Mobile Ad hoc Networks Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2013

C. Perkins
Futurewei
I. Chakeres
CenGen

October 23, 2012

# Dynamic MANET On-demand (AODVv2) Routing
# draft-ietf-manet-dymo-23

## Abstract

The Dynamic MANET On-demand (AODVv2) routing protocol is intended for use by mobile routers in wireless, multihop networks. AODVv2 determines unicast routes among AODVv2 routers within the network in an on-demand fashion, offering on-demand convergence in dynamic topologies.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 26, 2013.

described in the Simplified BSD License.

Table of Contents

## 1. Overview

The Dynamic MANET On-demand (AODVv2) routing protocol [formerly named DYMO] enables on-demand, multihop unicast routing among AODVv2 routers in mobile ad hod networks [MANETs][RFC2119]. The basic operations of the AODVv2 protocol are route discovery and route maintenance. Route discovery is performed when an AODVv2 router must transmit a packet towards a destination for which it does not have a route. Route maintenance is performed to avoid dropping packets, when a route being used to forward packets from the source to a destination breaks, and to avoid prematurely expunging routes from the route table.

During route discovery, an AODVv2 router initiates flooding of a Route Request message (RREQ) throughout the network to find a route to a particular destination, via the AODVv2 router responsible for this destination. During this hop-by-hop flooding process, each intermediate AODVv2 router receiving the RREQ message records a route to the originator. When the target's AODVv2 router receives the RREQ, it records a route to the originator and responds with a Route Reply (RREP) unicast hop-by-hop toward the originating AODVv2 router. Each intermediate AODVv2 router that receives the RREP creates a route to the target, and then the RREP is unicast hop-by-hop toward the originator. When the originator's AODVv2 router receives the RREP, routes have then been established between the originating AODVv2 router and the target AODVv2 router in both directions.

Route maintenance consists of two operations. In order to preserve routes in use, AODVv2 routers extend route lifetimes upon successfully forwarding a packet. In order to react to changes in the network topology, AODVv2 routers monitor traffic being forwarded. When a data packet is received for forwarding and a route for the destination is not known or the route is broken, then the AODVv2 router of the source of the packet is notified. A Route Error (RERR) is transmitted to indicate the route to one or more affected destination addresses is Broken or missing. When the source's AODVv2 router receives the RERR, it marks the route as broken. Before the AODVv2 router can forward a packet to the same destination, it has to perform route discovery again for that destination.

Similarly to AODV, AODVv2 uses sequence numbers to ensure loop freedom [Perkins99]. Sequence numbers enable AODVv2 routers to determine the temporal order of AODVv2 route discovery messages, thereby avoiding use of stale routing information. Also, AODVv2 uses RFC 5444 message and TLV formats.

## 2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Additionally, this document uses some terminology from [RFC5444].

This document defines the following terminology:

Adjacency
: A relationship between selected bi-directional neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers will necessarily form an adjacency. Neighboring routers may form an adjacency based on various information or other protocols; for example, exchange of AODVv2 routing messages, other protocols (e.g. NDP [RFC4861] or NHDP [RFC6130]), or manual configuration. Loss of a routing adjacency may also be based upon similar information; monitoring of adjacencies where packets are being forwarded is required (see Section 5.5.1).

Distance (Dist)
: An unsigned integer which measures the distance a message or information element has traversed. The minimum value of distance is the number of IP hops traversed, 0 for local information. The maximum value is 254. The value 255 is reserved to indicate that the distance is unknown.

AODVv2 Sequence Number (SeqNum)
: An AODVv2 Sequence Number is an unsigned integer maintained by each AODVv2 router. This sequence number guarantees the temporal order of routing information to maintain loop-free routes. The value zero (0) is reserved to indicate that the SeqNum for a destination address is unknown.

reactive
: A protocol operation is said to be "reactive" if it is performed only in reaction to specific events. As used in this document, "reactive" is essentially synonymous with "on-demand".

Router Client
: An AODVv2 router may be configured with a list of other IP addresses and networks which correspond to other non-router nodes which require the services of the AODVv2 router for route discovery and maintenance. An AODVv2 is always its own client, so that the list of client IP addresses is never empty. corresponds

to the AODVv2 router process currently performing a calculation or processing a message.

Flooding
: In this document, flooding a message refers to the process of delivering the message to every AODVv2 router in the network. This may be done according to methods specified in [RFC5148].

Routable Unicast IP Address
: A routable unicast IP address is a unicast IP address that when put into the IP.SourceAddress or IP.DestinationAddress field is scoped sufficiently to be forwarded by a router. Globally-scoped unicast IP addresses and Unique Local Addresses (ULAs) [RFC6130] are examples of routable unicast IP addresses.

Originating Node (OrigNode)
: The originating node is the data source node; if it is not itself an AODVv2 router, its AODVv2 router creates a AODVv2 RREQ message on its behalf in an effort to flood some routing information. The originating node is also referred to as a particular message's originator.

Target Node (TargetNode)
: The TargetNode denotes the ultimate destination of a message.

This Node (ThisNode)
: ThisNode denotes the AODVv2 router currently processing an AODVv2 message.

Route Error (RERR)
: A RERR message is used to indicate that an AODVv2 router no longer has a route to one or more particular destinations.

Route Reply (RREP)
: A RREP message is used to supply routing information about the RREQ TargetNode to the RREQ OrigNode and the AODVv2 routers between them.

Route Request (RREQ)
: An AODVv2 router uses a RREQ message to discover a valid route to a particular destination address, called the RREQ TargetNode. When an AODVv2 router processes a RREQ, it learns routing information on how to reach the RREQ OrigNode.

Type-Length-Value structure (TLV)
: A generic way to represent information as specified in [RFC5444].

Unreachable Node (UnreachableNode)
An UnreachableNode is a node for which a forwarding route is unknown.

## 3. Applicability Statement

The AODVv2 routing protocol is designed for stub (i.e., non-transit) or disconnected (i.e., from the Internet) mobile ad hoc networks (MANETs). AODVv2 handles a wide variety of mobility patterns by dynamically determining routes on-demand. AODVv2 also handles a wide variety of traffic patterns. In networks with a large number of routers, AODVv2 is best suited for sparse traffic scenarios where any particular router forwards packets to only a small percentage of the AODVv2 routers in the network, due to the on-demand nature of route discovery and route maintenance.

AODVv2 is applicable to memory constrained devices, since little routing state is maintained in each AODVv2 router. Only routing information related to routes between active sources and destinations is maintained, in contrast to proactive routing protocols that require routing information to all routers within the routing region be maintained.

AODVv2 supports routers with multiple interfaces. In addition to routing for their local processes, AODVv2 routers can also route on behalf of other non-routing nodes (i.e., "hosts"), reachable via those interfaces. Any such node which is not itself an AODVv2 router SHOULD NOT be served by more than one AODVv2 router. Although AODVv2 is closely related to AODV [RFC3561], and has some of the features of DSR [RFC4728], AODVv2 is not interoperable with either of those other two protocols.

AODVv2 routers perform route discovery to find a route to a particular destination. Therefore, AODVv2 routers MUST must be configured to respond to RREQs for a certain set of addresses. When AODVv2 is the only protocol interacting with the forwarding table, AODVv2 MAY be configured to perform route discovery for all unknown unicast destinations.

At all times within an AODVv2 routing region, only one AODVv2 router SHOULD be serve any routing client. The coordination among multiple AODVv2 routers to distribute routing information correctly for a shared address (i.e. an address that is advertised and can be reached via multiple AODVv2 routers) is not described in this document. The AODVv2 router operation of shifting responsibility for a routing client from one AODVv2 router to another is mentioned in Appendix B
Each AODVv2 router, if serving router clients other than itself, is

configured with information about the IP addresses of its clients. There is no requirement that an AODVv2 router have information about the router clients of other AODVv2 routers. Address assignment procedures are entirely out of scope for AODVv2.

