ROLL
Internet-Draft
Intended status: Standards Track
Expires: August 6, 2021

S. Anamalamudi
SRM University-AP
M. Zhang
Huawei Technologies
C. Perkins
Lupin Lodge
S.V.R.Anand
Indian Institute of Science
B. Liu
Huawei Technologies

February 2, 2021

AODV based RPL Extensions for Supporting Asymmetric P2P Links in Low-Power and Lossy Networks draft-ietf-roll-aodv-rpl-09

Abstract

Route discovery for symmetric and asymmetric Point-to-Point (P2P) traffic flows is a desirable feature in Low power and Lossy Networks (LLNs). For that purpose, this document specifies a reactive P2P route discovery mechanism for both hop-by-hop routing and source routing: Ad Hoc On-demand Distance Vector Routing (AODV) based RPL protocol (AODV-RPL). Paired Instances are used to construct directional paths, in case some of the links between source and target node are asymmetric.

Table of Contents

1. Introduction

RPL [RFC6550] (Routing Protocol for Low-Power and Lossy Networks) is an IPv6 distance vector routing protocol designed to support multiple traffic flows through a root-based Destination-Oriented Directed Acyclic Graph (DODAG). Typically, a router does not have routing information for most other routers. Consequently, for traffic between routers within the DODAG (i.e., Point-to-Point (P2P) traffic) data packets either have to traverse the root in non-storing mode, or traverse a common ancestor in storing mode. Such P2P traffic is thereby likely to traverse longer routes and may suffer severe congestion near the DAG root (for more information see [RFC6997], [RFC6998]).

The route discovery process in AODV-RPL is modeled on the analogous procedure specified in AODV [RFC3561]. The on-demand nature of AODV route discovery is natural for the needs of peer-to-peer routing in RPL-based LLNs. AODV terminology has been adapted for use with AODV-RPL messages, namely RREQ for Route Request, and RREP for Route Reply. AODV-RPL currently omits some features compared to AODV -- in particular, flagging Route Errors, blacklisting unidirectional links, multihoming, and handling unnumbered interfaces.

AODV-RPL reuses and provides a natural extension to the core RPL functionality to support routes with birectional asymmetric links. It retains RPL's DODAG formation, RPL Instance and the associated Objective Function (defined in [RFC6551]), trickle timers, and support for storing and non-storing modes. AODV adds basic messages RREQ and RREP as part of RPL DIO (DODAG Information Object) control messages, and does not utilize the DAO message of RPL. AODV-RPL specifies a new MOP running in a separate instance dedicated to discover P2P routes, which may differ from the P2MP routes discoverable by native RPL. AODV-RPL can be operated whether or not native RPL is running otherwise.

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 BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

AODV
: Ad Hoc On-demand Distance Vector Routing[RFC3561].

AODV-RPL Instance
: Either the RREQ-Instance or RREP-Instance

Asymmetric Route
: The route from the OrigNode to the TargNode can traverse different nodes than the route from the TargNode to the OrigNode. An asymmetric route may result from the asymmetry of links, such that only one direction of the series of links satisfies the Objective Function during route discovery.

Bi-directional Asymmetric Link
: A link that can be used in both directions but with different link characteristics.

DIO
: DODAG Information Object

DODAG RREQ-Instance (or simply RREQ-Instance)
: RPL Instance built using the DIO with RREQ option; used for control message transmission from OrigNode to TargNode, thus enabling data transmission from TargNode to OrigNode.

DODAG RREP-Instance (or simply RREP-Instance)
: RPL Instance built using the DIO with RREP option; used for control message transmission from TargNode to OrigNode thus enabling data transmission from OrigNode to TargNode.

Downward Direction
: The direction from the OrigNode to the TargNode.

Downward Route
: A route in the downward direction.

hop-by-hop routing
: Routing when each node stores routing information about the next hop.

on-demand routing
: Routing in which a route is established only when needed.

OrigNode
: The IPv6 router (Originating Node) initiating the AODV-RPL route discovery to obtain a route to TargNode.

Paired DODAGs
: Two DODAGs for a single route discovery process between OrigNode and TargNode.

P2P
: Point-to-Point -- in other words, not constrained a priori to traverse a common ancestor.

reactive routing
: Same as "on-demand" routing.

RREQ-DIO message
: An AODV-RPL MOP DIO message containing the RREQ option. The RPLInstanceID in RREQ-DIO is assigned locally by the OrigNode. The RREQ-DIO message has a secure variant as noted in [RFC6550].

RREP-DIO message
: An AODV-RPL MOP DIO message containing the RREP option. The RPLInstanceID in RREP-DIO is typically paired to the one in the associated RREQ-DIO message. The RREP-DIO message has a secure variant as noted in [RFC6550].

Source routing
: A mechanism by which the source supplies the complete route towards the target node along with each data packet [RFC6550].

Symmetric route
: The upstream and downstream routes traverse the same routers.

TargNode
: The IPv6 router (Target Node) for which OrigNode requires a route and initiates Route Discovery within the LLN network.

Upward Direction
: The direction from the TargNode to the OrigNode.

Upward Route
: A route in the upward direction.

ART option
: AODV-RPL Target option: a target option defined in this document.

3. Overview of AODV-RPL

With AODV-RPL, routes from OrigNode to TargNode within the LLN network are established "on-demand". In other words, the route discovery mechanism in AODV-RPL is invoked reactively when OrigNode has data for delivery to the TargNode but existing routes do not satisfy the application's requirements. AODV-RPL is thus functional without requiring the use of RPL or any other routing protocol.

The routes discovered by AODV-RPL are not constrained to traverse a common ancestor. AODV-RPL can enable asymmetric communication paths in networks with bidirectional asymmetric links. For this purpose, AODV-RPL enables discovery of two routes: namely, one from OrigNode to TargNode, and another from TargNode to OrigNode. When possible, AODV-RPL also enables symmetric route discovery along Paired DODAGs (see Section 5).

