ISSN 0974 - 9373

Vol. 16 No. 4 (2012) **Journal of International Academy of Physical Sciences** pp. 421-433

A Survey on QoS in AODV Routing Protocol for MANET

Amit Garg
Department of Computer Applications
Meerut Institute of Engineering & Technology, Meerut (U.P.)
Email: foramitgarg@gmail.com

Sandeep Kr. Agarwal
Department of Computer Applications
Bharat Institute of Technology, Meerut (U. P.)
Email: bit.sandeep@gmail.com

K. V. Arya
Department of Information Technolog
ABV-Indian Institute of Information Technology & Management (IIITM), Gwalior

(Received December 22, 2011)

Abstract: Mobile Ad-hoc Network (MANET) is an infrastructure less mobile network, where the nodes communicate with each other in spite of frequent changes in network topology due to mobility, interference and highly error prone environment. Multimedia communication within MANET requires certain Quality of Services (QoS) constraints. Providing QoS in MANET is not an easy task due to its broadcast and dynamic nature, node mobility and resource constraints. There exist many protocols which take care of the QoS. Ad-hoc On-Demand Distance Vector (AODV) routing protocol is one of the well known MANET protocol, but have some limitations in term of QoS constraints. Many modifications have been suggested towards improvement in AODV performance to meet QoS challenges through focusing on bandwidth, Packet delivery ratio, energy and mechanism overheads.This paper exclusively summarizes all such modifications suggested for AODV, along with their benefits and limitations. The aim of this paper is to facilitate literature survey in future researches such that several proposed modifications in AODV routing protocol can be probed quickly, and to identify areas for future research.

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

1. Introduction

A mobile ad hoc network (MANET)[1] can be defined as a network of nodes that communicate with each other through wireless links, in absence of a fixed network infrastructure. This form of networks is limited in range, node mobility, security of data, lack of proper communication and limited bandwidth. Having these characteristics, MANETs can be widely used in various application areas like military applications, disaster relief, shopping malls, other personal area networks, and all such areas where a fixed network infrastructure can not be established. There are few limitations also like the poor reliability of data transmission, due to MANET characteristics like dynamic topology, limited bandwidth, and other resource constraints. Likewise, regular updation of link state information results in extensive control overhead.

A key issue in MANETs is the necessity that the routing protocols must be able to respond rapidly to topological changes in the network while keeping minimum control traffic. The routing in MANETs depends on the cooperation of intermediate nodes. All the nodes of these networks behave as routers and take part in discovery and maintenance of routes. There are several existing protocols to address the problems of routing in mobile ad-hoc networks. Such protocols are divided into two classes, depending on when a node acquires a route to a destination[2].

1**. Proactive protocols** continuously learn the topology of the network by exchanging topological information among the network nodes. Thus, when there is a need for a route to a destination, such route information is available immediately. The early proactive protocols were based on the Distributed Bellman-Ford (DBF) algorithm. Another example is the Optimized Link State Routing protocol (OLSR) which proposes application of the Link State protocols to the ad hoc environment. These protocols are also known as Table driven routing protocols.

2**. Reactive protocols** are characterized by nodes acquiring and maintaining routes on-demand. In general, when a route to an unknown destination is required by a node, a query is flooded onto the network and replies, containing possible routes to the destination, are returned. As such, such protocols are often also referred to as on demand. Examples of reactive protocols include the Temporally Ordered Routing Algorithm (TORA), the Dynamic Source Routing (DSR), and Ad hoc On Demand Distance Vector (AODV)[2].

Ad-hoc On Demand Distance Vector (AODV) protocol is an example of on demand routing protocol that focuses on discovering the shortest path between two nodes. AODV has characteristics like simplicity, low computational complexity and low processing overhead. The major drawback of AODV is the shortage of the Quality of Service (QoS) provisions. 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. A key to provide QoS is to find a route to the desired destination that can, with high probability, survive for the duration of the session. It is a challenging task to ensure QoS provisioning in ad-hoc networks due to the mobile and dynamic nature of the nodes.

The objective of this paper is to present the discussion and analysis of various modifications proposed to the traditional AODV protocol, from QoS point of view. The following sections are having description of methodology, advantages & limitations, and result analysis of various enhancements proposed to the traditional AODV protocol. In the end, a summarized comparative view of different AODV extensions is given, which focuses on some major QoS metrics.