AODVv2 only utilizes bidirectional links. In the case of possible unidirectional links, either blacklists (see Section 5.13.2) or other means (e.g. adjacency establishment with only neighboring routers that have bidirectional communication as indicated by NHDP [RFC6130]) of ensuring and monitoring bi-directionality is recommended. Otherwise, persistent packet loss could occur.

The routing algorithm in AODVv2 may be operated at layers other than the network layer, using layer-appropriate addresses. The routing algorithm makes of some persistent state; if there is no persistent storage available for this state, recovery can exact a performance penalty in case of AODVv2 router reboots.

# 4. Data Structures

## 4.1. Route Table Entry

The route table entry is a conceptual data structure. Implementations may use any internal representation so long as it provides access to the same information as specified below.

Conceptually, a route table entry has the following fields:

Route.Address
: The (host or network) destination address of the node(s) associated with the routing table entry.

Route.Prefix
: The value is the length of the netmask/prefix. If the value of the Route.Prefix is different than the length of addresses in the address family used by the AODVv2 routers, the associated address is a routing prefix, rather than a host address.

Route.SeqNum
: The AODVv2 SeqNum associated with a route table entry.

Route.NextHopAddress
: An IP address of the adjacent AODVv2 router on the path toward the Route.Address.

Route.NextHopInterface
The interface used to send packets toward the Route.Address.

Route.Broken
A flag indicating whether this Route is broken. This flag is set to true if the next-hop becomes unreachable or in response to processing to a RERR (see Section 5.5.4).

The following field is optional:

Route.Dist
A dimensionless metric indicating the distance traversed before reaching the Route.Address node.

Not including optional information may cause performance degradation, but it will not prohibit the protocol from discovering valid routes.

In addition to a route table data structure, each route table entry may have several timers associated with the information. Timers and timeouts are discussed in Section 5.2.3.

## 4.2. AODVv2 Message Structure and Information Elements

IP Protocol Number 138 (manet) has been reserved for MANET protocols [RFC5498]. In addition to using this IP protocol number, AODVv2 may use UDP at destination port 269 (manet) [RFC5498].

AODVv2 messages are transmitted in packets that conform to the generalized packet and message format as described in [RFC5444]. Here is a brief description of the format.

A packet formatted according to RFC5444 contains zero or more messages.

A message contains a message header, message TLV block, and zero or more address blocks.

Each of the address blocks may also have an associated address TLV block.

All AODVv2 messages SHOULD be sent using the IP protocol number (138) reserved for manet protocols [RFC5498]; or the UDP destination port (269) reserved for manet protocols [RFC5498] and IP protocol number for UDP.

Most AODVv2 messages are sent with the IP destination address set to the link-local multicast address LL-MANET-Routers [RFC5498] unless otherwise specified. Therefore, all AODVv2 routers SHOULD subscribe to LL-MANET-Routers [RFC5498] to receiving AODVv2 messages. Note that multicast packets MAY be sent via unicast. For example, this may occur for certain link-types (non broadcast mediums), for manually configured router adjacencies, or in order to improve robustness.

When describing AODVv2 protocol messages, it is necessary to refer to fields in several distinct parts of the overall packet. These locations include the IP header, the UDP header, and fields from [RFC5444]. This document uses the notational conventions found in table 1.

| Information Location | Notational Prefix |
|---|---|
| IP header | IP. |
| RFC5444 message header | MsgHdr. |
| RFC5444 message TLV | MsgTLV. |
| RFC5444 address blocks | AddBlk. |
| RFC5444 address block TLV | AddTLV. |

Table 1

The IPv4 TTL (IPv6 Hop Limit) field for all packets containing AODVv2 messages is set to 255. If a packet is received with a value other than 255, any AODVv2 message contained in the packet MUST be ignored by AODVv2. This mechanism, known as "The Generalized TTL Security Mechanism" (GTSM) [RFC5082] helps to ensure that packets have not traversed any intermediate routers.

The length of an address (32 bits for IPv4 and 128 bits for IPv6) inside an AODVv2 message depends on the msg-addr-length (MAL) in the msg-header, as specified in [RFC5444].

IP packets containing AODVv2 protocol messages SHOULD be given priority queuing and channel access.

AODVv2 messages require the following information:

IP.SourceAddress
: The IP address of the node currently sending this packet. This field is generally filled automatically by the operating system and should not require special handling.

IP.DestinationAddress
The IP address of the packet destination. For multicast messages the IP.DestinationAddress is set to LL-MANET-Routers [RFC5498]. For unicast messages the IP.DestinationAddress is set to the NextHopAddress toward the TargetNode.

MsgHdr.HopLimit
The remaining number of hops this message is allowed to traverse. If an AODVv2 message within a RFC 5444 packet has exhausted its hop limit, then it should be removed from the packet.

## 4.3. RteMsg-specific Protocol Elements

AODVv2 message types RREQ and RREP are denoted as Routing Messages (RteMsgs) and used to flood routing information. RREQ and RREP have similar information and function, but have slightly different handling rules. The main difference between the two messages is that RREQ messages are generally broadcast to solicit a RREP, and conversely a RREP is the unicast response to RREQ. RteMsg creation and handling are described in Section 5.3.

Unicast AODVv2 RteMsgs (e.g. RREP) unless otherwise specified are sent with the IP destination set to the Route.NextHopAddress of the route to the TargetNode.

A RteMsg REQUIRES the following information in addition to the fields indicated in Section 4.2:

AddBlk.TargetNode.Address
The IP address of the message TargetNode. In a RREQ the IP address of the message TargetNode is the destination address for which route discovery is being performed. In a RREP the TargetNode is the RREQ OrigNode address. The TargetNode address is the first address in a routing message.

AddBlk.OrigNode.Address
The IP address of the originator and its associated prefix length. In a RREQ the OrigNode is the source's address and prefix. In a RREP the OrigNode is the RREQ TargetNode's address and prefix for which a RREP is being generated. This address is the second address in the message for RREQ.

OrigNode.AddTLV.SeqNum
The AODVv2 sequence number of the originator's AODVv2 router.

A RteMsg may optionally include the following information:

TargetNode.AddTLV.SeqNum
The last known AODVv2 sequence number of the TargetNode.

AddBlk.AdditionalNode.Address
The IP address of an additional node that can be reached via the AODVv2 router adding this information. Each AdditionalNode.Address MUST include its prefix. Each AdditionalNode.Address MUST also have an associated Node.SeqNum in the address TLV block.

AdditionalNode.AddTLV.SeqNum
The AODVv2 sequence number associated with this routing information.

OrigNode.AddTLV.Dist
A metric of the distance to reach the associated OrigNode.Address. This field is incremented by at least one at each intermediate AODVv2 router.

AdditionalNode.AddTLV.Dist
A metric of the distance to reach the associated AdditionalNode.Address. This field is incremented by at least one at each intermediate AODVv2 router.

## 4.4. Route Error (RERR)-specific Protocol Elements

A RERR message is used to flood the information that a route is not available for one or more particular addresses.

RERR creation and handling are described in Section 5.5.

A RERR requires the following information in addition to the field indicated in Section 4.2:

AddBlk.UnreachableNode.Address
The address of an UnreachableNode and its associated prefix length. Multiple unreachable addresses may be included in a RERR.

A Route Error may optionally include the following information:

UnreachableNode.AddTLV.SeqNum
The last known AODVv2 sequence number of the unreachable node. If a SeqNum for an address is zero (0) or not included, it is assumed to be unknown. This case occurs when a node receives a message to forward to a destination for which it does not have any information in its routing table.

# 5. Detailed Operation for the Base Protocol

## 5.1. AODVv2 Sequence Numbers

AODVv2 sequence numbers allow AODVv2 routers to judge the freshness of routing information and consequently ensure loop freedom.