In AODV-RPL, routes are discovered by first forming a temporary DAG rooted at the OrigNode. Paired DODAGs (Instances) are constructed according to the AODV-RPL Mode of Operation (MOP) during route formation between the OrigNode and TargNode. The RREQ-Instance is formed by route control messages from OrigNode to TargNode whereas the RREP-Instance is formed by route control messages from TargNode to OrigNode. Intermediate routers join the Paired DODAGs based on the Rank as calculated from the DIO message. Henceforth in this document, the RREQ-DIO message means the AODV-RPL mode DIO message from OrigNode to TargNode, containing the RREQ option (see Section 4.1). Similarly, the RREP-DIO message means the AODV-RPL mode DIO message from TargNode to OrigNode, containing the RREP option (see Section 4.2). The route discovered in the RREQ-Instance is used for transmitting data from TargNode to OrigNode, and the route discovered in RREP-Instance is used for transmitting data from OrigNode to TargNode.

4. AODV-RPL DIO Options

4.1. AODV-RPL RREQ Option

OrigNode sets its IPv6 address in the DODAGID field of the RREQ-DIO message. A RREQ-DIO message MUST carry exactly one RREQ option, otherwise it SHOULD be dropped.

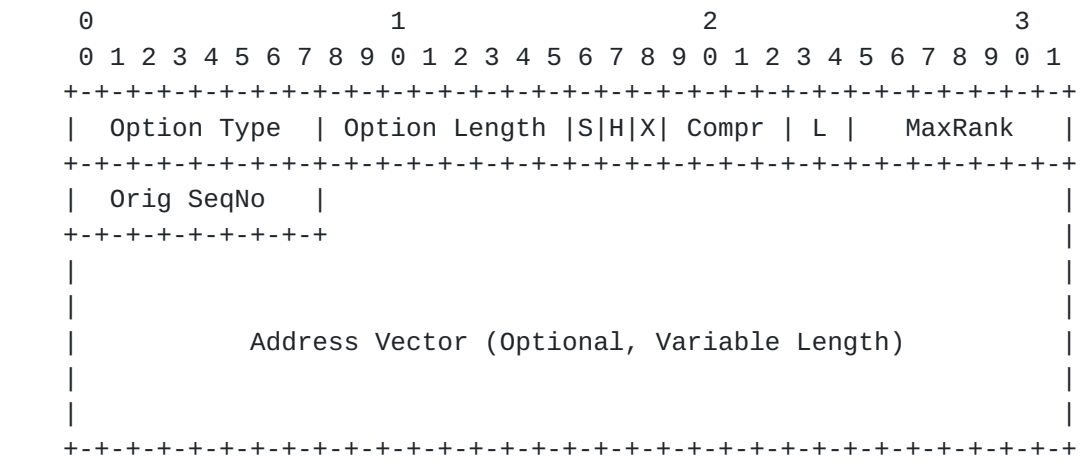

Figure 1: Format for AODV-RPL RREQ Option

OrigNode supplies the following information in the RREQ option:

Option Type
: TBD2

Option Length
: The length of the option in octets, excluding the Type and Length fields. Variable due to the presence of the address vector and the number of octets elided according to the Compr value.

S
: Symmetric bit indicating a symmetric route from the OrigNode to the router transmitting this RREQ-DIO.

H
: Set to one for a hop-by-hop route. Set to zero for a source route. This flag controls both the downstream route and upstream route.

X
: Reserved.

Compr
: 4-bit unsigned integer. Number of prefix octets that are elided from the Address Vector. The octets elided are shared with the IPv6 address in the DODAGID. This field is only used in source routing mode (H=0). In hop-by-hop mode (H=1), this field MUST be set to zero and ignored upon reception.

L

2-bit unsigned integer determining the duration that a node is able to belong to the temporary DAG in RREQ-Instance, including the OrigNode and the TargNode. Once the time is reached, a node MUST leave the DAG and stop sending or receiving any more DIOs for the temporary DODAG.

* 0x00: No time limit imposed.
* 0x01: 16 seconds
* 0x02: 64 seconds
* 0x03: 256 seconds

L is independent from the route lifetime, which is defined in the DODAG configuration option.

MaxRank
This field indicates the upper limit on the integer portion of the Rank (calculated using the DAGRank() macro defined in [RFC6550]). A value of 0 in this field indicates the limit is infinity.

Orig SeqNo
Sequence Number of OrigNode. See Section 6.1.

Address Vector
A vector of IPv6 addresses representing the route that the RREQ-DIO has passed. It is only present when the H bit is set to 0. The prefix of each address is elided according to the Compr field.

TargNode can join the RREQ instance at a Rank whose integer portion is equal to the MaxRank. Other nodes MUST NOT join a RREQ instance if its own Rank would be equal to or higher than MaxRank. A router MUST discard a received RREQ if the integer part of the advertised Rank equals or exceeds the MaxRank limit.

4.2. AODV-RPL RREP Option

TargNode sets its IPv6 address in the DODAGID field of the RREP-DIO message. A RREP-DIO message MUST carry exactly one RREP option, otherwise the message SHOULD be dropped. TargNode supplies the following information in the RREP option:

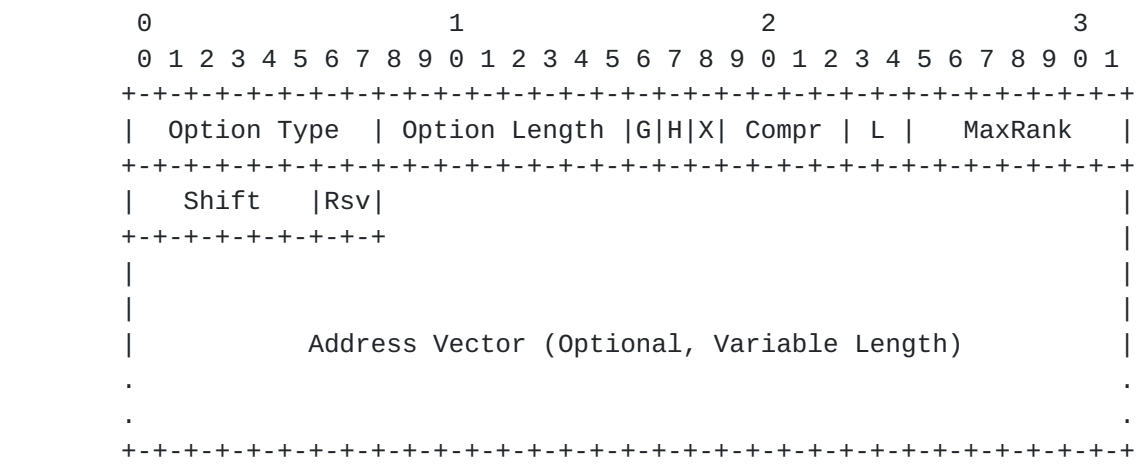

Figure 2: Format for AODV-RPL RREP option

Option Type
TBD3

Option Length
The length of the option in octets, excluding the Type and Length fields. Variable due to the presence of the address vector and the number of octets elided according to the Compr value.