2. QoS in MANETs

Quality of Service (QoS) refers to the set of mechanisms for sharing various resources offered by the network, among applications, in a fair manner[3]. The Quality of Service (QoS) specifications and management are required to support multimedia applications (such as video and audio transmissions)[4]. In multimedia, this might include picture quality, image quality, delay and speed of response. From a technical perspective, QoS characteristics may include timeliness (e.g. less delay and high response time), bandwidth (e.g. bandwidth required or available), and reliability. The QoS parameters can be summarized as:

- Bandwidth (The data rate for an application's traffic),
- Latency (delay between packet send time and packet arrival time.),
- Jitter (The variation in latency.),
- Loss (The percentage of packet loss.) and
- PDR (packet delivery ratio).

Implementing QoS in MANETs is difficult due to its broadcast and dynamic nature. First, unlike wired networks, a wireless link's bandwidth may be affected by the transmission of adjacent links. Second, unlike cellular networks, which only need to guarantee quality for one hop, in MANET we must guarantees the quality for the multiple hops in the path. Third, mobile hosts may leave or join at any location and time, existing links may get disappear and new links may be formed as host moves.

There are various existing QoS aware routing protocols, which use to reserve the bandwidth and to satisfy QoS needs of a flow. All such protocols have some limitations. Ad hoc On-Demand Distance Vector routing (AODV)[2] is one of the popular MANET protocol which takes care of QoS issues. AODV has faster bandwidth reservation process with delay and cost constraints.

3. QoS in AODV[2, 5]

AODV is designed to improve upon the performance characteristics of proactive protocols like Destination-Sequenced Distance-Vector (DSDV) in the creation and maintenance of routes. AODV decreases the control overhead by minimizing the number of broadcasts using a pure on-demand route acquisition method.

3.1 Route Discovery

A route discovery process is initiated when a node requires communicating with a node for which it has no route by broadcasting a Route Request (RREQ) packet. RREQ packet contains source IP address, source’s current sequence number; broadcast-ID, destination IP address, destination’s last sequence number, and hop-count. Hop-Count is initially 0 and is incremented by each node as it forwards the RREQ towards the destination. The broadcast ID is incremented each time the source node initiates RREQ. The sequence numbers are used to determine the timeliness of each data packet and the broadcast ID & the IP address together form a unique identifier for RREQ so as to uniquely identify each request. An intermediate node upon receiving a RREQ first checks that whether RREQ is received over a bi-directional link. Then the node matches with already processed RREQ. If it is same, the packet is discarded, otherwise it does the following:

1. The node checks if it has a route entry for the destination. If it has a routing table entry for the destination then it replies to the source only if the destination sequence number in RREQ is greater than the destination sequence number in its route table otherwise it rebroadcasts the RREQ packet,

2. Reverse Path is established as the RREQ traverses towards the Destination. The process is described in Fig.1 and 2, where the direction arrow indicates the movement of packets:

When the destination node or an intermediate node with a route to the destination receives the RREQ, it creates the RREP and unicasts the same towards the source node using the node from which it received the RREQ as the next hop. When RREP is routed back along the reverse path and received by an intermediate node, it sets up a forward path entry to the destination in its routing table. When the RREP reaches the source node, it means a route from source to the destination has been established and the source node can begin the data transmission.

A neighbor is considered active (for a destination) if it originates or relays at least one packet for the destination within the most recent active timeout period. This is maintained so that all active source nodes can be notified when a link along a path to destination breaks. When a new route is presented, the route entry is updated based on hop-count and sequence numbers. If the source node moves, the route discovery procedure is reinitiated to find the new route to destination.

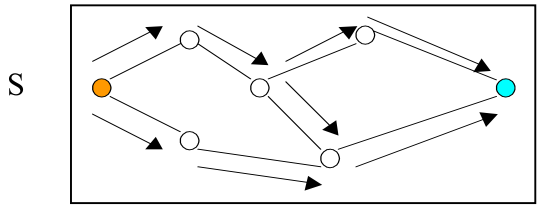

Fig.1: Propagation of the RREQ from Source 'S' to Dest. 'D'

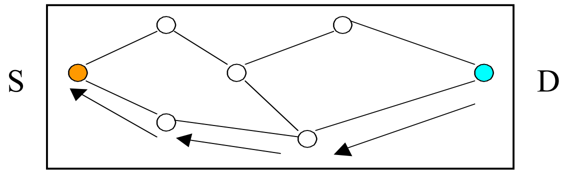

Figure 2: Propagation of the RREP from Dest. 'D' to Source S

If some intermediate node or the destination moves, a special Route Reply (RREP) message is sent towards the source containing a new sequence number (one greater than the previously known sequence number) and hop-count to infinity. The subsequent nodes relay it until it reaches source, which then initiates a new route discovery procedure if required.

