A Survey on QoS Based Routing Protocols for MANET

S.Sridhar
Department of Computer Applications,
S.A.Engineering college
Thiruverkadu post, Chennai – 77, India.

R.Baskaran
Department of Computer Science and Engineering,
CEG, Guindy, Anna University,
Chennai-25, India.

ABSTRACT

In mobile ad hoc networks (MANETs), the provision of quality of service (QoS) guarantees is much more challenging mainly due to node mobility and resource constraints. Therefore it is important that routing protocols incorporate QoS metrics in route finding and maintenance to support end-to-end QoS. The traditional AODV protocol seems less satisfactory in terms of routing data to end systems. Many revisions are done to the traditional AODV protocol to meet QoS challenges focused on bandwidth, end to end delay, Packet delivery ratio, energy and mechanism overheads. Hence , it becomes very necessary for MANETS to have an efficient routing and QoS mechanism to support various application. This article extensively and exclusively studies the issues involved with QoS routing and presents an overview and comparison of existing QoS based revisions done on AODV protocol, thus providing the reader with insight into their differences and allows to highlight trends in protocol design and identify areas for future research.

Keywords

Quality of Service, QoS metrics, MANET, AODV, Routing.

1. INTRODUCTION

A mobile ad hoc network (MANET) consists of mobile nodes that can communicate with each other through wireless links without an existence of fixed infrastructure, thus allowing users to set up the network fast and cost effective. For these characteristics, MANETs have been widely used in various application areas like military field, disaster relief, battlefields , sports stadiums , Personal Area Networks , the organization of conferences and so on. The reliability of data transmission in the network can not be guaranteed since MANETs are characterized by self-configured, dynamic changes of network topology, limited bandwidth, instability of link capacity and other resource constraints. The dynamic nature of an ad hoc network makes it extremely difficult to obtain accurate knowledge of the network state. Furthermore, constant updates of link state information are required to make optimal routing decisions, which results in extensive control overhead. Another characteristic of MANET's is mobility. All the nodes are allowed to move in different dimensions which result s in dynamic topology, since nodes are moving so they can go out of the range of network or come in the range of network at any time, a node which is part of one network at time can be part of an other network.

In Mobile Ad hoc Networks each node has limited wireless transmission range, so the routing in MANETs depends on the cooperation of intermediate nodes. Two types of routing protocols have been defined for ad hoc networks: Table-driven protocol and On-demand routing protocol. Table driven protocols are proactive in nature and consume excessive network bandwidth. On the other hand, on demand routing protocol exchange routing information only when needed. Ad-hoc On demand Distance Vector (AODV) routing protocol is an on demand routing protocol that focuses on discovering the shortest path between two nodes with no consideration of the reliability of a node. Ad-hoc On-Demand Distance Vector Routing has attracted great attention because of its simplicity, low computational complexity and low processing overhead. It is an on demand routing protocol, so that a route is only discovered when required by a source node. This eliminates periodic routing updates and only necessary information is propagated to minimize control overhead.

The major drawback of conventional AODV is the absence of the Quality of Service (QoS) provision that make routing protocols which requiring applications of QoS lower efficiency. In ensuring QoS provisioning, a network is expected to guarantee a set of measurable pre-specified service attributes to the users in terms of end-to-end performance, such as challenging task to ensure QoS provisioning including routing in ad-hoc networks due to the mobile and dynamic nature of the nodes

In fact, the conventional AODV routing protocol can be revised, for example, adding the corresponding QoS information to each node in its routing table. When a path discovery process is initiated, calculating the corresponding QoS provision values and finally we can find path with the best QoS provision. A key to provide QoS guarantees in ad-hoc networks is to find a route to the desired destination, that can, with high probability, survive for the duration of the session. When it comes to QoS routing, the routing protocols have to ensure that the QoS requirements are met . Unfortunately unlike wired networks, it is a challenging task to ensure QoS provisioning including routing in ad-hoc networks due to the mobile and dynamic nature of the nodes that exists in MANETS.

The work presented in this paper is to have discussion and analyses of various enhancements done to the traditional AODV protocol. The overview is presented in figure 1. The following section describes about various enhancements done to the traditional AODV protocol. The methodology behind the enhancements done to AODV protocol are explained along with the advantages and results of enhancements. A summary is provided which gives a clear view of result analysis of different AODV protocols along with the various parameters which provide quality of service which in turn affects the performance of the protocol while performing routing on mobile ad hoc networks. The findings are summarized which focuses on some major QOS metrics which play vital role in deciding routing performance of MANETs.

