# *QoS-Aware Routing and Admission Control for MANETs*

D.Uma[1], J.Gayathri[2],M.Deepika[3],D.Ramyalakshmi[4],

[1] *Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India*

[2] *Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India.*

[3]*Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India.*

[4]*Assistant professor,Electronics and Communication Department,Prince Shri Venkateshwara Padmavathy Engineering College,Tamilnadu,India.*

## ABSTRACT

Providing quality of service (QoS) assurances in a mobile ad hoc network (MANET) is difficult due to node mobility, contention for channel access, a lack of centralized co-ordination, and the unreliable nature of the wireless channel. A QoS-aware routing (QAR) protocol and an admission control (AC) protocol are two of the most important components of a system attempting to provide QoS when the above mentioned difficulties are faced. Many QAR and AC-based solutions have been proposed, but such network layer solutions are often designed and studied with idealized lower layer models in mind. This means that existing solutions are not designed for dealing with practical phenomena such as the link quality-dependent fluctuation of link transmission rates and shadow fading i.e., the phenomenon that occurs when a mobile node moves behind an obstruction and experiences a significant reduction in signal power. In this project two Protocols Ad Hoc On Demand Vector Routing (AODV)and a multirate aware version of Staggered Admission Control (StAC) which works along with the QAR, AC protocols are being proposed .The AODV provides loop free routes ,ie. Each mobile host operates as a specialized router and the routes are obtained when needed. The StAC co-operates with the QAR to cope up with the shadow fading environment. Here packet delay, throughput, packet data ratio and the packets received are used to analyze the performance of the proposed protocols.

**Keywords:** *Multirate mobile ad hoc networks, quality of service aware routing, admission control, shadowing/shadow fading, guaranteed throughput.*

## 1.INTRODUCTION

The interest in Mobile Ad hoc Networks (MANETs) has grown immensely over the last 15 years. Much hope has been placed in MANETs to provide spontaneous, robust, and ubiquitous communications in areas where central infrastructure is limited, lacking or cannot be accessed, or where its use is not desired. MANET is a dynamically re-configurable wireless network with no fixed infrastructure. In such a network, each mobile node operates not only as a host but also as a router. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

In areas with little infrastructure or the existing infrastructure is expensive, wireless mobile users may still be able to communicate through ad hoc networks MANET is expected to support various multimedia applications. Network control based on QoS requirements is a key issue for supporting these applications in MANET. QoS routing is a process of selecting a path based on given QoS requirements, such as bandwidth and delay.

Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures. On-demand routing protocols build and maintain only needed routes to reduce routing overheads. Examples include Ad Hoc On-Demand Distance Vector (AODV)**,** Dynamic Source Routing (DSR), and Temporally Ordered Routing Algorithm (TOM).

### 1.1 EXISTING SYSTEMS AND LIMITATIONS

Many previously proposed QAR and AC protocols have been aimed at addressing the channel allocation and Qos based limited issues. However, in MANETS, the operation of such protocols is hampered by the lack of centralized co-ordination,contention for channel access, node mobility, and the unreliable wireless channel. Most previous proposals either do not estimate residual resources sufficiently accurately, do not respond well to node mobility, do not deal with heterogeneous link rates, or were not designed for coping with realistic channel conditions caused by shadow fading.

## 2. METHODOLOGY

### A. *Node Creation*

The data transmission in which a node can receive packets that are neither broadcast nor addressed to itself Source Node determine routes dynamically and only as needed Source Node that wants to send a packet must check its route cache. If there is a valid entry for the destination, the node sends the packet using that route.

### B. *Route Discovery*

It is the mechanism by which a node source node(s) wishing to send a packet to a destination node(D) obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

### C. *Route Maintenance*

It is the mechanism by which node S is able to detect, while using a source route to D If the network topology has changed such that it can no longer use its route to D because a link along the route no longer works. When route maintenance indicates a source route is broken, S can attempt to use any other route it happens to know route to D or can invoke route discovery again to find a new route. Route Maintenance is used only when S is sending packet to D.

### D. *Route Discovery with Admission Control*

Each node has routing table which is the list of route entries. Each entry consists of: (sid, source, destination, pre node, next node, allocation bandwidth (bw), state). Where sid and state are session ID and status of the route respectively. In the entry for actually established route, state is ACTIVE. The entry “ACTIVE” entry. Self-traffic on each node is equal to the total volume of cons bw in every “ACTIVE” entry. Route discovery for one session works as the following procedure. Where required bandwidth for the session is represented as req bw.