3.2 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 a certain limit, the upstream node of the broken link sends a RREQ packet to the destination. If the local repair request is successful, a RREP packet is returned 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 Route Error (RERR) packet is sent to the source node. The RERR packet inludes all the unreachable destinations and their known sequence number. 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 node. After the source node receives the RERR packet, it may initiate route discovery if it still needs a route.

Among the benefits of AODV protocol is that it favors the least congested route instead of the shortest route and it also supports both unicast and multicast packet transmissions. It also responds very quickly to the topological changes that affects the active routes. AODV does not put any additional overhead on data packets as it does not make use of source routing. The limitation of AODV protocol is that it expects that the nodes in the broadcast medium could detect each others' broadcasts. It is also possible that a valid route is expired and the determination of a reasonable expiry time is difficult. The reason behind this is that the nodes are mobile and their sending rates may differ widely and can change dynamically from node to node. In addition, as the size of network grows, various performance metrics begin decreasing. AODV is vulnerable to various kinds of attacks as it based on the assumption that all nodes must cooperate and without their cooperation no route can be established.

4. QoS Enhancements in AODV – An Analysis

4.1 AODV – Backup Routing (AODV-BR)[6]

AODV-BR establishes multiple routes to destination. If the primary route breaks, alternate route can be initiated to carry out data transmission. Before sending packets, source node looks for routing information about destination through arrived packets entry in routing table. If there is routing information, source node transmits the data packets. Otherwise, it starts route discovery process.

Source node searches a route by flooding a route request (RREQ) packet to neighbor nodes. The neighbor node then either broadcasts the packet or sends back a route reply (RREP) packet to the source, if it has a route to the destination. When a node receives RREP from a neighbor, this neighbor node will be recorded in the routing table as the 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.
AODV – BR sets up the alternate routes in order to achieve reliability of communication without extra control message. However this algorithm has no repairing action when a route breaks. It simply rebuilds route according to the alternate routing table, so it is not fit for the networks whose topology change frequently.

4.2 QoS Enabled AODV (QoS-AODV)[7]

In QoS-AODV –, the original AODV is extended by adding new fields including maximum delay extension and minimum bandwidth extension. In order to provide QoS, extensions can be added to these messages during the route discovery process. Several extensions are also needed in the routing table structure and the RREQ and RREP messages as reported in[3,5].

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. 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. Future works can focus on keeping load under control.

4.3 Quality of service AODV (QAODV)[8]

QAODV is designed with the few modifications to traditional AODV protocol:

1. Only destination can reply to RREQ to ensure that the QoS requirements will be satisfied in all nodes from source to destination.
2. An intermediate node receiving RREQ/RREP with QoS extension must examine whether it can satisfy the specified QoS requirements or not, to forward the packet to the next hop.
3. Bandwidth reservation at a node is done at the time of forwarding RREP packet.
4. A mechanism to compute available bandwidth at a node.
5. A mechanism to calculate forwarding delay at each node.

QAODV focuses on two efficient route recovery mechanisms for QoS routing. One is QAODV-I (Route Maintenance in QAODV by intermediate node). The other one is QAODV-D (Route Maintenance in QAODV by destination node).

4.3.1 Route Maintenance by Intermediate node (QAODV -I)

The method is based on the observation that, when a link of an active flow breaks, there exists some neighbor of the upstream node through which the downstream node or the 2-hop downstream node of the broken link is reachable. If the node, detecting the link failure, finds such a neighbor, it can repair the path quickly just by adding an extra node in the repaired route with very little amount of extra control overhead.

4.3.2 Route maintenance by Destination node (QAODV -D)

The route break can be detected by the destination by observing the absence of traffic for the route through reservation time-out of the route. To recover a route, destination creates a special packet called Destination Route Recovery (RRDES) to find a new QoS path from destination to the source, which is similar to RREQ packet with QoS extension. All intermediate nodes process the RRDES like a RREQ, forming forward route entry, 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.

To detect end-to-end delay violation at the destination, destination can compute the end-to-end delay through the clock offset value and the sender's timestamp on the received data packets. The destination maintains a counter for the number of packets in a flow, which have delay violation continuously. If this counter exceeds a predefined limit, the destination initiates a route recovery procedure for the affected flow.

QAODV claims to reduce 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. There is a need to improve the efficiency of protocol in all environments.

4.4 Stability based QoS capable AODV (SQ-AODV)[9]

SQ-AODV focuses on how residual node energy can be used for route selection and maintenance and it also considers how a protocol can quickly adapt the network conditions. The proposed scheme is using only local information that is no additional communication between nodes is required. The two main features of SQ-AODV are:

1. Providing stable routes by accounting for the residual life-time using the Average Energy Drain Rate (AEDR) at intermediate nodes and the duration of the session.
2. Providing guard against link breakages that arise when the energy of node(s) along a path is depleted, by performing a make-before-break re-route.