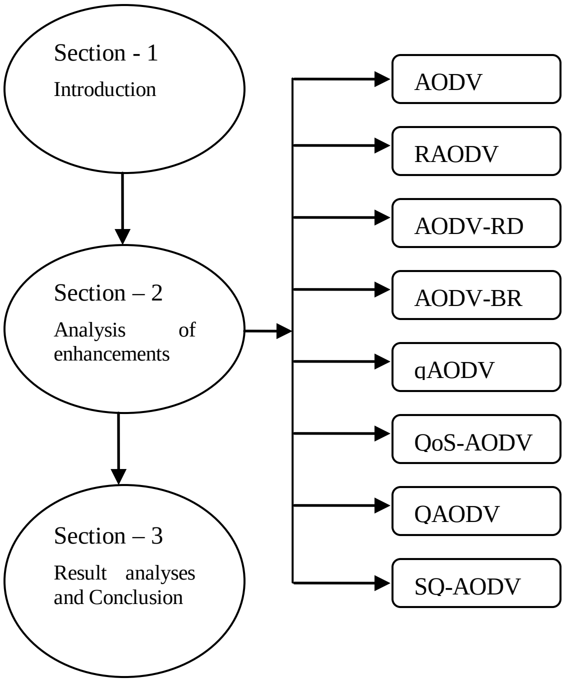

Figure – 1 : Overview

2. ANALYSES OF PROTOCOL ENHANCEMENTS

2.1 AODV [1]

AODV has attracted great attention because of its simplicity, low computational complexity and low processing overhead. It is an on demand routing protocol, so that a route is only discovered when required by a source node. This eliminates periodic routing updates and only necessary information is propagated to minimize control overhead. In AODV, each node maintains a routing table to record routing information obtained from routing packets.

Route Discovery:

When a source node needs to send data packets to a destination node, if there is no valid route entry in the routing table, a route discovery is performed. First, the source node creates a RREQ packet and broadcasts this to its neighbors. When a node receives a RREQ packet, it increases the hop count value in the packet and creates a reverse route entry in its routing table for both the source node and the neighbor node from which it received the request. After creating the reverse route, the node sends a RREP packet to the source if it is either the destination node, or has a "fresh enough" route to the destination. Otherwise, it just rebroadcasts the RREQ packet to its neighbors. The RREP packet is unicast to the source node from the destination node or an intermediate node. When a node receives the RREP packet, it creates a forward route entry for both the destination node and the neighbor node from which it received the RREP packet. The node then forwards the RREP packet to the next hop towards the source node according to the reverse route entry, and this continues until the RREP packet reaches the source node. If the source node receives multiple RREPs along different paths, it selects the route with the greatest destination sequence number.

Route Maintenance:

In a MANET, a route may break due to node movement. To increase the successful data transmission ratio, local repair can be performed on the upstream node of a broken link. If the destination node is not farther than MAX REPAIR TTL hops away, where MAX REPAIR TTL is based on the number of nodes in the network, the upstream node of the broken link sends a RREQ packet to the destination. The sequence number of the destination node in this RREQ packet is incremented by one to prevent route loops. If the local repair request is successful, a RREP packet is returned either by the destination or by an intermediate node with a valid route to the destination. If the node that initiated the request does not receive a RREP packet after a certain period of time, the local repair request fails and a RERR packet is sent to the source node. When a node creates a RERR packet, it lists all the unreachable destinations and their known sequence number, and invalidates all the active routing entries in its routing table that use the downstream node of the broken link as the next hop. When a node receives a RERR packet, it invalidates the related routes in its routing table and forwards the RERR packet to the previous hop nodes. In this manner, the RERR packet is forwarded to the source nodes. After the source node receives the RERR packet, it may initiate route discovery if it still needs a route.

2.2 RAODV [2]

RAODV – Reliable AODV protocol. This protocol focuses on the problem of misbehaving node affecting the behavior of MANET and presents a solution that detects and avoids misbehaving nodes, which agree to route packets for other nodes and subsequently drop these packets. Such misbehavior is of direct effect on Quality of Service solutions, namely the QoS goodput metric.

