Abstract

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol has been proposed for use with IPv4 as a network-layer protocol linking together 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 between sources and destinations. It uses destination sequence numbers to ensure loop freedom at all times. In this specification, we detail the necessary modifications to the messages given in the IPv4 specification so that AODV will be able to work for nodes using IPv6 addresses.
1. Introduction

The operation of AODV for IP version 6 (IPv6) is intended to mirror the operation of AODV for IP version 4 [3], with changes necessary to allow for transmission of 128-bit addresses in use with IPv6 instead of the more traditional 32-bit addresses. The reader is referred to [3] for most of the terminology, and the specification of the following protocol operations:

- Route discovery
- Sequence number maintenance
- Maintaining local connectivity
- Notifying precursors about broken routes
- Route expiry and deletion
- Actions after reboot

Broadcast is handled in AODV for IPv6 as specified in [4].

2. AODV Terminology

This protocol specification uses conventional meanings [1] for capitalized words such as MUST, SHOULD, etc., to indicate requirement levels for various protocol features.

3. Route Request (RREQ) Message Format

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Type       |J|R|G|       Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             32-bit Broadcast ID                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             32-bit Destination Sequence Number               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             32-bit Source Sequence Number                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                128-bit Destination IP Address                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   128-bit Source IP Address                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format of the IPv6 Route Request message (RREQ) is illustrated above, and contains the same fields with the same functions as the RREQ message defined for IP version 4 (in [3]), except as follows:

Type

16

Destination IP Address

The 128-bit IPv6 address of destination for which a route is desired.
Source IP Address

The 128-bit IPv6 address of the node which originated the Route Request.

Note also that the order of the fields has been changed to enable alignment along 128-bit boundaries.

4. Route Reply (RREP) Message Format

<table>
<thead>
<tr>
<th>Type</th>
<th>R</th>
<th>A</th>
<th>Prefix Sz</th>
<th>Hop Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The format of the IPv6 Route Reply message (RREP) is illustrated above, and contains the same fields with the same functions as the RREP message defined for IP version 4 (in [3]), except as follows:

Type 17

Destination Sequence Number

The destination sequence number associated to the route.

Destination IP Address

The 128-bit IP address of the destination for which a route is supplied.

Source IP Address

The 128-bit IP address of the source node which issued the RREQ for which the route is supplied.

Note also that the order of the fields has been changed for better alignment.
5. Route Error (RERR) Message Format

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |N|          Reserved           |   DestCount   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Unreachable Destination Sequence Number (1)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Unreachable Destination IPv6 Address (1)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Additional Unreachable Destination Sequence Numbers (if needed) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                   Additional Unreachable Destination IPv6 Addresses (if needed) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 18

The format of the Route Error message is illustrated above, and is identical to the format for the IPv4 RERR message except that the IP addresses are 128 bits, not 32 bits, and the Type is 18. The order of the fields for the IPv6 addresses and the associated sequence numbers has been changed to enable alignment along 64-bit boundaries.

6. Route Reply Acknowledgment (RREP-ACK) Message Format

```
0                   1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type 19

Reserved Sent as 0; ignored on reception.

The RREP-ACK message is used to acknowledge receipt of an RREP message. It is used in cases where the link over which the RREP message is sent may be unreliable. It is identical in format to the RREP-ACK message for IPv4, except that the type is 19.
7. AODV for IPv6 Operation

The handling of AODV for IPv6 messages in sections 3,4,5,6 is analogous to the operation of AODV for IPv4 [3], except that the RREQ, RREP, RERR, and RREP-ACK messages in this document are to be used instead; these messages have the formats appropriate for use with 128-bit IPv6 addresses.

Whenever AODV for IPv4 specifies use of ICMP, the operation for IPv6 requires that the analogous messages from ICMPv6 [2] are to be used instead.

8. Extensions

RREQ and RREP messages for IPv6 use extensions with the same numbers and format as those extensions defined for IPv4.

9. Configuration Parameters

The configuration parameters and default values used by AODV for IPv6 are the same as those used by AODV for IPv4.

10. Flooding Data to a Specific Destination

This section (including subsections) of the specification is not finished. It is only included in order to stimulate appropriate discussion from anyone who may be interested.

For situations in which a message has to be transmitted to a particular destination, the RREQ/RREP route discovery cycle may require a round trip across the entire ad hoc network and back before any data can be delivered. In many circumstances, this represents a significant and unwanted delay. The fewer packets that need to be transmitted to the destination, the more unwelcome the initial delay may be. This first round trip delay appears as an especially large fraction of the total transaction time between endpoints when only a few bytes of data have to be delivered, which could all fit within a single broadcast packet.

To avoid this problem, AODV defines a Flood Data hop-by-hop option that allows a packet to be targeted to a particular destination even when the source does not have a route to that destination. AODV furthermore specifies that this hop-by-hop option can start the route discovery process. Then the route request can be satisfied at an intermediate node after it unicasts the data packet towards the destination.
When the destination responds to such broadcast data packets, it typically needs to set up the reverse path back to the source. Therefore, a Route Reply hop-by-hop option is also specified to be inserted into the return data packet.

### 10.1. Flood Data Option

The format of the Flood Data Option is as follows:

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>J</td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32-bit Broadcast ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32-bit Destination Sequence Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32-bit Source Sequence Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+-----------------------------------------------+</td>
<td>+-----------------------------------------------+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sub-Options...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The fields of this hop-by-hop option are defined as for the RREQ message (see section 3), except that there is no longer any need to have the source and destination IPv6 addresses in the option data. Those fields are available in the IPv6 header. The rules for setting up reverse path route entries to the source IPv6 node are the same as for the RREQ message, which are the same as the rules for the analogous IPv4 messages [3].

### 10.2. Flood Data Reply Option

The broadcast reply hop-by-hop option is used to return data to the source of a data packet containing the Flood Data hop-by-hop option.

The format of the Flood Data Reply Option is as follows:
The fields of this option are defined in the same way as for the Route Reply (RREP) message (see section 4). The rules for setting up forward path route entries to the destination IPv6 node are the same as for the RREP message, which are the same as the rules for the analogous IPv4 messages [3].

11. Security Considerations

Currently, AODV does not specify any special security measures. Route protocols, however, are prime targets for impersonation attacks, and must be protected by use of authentication techniques involving generation of unforgeable and cryptographically strong message digests or digital signatures. It is expected that, in environments where security is an issue, that IPSec authentication headers will be deployed along with the necessary key management to distribute keys to the members of the ad hoc network using AODV.

References


Author’s Addresses

Questions about this memo can be directed to:

Charles E. Perkins
Communications Systems Laboratory
Nokia Research Center
313 Fairchild Drive
Mountain View, CA 94303
USA
+1 650 625 2986
+1 650 625 2502 (fax)
charliep@iprg.nokia.com

Elizabeth M. Royer
Dept. of Electrical and Computer Engineering
University of California, Santa Barbara
Santa Barbara, CA 93106
+1 805 893 7788
+1 805 893 3262 (fax)
eroyer@alpha.ece.ucsb.edu

Samir R. Das
Department of Electrical and Computer Engineering & Computer Science
University of Cincinnati
Cincinnati, OH 45221-0030
+1 513 556 2594
+1 513 556 7326 (fax)
sdas@ececs.uc.edu