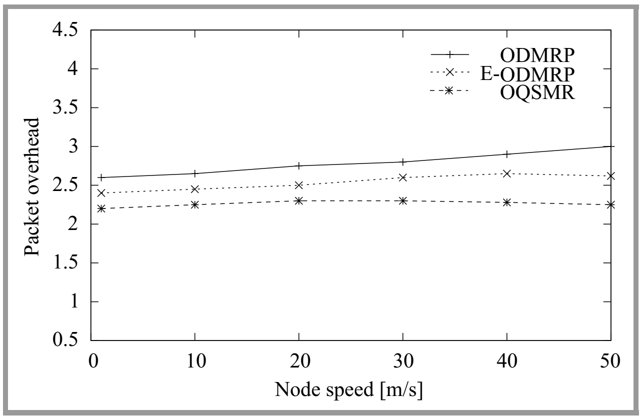

Fig. 16. Packet overhead vs. node speed (1 group, 1 source, 20 multicast receivers).

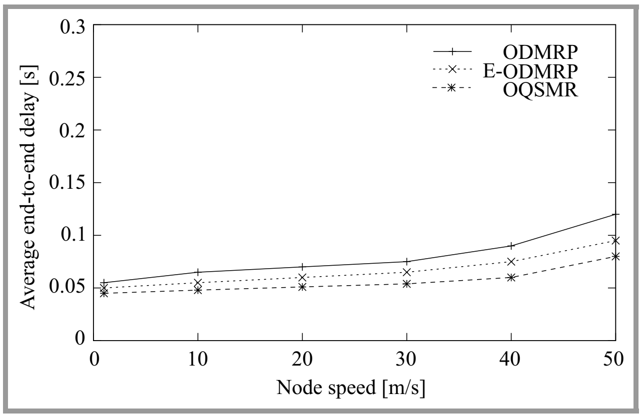

Fig. 17. Average end-to-end delay vs. node speed (1 group, 1 source, 20 multicast receivers).

terms of PDR with variation in node speed. This is because, path constructing techniques used in OQSMR employs stable nodes and stronger links. Figure 16 represents the routing overhead as a function of node mobility. As indicated, the gap between ODMRP to E-ODMRP and E-ODMRP to OQSMR is relatively large at nodes' high speed. The non-stable forwarding nodes impose frequent message rebroadcasting, which effects the performance of ODMRP and E-ODMRP compared to OQSMR. Average end-to-end delay performance with increase in node speed is better in OQSMR as compared to ODMRP and E-ODMRP, as depicted in Fig. 17.

5. Conclusions

Node's and link stability, delay, bandwidth are the important reliability and QoS metrics among several parameters for providing an efficient, low overhead QoS support for mesh based multicast routing in Mobile Ad hoc Networks. In this paper, an on demand QoS and stability based multicast routing (OQSMR) is proposed which is an enhancement of ad hoc on demand multicast routing protocol (ODMRP) to provide stable connection and QoS support for real time applications. The general conclusion from presented simulation experiments reveals that proposed OQSMR routing protocol performs better than ODMRP and E-ODMRP in terms of packet delivery ratio, packet overhead, average end-to-end delay as a function of varying number of receivers, sources and nodes speed.

In future works, the authors aim to study more by comparing our On-demand QoS and Stability based Multicast Routing (OQSMR) protocol with some more QoS based routing protocols in MANETs. The work can be extended by considering delay distribution among nodes in the path such that request packets may not be forwarded, if node/link delay does not satisfy the required node/link delay, and work out jitter based model at the nodes such that scheme must choose a node with less delay jitters. The plans cover also to work on any cast routing protocols to check the efficiency under high throughput applications, e.g. multimedia applications by employing negotiation parameters in route request packet in finding nearest server through non congested paths.

References

[1] R. Ramanathan and J. Redi, "A brief overview of ad hoc networks: challenges and directions", *IEEE Commun. Mag.*, vol. 40, no. 5, pp. 20–22, 2002.

[2] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad-hoc networks", *IEEE Commun. Surv. Tutor.*, vol. 11, no. 1, pp. 78–91, 2009.

[3] C. Siva, R. Murthy, and B. S. Monoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, 2nd ed. Pearson Education, 2004.

[4] W. Su, S. J. Lee, and M. Gerla, "On-demand multicast routing protocol in multihop wireless mobile networks (ODMRP)", *Mob. Netw. and Appl.*, vol. 7, no. 6, pp. 441–53, 2002.

[5] "IETF draft on ODMRP" [Online]. Available: http://tools.ietf.org/html/draft-ietf-manet-odmrp-04 (accessed on 10th Dec., 2013)

[6] S. J. Begdillo, H. Mohamamdzadeh, S. Jamali, and A. Norouzi, "Stable route selection in ODMRP with energy based strategy", in *Proc. IEEE 21st Int. Symp. Personal, Mob. Radio Commun.*, Istanbul, Turkey, 2010, pp. 1741–1745.