### 5.1.1. Maintaining A Node's Own Sequence Number

AODVv2 requires that each AODVv2 router in the network maintain its own AODVv2 sequence number (OwnSeqNum). OwnSeqNum a 16-bit unsigned integer. An AODVv2 router increments its OwnSeqNum under the circumstances described in Section 5.3.

Incrementing an OwnSeqNum whose value is the largest largest possible number representable as a 16-bit unsigned integer (i.e., 65,535), MUST be set to one (1). In other words, the sequence number after 65,535 is 1.

### 5.1.2. Actions After OwnSeqNum Loss

An AODVv2 router SHOULD maintain its own sequence number in persistent storage.

If an AODVv2 router's OwnSeqNum is lost, it MUST take certain actions to avoid creating routing loops. To prevent this possibility after OwnSeqNum loss an AODVv2 router MUST wait for at least ROUTE_DELETE_TIMEOUT before fully participating in the AODVv2 routing protocol. If an AODVv2 protocol message is received during this waiting period, the AODVv2 router SHOULD perform normal route table entry updates but MUST NOT transmit or retransmit any AODVv2 RREQ or RREP messages. If a data packet is received for forwarding to another destination during this waiting period, the AODVv2 router MUST transmit a RERR message indicating that this route is not available and reset its waiting timeout. At the end of the waiting period the AODVv2 router sets its OwnSeqNum to one (1) and begin participating.

The longest a node need wait is ROUTE_SEQNUM_AGE_MAX_TIMEOUT. At the end of the maximum waiting period a node SHOULD set its OwnSeqNum to one (1) and begins participating.

## 5.2. AODVv2 Routing Table Operations

### 5.2.1. Judging Routing Information's Usefulness

Given a route table entry (Route.SeqNum, Route.Dist, and Route.Broken) and incoming routing information for a particular

destination in a RteMsg (Node.SeqNum, Node.Dist, and RteMsg message type - RREQ/RREP), the incoming routing information is classified as follows:

1. Stale (Node.SeqNum < Route.SeqNum)
   If Node.SeqNum < Route.SeqNum (using signed 16-bit arithmetic) the incoming information is stale. Using stale routing information is not allowed, since that might result in routing loops.

2. Not safe against loops
   If Node.SeqNum == Route.SeqNum, additional information MUST be examined. If Route.Dist or Node.Dist is unknown or zero (0), or if Node.Dist > Route.Dist + 1, then the incoming information is not guaranteed to prevent routing loops. Using such incoming routing information is not allowed. The following pseudocode is offered to indicate the logical condition under which the incoming information is not guaranteed to protect against loops.

   ```
   (Node.SeqNum == Route.SeqNum) AND
   ((Node.Dist > Route.Dist + 1) OR
    (Route.Dist is unknown) OR (Node.Dist is unknown))
   ```

3. Offers no improvement
   In case of known equal SeqNum, the information is considered worse than the existing route table information in multiple cases: (case i) if Node.Dist > Route.Dist (it is a more expensive route) AND Route.Broken == false; (case ii) if Node.Dist == Route.Dist (equal distance route) AND Route.Broken == false AND this RteMsg is a RREQ. Such RREQs offer no improvement and SHOULD NOT be retransmitted. Updating route table entries using such incoming routing information is not allowed.

   ```
   ((Node.SeqNum == Route.SeqNum) AND
       (((Node.Dist > Route.Dist) AND (Route.Broken == false)) OR
         ((Node.Dist == Route.Dist) AND
          (RteMsg is RREQ) AND (Route.Broken == false))))
   ```

4. Offers improvement
   Incoming routing information that does not match any of the above criteria is loop-free and better than the existing routing table information. We provide the following pseudo-code to determine whether incoming routing information should be used to update an existing route table entry.

   ```
   (/* signed 16-bit arithmetic */ Node.SeqNum - Route.SeqNum > 0) OR
   ((Node.SeqNum == Route.SeqNum) AND
       [(Node.Dist < Route.Dist) OR
       ((Route.Broken == true) AND (Node.Dist <= Route.Dist + 1)) OR
   ```

((RteMsg is RREP) AND (Node.Dist == Route.Dist)]

### 5.2.2. Creating or Updating Route Table Entries

Each route table entry is populated with the following information:

1. the Route.Address is set to Node.Address,

2. the Route.Prefix is set to the Node.Prefix.

3. the Route.SeqNum is set to the Node.SeqNum,

4. the Route.NextHopAddress is set to the IP.SourceAddress (i.e., an address of the node that last transmitted the RteMsg packet)

5. the Route.NextHopInterface is set to the interface on which the incoming AODVv2 packet was received,

6. the Route.Broken flag is set to false,

7. if known, the Route.Dist is set to the Node.Dist,

The timer for the minimum delete timeout (ROUTE_AGE_MIN) is set to ROUTE_AGE_MIN_TIMEOUT. The timer for the maximum delete timeout (ROUTE_SEQNUM_AGE_MAX) is set to Node.AddTLV.VALIDITY_TIME [RFC5497] if included; otherwise, ROUTE_SEQNUM_AGE_MAX is set to ROUTE_SEQNUM_AGE_MAX_TIMEOUT. The usage of these timers and others are described in Section 5.2.3.

With these assignments to the route table entry, a route has been created and the Route.Forwarding flag set. Afterward, the route can be used to send any buffered data packets and to forward any incoming data packets for Route.Address. This route also fulfills any outstanding route discovery (RREQ) attempts for Node.Address.

### 5.2.3. Route Table Entry Timeouts

#### 5.2.3.1. Minimum Delete Timeout (ROUTE_AGE_MIN)

When an AODVv2 router transmits a RteMsg, other AODVv2 routers expect the transmitting AODVv2 router to have a forwarding route to the RteMsg originator. A route table entry SHOULD be kept in the route table for at least ROUTE_AGE_MIN after it has been updated. Failure to maintain the route table entry might result in lost messages/ packets, or several duplicate messages.

After the ROUTE_AGE_MIN timeout a route can safely be deleted.

#### 5.2.3.2. Maximum Sequence Number Delete Timeout (ROUTE_SEQNUM_AGE_MAX)

Sequence number information for route table entries is time sensitive, and MUST be deleted after a time in order to ensure loop-free routing.

After the ROUTE_SEQNUM_AGE_MAX timeout a route's sequence number information MUST be discarded.

#### 5.2.3.3. Recently Used Timeout (ROUTE_USED)

When a route is used to forward data packets, this timer is set to expire after ROUTE_USED_TIMEOUT, as discussed in Section 5.5.2.

If a route has not been used recently, then a timer for ROUTE_DELETE is set to ROUTE_DELETE_TIMEOUT.

#### 5.2.3.4. Delete Information Timeout (ROUTE_DELETE)

As time progresses the likelihood that old routing information is useful decreases, especially if the network nodes are mobile. Therefore, old information SHOULD be deleted.

After the ROUTE_DELETE timeout if a forwarding route exists it SHOULD be removed, and the routing table entry SHOULD also be deleted.

### 5.3. Routing Messages

#### 5.3.1. RREQ Creation

Before an AODVv2 router creates a RREQ it SHOULD increment its OwnSeqNum by one (1) according to the rules specified in Section 5.1. Incrementing OwnSeqNum will ensure that all nodes with existing routing information will consider this new information preferable to existing routing table information. If the sequence number is not incremented, certain AODVv2 routers might not consider this information preferable, if they have existing better routing information.

First, ThisNode adds the AddBlk.TargetNode.Address to the RREQ; the unicast IP Destination Address for which a forwarding route does not exist.

If a previous value of the TargetNode.SeqNum is known (from a routing table entry using longest-prefix matching), it SHOULD be placed in TargetNode.AddTLV.SeqNum in all but the last RREQ attempt. If a TargetNode.SeqNum is not included, it is assumed to be unknown by handling nodes. This operation ensures that no intermediate AODVv2

routers reply, and ensures that the TargetNode's AODVv2 router increments its sequence number.