G
Gratuitous route (see Section 7).

H
Requests either source routing (H=0) or hop-by-hop (H=1) for the downstream route. It MUST be set to be the same as the H bit in RREQ option.

X
Reserved.

Compr
4-bit unsigned integer. Same definition as in RREQ option.

L
2-bit unsigned integer defined as in RREQ option.

MaxRank
Similarly to MaxRank in the RREQ message, this field indicates the upper limit on the integer portion of the Rank. A value of 0 in this field indicates the limit is infinity.

Shift

6-bit unsigned integer. This field is used to recover the original RPLInstanceID (see Section 6.3.3); 0 indicates that the original RPLInstanceID is used.

Rsv
MUST be initialized to zero and ignored upon reception.

Address Vector
Only present when the H bit is set to 0. For an asymmetric route, the Address Vector represents the IPv6 addresses of the route that the RREP-DIO has passed. For a symmetric route, it is the Address Vector when the RREQ-DIO arrives at the TargNode, unchanged during the transmission to the OrigNode.

4.3. AODV-RPL Target Option

The AODV-RPL Target (ART) Option is based on the Target Option in core RPL [RFC6550]. The Flags field is replaced by the Destination Sequence Number of the TargNode and the Prefix Length field is reduced to 7 bits so that the value is limited to be no greater than 127.

A RREQ-DIO message MUST carry at least one ART Option. A RREP-DIO message MUST carry exactly one ART Option. Otherwise, the message MUST be dropped.

OrigNode can include multiple TargNode addresses via multiple AODV-RPL Target Options in the RREQ-DIO, for routes that share the same requirement on metrics. This reduces the cost to building only one DODAG.

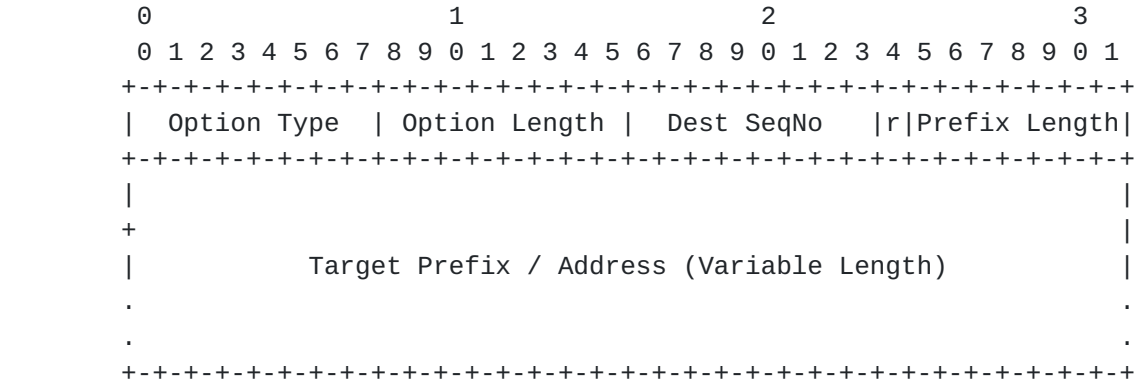

Figure 3: ART Option format for AODV-RPL MOP

Option Type
TBD4

Option Length
Length of the option in octets excluding the Type and Length fields

Dest SeqNo

In RREQ-DIO, if nonzero, it is the last known Sequence Number for TargNode for which a route is desired. In RREP-DIO, it is the destination sequence number associated to the route.

r
A one-bit reserved field. This field MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Prefix Length
7-bit unsigned integer. Number of valid leading bits in the IPv6 Prefix. If Prefix Length is 0, then the value in the Target Prefix / Address field represents an IPv6 address, not a prefix.

Target Prefix / Address
(variable-length field) An IPv6 destination address or prefix. The Prefix Length field contains the number of valid leading bits in the prefix. The length of the field is the least number of octets that can contain all of the bits of the Prefix, in other words Floor((7+(Prefix Length))/8) octets. The remaining bits in the Target Prefix / Address field after the prefix length (if any) MUST be set to zero on transmission and MUST be ignored on receipt.

5. Symmetric and Asymmetric Routes

Links are considered symmetric until additional information is collected. In Figure 4 and Figure 5, BR is the Border Router, O is the OrigNode, R is an intermediate router, and T is the TargNode. If the RREQ-DIO arrives over an interface that is known to be symmetric, and the S bit is set to 1, then it remains as 1, as illustrated in Figure 4. If an intermediate router sends out RREQ-DIO with the S bit set to 1, then all the one-hop links on the route from the OrigNode O to this router meet the requirements of route discovery, and the route can be used symmetrically.

