



An Overview of AODV Routing Protocol

Prateek Thakral

UIET, Kurukshetra University, Kurukshetra
Haryana, INDIA

Abstract: Mobile ad hoc networks can be defined as a collection of large number of mobile nodes that form temporary network without help of any existing network infrastructure or central access point. The ad hoc on-demand distance vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems associated with classical distance vector protocols. This paper describes AODV routing protocol in detail along with its message types, terminology and operation.

Keywords: MANET, Routing protocols, AODV, Route Request, Route Reply, Route Error, Sequence Number

I. INTRODUCTION

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication [1]. AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program [2]. The rest of the paper is organized as follows. Section II discusses the different types of messages used in AODV routing protocol. Section III discusses the AODV terminology whereas section IV gives detail information about various operations performed by AODV routing protocol. Finally conclusion is done in section V.

II. AODV MESSAGE TYPES

Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. These message types are received via UDP, and normal IP header processing applies. So, for instance, the requesting node is expected to use its IP address as the Originator IP address for the messages. For broadcast messages, the IP limited broadcast address (255.255.255.255) is used. This means that such messages are not blindly forwarded. However, AODV operation does require certain messages (e.g., RREQ) to be disseminated widely, perhaps throughout the ad hoc network. The range of dissemination of such RREQs is indicated by the TTL in the IP header. Fragmentation is typically not required. AODV is a routing protocol and it deals with route table management. Route Table information must be kept for short-lived routes, such as are created to temporarily store reverse paths towards nodes originating RREQs. AODV uses the following fields with each route table entry [3][4]:

- Destination IP Address
- Destination Sequence Number
- Valid Destination Sequence Number flag
- Network Interface
- Hop Count (number of hops needed to reach destination)
- Next Hop
- List of Precursors
- Lifetime (expiration or deletion time of the route)

Managing the sequence number is crucial to avoiding routing loops, even when links break and a node is no longer reachable to supply its own information about its sequence number. A destination becomes unreachable when a link breaks or is deactivated. When these conditions occur, the route is invalidated by operations involving the sequence number and marking the route table entry state as invalid.

III. AODV TERMINOLOGY

This protocol specification uses conventional meanings for capitalized words such as MUST, SHOULD, etc. to indicate requirement levels for various protocol features. This section defines other terminology used with AODV [5]:

- **Active Route:** A route towards a destination that has a routing table entry that is marked as valid. Only active routes can be used to forward data packets.
- **Broadcast:** Broadcasting means transmitting to the IP Limited Broadcast address, 255.255.255.255. A broadcast packet may not be blindly forwarded, but broadcasting is useful to enable dissemination of AODV messages throughout the ad hoc network.
- **Destination:** An IP address to which data packets are to be transmitted. Same as "destination node". A node knows it is the destination node for a typical data packet when its address appears in the appropriate field of the IP header. Routes for destination
- **Forward Route:** A route set up to send data packets from a node originating a Route Discovery operation towards its desired destination.
- **Invalid Route:** A Route that has expired, denoted by a state of invalid in the routing table entry. An invalid route is used to store previously valid route information for an extended period of time. An invalid route cannot be used to forward data packet, but it can provide information useful for route repairs, and also for future RREQ messages.
- **Sequence Number:** A monotonically increasing number maintained by each originating node. In AODV routing protocol messages, it is used by other nodes to determine the freshness of the information contained from the originating node.

IV. AODV OPERATION

This section describes the scenarios under which nodes generate Route Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages for unicast communication towards a destination, and how the message data are handled. In order to process the messages correctly, certain state information has to be maintained in the route table entries for the destinations of interest [6][7].