[7] S. Y. Oh, J.-S. Park, and M. Gerla, "E-ODMRP: Enhanced ODMRP with motion adaptive refresh", *J. Parallel and Distrib. Comput.*, vol. 68, no. 8, pp. 1044–1053, 2008.

[8] R. C. Biradar, S. S. Manvi, and M. Reddy, "Link stability based multicast routing in MANET", *Comp. Netw.*, vol. 54, no. 7, pp. 1183–1196, 2010.

[9] D. Promkotwong and O. Sornil, "A Mesh-based QoS aware multicast routing protocol", in *Proc. 1st Int. Conf. Network-based Inform. Sys.*, Regensburg, Germany, 2007, pp. 466–475.

[10] P. Deepalakshmi and S. Radhakrishnan, "Source initiated QoS multicasting scheme for MANETs using ACO", in *Proc. Int. Conf. Process Autom., Contr. Comput. PACC 2011*, Kalasalingam, India, 2011, pp. 1–4.

[11] J. A. Torkestani and M. Reza Meybodi, "A link stability-based multicast routing protocol for wireless mobile ad hoc networks", *Netw. Comp. Appl.*, vol. 34, no. 4, pp. 1429–1440, 2011.

[12] K. Paul, S. Bandyopadhyay, A. Mukherjee, and D. Saha, "A stability-based distributed routing mechanism to support unicast and multicast routing in ad hoc wireless network", *Comp. Commun.*, vol. 24, no. 18, pp. 1828–1845, 2001.

[13] H. Wang, H. Xu, S. Yi, and Z. Shi, "A tree-growth based ant colony algorithm for QoS multicast routing problem", *Expert Sys. with Appl.*, vol. 38, no. 9, pp. 11787–11795, 2011.

[14] B.-L. Su, M.-S. Wang, and Y.-M. Huang, "Fuzzy logic weighted multi-criteria of dynamic route lifetime for reliable multicast routing in ad hoc networks", *Expert Sys. with Appl.*, vol. 35, no. 1–2, pp. 476–484, 2008.

[15] Y.-S. Yen, H.-C. Chao, R.-S. Chang, and A. Vasilakos, "Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs", *Math. Comp. Model.*, vol. 53, no. 11–12, pp. 2238–2250, 2011.

[16] M.-A. Kharraz, H. Sarbazi-Azad, and A. Y. Zomaya, "On-demand multicast routing protocol with efficient route discovery", *J. Netw. Comp. Appl.*, vol. 35, no. 3, pp. 942–950, 2012.

[17] K. Bur and C. Ersoy, "Performance evaluation of a mesh-evolving quality-of-service-aware multicast routing protocol for mobile ad hoc networks", *Perform. Eval.*, vol. 66, no. 12, pp. 701–721, 2009.

[18] K. Viswanath, K. Obraczka, and G. Tsudik, "Exploring mesh and tree-based multicast routing protocols for MANETs", *IEEE Trans. Mob. Comput.*, vol. 5, no. 1, pp. 28–42 , 2006.

[19] Neng-Chung Wang, Chao-Yang Lee, "A multi-path QoS multicast routing protocol with slot assignment for mobile ad hoc networks", *Elsevier Information Sciences*, vol. 208, pp. 1–13, 2012.

[20] X. Xiang, X. Wang, Y. Yang, "Supporting efficient and scalable multicasting over mobile ad hoc networks", *IEEE Transactions on Mobile Computing*, vol. 10, no. 4, pp. 544–559, 2011.

[21] R. K. Gujral, J. Grover, A. Anjali, and S. Rana, "Impact of transmission range and mobility on routing protocols over ad hoc networks", in *Proc. IEEE Int. Conf. Comput. Sci. ICCS 2012*, Phagwara, India, 2012, pp. 201–206.

[22] S.-J. Lee, W. Su, and M. Gerla, "Ad hoc wireless multicast with mobility prediction", in *Proc. 8th Int. Conf. Comp. Commun. Netw.*, Boston, MA, USA, 1999, pp. 4–9.

[23] G. Guichal and S. Bunchua, "ABAM: on-demand associativity-based multicast routing for ad hoc mobile networks", in *Proc. 52nd Int. Conf. Veh. Technol. IEEE-VTS 2000*, Boston, MA, USA, 2000, vol. 3, pp. 987–993.

[24] C. K. Toh, D. Kim, S. Oh, and H. Yoo, "The controversy of selfish nodes in ad hoc networks", in *Proc. 12th Int. Conf. Adv. Commun. Technol. ICACT 2010*, Phoenix Park, Gangwon-Do, Korea, 2010, vol. 2, pp. 1087–1092.