Next, ThisNode adds AddBlk.OrigNode.Address, its prefix, and the OrigNode.AddTLV.SeqNum (OwnSeqNum) to the RteMsg.

The OrigNode.Address is the address of the source for which this AODVv2 router is initiating this route discovery. The OrigNode.Address MUST be a unicast address. This information will be used by nodes to create a route toward the OrigNode, enabling delivery of a RREP, and eventually used for proper forwarding of data packets.

If OrigNode.Dist is included it is set to a number, greater than zero (0), representing the distance between OrigNode and ThisNode.

The MsgHdr.HopLimit SHOULD be set to MSG_HOPLIMIT.

### 5.3.2. RREP Creation

First, the AddBlk.TargetNode.Address is added to the RREP. The TargetNode is the ultimate destination of this RREP; the RREQ OrigNode.Address.

Next, AddBlk.OrigNode.Address and prefix are added to the RREP. The AddBlk.OrigNode.Address is the RREQ TargetNode.Address. The AddBlk.OrigNode.Address MUST be a unicast IP address. ThisNode SHOULD advertise the largest known prefix containing AddBlk.OrigNode.Address.

When the RteMsg TargetNode's AODVv2 router creates a RREP, if the TargetNode.SeqNum was not included in the RREQ, ThisNode MUST increment its OwnSeqNum by one (1) according to the rules specified in Section 5.1.

If TargetNode.SeqNum was included in the RteMsg and TargetNode.SeqNum - OwnSeqNum < 0 (using signed 16-bit arithmetic), OwnSeqNum SHOULD be incremented by one (1) according to the rules specified in Section 5.1.

If TargetNode.SeqNum is included in the RteMsg and TargetNode.SeqNum == OwnSeqNum (using signed 16-bit arithmetic) and OrigNode.Dist will not be included in the RREP being generated, OwnSeqNum SHOULD be incremented by one (1) according to the rules specified in Section 5.1.

If OwnSeqNum is not incremented the routing information might be considered stale. In this case, the RREP might not reach the RREP

Target.

After any of the sequence number operations above, the RREP OrigNode.AddTLV.SeqNum (OwnSeqNum) MUST also be added to the RREP.

Other AddTLVs in the RREP for the OrigNode and TargetNode SHOULD be included and set accordingly. If OrigNode.Dist is included it is set to a number greater than zero (0) and less than or equal to 254. The Distance value will influence judgment of the routing information (Section 5.2.1) against known information at other AODVv2 routers that handle this RteMsg.

The MsgHdr.HopLimit is set to MSG_HOPLIMIT.

The IP.DestinationAddress for RREP is set to the IP address of the Route.NextHopAddress for the route to the RREP TargetNode.

### 5.3.3. RteMsg Handling

First, ThisNode examines the RteMsg to ensure that it contains the required information: MsgHdr.HopLimit, AddBlk.TargetNode.Address, AddBlk.OrigNode.Address, and OrigNode.AddTLV.SeqNum. If the required information does not exist, the message is discarded and further processing stopped.

ThisNode MUST only handle AODVv2 messages from adjacent routers.

ThisNode checks if the AddBlk.OrigNode.Address is a valid routable unicast address. If not, the message is ignored and further processing stopped.

ThisNode also checks whether AddBlk.OrigNode.Address is an address handled by this AODVv2 router. If this node is the originating AODVv2 router, the RteMsg is dropped.

ThisNode checks if the AddBlk.TargetNode.Address is a valid routable unicast address. If the address is not a valid unicast address, the message is discarded and further processing stopped.

Next, ThisNode checks whether its routing table has an entry to the AddBlk.OrigNode.Address using longest-prefix matching [RFC1812]. If a route with a valid Route.SeqNum does not exist, then the new routing information is used to create a new route table entry is created and updated as described in Section 5.2.2. If a route table entry does exists and it has a known Route.SeqNum, the incoming routing information is compared with the route table entry following the procedure described in Section 5.2.1. If the incoming routing information is considered preferable, the route table entry is

updated as described in Section 5.2.2.

At this point, if the routing information for the OrigNode was not preferable then this RteMsg SHOULD be discarded and no further processing of this message SHOULD be performed.

If the TargetNode is a router client of ThisNode this RteMsg is a RREQ, then ThisNode responds with a RREP to the RREQ OrigNode (the new RREP's TargetNode). The procedure for issuing a new RREP is described in Section 5.3.2. Afterwards, ThisNode need not perform any more operations for the RteMsg being processed.

As an alternative to issuing a RREP, ThisNode MAY choose to distribute routing information about ThisNode (the RREQ TargetNode) more widely. That is, ThisNode MAY optionally perform a route discovery by issuing a RREQ with ThisNode listed as the TargetNode, using the procedure in Section 5.3.1. At this point, ThisNode need not perform any more operations for the RteMsg being processed.

For each address (except the TargetNode) in the RteMsg that includes AddTLV.Dist information, the AddTLV.Dist information is incremented by at least one (1). The updated Distance value will influence judgment of the routing information (Section 5.2.1) against known information at other AODVv2 routers that handle this RteMsg.

If the resulting Distance value for the OrigNode is greater than 254, the message is discarded. If the resulting Distance value for another node is greater than 254, the associated address and its information are removed from the RteMsg. If the MsgHdr.HopLimit is equal to one (1), then the message is discarded. Otherwise, the MsgHdr.HopLimit is decremented by one (1).

If ThisNode is not the TargetNode, AND this RteMsg is a RREQ, then the current RteMsg (as altered by the procedure defined above) SHOULD be sent to the IP multicast address LL-MANET-Routers [RFC5498]. If the RREQ is unicast, the IP.DestinationAddress is set to the NextHopAddress.

If ThisNode is not the TargetNode, AND this RteMsg is a RREP, then the current RteMsg is sent to the Route.NextHopAddress for the RREP's TargetNode.Address. If no forwarding route exists to TargetNode.Address, then a RERR SHOULD be issued to the OrigNode of the RREP.

By sending the updated RteMsg, ThisNode advertises that it will route for addresses contained in the outgoing RteMsg based on the information enclosed. ThisNode MAY choose not to send the RteMsg, though not resending this RteMsg could decrease connectivity in the

network or result in a non-shortest distance path.

The circumstances under which ThisNode might choose to not re-issue a RteMsg are not specified in this document. Some examples might include the following:

- if ThisNode does not want to advertise routing for the contained addresses because it is already heavily loaded
- if ThisNode has already issued identical routing information (e.g. ThisNode had recently issued a RteMsg with the same distance)
- if ThisNode is low on energy and does not want to expend energy for protocol message sending or packet forwarding

## 5.4. Route Discovery

When an AODVv2 router needs to forward a data packet and it does not have a forwarding route to the destination address, it sends a RREQ (described in Section 5.3.1) to discover a route to the particular destination (TargetNode).

After issuing a RREQ, the AODVv2 router (OrigNode) waits for a RREP indicating the next hop for a route to the TargetNode. If a route is not created within RREQ_WAIT_TIME, OrigNode may again try to discover a route by issuing another RREQ using the procedure defined in Section 5.3.1 again. Route discovery SHOULD be considered to have failed after DISCOVERY_ATTEMPTS_MAX and the corresponding wait time for a response to the final RREQ.

To reduce congestion in a network, repeated attempts at route discovery for a particular TargetNode SHOULD utilize an binary exponential backoff.

Data packets awaiting a route SHOULD be buffered by the source's AODVv2 router. This buffer SHOULD have a fixed limited size (BUFFER_SIZE_PACKETS or BUFFER_SIZE_BYTES). Determining which packets to discard first is a matter of policy at each AODVv2 router; in the absence of policy constraints, by default older data packets SHOULD be discarded first. Buffering of data packets can have both positive and negative effects, and therefore settings for buffering (BUFFER_DURING_DISCOVERY) SHOULD be administratively configurable. Nodes without sufficient memory available for buffering may be configured with BUFFER_DURING_DISCOVERY = FALSE; this will affect the latency required for launching TCP applications to new destinations.