The following assumptions are made; Links between nodes support bi-directional communication symmetry. Wireless interfaces that support promiscuous mode operation (eavesdropping). The power needed to receive a packet is substantially lower than the power needed to transmit a packet. The RAODV adds two tables to each mobile node to be utilized in maintaining information about the behavior of the neighborhood. AODV's packet forwarding function is modified to enable misbehaving nodes to drop data packets other than address filtering is done to allow eavesdropping on neighboring nodes. Each mobile node keeps track of the packets it sends in a pending packet buffer. Each buffer entry contains a unique packet identifier, the address of the next hop to which the packet was forwarded, the packet's destination address and an expiry time after which a still-existing packet in the buffer is considered not forwarded by the next hop. Each node also keeps ratings of neighboring nodes it knows about in a node rating table node (addr, count). Each entry in this table contains the node address, a counter of successfully forwarded data packets by this node.

Detection:

Initially, all nodes are marked as legitimate well behaving nodes. Each node listens to packets sent by nodes within its wireless range. When forwarding a data packet to a neighbor node (other than the destination node), the node adds an entry for this packet in its pending packet buffer. If the timer of an entry in the pending packet buffer expires without the node hearing it being forwarded, the node to which it was forwarded is considered to have committed misbehavior. This results in incrementing its forwarding failure counter in the node-rating table. If the new rate exceeds the threshold then the node is marked as misbehaving.

If while eavesdropping the node observes a data packet being transmitted by one of its neighbors, it checks to see if the packet exists in the pending packet buffer. If it is in the pending packet buffer it removes its entry and increments the node's forwarding success counter. If the new rating is below the threshold, then the node is rewarded with a well-behaving status.

On the other hand, if the packet it heard did not exist in the pending packet buffer it increments the node's forwarding success counters. This restriction insures that a source node does not gain forwarding credit for its own traffic. This punishes selfish nodes, which only forward their own traffic. Also this insures that the rating of a congested well-behaving node that forwards the data packets after their entry in the pending buffer expires gets credit for its well behavior.

Avoidance:

Upon detecting a misbehaving node, the detecting node tries to do a local repair for all routes passing through the misbehaving node. This involves replacing each route that includes this misbehaving node with another one that does not contain any misbehaving nodes that this node knows about. If it fails to do so, it will not send any RERR (Routing Error) messages upstream. To avoid constructing new routes, which traverse misbehaving nodes, nodes drop/ignore all RREP messages coming from nodes currently marked as misbehaving. Also, all packets originating from a misbehaving node can be dropped as a form of punishment. Only dropping data packets will decrease node's rating. Dropping or forwarding control packets, such as RREP, does not affect the rating.

RAODV protocol has increased goodput by 25% and has lowered misbehaving ratio. Protocol still lacks to avoid partial dropping. It consumes power in processing packets not destined to it , cannot defend against changing the packet’s payload and performance degrades when mobility is high. Enhancements could have still more focused on the ways through which partial dropping could have been avoided. Necessary action should have been taken to defend against changing packets payload and mobility impact.

2.3 AODV-RD [3]

AODV-RD— AODV – Reliable Delivery , focuses on a link failure fore-warning mechanism, metric of alternate node in order to better select and also repairing action after primary route breaks.

Link Failure Prediction Mechanism:

In MANETs, the strength of the packet signal [4] which the node receives may be defined as formula (1).

$$P_r = \frac{P_t G_t G_r H_t^2 H_r^2}{d^4} \qquad (1)$$

Among them, P_r is the strength of received signal, P_t is the strength of the transmitting signal, G_t , G_r is the antenna gain of the receiver and transmitter, respectively. H_t , H_r is the antenna altitude of the receiver and transmitter respectively, *d* is the distance between the sending node and the received node. *d* can be defined as formula (2).

$$d = \sqrt[4]{P_t G_t G_r H_t^2 H_r^2 / P_r} \qquad (2)$$

Supposing each node has the same transmit power, from formula(2), then the changing strength of the received packet node signal reflects the fluctuation of the distance among nodes. Therefore, a receiving power warning threshold is defined as $P_r\_critical$. When P_r is lower than $P_r\_$ critical, determines that the link in the warning stage and link state is unstable and possible interrupts at any time. So when the node in primary route detects $P_r<P_r\_critical$, immediate access to the alternate route selecting process. After selection, the primary route switches to alternate routes in order to eliminate the required time interval to rebuild route.

