Ad hoc On-Demand Distance Vector (AODV) Routing

Joe Barnes
Chad Magers

Introduction

- AODV enables "dynamic, self-starting, multi-hop routing between mobile nodes wishing to establish and maintain an ad hoc network"[1] .
- AODV allows for the construction of routes to specific destinations and does not require that nodes keep these routes when they are not in active communication.
- AODV avoids the "counting to infinity" problem by using destination sequence numbers. This makes AODV loop-free.

Overview

- AODV defines 3 message types:
  - Route Requests (RREQs)
  - Route Replies (RREPs)
  - Route Errors (RERRs)

- RREQ messages are used to initiate the route finding process.

- RREP messages are used to finalize the routes.

- RERR messages are used to notify the network of a link breakage in an active route.

Overview

- The AODV protocol is only used when two endpoints do not have a valid active route to each other.
- Nodes keep a “precursor list” that contains the IP address for each of its neighbors that are likely to use it for a next hop in their routing table.
- Route table information must be kept for all routes even short-lived routes.

Overview

- The routing table fields used by AODV are:
  - Destination IP Address
  - Destination Sequence Number
  - Valid Destination Sequence number flag
  - Other state and routing flags
  - Network Interface
  - Hop Count
  - Next Hop
  - List of Precursors
  - Lifetime

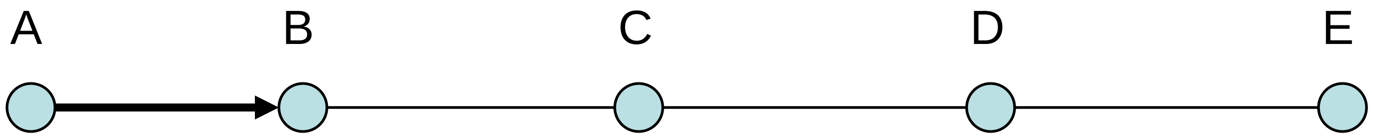
Overview

- The authors point out that the AODV protocol is designed for mobile ad hoc networks of tens to thousands of nodes.

- The protocol was also designed to work in a network where all the nodes trust each other.

Simple Example

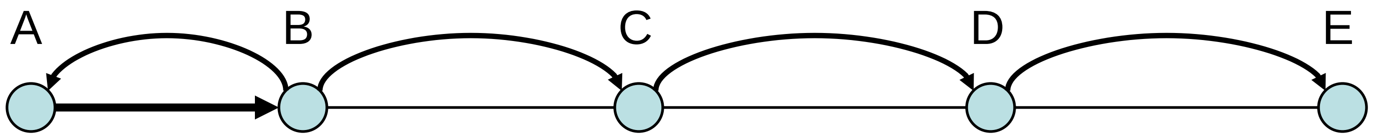
- Node A wants to send a message to node E.
- A valid route must be created between A and E.



- Node A generates a RREQ message with initial TTL of 1 and broadcast it to its neighbors. (In this case node B)
- The Message contains among other items node A's IP address and the IP address of node E.

Simple Example

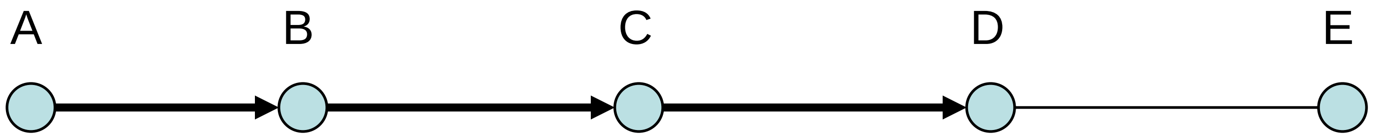
- IF node B has an active route to node E then B will send a RREP message back to node A.



- If A sets a special flag in the RREQ message, node B will also send a “gratuitous” RREP message to node E.
- This will be necessary if node B will need to send packets back to A, i.e. TCP connection.
- RREP messages are unicast to the next hop toward the originator or destination if it is a gratuitous RREP.

Simple Example

- If A does not receive a RREP message within a certain time, it will re-broadcast the RREQ message with an incremented TTL value.



- Default increment is 2
- “Reverse” routes to the originator, in this case node A, are created as RREQ messages are forwarded.
- Active route is established when A receives a RREP message.
- This behavior (Incrementing TTL) keeps network utilization down.

Maintaining Sequence Numbers

- The proper maintenance of sequence numbers is crucial to keeping AODV loop-free and thereby avoiding the "counting to infinity" problem.
- Forwarding nodes only update their stored sequence number for a given destination when forwarding RREP messages and only when:
  - The sequence number in the routing table is invalid, or
  - The sequence number in the RREP message is greater than the stored number, or
  - The sequence numbers are identical, but the route is marked as inactive, or
  - The sequence numbers are the same, but the hop count is smaller for the RREP message.

Maintaining Sequence Numbers

- Nodes originating RREQ messages must increment their own sequence number before transmitting the RREQ.
- Destination nodes increment their sequence numbers when the sequence number in the RREQ is equal to their stored number.

Link Breaks

- Nodes can keep track of connectivity to neighbors using available data link or network layer mechanisms.

- RERR message processing is initiated when:
  - Node detects a link break for the next hop of an active route, or
  - Receives a data packet destined for a node for which it has no (active) route, or
  - Receives a RERR message from a neighbor for at least one active route in its routing table

Link Breaks

- Nodes must **increment** the destination sequence numbers of the routing entries contained in the RERR message before transmitting to nodes in precursor list.
- Nodes receiving RERR messages simply update their sequence numbers with those contained in the RERR message.
- Nodes must also mark these routing entries as invalid regardless of whether they are transmitting and/or receiving.

Link Breaks

- This ensures that no predecessors may reply to a RREQ from a node on their successor path, thus providing loop-freedom.

- RREQ messages are ultimately forwarded back to the originator who may initiate another RREQ message.

Local Repairs

- Nodes detecting a link breakage can choose to repair the link if possible.
- The node simply increments the destination sequence number and broadcasts a RREQ message.
- If it receives a RREP message then the repair was successful

Security Considerations

- Currently AODV has no security measures built in.
- If the network membership is known, then authentication can be used on the AODV control messages.

References

[1] Perkins, et. al. "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003