[25] G. Xylomenos, K. Katsaros, and V. Tsakanikas, "Support of multiple content variants in the multimedia broadcast/multicast service", *Int. J. Commun. Sys.*, vol. 24, no. 6, pp. 691–708, 2011.

[26] J. Garofalakis and E. Stergiou, "Performance evaluation for single- and semi-layer multistage interconnection networks servicing multicast traffic by full multicast operation", *Int. J. Commun. Sys.*, vol. 24, no. 4, pp. 415–437, 2011.

[27] M. Kim, M. W. Mutka, H.-Y. Kim, "ESC: Estimation of selecting core for reducing multicast delay variation under delay constraints", *Int. J. Commun. Sys.*, vol. 24, no. 1, pp. 40–52, 2011.

[28] J. G. Jetcheva and D. B. Johnson, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks", in *Proc. 2nd ACM Int. Symp. Mob. Ad Hoc Netw. and Comput.*, New York, NY, USA, 2001, pp. 33–44.

[29] L. Klos, Golden G. Richard III, "A reliable extension to the ODMRP ad hoc multicast protocol", in *Proc. Int. Conf. Wirel. Netw. ICWN 2005*, Las Vegas, NV, USA, 2005, pp. 45–51.

[30] D. Pathirana and M. Kwon, "RODMRP – Resilient on demand multicast routing protocol", in *Proc. 21st Int. Conf. Adv. Inform. Netw. and Appl. Worksh.*, Niagara Falls, Ontario, Canada, 2007, pp. 85–92.

[31] P. I. Basarkod, S. S. Manvi, and D. S. Albur, "Mobility based estimation of node stability in MANETs", in *Proc. Int. Conf. Emerg. Trends in Comput., Commun. and Nanotechnol. ICE-CCN 2013*, Tuticorin, India, 2013, pp. 126–130.

[32] GPS.gov – Official U.S. Government information about the Global Positioning System (GPS) and related topics [Online]. Available: http://www.gps.gov/systems/gps/performance/accuracy/ (accessed on 15 Oct., 2012)

[33] H. M. Ali, A. M. Naimi, A. Busson, and V. Veque, "Signal strength based link sensing for mobile ad-hoc networks", *Special Issue of Telecommunication Systems, Springer*, vol. 42, no. 3–4, pp. 201–212, 2009.

[34] Z. Li, Lingfen Sun, and E. C. Ifeachor, "Range-based relative velocity estimations for networked mobile devices", *IEEE Trans. Veh. Technol.*, vol. 58, no. 58, pp. 2095–2099, 2009.

[35] K. S. Trivedi, *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*, 2 ed. Wiley Intersceince, 2005.

[36] P. I. Basarkod and S. S. Manvi, "Multiple parameters based approach to estimate bandwidth in mobile ad hoc networks", *Int. J. Comp. Sci. Issues, Special Issue (IJCSI)*, vol. 1, no. 1, pp. 37–43, 2011.

P. I. Basarkod received B.E. degree in Electronics and Communication from National Institute of Engineering, Mysore, M.E. degree in Electronics from the BMS college of Engineering, Bangalore and M.Sc. in Software Systems from Birla Institute of Technology and Science, Pillani and currently doing research under the guidance of Dr. Sunilkumar S. Manvi from Kuvempu University, Shankaragatta, Shimoga. He is currently working as a Professor in Electronics and Communication Department of Reva Institute of Technology and Management, Bangalore. He is having a teaching experience of 26 years and his areas of interest are Wireless Communication and Computer Networking. He is a member of ISTE (MISTE, India), member of IEEE (MIEEE, USA).

E-mail: basarkod@revainstitution.org
Wireless Information Systems Research Lab
Department of Electronics and Communication Engineering
Reva Institute of Technology and Management
Bangalore-560064, India

Sunilkumar S. Manvi received M.E. degree in Electronics from the University of Visvesvaraya College of Engineering, Bangalore and Ph.D. degree in Electrical Communication Engineering, Indian Institute of Science, Bangalore, India. He is presently working at Reva Institute of Technology and Management, Bangalore, India, as Dean of Research and Development. He is involved in research of agent based applications in multimedia communications, grid computing, vehicular ad-hoc networks, e-commerce and mobile computing. He has published about 140 papers and 3 books in national and international conferences and 90 papers in national and international journals. He is a Fellow IETE (FIETE, India), Fellow IE (FIE, India), member ISTE (MISTE, India), and member of IEEE (MIEEE, USA).

E-mail: sunil.manvi@revainstitution.org
Wireless Information Systems Research Lab
Department of Electronics and Communication Engineering
Reva Institute of Technology and Management
Bangalore-560064, India