Select Alternate Node:

For selecting a alternate node, a Signal Stability-Based Adaptive Routing (SSA) [5 , 6] is referred. SSA method is based on the strong or weak communication signals of the two adjacent nodes to identify the good or bad link between them. Communication signals, strong or weak, divide the neighbor's communication channel into "strong channel" and "weak channel". Choose "strong channel" corresponding to the node as a selected alternate node. Its communications ability can be set up by formula (3).

$$M = f(V, P_r, D) = A \times V + B \times P_r - C \times D \quad (3)$$

Among them, *V* is transfer rate, unit is packets/s. *D* is transfer delay, unit is ms. *A* , *B* ,*C* are constant. *M* retain one after the decimal point. To avoid the alternate nodes having the same metric, a random number of 0.001- 0.099 are added to it. Finally put the calculated value of *M* stored in the alternate routing table. Set a criticality value $M_{critical}$, reflects stability of communication ability. When metric $M < M_{critical}$ in the alternate routing table, it is determined that alternate node is unstable, and unfit for use. When $M \geq M_{critical}$, a higher metric is selected in the alternate node information for forwarding.

Repair Action of AODV-RD:

In AODV-RD, when a node detects primary route break, that node broadcasts RREQ that TTL=1, asks if the neighbor node has an alternate route to be used. At the same time, send RRER to the direction of the source. When neighbor nodes contain a alternate route, they will reply back RREP that TTL = 1, and a metric reflects stability of communication ability in RREP. Node will compare with metric after receiving RREP that TTL=1, and it will select the alternate node which has a Maximum metric $M_{max}(M_{max} \geq M_{critical})$. If max $M < M_{critical}$, it does not contain a stable alternate route, wait for the source to receive RRER and rebuild route.

AODV-RD protocol has increased PDR and has shortened end to end delay compared with AODV – BR. Still protocol has longer end to end delay compared with traditional AODV. Methodology could have concentrated more on reducing end to end delay and further optimization techniques could have been specified for special nodes.

2.4 AODV-BR [3]

AODV-BR – AODV – Base Routing , establishes the mesh and multi-paths to destination. When primary route breaks, alternate routes can be initiated to carry out data transmission. Before sending packets, source node will search routing table to see if there are arrival destination routing. If there is routing information, date packets begin to transmit. Otherwise, it will start route discovery process

Route discovery process:

Source node searches a route by flooding a route request (RREQ) to neighbor node, after receiving RREQ, node will search their routing table. It then broadcasts the packet or sends back a route reply (RREP) packet to the source if it has a route to the destination. If it has not, they will flood RREQ to their neighbor node and so on, until arrival destination node or one node that knows routing to the destination. When a node out of primary route receives RREP from a neighbor, this neighbor node will be recorded in the alternate routing table as “next hop” to the destination. When the RREP packet reaches the source of the route, the primary route between the source and the destination is established and ready for use.

Route maintenance process:

When a node detects a link break, it performs a one hop data broadcast to its immediate neighbors. The node specifies in the data header that the link is disconnected and thus the packet is candidate for “alternate routing”. At the same time, the node sends route error (RRER) to the source node.

AODV-BR protocol has increased PDR compared to traditional AODV with longer end to end delay . Refinement should have focused more on reducing end to end delay.

2.5 qAODV [7]

qAODV—Quality of service AODV . The AODV routing protocol is revised by calculating the corresponding QoS provision values to find the best routes and applying the mechanism of carrier sense in IEEE 802.11b to obtain the available bandwidth. This revised protocol will take bandwidth and delay into consideration .

Calculation of the Available Bandwidth:

The idle time which is decided by the node and the neighbor nodes throughput comprehensively is a very important parameter for the calculation of bandwidth, during this period of time the node can successfully transmit data. Therefore, idle time which reflects the available bandwidth of nodes can be calculated by the following formula (4):

$$B_{available}(I) = \frac{B(I) \times T_{idle}}{T_{\text{int}erval}} \tag{4}$$

Based on the above numerical formula, the main difficulty of measuring the available bandwidth $B_{available}$ (I) lies in calculating the T_{idle} which stands for interval time $T_{interval}$

during the channel idle time. We will set $T_{interval}$ l 2 seconds, the value should not reflect changes in available bandwidth if it is too large, and it will add too much overhead if the setting is too small. Then the available bandwidth in the recent $T_{interval}$ which can be calculated through statistical T_{idle} during $T_{interval}$. The mechanism of carrier sense in IEEE 802.11b protocol can be used to determine the channel idle or busy. Carrier sense is divided into two ways: physical and virtual, the physical layer provides the physical carrier sense mechanism and the MAC layer provides virtual carrier sense mechanism. Any way determine the media busy, the media will be considered in a busy state. During the unit interval, the period of time that from the channel in busy to idle is the required T_{busy}. T_{idle} can be expressed as (5).Put the calculated T_{idle} into the formula (5) can easily obtain $B_{available}$ (I).

$$T_{idle} = T_{\text{int}erval} - T_{busy} \tag{5}$$

Calculation of the End-to-end Delay:

The end-to-end delay is forecast via obtaining some parameters from the MAC layer. For example, considering the delay of date packet p via a path $r_i = n_0, n_1, n_2, \ldots n_m$ $(m \geq 2)$ from n_0 to n_m. For the node n_i take packet receiving speed μ_i, packet sending speed η_i and packet queue length l_i into consideration. Received by the node n_i, the packet will stay in the queue till it is sent, the time this process cost is called the delay in the n_i, the packet from n_i to n_i is called transmitting delay . So the delay can be obtained from the following formulas (6) (7) (8):

$$d_i = \frac{l_i + d_0^{i-1} \times (\eta_i - \mu_i)}{\eta_i}, i = 1, .. m \tag{6}$$

$$d_i = \frac{l_i}{\eta_i}, i = 0 \tag{7}$$

$$d_0^{i-1} = \sum_{j=0}^{i-1} d_j \tag{8}$$

When a node needs a new route to a destination, it initiates a route discovery process. The source node first calculate the needed bandwidth and examine the links between itself and neighbor nodes. If there are enough available bandwidth, the source node generates a RREQ packet, and sets up a routing table for this date packet and broadcast the RREQ packet. An intermediate node receiving a RREQ examines the links between itself and neighbor nodes, the RREQ packet is rebroadcast and a reverse path to the source node is set up if there are enough available bandwidth till the destination receives the RREQ packet. When there are more than one nodes meet the need of bandwidth, the source node will choose the best path basing on the delay. When the destination receives a RREQ it generates a RREP. The RREP is routed back to the source node via the reverse path established previously. As the RREP travels towards the source, a forward path to the destination is established. Then the source node sends a packet to reserve the bandwidth, ensuring that the resources are not used by other applications.

qAODV protocol reduces end to end delay and increases packet delivery ratio at high load and moderate to high mobility. Still, routing load of qAODV is slightly higher than traditional AODV. More optimization could have specified in such a way the load could have been controlled.

2.6 QoS-AODV [8]

In QoS-AODV – Quality of service AODV, the original AODV is extended by adding necessary new fields including maximum delay extension and minimum bandwidth extension. Highlights the combination of both metrics: delay and bandwidth respectively.

In order to provide QoS, extensions can be added to these messages during the route discovery process. Several extensions are needed in the routing table structure and the RREQ and RREP messages as reported in [9] [10].

The additional fields to each route table entry corresponding to each destination are: maximum delay, minimum available bandwidth as well as list of sources requesting delay and bandwidth guarantees.

Special messages which are called QoS LOST messages are forwarded to all sources potentially affected by the change in QoS parameter. These are the sources to which a RREP with QoS extension has been forwarded before [11].

Instead of only extending AODV messages with minimum available bandwidth, maximum delay field will also be extended in this implementation.

QoS-AODV guarantees packet delivery ratio, normalized overhead load and average latency in mobility. But average latency decreases when load increases. Enhancements should have concentrated on keeping load under control.

2.7 QAODV [12]

QAODV – Quality of service AODV, focuses on two efficient route recovery mechanisms for QoS routing based on an extension of the AODV routing protocol that deals with delay and bandwidth constraints. Two route maintenance mechanisms for QAODV - one is based on a special local route repair by limiting route recovery flooding to one hop neighbors only. This approach is QAODV-I (Route Maintenance in QAODV by intermediate node). Other one is route recovery by the destination node itself named QAODV-D (Route Maintenance in QAODV by destination node).

QoS routing based on AODV called QAODV[13] is designed with the following modifications; First modification says, Only destination can reply to RREQ to ensure that the QoS requirements will be satisfied in all nodes from source to destination. Second, an intermediate node receiving RREQ/RREP with QoS extension must examine whether it can satisfy the QoS requirements specified in the RREQ/RREP or not to rebroadcast/forward the packet to the next hop. Third, bandwidth reservation at a node is done at the time of forwarding RREP packet. Fourth, a mechanism to compute available bandwidth at a node, based on neighborhood's bandwidth used information obtained through Hello message exchange is required. Finally a mechanism to calculate forwarding delay at each node. The methodology works based on these modifications to original AODV.