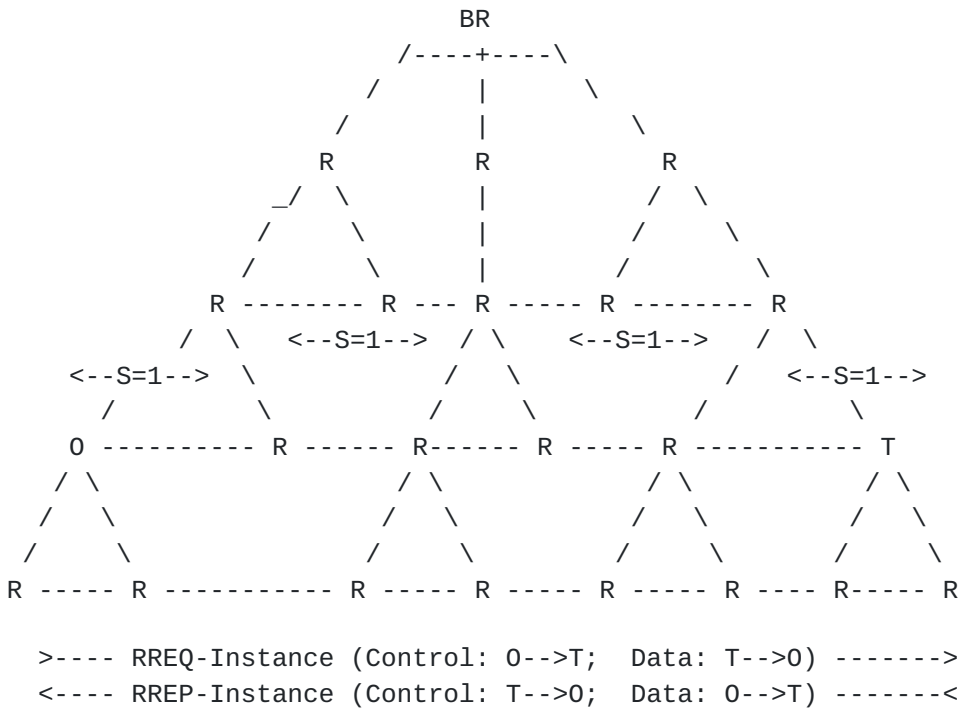

Figure 4: AODV-RPL with Symmetric Paired Instances

Upon receiving a RREQ-DIO with the S bit set to 1, a node determines whether this one-hop link can be used symmetrically, i.e., both the two directions meet the requirements of data transmission. If the RREQ-DIO arrives over an interface that is not known to be symmetric, or is known to be asymmetric, the S bit is set to 0. If the S bit arrives already set to be '0', it is set to be '0' on retransmission (Figure 5). For an asymmetric route, there is at least one hop which doesn't satisfy the Objective Function. Based on the S bit received in RREQ-DIO, TargNode T determines whether or not the route is symmetric before transmitting the RREP-DIO message upstream towards the OrigNode O.

The criteria used to determine whether or not each link is symmetric is beyond the scope of the document. For instance, intermediate routers can use local information (e.g., bit rate, bandwidth, number of cells used in 6tisch), a priori knowledge (e.g. link quality according to previous communication) or use averaging techniques as appropriate to the application. Other link metric information can be acquired before AODV-RPL operation, by executing evaluation procedures; for instance test traffic can be generated between nodes of the deployed network. During AODV-RPL operation, OAM techniques for evaluating link state (see([RFC7548], [RFC7276], [co-ioam]) MAY be used (at regular intervals appropriate for the LLN). The evaluation procedures are out of scope for AODV-RPL.

Appendix A describes an example method using the upstream Expected Number of Transmissions" (ETX) and downstream Received Signal Strength Indicator (RSSI) to estimate whether the link is symmetric in terms of link quality is given in using an averaging technique.

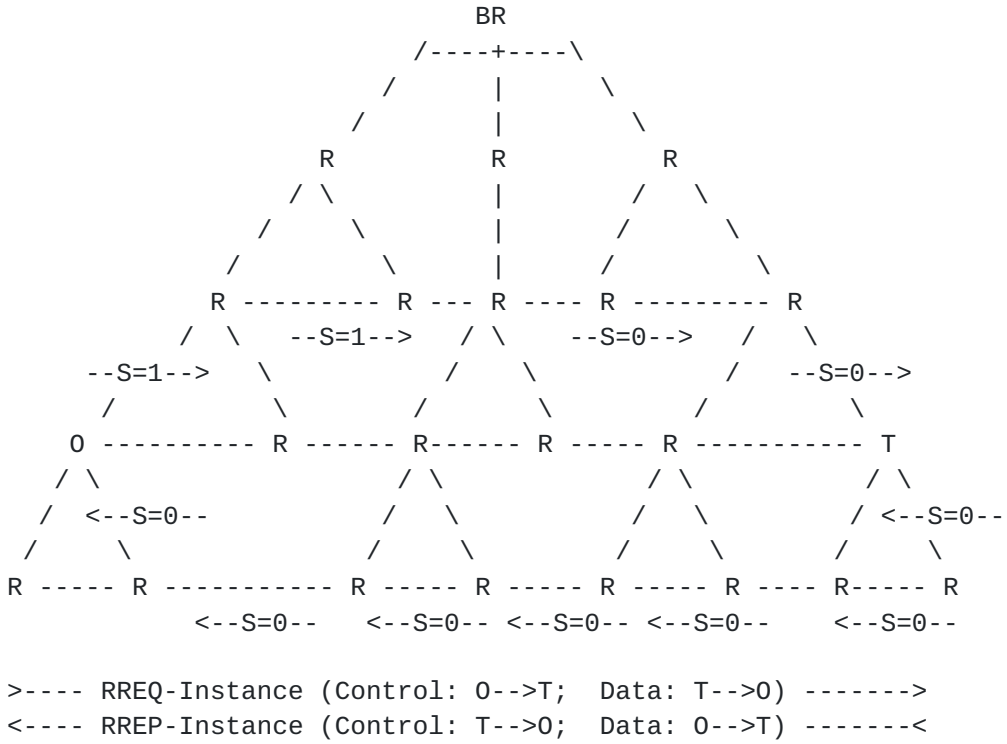

Figure 5: AODV-RPL with Asymmetric Paired Instances

6. AODV-RPL Operation

6.1. Route Request Generation

The route discovery process is initiated when an application at the OrigNode has data to be transmitted to the TargNode, but does not have a route that satisfies the Objective Function for the target of the data transmission. In this case, the OrigNode builds a local RPLInstance and a DODAG rooted at itself. Then it transmits a DIO message containing exactly one RREQ option (see Section 4.1) via link-local multicast. The DIO MUST contain at least one ART Option (see Section 4.3). The S bit in RREQ-DIO sent out by the OrigNode is set to 1.

Each node maintains a sequence number; the operation is specified in section 7.2 of [RFC6550]. When the OrigNode initiates a route discovery process, it MUST increase its own sequence number to avoid conflicts with previously established routes. The sequence number is carried in the Orig SeqNo field of the RREQ option.