- **Maintaining Sequence Numbers:** Every route table entry at every node MUST include the latest information available about the sequence number for the IP address of the destination node for which the route table entry is maintained. This sequence number is called the "destination sequence number". It is updated whenever a node receives new (i.e., not stale) information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination. AODV depends on each node in the network to own and maintain its destination sequence number to guarantee the loop-freedom of all routes towards that node. A destination node increments its own sequence number in two circumstances:
 - i. Immediately before a node originates a route discovery, it MUST increment its own sequence number. This prevents conflicts with previously established reverse routes towards the originator of a RREQ.
 - ii. Immediately before a destination node originates a RREP in response to a RREQ, it MUST update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet.
- **Route Table Entries and Precursor Lists:** When a node receives an AODV control packet from a neighbor, or creates or updates a route for a particular destination or subnet, it checks its route table for an entry for the destination. In the event that there is no corresponding entry for that destination, an entry is created. The sequence number is either determined from the information contained in the control packet, or else the valid sequence number field is set to false. The route is only updated if the new sequence number is either:
 - i. Higher than the destination sequence number in the route table, or
 - ii. The sequence numbers are equal, but the hop count (of the new information) plus one, is smaller than the existing hop count in the routing table, or
 - iii. The sequence number is unknown. The Lifetime field of the routing table entry is either determined from the control packet, or it is initialized to ACTIVE_ROUTE_TIMEOUT. This route may now be used to send any queued data packets and fulfills any outstanding route requests.
- **Generating Route Requests:** A node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node; or if a previously valid route to the destination expire or is marked as invalid. The Destination Sequence Number field in the RREQ message is the last known destination sequence number for this destination and is copied from the Destination Sequence Number field in the routing table. If no sequence number is known, the unknown sequence number flag MUST be set. The

Originator Sequence Number in the RREQ message is the node's own sequence number, which is incremented prior to insertion in a RREQ. The RREQ ID field is incremented by one from the last RREQ ID used by the current node. Each node maintains only one RREQ ID. The Hop Count field is set to zero.

- **Processing and Forwarding Route Requests:** When a node receives a RREQ, it first creates or updates a route to the previous hop without a valid sequence number then checks to determine whether it has received a RREQ with the same Originator IP Address and RREQ ID within at least the last PATH_DISCOVERY_TIME. If such a RREQ has been received, the node silently discards the newly received RREQ. The rest of this subsection describes actions taken for RREQs that are not discarded. First, it first increments the hop count value in the RREQ by one to account for the new hop through the intermediate node. Then the node searches for a reverse route to the Originator IP Address, using longest-prefix matching. If need be, the route is created, or updated using the Originator Sequence Number from the RREQ in its routing table. This reverse route will be needed if the node receives a RREP back to the node that originated the RREQ (identified by the Originator IP Address).

- **Generating Route Replies:** A node generates a RREP if either:
 - i. it is itself the destination, or
 - ii. it has an active route to the destination, the destination sequence number in the node's existing route table entry for the destination is valid and greater than or equal to the Destination Sequence Number of the RREQ (comparison using signed 32-bit arithmetic), and the "destination only" ('D') flag is NOT set.

When generating a RREP message, a node copies the Destination IP Address and the Originator Sequence Number from the RREQ message into the corresponding fields in the RREP message. Processing is slightly different, depending on whether the node is itself the requested destination, or instead if it is an intermediate node with fresh enough route to the destination. Once created, the RREP is unicast to the next hop toward the originator of the RREQ, as indicated by the route table entry for that originator. As the RREP is forwarded back towards the node which originated the RREQ message, the Hop Count field is incremented by one at each hop. Thus, when the RREP reaches the originator, the Hop Count represents the distance, in hops, of the destination from the originator.

- **Receiving and Forwarding Route Replies:** When a node receives a RREP message, it searches (using longest-prefix matching) for a route to the previous hop. If needed, a route is created for the previous hop, but without a valid sequence number. Next, the node then increments the hop-count value in the RREP by one, to account for the new hop through the intermediate node. Call this incremented value the "New Hop Count". Then the forward route for this destination is created if it does not already exist. Otherwise, the node compares the Destination Sequence Number in the message with its own stored destination sequence number for the Destination IP Address in the RREP message. Upon comparison, the existing entry is updated only in the following circumstances:

- i. The sequence number in the routing table is marked as invalid in route table entry
- ii. The Destination Sequence Number in the RREP is greater than the node's copy of the destination sequence number and the known value is valid, or
- iii. The sequence numbers are the same, but the route is marked as inactive, or
- iv. The sequence numbers are the same, and the New Hop Count is smaller than the hop count in route table entry.