Route Maintenance by Intermediate node (QAODV -I):

Sending RERR back to the source and subsequently initiating a route discovery by the source, for route recovery due to link failure, gives rise to large amount of control overhead, packet loss and delay in the system. For providing QoS support, an efficient and faster route recovery/maintenance mechanism is needed. In this method, each node in an active route remembers the node ID of the second downstream node and updates this information during local route recovery process. The method is based on the observation that, when a link of an active flow breaks, there still exists some neighbor of the upstream node through which the downstream node and/or the 2-hop downstream node of the broken link is reachable with single hop. This is true in a moderately dense network. In the case, the node detecting the link failure finds one such neighbor, it can repair the path very fast by adding an extra node in the repaired path with very little amount of extra control overhead. To incorporate this local route repair in QAODV, a number of control packets are used as follows. LRREQ (Local Route Repair Request) is used to locally broadcast (with TTL=1) local repair request to the neighbor of the node which detects a link failure. LRREP (Local Route Repair Reply) is used to reply to the LRREQ, if a neighbor node can locally repair the route which satisfies the required QoS constraints.

Route maintenance by Destination node (QAODV -D):

The route break will be implicitly detected by the destination by observing the absence of traffic for the route through reservation time- out T of the route. Therefore, the route break detection time used by the destination is implicitly upper bounded by T and defined as $T = (k * N * 8)/B$ [14]. Where k is the allowed packet loss, N is the maximum length of a packet in physical layer (e.g. N is 4095 in IEEE 802.11a) and B is the minimum bandwidth requirement of the flow. Thus, T controls the burstiness and delay jitters of the flow according to minimum bandwidth requirement B of the flow. Route break detection by neighbor lost normally takes several seconds, but for most of the practical real-time application maximum value of T is of the order of 1 sec. Therefore, the bandwidth reservation timer at destination can detect the possible route break due to link failures in the intermediate nodes.

To detect end-to-end delay violation at the destination, each packet sent by source is time stamped with sending time of source. The clock offset of source with respect to destination is computed by the source from round trip delay between source and destination and the destination's timestamp on RREP packets. Destination stores the clock offset value in the routing table entry for the flow. From the clock offset value and the sender's timestamp on the received data packets, destination can compute the end-to-end delay of the data packets. The destination keeps a counter for the number of continuously delay violated packets for a flow. If this counter exceeds a predefined limit the delay violation is triggered and destination initiates a route recovery procedure for the affected flow.

The destination recovers a QoS route with the help a special packet called Destination Route Recovery (RRDES) which is similar to RREQ packet with QoS extension. To recover a route, destination increments its sequence number (to invalidate the previous route entry for the flow) and creates a RRDES packet to find a new QoS path from destination to the source with TTL set to hop count of the failed or QoS violated route plus a small constant. Here, a symmetric connection is assumed. All intermediate nodes process the RRDES like a RREQ, forming forward route entry (like reverse entry during RREQ processing), reserving bandwidth for the flow and rebroadcast RRDES, if the nodes can satisfy QoS constraints specified in the packet. Once source receives a RRDES for an already exists flow in the routing table, it updates the routing table to use the newly formed route.

QAODV reduces control overhead, delay and improves end-to-end delivery ratio and connection setup latency. But the protocol has not proved to be feasible in large and heavily loaded networks. Enhancements should have focused on improving the efficiency of protocol on all environments, like heavily or lightly loaded networks or on large or small networks.

2.8 SQ-AODV [15]

SQ-AODV-- Stability-based QoS-capable Ad-hoc On-demand Distance Vector protocol, is an enhancement AODV protocol focusing on, how residual node energy is used for route selection and maintenance and also focuses on how Protocol quickly adapting to network conditions. The uniqueness of this scheme is that it uses only local information, requires no additional communication or co-operation between nodes It possesses a make- before-break capability that minimizes packet drops and is compatible with the basic AODV data formats and operation, making it easy to adopt.

The two main features of SQ-AODV are that it; Provides stable routes by accounting for the residual life-time (calculated using the current Average- Energy-Drain-Rate (AEDR)) at intermediate nodes and the duration of the session at the route selection stage. *Threshold-1* and *Threshold-2* are the residual energy of a node with which the node is alive for the next X and Y seconds respectively, where in this implementation X = 5 and Y = 1. This also guards against link breakages that arise when the energy of a node(s) along a path is depleted, by performing a make-before-break re-route. This minimizes packet loss and session disruptions. SQ-AODV proactively re-routes sessions, without losing any packets. Once again, this provides near-zero packet loss and superior QoS performance.