The address in the ART Option can be a unicast IPv6 address or a prefix. The OrigNode can initiate the route discovery process for multiple targets simultaneously by including multiple ART Options, and within a RREQ-DIO the requirements for the routes to different TargNodes MUST be the same.

OrigNode can maintain different RPLInstances to discover routes with different requirements to the same targets. Using the RPLInstanceID pairing mechanism (see Section 6.3.3), route replies (RREP-DIOs) for different RPLInstances can be distinguished.

The transmission of RREQ-DIO obeys the Trickle timer [RFC6206]. If the duration specified by the L bit has elapsed, the OrigNode MUST leave the DODAG and stop sending RREQ-DIOs in the related RPLInstance.

6.2. Receiving and Forwarding RREQ messages

6.2.1. General Processing

Upon receiving a RREQ-DIO, a router goes through the steps below. If the router does not belong to the RREQ-Instance, then the maximum useful rank (MaxUseRank) is MaxRank. Otherwise, MaxUseRank is set to be the Rank value that was stored when the router processed the best previous RREQ for the DODAG with the given RREQ-Instance.

Step 1:

If the S bit in the received RREQ-DIO is set to 1, the router MUST determine whether each direction of the link (by which the RREQ-DIO is received) satisfies the Objective Function. In case that the downward (i.e. towards the TargNode) direction of the link does not satisfy the Objective Function, the link can't be used symmetrically, thus the S bit of the RREQ-DIO to be sent out MUST be set as 0. If the S bit in the received RREQ-DIO is set to 0, the router MUST determine into the upward direction (towards the OrigNode) of the link.

If the upward direction of the link can satisfy the Objective Function, and the router's Rank would not exceed the MaxUseRank limit, the router joins the DODAG of the RREQ-Instance. The router that transmitted the received RREQ-DIO is selected as the preferred parent. Otherwise, if the Objective Function is not satisfied or the MaxUseRank limit is exceeded, the router MUST discard the received RREQ-DIO and MUST NOT join the DODAG.

Step 2:

Then the router checks if one of its addresses is included in one of the ART Options. If so, this router is one of the TargNodes. Otherwise, it is an intermediate router.

Step 3:

If the H bit is set to 1, then the router (TargNode or intermediate) MUST build an upward route entry towards OrigNode which includes at least the following items: Source Address, RPLInstanceID, Destination Address, Next Hop, Lifetime, and Sequence Number. The Destination Address and the RPLInstanceID respectively can be learned from the DODAGID and the RPLInstanceID of the RREQ-DIO, and the Source Address is the address used by the local router to send data to the OrigNode. The Next Hop is the preferred parent. The lifetime is set according to DODAG configuration (i.e., not the L bit) and can be extended when the route is actually used. The sequence number represents the freshness of the route entry, and it is copied from the Orig SeqNo field of the RREQ option. A route entry with the same source and destination address, same RPLInstanceID, but stale sequence number, MUST be deleted.

Step 4:

If the router is an intermediate router, then it transmits a RREQ-DIO via link-local multicast; if the H bit is set to 0, the intermediate router MUST include the address of the interface receiving the RREQ-DIO into the address vector. Otherwise, if the router (i.e., TargNode) was not already associated with the RREQ-Instance, it prepares a RREP-DIO (Section 6.3). If, on the other hand TargNode was already associated with the RREQ-Instance, it takes no further action and does not send an RREP-DIO.

6.2.2. Additional Processing for Multiple Targets

If the OrigNode tries to reach multiple TargNodes in a single RREQ-Instance, one of the TargNodes can be an intermediate router to the others, therefore it MUST continue sending RREQ-DIO to reach other targets. In this case, before rebroadcasting the RREQ-DIO, a TargNode MUST delete the Target Option encapsulating its own address, so that downstream routers with higher Rank values do not try to create a route to this TargNode.

An intermediate router could receive several RREQ-DIOs from routers with lower Rank values in the same RREQ-Instance but have different lists of Target Options. When rebroadcasting the RREQ-DIO, the intersection of these lists MUST be included. For example, suppose two RREQ-DIOs are received with the same RPLInstance and OrigNode.

Suppose further that the first RREQ has (T1, T2) as the targets, and the second one has (T2, T4) as targets. Then only T2 needs to be included in the generated RREQ-DIO. If the intersection is empty, it means that all the targets have been reached, and the router MUST NOT send out any RREQ-DIO. For the purposes of determining the intersection with previous incoming RREQ-DIOs, the intermediate router maintains a record of the targets that have been requested associated with the RREQ-Instance. Any RREQ-DIO message with different ART Options coming from a router with higher Rank is ignored.

6.3. Generating Route Reply (RREP) at TargNode

6.3.1. RREP-DIO for Symmetric route

If a RREQ-DIO arrives at TargNode with the S bit set to 1, there is a symmetric route along which both directions satisfy the Objective Function. Other RREQ-DIOs might later provide asymmetric upward routes (i.e. S=0). Selection between a qualified symmetric route and an asymmetric route that might have better performance is implementation-specific and out of scope. If the implementation selects the symmetric route, and the L bit is not 0, the TargNode MAY delay transmitting the RREP-DIO for duration RREP_WAIT_TIME to await a symmetric route with a lower Rank. The value of RREP_WAIT_TIME is set by default to 1/4 of the time duration determined by the L bit.

For a symmetric route, the RREP-DIO message is unicast to the next hop according to the accumulated address vector (H=0) or the route entry (H=1). Thus the DODAG in RREP-Instance does not need to be built. The RPLInstanceID in the RREP-Instance is paired as defined in Section 6.3.3. In case the H bit is set to 0, the address vector received in the RREQ-DIO MUST be included in the RREP-DIO. TargNode increments its current sequence number and uses the incremented result in the Dest SeqNo in the ART option of the RREQ-DIO. The address of the OrigNode MUST be encapsulated in the ART Option and included in this RREP-DIO message.

6.3.2. RREP-DIO for Asymmetric Route

When a RREQ-DIO arrives at a TargNode with the S bit set to 0, the TargNode MUST build a DODAG in the RREP-Instance rooted at itself in order to discover the downstream route from the OrigNode to the TargNode. The RREP-DIO message MUST be re-transmitted via link-local multicast until the OrigNode is reached or MaxRank is exceeded. The TargNode MAY delay transmitting the RREP-DIO for duration RREP_WAIT_TIME to await a route with a lower Rank. The value of RREP_WAIT_TIME is set by default to 1/4 of the time duration determined by the L bit.