- **Route Error (RERR) Messages, Route Expiry and Route Deletion:** Generally, route error and link breakage processing requires the following steps:

- i. Invalidating existing routes
- ii. Listing affected destinations
- iii. Determining which, if any, neighbors may be affected
- iv. Delivering an appropriate RERR to such neighbors

A Route Error (RERR) message MAY be either broadcast (if there are many precursors), unicast (if there is only 1 precursor), or iteratively unicast to all precursors (if broadcast is inappropriate). Even when the RERR message is iteratively unicast to several precursors, it is considered to be a single control message for the purposes of the description in the text that follows. With that understanding, a node SHOULD NOT generate more than RERR_RATELIMIT RERR messages per second. A node initiates processing for a RERR message in three situations:

- i. if it detects a link break for the next hop of an active route in its routing table while transmitting data (and route repair, if attempted, was unsuccessful), or
- ii. if it gets a data packet destined to a node for which it does not have an active route and is not repairing (if using local repair), or

- iii. if it receives a RERR from a neighbor for one or more active routes.

➤ **Interfaces:** Because AODV should operate smoothly over wired, as well as wireless, networks, and because it is likely that AODV will also be used with multiple wireless devices, the particular interface over which packets arrive must be known to AODV whenever a packet is received. This includes the reception of RREQ, RREP, and RERR messages. Whenever a packet is received from a new neighbor, the interface on which that packet was received is recorded into the route table entry for that neighbor, along with all the other appropriate routing information. Similarly, whenever a route to a new destination is learned, the interface through which the destination can be reached is also recorded into the destination's route table entry. When multiple interfaces are available, a node retransmitting a RREQ message rebroadcasts that message on all interfaces that have been configured for operation in the ad-hoc network, except those on which it is known that all of the nodes neighbors have already received the RREQ. For instance, for some broadcast media (e.g., Ethernet) it may be presumed that all nodes on the same link receive a broadcast message at the same time. When a node needs to transmit a RERR, it SHOULD only transmit it on those interfaces that have neighboring precursor nodes for that route.

V. CONCLUSION

An Ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or infrastructure. Such networks have no fixed topology due to the high degree of node mobility. Hence, efficient and reliable routing is one of the key challenges in mobile ad hoc networks. Many routing algorithms have been proposed and developed for accomplishing this task. This paper describes the one of the most commonly used routing protocol known as ad-hoc on demand distance vector (AODV) protocol. The various message types such as Route Request, Route Reply, Route Error, etc supported by AODV are discussed here. Also the focus is made on AODV terminology which includes active route, sequence number, destination, and various other factors which plays an important role in AODV routing protocol. Finally, the complete operation of this routing protocol is discussed in detail where function of each message type and various other parameters are included.

REFERENCES

- [1] C.Siva Ram Murthy & B.S Manoj, "Mobile Ad Hoc Networks- Architectures & Protocols" Pearson Education, New Delhi, 2004.
- [2] Zhou and Haas, December 1999 "Securing Ad Hoc Networks". IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30.
- [3] Elizabeth M. Royer and Chai-Keong Toh. "A review of current routing protocols for ad hoc mobile wireless networks". Technical report, University of California and Georgia Institute of Technology, USA, 1999.
- [4] Jerry Svedlund and Johan Köpman, "Routing protocols in wireless ad-hoc networks – An implementation study". Uppsala: Uppsala University. Master thesis.
- [5] Charles E. Perkins and Elizabeth M. Royer. "Ad-hoc on-demand distance vector routing". Technical report, Sun Micro Systems Laboratories, Advanced Development Group, USA.
- [6] Charles E. Perkins, Elizabeth M. Royer, Samir R. Das. Ad Hoc On-Demand Distance Vector (AODV) Routing draft-ietf-manet-aodv-03.
- [7] C. Perkins, E. Royer, and S. Das. Ad hoc on demand distance vector (AODV) routing for ip version 6 Internet Draft, Internet Engineering Task Force, November 2001.