If a route discovery attempt has failed (i.e. an attempt or multiple attempts have been made without receiving a RREP) to find a route to

the TargetNode, any data packets buffered for the corresponding TargetNode MUST BE dropped and a Destination Unreachable ICMP message (Type 3) SHOULD be delivered to the source of the data packet. The code for the ICMP message is 1 (Host unreachable error). If the AODVv2 router is not the source (OrigNode), then the ICMP is sent over the interface from which the source sent the packet to the AODVv2 router.

## 5.5. Route Maintenance

A RERR SHOULD be issued if a data packet is to be forwarded and it cannot be delivered to the next-hop because no forwarding route for the IP.DestinationAddress exists; RERR generation is described in Section 5.5.3.

Upon this condition, an ICMP Destination Unreachable message SHOULD NOT be generated unless this router is responsible for the IP.DestinationAddress and that IP.DestinationAddress is known to be unreachable.

In addition to inability to forward a data packet, a RERR SHOULD be issued immediately after detecting a broken link (see Section 5.5.1) of a forwarding route to quickly notify AODVv2 routers that certain routes are no longer available. If a newly unavailable route has not been used recently (indicated by ROUTE_USED), the RERR SHOULD NOT be generated.

### 5.5.1. Active Next-hop Router Adjacency Monitoring

Nodes SHOULD monitor connectivity to adjacent next-hop AODVv2 routers on forwarding routes. This monitoring can be accomplished by one or several mechanisms, including:

- Neighborhood discovery [RFC6130]
- Route timeout
- Lower layer trigger that a neighboring router is no longer reachable
- Other monitoring mechanisms or heuristics

Upon determining that a next-hop AODVv2 router has become unreachable, ThisNode MUST remove the affected forwarding routes (those using the unreachable next-hop) and unset the Route.Forwarding flag. ThisNode also flags the associated routes in AODVv2's routing table as Broken. For each broken route the timer for ROUTE_DELETE is set to ROUTE_DELETE_TIMEOUT.

### 5.5.2. Updating Route Lifetimes During Packet Forwarding

To avoid removing the forwarding route to reach an IP.SourceAddress, ThisNode SHOULD set the "ROUTE_USED" timeout to the value ROUTE_USED_TIMEOUT for the route to that IP.SourceAddress upon receiving a data packet or an AODVv2 message. If the timer for ROUTE_DELETE is set, that timer is removed. The Route.Broken flag is unset.

To avoid removing the forwarding route to the IP.DestinationAddress that is being used, ThisNode SHOULD set the "ROUTE_USED" timeout to the value ROUTE_USED_TIMEOUT for the route to the IP.DestinationAddress upon sending a data packet or an AODVv2 message. If the timer for ROUTE_DELETE is set, it is removed. The Route.Broken flag is unset.

### 5.5.3. RERR Generation

When an AODVv2 router receives a packet (from PrevHopAddress), and the router (ThisNode) does not have a route available for the destination of the packet, ThisNode uses an RERR message is used to inform one or more neighboring AODVv2 routers that its route to the packet destination is no longer available.

When ThisNode creates a new RERR, the address of the first UnreachableNode (IP.DestinationAddress from a data packet or RREP.TargetNode.Address) is inserted into an Address Block AddBlk.UnreachableNode.Address. If a prefix is known for the UnreachableNode.Address, it SHOULD be included. Otherwise, the UnreachableNode.Address is assumed to be a host address with a full length prefix. If a value for the UnreachableNode's SeqNum (UnreachableNode.AddTLV.SeqNum) is known, it SHOULD be placed in the RERR. The MsgHdr.HopLimit SHOULD be set to MSG_HOPLIMIT.

If SeqNum information is not known or not included in the RERR, all nodes handling the RERR will assume their routing information associated with the UnreachableNode is no longer valid and flag those routes as broken.

A RERR MAY be sent to the multicast address LL-MANET-Routers [RFC5498], thus notifying all nearby AODVv2 routers that might depend on the now broken link. If the RERR is unicast, the IP.DestinationAddress is set to the PrevHopAddress.

After sending the RERR, ThisNode SHOULD discard the packet or message that triggered generation of the RERR.

### 5.5.4. RERR Handling

First, ThisNode examines the incoming RERR to ensure that it contains MsgHdr.HopLimit and AddBlk.UnreachableNode.Address. If the required information does not exist, the incoming RERR message is discarded and further processing stopped.

When an AODVv2 router handles a RERR, it examines the information for each UnreachableNode. The AODVv2 router removes the forwarding route, unsets the Route.Forwarding flag, sets the Route.Broken flag, and the timer for ROUTE_DELETE is set to ROUTE_DELETE_TIMEOUT for each UnreachableNode.Address found using longest prefix matching that meets all of the following conditions:

1. The UnreachableNode.Address is a routable unicast address.

2. The Route.NextHopAddress is the same as the RERR IP.SourceAddress.

3. The Route.NextHopInterface is the same as the interface on which the RERR was received.

4. The Route.SeqNum is zero (0), unknown, OR the UnreachableNode.SeqNum is zero (0), unknown, OR Route.SeqNum - UnreachableNode.SeqNum <= 0 (using signed 16-bit arithmetic).

If Route.SeqNum is zero (0) or unknown and UnreachableNode.SeqNum exists in the RERR and is not zero (0), then Route.SeqNum SHOULD be set to UnreachableNode.SeqNum. Setting Route.SeqNum can reduce future RERR handling and forwarding.

Each UnreachableNode that did not result in marking a route table entry as broken route is removed from the RERR, since propagation of such information will not result in any benefit.

Each UnreachableNode that did indicate a broken route SHOULD remain in the RERR.

If any UnreachableNode was removed, all other information (AddTLVs) associated with the UnreachableNode address(es) MUST also be removed.

If Route.SeqNum is known and an UnreachableNode.SeqNum is not included in the RERR, then Route.SeqNum (i.e. UnreachableNode.SeqNum) MAY be included with the RERR. Including UnreachableNode.SeqNum can reduce future RERR handling and forwarding.

If no UnreachableNode addresses remain in the RERR, or if the

MsgHdr.HopLimit is equal to one (1), then the RERR MUST be discarded.

Otherwise, the MsgHdr.HopLimit is decremented by one (1). The RERR SHOULD be sent to the multicast address LL-MANET-Routers [RFC5498]. Alternatively, if the RERR is unicast, the IP.DestinationAddress is set to the PrevHopAddress.

### 5.6. Unknown Message and TLV Types

If a message with an unknown type is received, the message is ignored.

For handling of messages that contain unknown TLV types, ignore the information for processing, preserve it unmodified for forwarding.

### 5.7. Advertising Network Addresses

AODVv2 routers MAY specify a prefix length for each advertised address. Any nodes (other than the advertising AODVv2 router) within the advertised prefix MUST NOT participate in the AODVv2 protocol directly. For example, advertising 192.0.2.1 with a prefix length of 24 indicates that all nodes with the matching 192.0.2.X are reachable through this AODVv2 router. An AODVv2 router MUST NOT advertise network addresses unless it can guarantee its ability for forwarding packets to any host address within the address range of the corresponding network.

### 5.8. Simple Internet Attachment

Simple Internet attachment consists of a stub (i.e., non-transit) network of AODVv2 routers connected to the Internet via a single Internet AODVv2 router (IAR).

As in any Internet-attached network, AODVv2 routers, and hosts behind these routers, wishing to be reachable from hosts on the Internet MUST have IP addresses within the IAR's routable and topologically correct prefix (e.g. 192.0.2.0/24).