The settings of the fields in RREP option and ART option are the same as for the symmetric route, except for the S bit.

6.3.3. RPLInstanceID Pairing

Since the RPLInstanceID is assigned locally (i.e., there is no coordination between routers in the assignment of RPLInstanceID), the tuple (OrigNode, TargNode, RPLInstanceID) is needed to uniquely identify a discovered route. It is possible that multiple route discoveries with dissimilar Objective Functions are initiated simultaneously. Thus between the same pair of OrigNode and TargNode, there can be multiple AODV-RPL route discovery instances. To avoid any mismatch, the RREQ-Instance and the RREP-Instance in the same route discovery MUST be paired using the RPLInstanceID.

When preparing the RREP-DIO, a TargNode could find the RPLInstanceID to be used for the RREP-Instance is already occupied by another RPL Instance from an earlier route discovery operation which is still active. In other words, it might happen that two distinct OrigNodes need routes to the same TargNode, and they happen to use the same RPLInstanceID for RREQ-Instance. In this case, the occupied RPLInstanceID MUST NOT be used again. Then the second RPLInstanceID MUST be shifted into another integer so that the two RREP-instances can be distinguished. In RREP option, the Shift field indicates the shift to be applied to original RPLInstanceID. When the new RPLInstanceID after shifting exceeds 63, it rolls over starting at 0. For example, the original RPLInstanceID is 60, and shifted by 6, the new RPLInstanceID will be 2. Related operations can be found in Section 6.4.

6.4. Receiving and Forwarding Route Reply

Upon receiving a RREP-DIO, a router which does not belong to the RREQ-Instance goes through the following steps:

Step 1:

If the S bit is set to 1, the router MUST proceed to step 2.

If the S bit of the RREP-DIO is set to 0, the router MUST determine whether the downward direction of the link (towards the TargNode) over which the RREP-DIO is received satisfies the Objective Function, and the router's Rank would not exceed the MaxRank limit. If so, the router joins the DODAG of the RREP-Instance. The router that transmitted the received RREP-DIO is selected as the preferred parent. Afterwards, other RREP-DIO messages can be received.

If the Objective Function is not satisfied, the router MUST NOT join the DODAG; the router MUST discard the RREQ-DIO, and does not execute the remaining steps in this section.

Step 2:

The router next checks if one of its addresses is included in the ART Option. If so, this router is the OrigNode of the route discovery. Otherwise, it is an intermediate router.

Step 3:

If the H bit is set to 1, then the router (OrigNode or intermediate) MUST build a downward route entry towards TargNode which includes at least the following items: OrigNode Address, RPLInstanceID, TargNode Address as destination, Next Hop, Lifetime and Sequence Number. For a symmetric route, the Next Hop in the route entry is the router from which the RREP-DIO is received. For an asymmetric route, the Next Hop is the preferred parent in the DODAG of RREQ-Instance. The RPLInstanceID in the route entry MUST be the original RPLInstanceID (after subtracting the Shift field value). The source address is learned from the ART Option, and the destination address is learned from the DODAGID. The lifetime is set according to DODAG configuration (i.e., not the L bit) and can be extended when the route is actually used. The sequence number represents the freshness of the route entry, and is copied from the Dest SeqNo field of the ART option of the RREP-DIO. A route entry with same source and destination address, same RPLInstanceID, but stale sequence number, MUST be deleted.

Step 4:

If the receiver is the OrigNode, it can start transmitting the application data to TargNode along the path as provided in RREP-Instance, and processing for the RREP-DIO is complete. Otherwise, in case of an asymmetric route, the intermediate router MUST include the address of the interface receiving the RREP-DIO into the address vector, and then transmit the RREP-DIO via link-local multicast. In case of a symmetric route, the RREP-DIO message is unicast to the Next Hop according to the address vector in the RREP-DIO (H=0) or the local route entry (H=1). The RPLInstanceID in the transmitted RREP-DIO is the same as the value in the received RREP-DIO. The local knowledge for the TargNode's sequence number SHOULD be updated.

Upon receiving a RREP-DIO, a router which already belongs to the RREQ-Instance SHOULD drop the RREP-DIO.

7. Gratuitous RREP

In some cases, an Intermediate router that receives a RREQ-DIO message MAY transmit a "Gratuitous" RREP-DIO message back to OrigNode instead of continuing to multicast the RREQ-DIO towards TargNode. The intermediate router effectively builds the RREP-Instance on behalf of the actual TargNode. The G bit of the RREP option is provided to distinguish the Gratuitous RREP-DIO (G=1) sent by the Intermediate node from the RREP-DIO sent by TargNode (G=0).

The gratuitous RREP-DIO can be sent out when an intermediate router receives a RREQ-DIO for a TargNode, and the router has a more recent (larger destination sequence number) pair of downward and upward routes to the TargNode which also satisfy the Objective Function.

In case of source routing, the intermediate router MUST unicast the received RREQ-DIO to TargNode including the address vector between the OrigNode and the router. Thus the TargNode can have a complete upward route address vector from itself to the OrigNode. Then the router MUST send out the gratuitous RREP-DIO including the address vector from the router itself to the TargNode.

In case of hop-by-hop routing, the intermediate router MUST unicast the received RREQ-DIO to the Next Hop on the route. The Next Hop router along the route MUST build new route entries with the related RPLInstanceID and DODAGID in the downward direction. The above process will happen recursively until the RREQ-DIO arrives at the TargNode. Then the TargNode MUST unicast recursively the RREP-DIO hop-by-hop to the intermediate router, and the routers along the route SHOULD build new route entries in the upward direction. Upon receiving the unicast RREP-DIO, the intermediate router sends the gratuitous RREP-DIO to the OrigNode as defined in Section 6.3.

8. Operation of Trickle Timer

The trickle timer operation to control RREQ-Instance/RREP-Instance multicast uses [RFC6206] to control RREQ-DIO and RREP-DIO transmissions. The Trickle control of these DIO transmissions follow the procedures described in the Section 8.3 of [RFC6550] entitled "DIO Transmission".