The first feature helps in choosing an appropriate sequence of intermediate nodes for the requesting session. It is assumed that, if the session-duration is known, the application layer would directly provide that information 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. When a RREQ packet reaches an intermediate node, queries the physical layer for the current residual energy, and checks whether the residual energy is sufficient to last the duration of the flow. The session is only admitted if that is the case. Finally, when the RREQ packets reach the destination, it picks a route that maximizes the route life-time

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. The physical layer sends an alarm to the network layer, shortly before the node is about to drain completely. If the node receiving the drain alarm from its physical layer is an intermediate node, it sends a Route Change Request (RCR) packet to all source nodes. 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. 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. If a source node itself is about to drain, it simply continues to transmit data until it cannot transmit anymore.

SQ-AODV has shown increased PDR, better node expiration time, low control over head and low packet delay. However, SQ-AODV has not incorporated bandwidth and delay constraints. It is desirable that an enhancement should consider all such QoS metrics which affect routing in MANET.

4.5 AODV – Reliable Delivery (AODV-RD)[10]

AODV-RD focuses on a link failure fore-warning mechanism, in order to select a better route and repairing action if the primary route breaks.

In MANETs, the strength of the received packet signal *Pr*[8] depends on several parameters like strength of the transmitting signal, antenna gain of the receiver and transmitter, and the distance between the sending node and the received node. A power warning threshold is defined as *Pr_critical.* When *Pr* is lower than *Pr_critical*, it means the link state is unstable and it can interrupt at any time. Then the source node immediately accesses the alternate route selection process. After selection, the primary route switches to alternate route.

For selecting an alternate node, AODV-RD follows Signal Stability-Based Adaptive Routing (SSA)[11]. SSA method is based on the strong or weak communication signals of the two adjacent nodes. Choose the node as an alternate node, which corresponds to a strong link.

AODV-RD protocol has shown increased PDR and has shortened end to end delay in comparison to AODV – BR. But it has longer end to end delay in comparison to traditional AODV. The future works can concentrate on reducing end to end delay and further optimization.

4.6 Reliable AODV (RAODV)[12]

RAODV focuses on a solution that detects and avoids misbehaving nodes, which agree to route packets for other nodes and subsequently drop these packets. The misbehavior of nodes has a direct impact on QoS good put metric. RAODV covers two type of misbehaving nodes: selfish nodes and malicious node. Selfish nodes use the network but do not cooperate, in order to save battery life for their own communication. Malicious nodes on the other hand aim to damaging other nodes communication by blackmailing a legitimate node by unjustifiable advertising that this node is misbehaving.

The RAODV adds two tables to each mobile node to maintain information about the behavior of the neighbor nodes. Initially, all nodes are marked as well behaving nodes. Each node keeps track of the sent packets in a pending packet buffer. Each buffer entry contains an expiry time after which a still-existing packet in the buffer is considered not forwarded by the next hop, besides other parameters. Each node also keeps ratings of neighboring nodes in a node rating table. Each entry in this table contains the node address and a counter of successfully forwarded data packets by this node. If the timer of an entry in the pending packet buffer expires without being forwarded, the node is considered to have committed misbehavior. This results in incrementing its forwarding failure counter in the node-rating table. If the value exceeds the threshold then the node is marked as misbehaving. After detecting a misbehaving node, the detecting node performs a local repair for all routes passing through the misbehaving node. This involves replacing each route consisting of this misbehaving node with another one. To avoid constructing new routes, all packets originating from a misbehaving node can be dropped as a form of punishment. Only dropping data packets will decrease node rating.

RAODV protocol claims to increase good put by 25% and to decrease the misbehaving ratio. But RAODV 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. Necessary actions are suggested to avoid partial dropping and defense against changing packets payload and mobility impact.

4.7 Modified AODV (MAODV)[13]

MAODV suggests a new mechanism for determining multiple disjoint routes from source to destination. In MAODV, all possible paths are discovered between sources and destinations. The path information is maintained during all data transfers. In case of a failure of primary route, the data transfer will use an alternate route from previously discovered routes. The failure state is declared only if all discovered paths are not usable.

MAODV focuses on reducing the packet loss. There are two main reasons, which cause packet loss. The first reason is broken link due to frequent topology changes. Another reason is queue overflow associated with each node because the source node continues to send data packets, because of being unaware about the local root repair. Packet loss can be reduced by discovering multiple paths and rationalizing the bandwidth usage by transferring more data packets and less control packets.