The IAR is responsible for generating RREQ to find nodes within the AODVv2 Region on behalf of nodes on the Internet, as well as responding to route requests from the AODVv2 region on behalf of the nodes on the Internet.

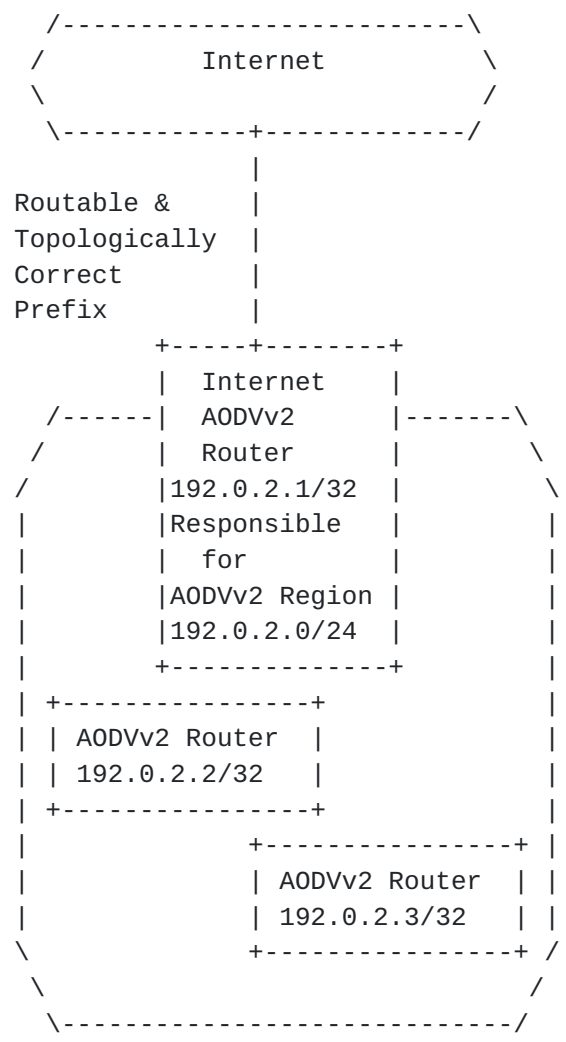


Figure 1: Simple Internet Attachment Example

When an AODVv2 router within the AODVv2 Region wants to discover a route to a node on the Internet, it uses the normal AODVv2 route discovery for that IP Destination Address. The IAR MUST respond to RREQ on behalf of the Internet destination.

When a packet from a node on the Internet destined for a node in the AODVv2 region reaches the IAR, if the IAR does not have a route to that destination it will perform normal AODVv2 route discovery for that destination.

## 5.9. Multiple Interfaces

AODVv2 may be used with multiple interfaces; therefore, the particular interface over which packets arrive MUST be known whenever a packet is received. Whenever a new route is created, the interface through which the Route.Address can be reached is also recorded in

the route table entry.

When multiple interfaces are available, a node transmitting a multicast packet with IP.DestinationAddress set to LL-MANET-Routers SHOULD send the packet on all interfaces that have been configured for AODVv2 operation.

Similarly, AODVv2 routers SHOULD subscribe to LL-MANET-Routers on all their AODVv2 interfaces.

### 5.10. AODVv2 Control Packet/Message Generation Limits

To ensure predictable messaging overhead, AODVv2 router's rate of packet/message generation SHOULD be limited. The rate and algorithm for limiting messages (CONTROL_TRAFFIC_LIMITS) is left to the implementor and should be administratively configurable. AODVv2 messages SHOULD be discarded in the following order of preference: RREQ, RREP, and finally RERR.

### 5.11. Optional Features

Several optional features of AODVv2, and associated with AODV, are not required by minimal implementations. These features are expected to be useful in networks with greater mobility, or larger node populations, or requiring shorter latency for application launches. The optional features are as follows:

- Expanding Rings Multicast
- Intermediate RREPs (iRREPs): Without iRREP, only the destination can respond to a RREQ.
- Precursor lists.
- Reporting Multiple Unreachable Nodes. An RERR message can carry more than one Unreachable Destination node for cases when a single link breakage causes multiple destinations to become unreachable from an intermediate router.

#### 5.11.1. Expanding Rings Multicast

For multicast RREQ, the MsgHdr.HopLimit MAY be set in accordance with an expanding ring search as described in [RFC3561] to limit the RREQ propagation to a subset of the local network and possibly reduce route discovery overhead.

### 5.11.2. Intermediate RREP

This specification has been published as a separate Internet Draft .

### 5.11.3. Precursor Notification

The Dynamic MANET On-demand (AODVv2) routing protocol is intended for use by mobile routers in wireless, multihop networks. AODVv2 determines unicast routes among AODVv2 routers within the network in an on-demand fashion, offering on-demand convergence in dynamic topologies. This document specifies a simple modification to AODVv2 (and possibly other reactive routing protocols) enabling faster notifications to known sources of traffic upon determination that a route for such traffic's destination has become Broken.

#### 5.11.3.1. Overview

If an AODVv2 router, while attempting to forward a packet to a particular destination, determines that the next hop (one of its neighbors) is no longer reachable, AODVv2 specifies that the router notify the source of that packet that the route to the destination has become Broken. In the existing specification, the notification to the source is a unicast RERR message.

However, in many cases there will be several sources of of traffic for that particular destination. In fact, the broken link for the next hop in question may be a path component of numerous other routes for other destinations, and in that case the node detecting the broken link must mark as Broken multiple routes, one for each of the newly unreachable destinations. Each route that uses the newly broken link is no longer valid. For each such route, every node along the way from the source using that route, to the node detecting the broken link, is known as a "precursor" for the broken next hop. All the precursors for a particular next hop should be notified about the change in status of their route to a destination downstream from the broken next hop.

#### 5.11.3.2. Precursor Notification

During normal operation, each node wishing to enable the improved notification for precursors of any links to its next hop neighbors has to keep track of the precursors. This is done by maintaining a precursor table and updating the table whenever the node initiates or relays a RREP message back to a node originating a RREQ message. When the node transmits the RREP message, it is implicitly agreeing to forward traffic from the RREQ originator towards the RREP originator (i.e., along the next hop link to the neighbor from which the RREP was received). The "other" next hop, which is the neighbor

along the way towards the originator of the RREQ message, is then the next precursor for the route towards the destination requested by the RREQ.

Each such precursor should then be recorded as a precursor for a route along the next hop. The same next hop may be in service for routes to multiple destinations, but for precursor list management it is only important to keep track of precursors for a particular next hop; the exact destination does not matter, only the particular next hop towards the destination(s).

When a node observes that one of its neighbors is no longer reachable, the node first checks to see whether the link to that neighbor is a next hop for any more distant destination in its route table. If not, then the node simply updates any relevant neighorhood information and takes no further action.

Otherwise, for all destinations no longer reachable because of the changed status of the next hop, the node first checks to see whether the link to that neighbor is a next hop for any more distant destination in its route table. If not, then the node simply updates any relevant neighorhood information and takes no further action.

For each precursor of the next hop, the node MAY notify the precursor in one of three ways:

- unicast RERR
- broadcast RERR
- multicast RERR to multicast group PRECURSOR_RERR_RECEIVERS

Each precursor then MAY execute the same procedure until all affected traffic sources have received the RERR route maintenance information.

When a precursor receives a unicast RERR, the precursor MUST further unicast the RERR message towards the affected traffic source. If a precursor receives a broadcast or multicast RERR, the precursor MAY further retransmit the RERR towards the traffic source.

### 5.11.4. Reporting Multiple Unreachable Nodes

### 5.11.5. Message Aggregation

The aggregation of multiple messages into a packet is not specified in this document, but if aggregation does occur the IP.SourceAddress and IP.DestinationAddress of all contained messages MUST be the same.

Implementations MAY choose to temporarily delay transmission of messages for the purpose of aggregation (into a single packet) or to improve performance by using jitter [RFC5148].