9. IANA Considerations

9.1. New Mode of Operation: AODV-RPL

IANA is asked to assign a new Mode of Operation, named "AODV-RPL" for Point-to-Point(P2P) hop-by-hop routing from the "Mode of Operation" Registry. The parenthesized number 5 is only a suggestion.

Value	Description	Reference
TBD1 (5)	AODV-RPL	This document

Figure 6: Mode of Operation

9.2. AODV-RPL Options: RREQ, RREP, and Target

IANA is asked to assign three new AODV-RPL options "RREQ", "RREP" and "ART", as described in Figure 7 from the "RPL Control Message Options" Registry. The parenthesized numbers are only suggestions.

Value	Meaning	Reference
TBD2 (0x0B)	RREQ Option	This document
TBD3 (0x0C)	RREP Option	This document
TBD4 (0x0D)	ART Option	This document

Figure 7: AODV-RPL Options

10. Security Considerations

In general, the security considerations for the operation of AODV-RPL are similar to those for the operation of RPL (as described in Section 19 of the RPL specification [RFC6550]). Sections 6.1 and 10 of [RFC6550] describe RPL's security framework, which provides data confidentiality, authentication, replay protection, and delay protection services. Additional analysis for the security threats to RPL can be found in [RFC7416].

A router can join a temporary DAG created for a secure AODV-RPL route discovery only if it can support the Security Configuration in use, which also specifies the key in use. It does not matter whether the key is preinstalled or dynamically acquired. The router must have the key in use before it can join the DAG being created for a secure P2P-RPL route discovery.

If a rogue router knows the key for the Security Configuration in use, it can join the secure AODV-RPL route discovery and cause various types of damage. Such a rogue router could advertise false information in its DIOs in order to include itself in the discovered route(s). It could generate bogus RREQ-DIO, and RREP-DIO messages

carrying bad routes or maliciously modify genuine RREP-DIO messages it receives. A rogue router acting as the OrigNode could launch denial-of-service attacks against the LLN deployment by initiating fake AODV-RPL route discoveries. In this type of scenario, RPL's preinstalled mode of operation, where the key to use for a P2P-RPL route discovery is preinstalled, SHOULD be used. If a future IETF document specifies the authenticated mode of operation as described in [RFC6550], then future AODV-RPL implementations SHOULD use the authenticated mode of operation.

When a RREQ-DIO message uses the source routing option by setting the H bit to 0, a rogue router may populate the Address Vector field with a set of addresses that may result in the RREP-DIO traveling in a routing loop. The TargNode MUST NOT generate a RREP if one of its addresses is present in the Address Vector. An Intermediate Router MUST NOT forward a RREP if one of its addresses is present in the Address Vector.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, DOI 10.17487/RFC6206, March 2011, <https://www.rfc-editor.org/info/rfc6206>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

[RFC6551] Vasseur, JP., Ed., Kim, M., Ed., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, DOI 10.17487/RFC6551, March 2012, <https://www.rfc-editor.org/info/rfc6551>.

[RFC6998] Goyal, M., Ed., Baccelli, E., Brandt, A., and J. Martocci, "A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network", RFC 6998, DOI 10.17487/RFC6998, August 2013, <https://www.rfc-editor.org/info/rfc6998>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <https://www.rfc-editor.org/info/rfc7416>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

11.2. Informative References

[co-ioam] Ballamajalu, Rashmi., S.V.R., Anand., and Malati Hegde, "Co-iOAM: In-situ Telemetry Metadata Transport for Resource Constrained Networks within IETF Standards Framework", 2018 10th International Conference on Communication Systems & Networks (COMSNETS) pp.573-576, Jan 2018.

[contiki] Contiki contributors, "The Contiki Open Source OS for the Internet of Things (Contiki Version 2.7)", Nov 2013, <https://github.com/contiki-os/contiki>.

[Contiki-ng] Contiki-NG contributors, "Contiki-NG: The OS for Next Generation IoT Devices (Contiki-NG Version 4.6)", Dec 2020, <https://github.com/contiki-ng/contiki-ng>.

[cooja] Contiki/Cooja contributors, "Cooja Simulator for Wireless Sensor Networks (Contiki/Cooja Version 2.7)", Nov 2013, <https://github.com/contiki-os/contiki/tree/master/tools/cooja>.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, DOI 10.17487/RFC3561, July 2003, <https://www.rfc-editor.org/info/rfc3561>.

[RFC6997] Goyal, M., Ed., Baccelli, E., Philipp, M., Brandt, A., and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks", RFC 6997, DOI 10.17487/RFC6997, August 2013, <https://www.rfc-editor.org/info/rfc6997>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <https://www.rfc-editor.org/info/rfc7276>.

[RFC7548] Ersue, M., Ed., Romascanu, D., Schoenwaelder, J., and A. Sehgal, "Management of Networks with Constrained Devices: Use Cases", RFC 7548, DOI 10.17487/RFC7548, May 2015, <https://www.rfc-editor.org/info/rfc7548>.

Appendix A. Example: Using ETX/RSSI Values to determine value of S bit

The combination of Received Signal Strength Indication(downstream) (RSSI) and Expected Number of Transmissions(upstream)" (ETX) has been tested to determine whether a link is symmetric or asymmetric at intermediate nodes. We present two methods to obtain an ETX value from RSSI measurement.

Method 1: In the first method, we constructed a table measuring RSSI vs ETX using the Cooja simulation [cooja] setup in the Contiki OS environment[contiki]. We used Contiki-2.7 running 6LoWPAN/RPL protocol stack for the simulations. For approximating the number of packet drops based on the RSSI values, we implemented simple logic that drops transmitted packets with certain pre-defined ratios before handing over the packets to the receiver. The packet drop ratio is implemented as a table lookup of RSSI ranges mapping to different packet drop ratios with lower RSSI ranges resulting in higher values. While this table has been defined for the purpose of capturing the overall link behavior, it is highly recommended to conduct physical radio measurement experiments, in general. By keeping the receiving node at different distances, we let the packets experience different packet drops as per the described method. The ETX value computation is done by another module which is part of RPL Objective Function implementation. Since ETX value is reflective of the extent of pakcet drops, it allowed us to prepare a useful ETX vs RSSI table. ETX versus RSSI values obtained in this way may be used as explained below:

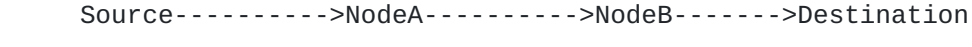

Figure 8: Communication link from Source to Destination

RSSI at NodeA for NodeB	Expected ETX at NodeA for NodeB->NodeA
> -60	150
-70 to -60	192
-80 to -70	226
-90 to -80	662
-100 to -90	3840

Table 1: Selection of S bit based on Expected ETX value

Method 2: One could also make use of the function guess_etx_from_rssi() defined in the 6LoWPAN/RPL protocol stack of Contiki-ng OS [Contiki-ng] to obtain RSSI-ETX mapping. This function outputs ETX value ranging between 128 and 3840 for -60 <= rssi <= -89. The function description is beyond the scope of this document.