In this protocol, when the source wishes to transmit, it broadcasts RREQ for route discovery. As soon as source receives RREP from an intermediate node, which has any path to destination, or from destination, different routes are identified. Among them completely disjoint routes are selected, one will be taken as primary route and other as alternate routes. Source is responsible for route management but intermediate nodes are responsible only for updating routing tables. In case of link failure, source stops transmission and repeats operations from the spare path available.

MAODV has given better results then the traditional AODV protocol with respect to QoS parameters and different constraints like load control overhead, packet loss and reliability. Still the protocol can be extended for large scale networks.

5. Results Summary

All the above discussed extensions of AODV protocol are focusing on metrics which primarily affects Quality of service. Results show that the various improvements have contributed towards increase in the performance of traditional AODV. But still a number of drawbacks and shortcomings are there. The findings are summarized as following:

QoS Parameter	**Performance Remarks**
Throughput	Almost all enhancements have better throughput, specially RAODV.
Packet Delivery Ratio (PDR)	Every extension has shown improvement in PDR in comparison to traditional AODV.
End to end delay	Every extension has shown shorter end to end delay. But, in AODV-RD, end to end delay is longer in comparison to traditional AODV
Control overhead	QoS-AODV, QAODV, SQAODV, and MAODV have shown low control overhead in their results.
Scalability	QAODV, RAODV, and MAODV are not fit for large/ growing networks.
Effect of Mobility	AODV-BR and RAODV are not suitable for highly mobile networks, where topology changes frequently.
Reliability	AODV-BR, SQAODV, RAODV, and MAODV have shown improved reliability in their results.

6. Conclusion

In this paper, various modifications proposed to the traditional AODV protocol, from QoS point of view have been discussed and analyzed in a chronological manner. The effort is made to analyze/ discuss all extensions proposed, to highlight different approaches towards QoS routing in MANETs. We have tried to summarize the working principles, available mechanisms, strengths, and weaknesses of all extensions available till date including past surveys. The above findings show that every new extension has a challenge to come up with improved PDR and throughput with short delay, while managing the effects of mobility. Future works should concentrate on extensions which can improve the performance of AODV without affecting its qualities. A number of further research areas are also indicated in the paper.

References

1. Haas Z. J., Deng Jing, Deng Ben, Papadimitratos Panagiotis, and Sajama S, *Wireless Ad Hoc Networks*, Wiley Encyclopedia of Telecommunications (2003).
2. Perkins C. and Royer E. M., Ad Hoc On Demand Distance Vector (AODV) Routing, IEEE WMCAS', **99** (1999) 90-100.
3. Jawhar and J. Wu., Quality *of Service Routing in Mobile Ad Hoc Network*, M Cardei, I Cardei & DZ Du (eds), Resource Management and Wireless Networking, Kluwer Academic Publishers.
4. Zeinalipour-Yazti Dermetrios, *A Glance at Quality of Services in Mobile Ad-Hoc Network*, Final research report for CS260- seminar in MANET (2001).
5. Perkins C.E, 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(2000).
6. Lee S. J. and Gerla M., *AODV-BR: Backup Routing in Ad hoc Networks*, Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), (2000) 1311–1316.
7. Nur Idawati Md Enzai, Farhat Anwar and Omer Mahmoud, *Evaluation Study of QoS-Enabled AODV*, International Conference on Computer and Communication Engineering (2008).
8. Sarma Nityananda, Nandi Sukumar, and Tripathi Rakesh , *Enhancing Route Recovery for QAODV Routing in Mobile Ad Hoc Networks*, International Symposium on Parallel Architectures Algorithms and Networks (2008).
9. Veerayya Mallapur, Sharma Vishal and Karandikar Abhay, SQ-AODV, *a novel energy-aware stability-based routing protocol for enhanced qos in wireless ad-hoc networks* (2008).
10. Jian LIU and Fang-min LI, *An Improvement of AODV Protocol Based on Reliable Delivery in Mobile Ad hoc Networks* , Fifth International Conference on Information Assurance and Security (2009).
11. Rohit Dube, D. Cynthia Rais, Wang Kuang-Yeh and Satish K.. Tripathi, *Signal Stability-Based Adaptive Routing (SSA) for Ad Hoc Mobile Networks*, IEEE Personal Communications (1997).
12. Ashwin Perti, Pradeep Sharma, Reliable *AODV Protocol for Wireless Ad Hoc Networking*, IEEE International Advance Computing Conference (2009).
13. Maamar Sedrati, Azeddine Bilami and Mohamed Benmohamed, January M-AODV: AODV Variant to Improve Quality of Service in MANETs, *IJCSI International Journal of Computer Science Issues*, **8**(2011).