The first feature helps in choosing an appropriate sequence of intermediate nodes for the requesting session. The application layer of a source that wishes to communicate with a destination, generates data packets and transmits them to the network layer. At the network layer, the routing protocol responsible for finding a route to the desired destination initiates a route discovery procedure, if it does not already have a route for that destination. An assumption made here is that, if the session-duration is known, the application layer directly provides that to the network layer. If not, each intermediate node uses a heuristic and accepts a session only if it has at least *Threshold-1* of residual life. The source broadcasts Route Request (RREQ) packets to its neighbors when it has no route to the desired destination. When a RREQ packet reaches an intermediate node, queries the physical layer for the current residual energy, and checks whether the residual energy at the current AEDR is sufficient to last the duration of the flow. The session is only admitted if that is the case. If the session-duration is unknown, the algorithm admits the session only if the residual energy at the node is above *Threshold-1*. Before forwarding, the node updates the bottleneck life-time field of the RREQ packet. The Energy-Drain-Rate (EDR) is computed as a difference between the energy En of the node at periodic intervals divided by the length of the interval. Thus, EDR(t2) is calculated by the formula(9)

$$EDR(t_2) = \frac{En(t_1) - En(t_2)}{t_2 - t_1}, \qquad (9)$$

where En(t_1) and En(t_2) are energy levels of the node at times t1 and t_2 respectively. This EDR is averaged using exponential averaging with α = 0.5 to compute the AEDR given by formula(10)

$$AEDR(t) = \alpha \times EDR(t) + (1-\alpha) \times AEDR(t-1) \quad (10)$$

Finally, when the RREQ packets reach the destination, it picks a route that maximizes the route life-time by selecting the one with maximum life-time of the bottleneck node.

The second feature helps the routing protocol to adapt quickly to imminent link breakage likely to occur when the energy of a node is fully drained. Since the physical layer keeps track of the AEDR, it sends an alarm to the network layer, shortly before it is about to drain completely i.e., when the current energy of the node is less than a *Threshold-2*. The routing protocol adapts to this event, and its behavior depends on whether the node is an intermediate (**I**) or a destination (**D**) node. If the node receiving the drain alarm from its physical layer is an **I** node, it sends a Route Change Request (RCR) packet to all source nodes using it as an intermediate hop towards their respective destinations. The source upon receiving the RCR packet, begins a new route discovery procedure for the session, and thus, with high probability, finds a new route before an actual link break occurs on the original route, leading to the *make- before-break* behavior.

This reduces packet drops due to link breakage and the consequent delay incurred, and enables the routing protocol to quickly adapt to network changes, if an alternate path to the desired destination exists. If the node being drained is a **D** node, it sends a request to the source to stop all traffic transmission to itself. When the request reaches the source, the network layer sends a stop signal to the application, preventing further transmission of data. This reduces the number of packet drops in the network and increases packet delivery ratio, and reduces resource usage by avoiding packet transmissions to unavailable destinations. If a source node itself is about to drain, it simply continues to transmit data until it cannot transmit anymore.

SQ-AODV has increased PDR to 10% - 15%, node expiration time is 10 to 50% better , control over head is low and packet delay is low. This still uses only local information at a node without adding any significant overhead in the network. Protocol has not incorporated bandwidth and delay constraints . Enhancements should have taken up all QoS metrics which affects routing on MANET.

Table 1. RESULT ANALYSES OF AODV ENHANCED PROTOCOL

Protocols / QoS parameters	**RAODV**			**AODV-RD**	**AODV-BR**	**qAODV**	**QoS-AODV**			**QSAODV**	**SQ-AODV**
	Mobility						**AODV-BD**			**Heavy traffic**	
	Cont	**low**	**high**				**Nn**	**MT**	**TL**		
Throughput / Good put	high										
Light traffic	Best	better	Poor								
Heavy Traffic	Best	poor	Poor								
PDR				high	good	high	H	SL	H	High	10% - 15% high
Overhead load	Best	more	poor			slightly high	L	L	L	low	
End to end Delay				short	long	short	L	SL	L	long	short
General comments	Cont. – Continues Improves good put by 25%			optimizes the network performance and guarantees the communication quality.	Long Delay compared to AODV	conditions of high load and moderate to high mobility ; though the routing load of AODV is slightly less than that of qAODV	AODV-BD bandwidth and delay Nn – No. of nodes MT – Mobility TL – Traffic Load H – High L – Low SL – slightly low			QS-AODV can provide performance comparable to AODV in light traffic. Mobility affects QSAODV than AODV	The Node expiration time is 10 to 50 % better.