We tested the operations in this specification by making the following experiment, using the above parameters. In our experiment, a communication link is considered as symmetric if the ETX value of NodeA->NodeB and NodeB->NodeA (see Figure 8) are within, say, a 1:3 ratio. This ratio should be understood as determining the link's symmetric/asymmetric nature. NodeA can typically know the ETX value in the direction of NodeA -> NodeB but it has no direct way of knowing the value of ETX from NodeB->NodeA. Using physical testbed experiments and realistic wireless channel propagation models, one can determine a relationship between RSSI and ETX representable as an expression or a mapping table. Such a relationship in turn can be used to estimate ETX value at nodeA for link NodeB--->NodeA from the received RSSI from NodeB. Whenever nodeA determines that the link towards the nodeB is bi-directional asymmetric then the S bit is set to 0. Afterwards, the link from NodeA to Destination remains designated as asymmetric and the S bit remains set to 0.

Appendix B. Changelog

Note to the RFC Editor: please remove this section before publication.

B.1. Changes from version 08 to version 09

- Removed section "Link State Determination" and put some of the relevant material into Section 5.

- Cited security section of [RFC6550] as part of the RREP-DIO message description in Section 2.

- SHOULD has been changed to MUST in Section 4.2.
- Expanded the terms ETX and RSSI in Section 5.
- Section 6.4 has been expanded to provide a more precise explanation of the handling of route reply.
- Added [RFC7416] in the Security Considerations (Section 10) for RPL security threats. Cited [RFC6550] for authenticated mode of operation.
- Appendix A has been mostly re-written to describe methods to determine whether or not the 'S' bit should be set to 1.
- For consistency, adjusted several mandates from SHOULD to MUST and from SHOULD NOT to MUST NOT.
- Numerous editorial improvements and clarifications.

B.2. Changes from version 07 to version 08

- Instead of describing the need for routes to "fulfill the requirements", specify that routes need to "satisfy the Objective Function".
- Removed all normative dependencies on [RFC6997]
- Rewrote Section 10 to avoid duplication of language in cited specifications.
- Added a new section "Link State Determination" with text and citations to more fully describe how implementations determine whether links are symmetric.
- Modified text comparing AODV-RPL to other protocols to emphasize the need for AODV-RPL instead of the problems with the other protocols.
- Clarified that AODV-RPL uses some of the base RPL specification but does not require an instance of RPL to run.
- Improved capitalization, quotation, and spelling variations.
- Specified behavior upon reception of a RREQ-DIO or RREP-DIO message for an already existing DODAGID (e.g, Section 6.4).
- Fixed numerous language issues in IANA Considerations Section 9.

- For consistency, adjusted several mandates from SHOULD to MUST and from SHOULD NOT to MUST NOT.

- Numerous editorial improvements and clarifications.

B.3. Changes from version 06 to version 07

- Added definitions for all fields of the ART option (see Section 4.3). Modified definition of Prefix Length to prohibit Prefix Length values greater than 127.

- Modified the language from [RFC6550] Target Option definition so that the trailing zero bits of the Prefix Length are no longer described as "reserved".

- Reclassified [RFC3561] and [RFC6998] as Informative.

- Added citation for [RFC8174] to Terminology section.

B.4. Changes from version 05 to version 06

- Added Security Considerations based on the security mechanisms defined in [RFC6550].

- Clarified the nature of improvements due to P2P route discovery versus bidirectional asymmetric route discovery.

- Editorial improvements and corrections.

B.5. Changes from version 04 to version 05

- Add description for sequence number operations.

- Extend the residence duration L in section 4.1.

- Change AODV-RPL Target option to ART option.

B.6. Changes from version 03 to version 04

- Updated RREP option format. Remove the T bit in RREP option.

- Using the same RPLInstanceID for RREQ and RREP, no need to update [RFC6550].

- Explanation of Shift field in RREP.

- Multiple target options handling during transmission.

B.7. Changes from version 02 to version 03

- Include the support for source routing.
- Import some features from [RFC6997], e.g., choice between hop-by-hop and source routing, the L bit which determines the duration of residence in the DAG, MaxRank, etc.
- Define new target option for AODV-RPL, including the Destination Sequence Number in it. Move the TargNode address in RREQ option and the OrigNode address in RREP option into ADOV-RPL Target Option.
- Support route discovery for multiple targets in one RREQ-DIO.
- New RPLInstanceID pairing mechanism.

Appendix C. Contributors

Abdur Rashid Sangi
Huaiyin Institute of Technology
No.89 North Beijing Road, Qinghe District
Huaian 223001
P.R. China
Email: sangi_bahrian@yahoo.com

Authors' Addresses

Satish Anamalamudi
SRM University-AP
Amaravati Campus
Amaravati, Andhra Pradesh 522 502
India

Email: satishnaidu80@gmail.com

Mingui Zhang
Huawei Technologies
No. 156 Beiqing Rd. Haidian District
Beijing 100095
China

Email: zhangmingui@huawei.com

Charles E. Perkins
Lupin Lodge
Saratoga 95070
United States

Email: charliep@computer.org

S.V.R Anand
Indian Institute of Science
Bangalore 560012
India

Email: anandsvr@iisc.ac.in

Bing Liu
Huawei Technologies
No. 156 Beiqing Rd. Haidian District
Beijing 100095
China

Email: remy.liubing@huawei.com