### E. *Performance Metrics*

The performance metrices is used to define the performance of the proposed system by considering,

PACKET DELAY RATE IN QOS MANET:

- This parameter defines higher the packet delay rate, the degraded is the quality of service of the system.
- This parameter is indirectly proportional to the quality of service.

DATA RATE FOR QOS MANET:

- This parameter defines higher the amount of data received, the better is the quality of service of the system.
- This parameter is directly proportional to the quality of service.

PACKETS RECEIVED IN QOS MANET:

- This parameter defines lower the packet delay rate, the better is the quality of service of the system.
- This parameter is directly proportional to the quality of service.

THROUGHPUT:

- The Throughtput is the average rate of successful message delivery It can also be defined as the ratio of the total number of packets sent to the response time of each packets.

## 3.PROPOSED SYSTEM

### 3.1 PROTOCOL AND ALGORITHM

AD HOC ON DEMAND DISTANCE VECTOR(AODV)

The route discovery is used by broadcasting the RREQ message to the neighbors with the requested destination sequence number, which prevents the old information to be replied to the request and also prevents looping problem, which is essential to the traditional distance vector protocols. The route request does not add any new information about the hosts only it increases its hop metric. Each passed host makes update in their own routing table about the requested host. This information helps the destination reply to be easily routed back to the requested host. The route reply use RREP message that can be only generated by the destination host or the hosts who have the information that the destination host is alive and the connection is fresh.

The route request message (RREQ) is sent when the host does not know the route to the needed destination host or the existed route is expired. The RREQ message includes the destination sequence number which is the last known sequence number of the destination host entry found in the routing table. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically traveling from the source to the destination along that path.

Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery.

Although AODV is a reactive protocol it uses the Hello messages periodically to inform its neighbors that the link to the host is alive. The Hello messages are broadcasted with TTL equals to 1, so that the message will not be forwarded further. When host receives the Hello message it will update the lifetime of the host information in the routing table. If the host does not get information from the host's neighbor for specified amount of time, then the routing information in the routing table is marked as lost. This action generates needed RRER message to inform other hosts of the link breakage. The routes that were created by the Hello message and were not used for any routing actions should not generate the RERR message when the link breakage occurs.

I. STAGGERED ADMISSION CONTROL (STAC)

The staggered admission control (StAC) protocol is able to uphold admitted data sessions throughput guarantees more reliably than other advanced related, mostly due to its fast rerouting of data sessions after route failures, and its gradual admission of traffic while directly testing the achievable QoS prior to session admission. The fact that the QoS is tested directly as part of the AC process allows not only the capacity of routes to be tested, but also the reliability of their composing links, which may fluctuate due to phenomena such as shadow fading. However, further measures were deemed to be required to improve the achievable throughput-QoS in the face of link quality fluctuations

.

StAC utilizes pretested backup routes to help uphold throughput assurances in the face of route failures. Second, a multirate-aware version of StAC is also proposed, which co-operates with a modified rate switching mechanism at the MAC layer, and a QAR protocol to aid in coping with shadow-fading-induced signal strength fluctuations. The forementioned protocols are also combined and all of the new protocols are evaluated in a simulated highly dynamic mobile and shadow fading-afflicted environment.

The first stage consists of capacity-constrained route discovery, wherein each node forwards the flooded route request (RReq) or the route reply (RRep) if and only if it has sufficient residual capacity to support the session. Residual capacity is estimated using the CITR, a fixed transmission rate, and a "CS-range = two maximum length hops" model, as with most previous works.

StAC allows all routing information that are discovered and cached by DSR to be utilized. To test such routes, a second stage of AC also performs the above test at each node by exchanging session request (SREQ) and session reply (SREP) packets between source and destination nodes along a previously discovered route. At this stage, the SREQ is also cached at each node, while its CS neighbors are tested for adequate capacity using a method similar to CACP multihop.

If the SREP is received at the source node (the route's CS neighborhood has sufficient residual capacity), the reliability of the route is also tested in the third stage of AC. During this stage, which lasts a few seconds, the session is partially admitted, its packet generation and transmission rate is gradually ramped up and the achievable throughput is tested along the route. Any node detecting a lower than expected throughput at any of the staggered rate stages rejects the session, informing the source node. If the session is not rejected immediately after reaching its desired packet sending rate, it is fully admitted.