3. RESULT ANALYSES OF AODV ENHANCED PROTOCOLS

The table1 depicts the result analyses of enhanced AODV protocols which have all focused on metrics which affects Quality of service. Results show that the enhancements done has increased the performance of the protocol. But still every enhanced protocol has a draw back and has still failed to show progress in routing metric. The findings are;

Throughput : Increased by 25%(RAODV)

Mobility : Affects the performance of protocol (RAODV, qAODV, QoS-AODV,QSAODV)

PDR : Good for all enhanced protocols

Load : Mobility increases load (RAODV, qAODV)

Delay : Long for certain protocols(AODV-BR, QoS-AODV,QSAODV)

The above findings shows that the traditional AODV protocol which has undergone lot of extensions is still lacking in certain metrics like load and delay. If load and delay regularized it increases PDR and throughput and also reduces unnecessary overheads. Throughput and PDR can still be higher and mobility almost affects all enhanced protocols. Future works should concentrate on enhancements which can be done on AODV in improving its performance without affecting load and delay.

Extensions on protocol should also concentrate on increasing PDR and throughput still higher than the previous enhanced protocols provide. Steps to be taken for controlling the effects of mobility which has great impact on the performance of the protocol.

4. CONCLUSION

In this article , the review of challenges and concepts behind QoS routing in MANETs based on AODV protocol were presented . The enhancements made to the protocol were analyzed. The protocols were selected in such a way as to highlight many different approaches to QoS routing in MANETs, while simultaneously covering most of the important advances in the field since the last such survey was published. This article summarized the operation, strengths, drawbacks and results of these protocols in order to enunciate the variety of approaches proposed and to expose the trends in designers' thinking.

The new protocol should provide high PDR and throughput with short delay, less load and managing the effects of mobility. Enhancements to be done such a way the protocol proves to be best in performing routing in MANETS.

5. REFERENCES

[1] Ashwin Perti, Pradeep Sharma, 2009, "Reliable AODV Protocol for Wireless Ad Hoc Networking", IEEE International Advance Computing Conference.

[2] C.E.Perkins and E.M.Belding-Royer, October 2003, "Quality of service for ad hoc on-demand distance vector routing", IETF MANET Working Group, Internet Draft.

[3] C.E.Perkins, E.M. Royer and S.R. Das," *Ad hoc On-Demand Distance Vector(AODV) Routing"*, IETF Internet Draft: draftietf- manet-aodv-05.txt. (2000a).

[4] C.E Perkins, E.M. Royer and S.R. Das, " Quality of Service for Ad hoc on-demand distance vector routing", IETF Internet Draft: draft-ietf-manet- aodvqos-00.txt. (2000b).

[5] Geunhwi Lim, Kwangwook Shin, Seunghak Lee, Yoon H., 2002, " Link stability and route lifetime in ad-hoc wireless networks ", Proceedings of the International Conference on Parallel Processing Work shops.

[6] I.Jawhar, and J. Wu, "Quality of Service Routing in Mobile Ad Hoc Networks", in M Cardei, I Cardei & DZ Du (eds), Resource Management and Wireless Networking, Kluwer Academic Publishers.

[7] LIU Jian , LI Fang-min ,2009, " An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks", Fifth International Conference on Information Assurance and Security.

[8] Mallapur Veerayya, Vishal S harma, Abhay Karandikar, 2008, "SQ-AODV: a novel energy-aware stability-based routing protocol for enhanced qos in wireless ad-hoc networks".

[9] Nityananda Sarma, Sukumar Nandi, Rakesh Tripathi, 2008, " Enhancing Route Recovery for QAODV Routing in Mobile Ad Hoc Networks", International Symposium on Parallel Architectures Algorithms and Networks.

[10] Nur Idawati Md Enzai, Farhat Anwar, Omer Mahmoud, 2008, "Evaluation Study of QoS-Enabled AODV", International Conference on Computer and Communication Engineering.

[11] Qing Li, Cong Liu, Han-Hong Jiang, 2008, "The routing protocol of AODV based on link failure Pridiction ", Proceedings of the International Conference on Software Process.

[12] Rohit Dube, Cynthia D. Rais, Kuang-Yeh Wang, and Satish K. Tripathi, Feb 1997, " Signal Stability-Based Adaptive Routing (SSA)for Ad Hoc Mobile Networks", IEEE Personal Communications.

[13] Xue and A. Ganz, February 2003, "Ad hoc qos on-demand routing (aqor) in mobile ad hoc networks", *Journal of Parallel and Distributed Computing* 63(2):154–165.

[14] Yihai Zhang and T. Aaron Gulliver, 2005, "Quality of Service for Ad hoc On-demand Distance Vector Routing.

[15] Yu Ping, Wang Ying, 2009, " A Revised AODV Protocol with QoS for Mobile Ad hoc Network".