### 5.11.6. Adding Additional Routing Information to a RteMsg

DSR [RFC4728] includes source routes as part of the data of its RREPs and RREQs. Doign so allows additional topology information to be flooded along with the RteMsg, and potentially allows updating for stale routing information at MANET routers along new paths between source and destination. To maintain this functionality, AODVv2 has defined a somewhat more general method that enables inclusion of source routes in RteMsgs.

Appending routing information can alleviate route discovery attempts to the nodes whose information is included, if other AODVv2 routers use this information to update their routing tables.

Note that, since the initial merger of DSR with AODV to create this protocol, further experimentation has shown that including the additional routing information is not always helpful. Sometimes it seems to help, and other times it seems to reduct overall performance.

AODVv2 routers can append routing information to a RteMsg. This is controllable by an option (APPEND_INFORMATION) which SHOULD be administratively configurable or controlled according to the traffic characteristics of the network.

Prior to appending an address controlled by this AODVv2 router to a RteMsg, ThisNode MAY increment its OwnSeqNum as defined in Section 5.1. If OwnSeqNum is not incremented the appended routing information might not be considered preferable, when received by nodes with existing routing information. Incrementation of the sequence number when appending information to a RteMsg in transit (APPEND_INFORMATION_SEQNUM) SHOULD be administratively configurable. Note that, during handling of this RteMsg OwnSeqNum may have already been incremented; and in this case OwnSeqNum need not be incremented again.

If an address controlled by this AODVv2 router includes ThisNode.Dist, it is set to a number greater than zero (0).

For added addresses (and their prefixes) not controlled by this AODVv2 router, Route.Dist can be included if known.

The VALIDITY_TIME of routing information for appended address(es) MUST be included, to inform routers about when to delete this

information. The VALIDITY_TIME TLV is defined in Section 5.13.3.

Additional information (e.g. SeqNum and Dist) about any appended address(es) SHOULD be included.

Note that the routing information about the TargetNode MUST NOT be added. Also, duplicate address entries SHOULD NOT be added. Instead, only the best routing information (Section 5.2.1) for a particular address SHOULD be included.

Intermediate nodes obey the following procedures when processing AddBlk.AdditionalNode.Address information and other associated TLVs that are included with a RteMsg. For each address (except the TargetNode) in the RteMsg that includes AddTLV.Dist information, the AddTLV.Dist information MUST be incremented. If the resulting Distance value for the OrigNode is greater than 254, the message is discarded. If the resulting Distance value for another node is greater than 254, the associated address and its information are removed from the RteMsg.

After handling the OrigNode's routing information, then each address that is not the TargetNode MAY be considered for creating and updating routes. Creating and updating routes to other nodes can eliminate RREQ for those IP destinations, in the event that data needs to be forwarded to the IP destination(s) now or in the near future.

For each of the additional addresses considered, ThisNode first checks that the address is a routable unicast address. If the address is not a unicast address, then the address and all related information MUST be removed.

If the routing table does not have a matching route with a known Route.SeqNum for this additional address using longest-prefix matching, then a route MAY be created and updated as described in Section 5.2.2. If a route table entry exists with a known Route.SeqNum, the incoming routing information is compared with the route table entry following the procedure described in Section 5.2.1. If the incoming routing information is used, the route table entry SHOULD be updated as described in Section 5.2.2.

If the routing information for an AdditionalNode.Address is not used, then it is removed from the RteMsg.

## 5.12. Administratively Configured Parameters and Timer Values

AODVv2 contains several parameters which MUST be administratively configured. The list of these follows:

Required Administratively Configured Parameters

| Name | Description |
|---|---|
| RESPONSIBLE_ADDRESSES | List of addresses or routing prefixes, for which this AODVv2 router is responsible. If, RESPONSIBLE_ADDRESSES is zero, this AODVv2 router is only responsible for its own addresses. |
| AODVv2_INTERFACES | List of the interfaces participating in AODVv2 routing protocol. |

Table 2

AODVv2 contains a number of timers. The default timing parameter values follow:

Default Timing Parameter Values

| Name | Value |
|---|---|
| ROUTE_TIMEOUT | 5 seconds |
| ROUTE_AGE_MIN_TIMEOUT | 1 second |
| ROUTE_SEQNUM_AGE_MAX_TIMEOUT | 600 seconds |
| ROUTE_USED_TIMEOUT | ROUTE_TIMEOUT |
| ROUTE_DELETE_TIMEOUT | 2 * ROUTE_TIMEOUT |
| ROUTE_RREQ_WAIT_TIME | 2 seconds |
| UNICAST_MESSAGE_SENT_TIMEOUT | 1 second |

Table 3

The above timing parameter values work well for small and medium well-connected networks with moderate topology changes.

The timing parameters SHOULD be administratively configurable for the network where AODVv2 is used. Ideally, for networks with frequent topology changes the AODVv2 parameters should be adjusted using either experimentally determined values or dynamic adaptation. For example, in networks with infrequent topology changes ROUTE_USED_TIMEOUT may be set to a much larger value.

Default Parameter Values

| Name | Value | Description |
|---|---|---|
| MSG_HOPLIMIT | 20 hops | This value MUST be larger than the AODVv2 network diameter. Otherwise, routing messages may not reach their intended destinations. |
| DISCOVERY_ATTEMPTS_MAX | 3 | The number of route discovery attempts to make before indicating that a particular address is not reachable. |

Table 4

In addition to the above parameters and timing values, several administrative options exist. These options have no influence on correct routing behavior, although they may potentially reduce AODVv2 protocol messaging in certain situations. The default behavior is to NOT enable any of these options; and although many of these options can be administratively controlled, they may be better served by intelligent control. The following table enumerates several of the options.

Administratively Controlled Options

| Name | Description |
|---|---|
| BUFFER_DURING_DISCOVERY | Whether and how much data to buffer during route discovery. |
| APPEND_EXTRA_UNREACHABLE | Whether to append additional Unreachable information to RERR. |
| CONTROL_TRAFFIC_LIMITS | AODVv2 messaging SHOULD be limited to avoid consuming all the network bandwidth. |

Table 5

Note: several fields have limited size (bits or bytes) these sizes and their encoding may place specific limitations on the values that can be set. For example, MsgHdr.HopLimit is a 8-bit field and therefore MSG_HOPLIMIT cannot be larger than 255.

## 5.13. IANA Considerations

In its default mode of operation, AODVv2 uses the UDP port 269 [RFC5498] to carry protocol packets. AODVv2 also uses the link-local multicast address LL-MANET-Routers [RFC5498].

This section specifies several message types, message tlv-types, and address tlv-types.

### 5.13.1. AODVv2 Message Types Specification

AODVv2 Message Types

| Name | Type |
|---|---|
| Route Request (RREQ) | 10 - TBD |
| Route Reply (RREP) | 11 - TBD |
| Route Error (RERR) | 12 - TBD |

Table 6

### 5.13.2. Message and Address Block TLV Type Specification

Message TLV Types

| Name | Type | Length | Value |
|---|---|---|---|
| Unicast Response Request | 10 - TBD | 0 octets | Indicates to the processing node that the previous hop (IP.SourceAddress) expects a unicast reply message within UNICAST_MESSAGE_SENT_TIMEOUT. Any unicast packet will serve this purpose, and it MAY be an ICMP REPLY message. If the reply is not received, then the previous hop can assume that the link is unidirectional and MAY blacklist the link to this node. |

Table 7

### 5.13.3. Address Block TLV Specification

Address Block TLV Types

| Name | Type | Length | Value |
|---|---|---|---|
| AODVv2 Sequence Number (AODVv2SeqNum) | 10 - TBD | up to 2 octets | The AODVv2 sequence num associated with this address. The sequence number may be the last known sequence number. |
| Distance | 11 - TBD | up to 2 octets | A metric of the distance traversed by the information associated with this address. |
| VALIDITY_TIME | 1[RFC5497] | | The maximum amount of time that information can be maintained before being deleted. The VALIDITY_TIME TLV is defined in [RFC5497]. |

Table 8

## 5.14. Security Considerations

The objective of the AODVv2 protocol is for each router to communicate reachability information to addresses for which it is responsible. Positive routing information (i.e. a route exists) is distributed via RteMsgs and negative routing information (i.e. a route does not exist) via RERRs. AODVv2 routers that handle these messages store the contained information to properly forward data packets, and they generally provide this information to other AODVv2 routers.