**3.2 STAC –BACK UP**

` MACMAN utilizes periodic residual capacity query messages to retest backup routes to ensure that they still have sufficient capacity to support their corresponding data session. This incurs extra overhead. By contrast, StAC-backup avoids this overhead in the following manner:

The lists of nodes comprising a session's primary and backup routes are delivered to the backup route's nodes via the SREP backup packet.

Each backup route node continually monitors its CS neighborhood capacity using the lower NCS monitoring threshold. Once per second, in the same manner as for the original SREQ backup driven route test, each node tests if its residual capacity could still support the session, in case it was rerouted to the backup route.

If not, a reject message is sent to the source node, containing the rejected route. This message is only forwarded by any node that has knowledge of the session, provided furthermore that the rejected backup route matches the record of the backup route stored for the session. If the source node still has the rejected route stored as a backup route, it erases the corresponding record from the session state information table (but not from the route cache, as it is still valid routing information), marks the route as "unusable" (by that session) for a timeout period, and attempts to find a new backup route.

### 3.3 STAC MULTIRATE

The combination of a rate-switching mechanism with a multirate 802.11 model and proposes a new multirate-aware version of StAC called StAC-multirate. If multiple routes are stored in the cache, the "fewest hops" metric utilized by StAC for choosing between them may no longer be optimal. Therefore, StAC-multirate selects the route that minimizes the channel time utilization of the session in the network. StAC uses a source route header extension to carry a source node's view of the available residual capacity at the nodes on a session's route. If, upon forwarding a data packet, a node detects that the source's view differs from its own estimate of the residual capacity by a given amount, and no update has been sent to that source node recently, an update packet is sent. All nodes forwarding the update packets add their own updates, if required, in order to avoid having to send separate update packets. This means that a given node always has up-to date information about the residual capacity of all nodes that lie along any active routes passing through it. This aids StAC in its rerouting procedure, since the delivery of a single data packet on a route is enough to trigger an update. In StAC-multirate, this behavior is merely extended to enable updates to be triggered by a change in a link rate. When StAC-multirate is combined with StAC-backup (which does not use the update packets), the backup route maintenance scheme detects any change in link rates that would render a backup route's capacity inadequate for its session. The multirate versions of StAC are also able to admit more sessions, since they are more likely to maintain the required throughput during AC by switching to 0 bps modes for temporarily low quality links and routing around them.

StAC-backup and StAC-multirate- Backup is more effective with high shadowing variance, than the use of adaptive modulation and local rerouting alone. This is most likely to be due to the greater average route length resulting from the algorithm that adds extra relay nodes to routes. A longer route, with more retransmissions of each packet, inherently causes more collisions, especially when, due to shadowing, interference may peak at very high levels and the troughs in received signal power may be very low. An extended version of StAC, termed as StAC-backup, which exploits the knowledge of alternative or backup routes to a source's destination in order to improve the robustness of throughput-QoS assurances in the face of route failures.

## 4 CONCLUSION

In this project, we propose a new protocol related to the StAC protocol, and evaluated their performance in comparison with the adhoc On Distance Vector Routing(AODV) against the increasingly severe shadowing attenuation fluctuations. First, the StAC backup protocol added a feature that attempts to provide a pre-capacity-tested backup route to each active data session. The novelty lay in the method of maintaining the status of backup routes regarding their capacity at data source nodes without incurring any test packet overhead, as well as in the combination with StAC. Use of such backup routes allowed the elimination of "available capacity" status update packets used by StAC [5].

Thus the proposed model is executed using the network simulator. It provides much flexibility in the transferring of data from the source node to the destination node by overcoming shadow fading and the reliable nature of the wireless network.

## 5.REFERENCES

[1] Lei Chen, Student Member, IEEE, and Wendi B. Heinzelman, Member, IEEE "Cross-layer cooperation for accurate admission control decisions in mobile ad hoc networks".

[2] Lajos Hanzo II. and Rahim Tafazolli Centre for Communication Systems Research (CCSR), University of Surrey, UK "Throughput assurances through admission control for multi-hop manets".

[3] Kamal Deep Meka Mohit Virendra Shambhu Upadhyaya "Trust Based Routing Decisions in Mobile Ad-hoc Networks"

[4] L. Hanzo II and R. Tafazolli, "The Effects of Shadow Fading on QoS-Aware Routing and Admission Control Protocols Designed for Multi-Hop MANETs," Wiley J. Wireless Comm. and Mobile Computing, Jan. 2010.