This section does not mandate any specific security measures. Instead, this section describes various security considerations and potential avenues to secure AODVv2 routing.

The most important security mechanisms for AODVv2 routing are integrity/authentication and confidentiality.

In situations where routing information or router identity are suspect, integrity and authentication techniques SHOULD be applied to AODVv2 messages. In these situations, routing information that is distributed over multiple hops SHOULD also verify the integrity and

identity of information based on originator of the routing information.

A digital signature could be used to identify the source of AODVv2 messages and information, along with its authenticity. A nonce or timestamp SHOULD also be used to protect against replay attacks. S/MIME and OpenPGP are two authentication/integrity protocols that could be adapted for this purpose.

In situations where confidentiality of AODVv2 messages is important, cryptographic techniques can be applied.

In certain situations, for example sending a RREP or RERR, an AODVv2 router could include proof that it has previously received valid routing information to reach the destination, at one point of time in the past. In situations where routers are suspected of transmitting maliciously erroneous information, the original routing information along with its security credentials SHOULD be included.

Note that if multicast is used, any confidentiality and integrity algorithms used MUST permit multiple receivers to handle the message.

Routing protocols, however, are prime targets for impersonation attacks. In networks where the node membership is not known, it is difficult to determine the occurrence of impersonation attacks, and security prevention techniques are difficult at best. However, when the network membership is known and there is a danger of such attacks, AODVv2 messages must be protected by the use of authentication techniques, such as those involving generation of unforgeable and cryptographically strong message digests or digital signatures. While AODVv2 does not place restrictions on the authentication mechanism used for this purpose, IPsec Authentication Message (AH) is an appropriate choice for cases where the nodes share an appropriate security association that enables the use of AH.

In particular, routing messages SHOULD be authenticated to avoid creation of spurious routes to a destination. Otherwise, an attacker could masquerade as that destination and maliciously deny service to the destination and/or maliciously inspect and consume traffic intended for delivery to the destination. RERR messages SHOULD be authenticated in order to prevent malicious nodes from disrupting active routes between communicating nodes.

If the mobile nodes in the ad hoc network have pre-established security associations, the purposes for which the security associations are created should include that of authorizing the processing of AODVv2 control packets. Given this understanding, the mobile nodes should be able to use the same authentication mechanisms

based on their IP addresses as they would have used otherwise.

### 5.15. Acknowledgments

AODVv2 is a descendant of the design of previous MANET on-demand protocols, especially AODV [RFC3561] and DSR [RFC4728]. Changes to previous MANET on-demand protocols stem from research and implementation experiences. Thanks to Elizabeth Belding-Royer for her long time authorship of AODV. Additional thanks to Luke Klein-Berndt, Pedro Ruiz, Fransisco Ros, Koojana Kuladinithi, Ramon Caceres, Thomas Clausen, Christopher Dearlove, Seung Yi, Romain Thouvenin, Tronje Krop, Henner Jakob, Alexandru Petrescu, Christoph Sommer, Cong Yuan, Lars Kristensen, and Derek Atkins for reviewing of AODVv2, as well as several specification suggestions.

This revision of AODVv2 isolates the minimal base specification and other optional features to simplify the process of ensuring compatibility with the existing LOADng specification [I-D.clausen-lln-loadng] (minimal reactive routing protocol specification). Thanks are due to T. Clausen, A. Colin de Verdiere, J. Yi, A. Niktash, Y. Igarashi, Satoh. H., and U. Herberg for their development of LOADng and sharing details for ensuring appropriateness of AODVv2 for LLNs.

## 6. References

### 6.1. Normative References

[RFC1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5082] Gill, V., Heasley, J., Meyer, D., Savola, P., and C. Pignataro, "The Generalized TTL Security Mechanism (GTSM)", RFC 5082, October 2007.

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format", RFC 5444, February 2009.

[RFC5497] Clausen, T. and C. Dearlove, "Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)", RFC 5497, March 2009.

[RFC5498] Chakeres, I., "IANA Allocations for Mobile Ad Hoc Network

(MANET) Protocols", RFC 5498, March 2009.

## 6.2. Informative References

[I-D.clausen-lln-loadng]
Clausen, T., Verdiere, A., Yi, J., Niktash, A., Igarashi, Y., Satoh, H., Herberg, U., Lavenu, C., Lys, T., and C. Perkins, "The LLN On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng)", draft-clausen-lln-loadng-05 (work in progress), July 2012.

[Perkins99]
Perkins, C. and E. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp. 90-100, February 1999.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC2501] Corson, M. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4728] Johnson, D., Hu, Y., and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, February 2007.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC5148] Clausen, T., Dearlove, C., and B. Adamson, "Jitter Considerations in Mobile Ad Hoc Networks (MANETs)", RFC 5148, February 2008.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, April 2011.

[RFC6549] Lindem, A., Roy, A., and S. Mirtorabi, "OSPFv2 Multi-Instance Extensions", RFC 6549, March 2012.

[RFC6621] Macker, J., "Simplified Multicast Forwarding", RFC 6621, May 2012.

## Appendix A. Changes since the Previous Version

- Internet-Facing AODVv2 router renamed to be IAR
- "Optional Features" section created to contain features not required within base specification, including:
- 
  - Intermediate RREPs (iRREPs): Without iRREP, only the destination can respond to a RREQ.
  - Precursor lists.
  - An RERR may reporting multiple unreachable nodes.
  - Message Aggregation.
- Sequence number MUST (instead of SHOULD) be set to 1 after rollover.
- ThisNode MUST (instead of SHOULD) only handle AODVv2 messages from adjacent routers.
- Clarification that Additional Routing information in RteMsgs is optional (MAY) to use.
- Clarification that if Additional Routing information in RteMsgs is used, then the Route Table Entry SHOULD be updated using normal procedures as described in Section 5.2.2.
- Clarification in Section 5.4 that nodes may be configured to buffer zero packets.
- Clarification in Section 5.4 that buffered packets MUST be dropped if route discovery fails.
- In Section 5.5.1, relax mandate for monitoring connectivity to next-hop AODVv2 neighbors (from MUST to SHOULD), in order to allow for minimal implementations

- Remove Route.Forwarding flag; identical to "NOT" Route.Broken.

- Routing Messages MUST be originated with the MsgHdr.HopLimit set to MSG_HOPLIMIT. Previously, this was not mandated.

- Maximum hop count set to 254, with 255 reserved for "unknown". Since the current draft only uses hop-count as distance, this is also the current maximum distance.

## Appendix B. Shifting Network Prefix Advertisement Between AODVv2 Routers

Only one AODVv2 router within a routing region SHOULD be responsible for a particular address at any time. If two AODVv2 routers dynamically shift the advertisement of a network prefix, correct AODVv2 routing behavior must be observed. The AODVv2 router adding the new network prefix must wait for any existing routing information about this network prefix to be purged from the network. Therefore, it must wait at least ROUTER_SEQNUM_AGE_MAX_TIMEOUT after the previous AODVv2 router for this address stopped advertising routing information on its behalf.

## Authors' Addresses

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1-408-330-5305
Email: charliep@computer.org

Ian D Chakeres
CenGen
9250 Bendix Road North
Columbia, Maryland 21045
USA

Email: ian.chakeres@gmail.com
URI: http://www.ianchak.com/