ROLL
Internet Draft
Intended status: Standards Track
Expires: June 20 2013

D.S. Do
N.T. Dinh
Y. Kim
Soongsil University

December 20, 2012

Backup Path for Point-to-Point Routes in Low Power and Lossy Networks
draft-do-roll-p2p-backup-00

Abstract

In this draft, a backup path setup mechanism is proposed for the P2P-RPL protocol in Low Power and Lossy Networks (LLNs). This mechanism allows sensor nodes to send packets over the backup path without rediscovering the p2p path in case of path failure, thus improving the reliability of p2p transmission.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on June 20, 2013.

Table of Contents

1. Introduction

Reliable routing is the general name for those mechanisms in which data is transmitted from a node to another node with a highly successful delivering ratio. Normally, reliable routing establishes a reliable path from the source to the destination. Then, the data packet is forwarded to the destination based on those paths. However, links in WSNs maybe frequently broken due to scheduling or sensor node failure. Therefore, data may not reach the destination. Then, the source needs to reestablish the path to the destination to send these packets. This increases costs and delays the transmission process. However, nodes in WSNs have resource constraints in terms of energy and memory. Thus, energy efficiency, reliability, and delay are crucial problems.

Currently, the P2P-RPL routing protocol [1] in the ROLL working group provides a standard protocol for communication between two nodes in Low power and Lossy Networks. This protocol relies on the

RPL routing protocol [RFC6550]. First, the source acts as a sink and builds its own directed acyclic graph (DAG) to discover the destination. Then, the destination sends a unicast message back to the source node to confirm the path from the source to the destination. The current P2P-RPL routing protocol focuses on building only one point-to-point path. However, in an LLN environment, this path can be frequently broken at any time during the transmission phase. In this case, the overhead to rebuild the path from the beginning is very high.

This document describes an extension to the P2P-RPL routing protocol on recovery after path failure. Nodes utilize the interactive path as alternative to quickly recover from failure to send packets to the destination instead of recreating the path. In particular, the purpose of the P2P-RPL-BACKUP is to immediately repair the path locally at the failed point to minimize cost and latency. The interactive path was created for this purpose without high extra overhead, which is composed of links including primary links and backup links for an optimal recovery path. In addition, this mechanism helps improve the performance of p2P-RPL routing in case of failure. Primary links and interactive links are defined in the terminology section.

2. Targeted Use Cases

This document aims at point-to-point communication in LLN scenarios where reliability and delay constraints are not satisfied by P2P routes, especially in high broken link scenarios, including in industrial zone, home automation, and building automation.

One typical example is due to the changes in the climate, a sensor to inform the cluster head of sensors in an area to change its parameters related to living conditions. In these applications, reliable transmission and delay are important. The message should be sent as quickly as possible. Then, retransmission of messages should be minimized.

3. Terminology

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

Besides the terminology from [1], this draft also uses the following terms:

Source: The node that initiates route discovery.

Destination: The node at the end point of the discovery process.

Intermediate: The nodes between the Source and the Destination.

Primary path: The path is established between the source and the destination based on P2P-RPL routing protocol.

Primary node: The nodes on the Primary path.

Primary link: The links on the Primary path.

Backup node: The nodes selected for backup forwarding in case of failure on the Primary path.

Backup link: The links created between a primary node and a backup node or between two backup nodes.

Backup path: The path created by backup nodes.

Interactive path: The path created between the primary link and backup link for an optimal recovery path from the failure.

Forward direction: The direction from a primary node to a backup node.

Backward direction: The direction from a backup node to a primary node.

Hop-by-hop route: The route by which each node uses the routing table to determine the next-hop.

4. P2P backup path setup in LLNs

This section briefly describes the P2P-RPL-BACKUP process.

Our proposal is an extension of the P2P-RPL routing algorithm [1]. As with the P2P-RPL routing protocol, the Source starts building its own new DAG by using IPv6 link-local multicast DIO messages to discover the destination. However, unlike P2P-RPL routing, which only focuses on creating one path, the P2P-RPL-BACKUP tries to build a recovery path in addition to the Primary path. The recovery path is used in case of failure in the Primary path. The backup path can be used as a recovery path to avoid rediscovering processes that may result in high overhead and latency.

However, the failure may occur at any node or link on the Primary path. Therefore, retransmission on the backup path is not an optimal

solution. P2P-RPL-BACKUP aims at repairing the path locally at the failed point immediately to minimize cost and latency. The interactive path is created for this purpose without high extra overhead and is composed of links, such as the primary link and backup link, for an optimal recovery path.

The interactive path has special characteristics. The Primary path is responsible for transmitting packets from the Source to the Destination. The other paths are used as backup paths in the event a link is lost in the primary path. In this context, each node in the primary path has only one backup node in the secondary path. In addition, a node in the secondary path has connections with two nodes in the primary path. Once a packet arrives at a node, it has two options: It can be forwarded along the primary path or along the secondary path. Naturally, by utilizing the backup link at each node, the probability of a packet's successful transmission to the Destination is increased. Moreover, this algorithm helps reduce data packet transmission when the primary path is disrupted. Furthermore, the number of nodes in the secondary path are estimated and limited by the number of nodes in the primary path because each node in the primary path has a backup node.

The Interactive-path-establishing process relies on the above characteristics. After the destination discovery phase, each node has its own position in the DAG of the Source by setting up its own rank [RFC6206]. Next, the Destination sends a discovery reply message back to its parent in the DAG of the Source to establish the Primary node. Then, this process is repeated until the Primary path is completely setup. The process of setting up the Interactive path occurs simultaneously. This is also based on the Discovery Reply message, which contains the Backup Path Establishing option and is defined in the next section, and includes two processes—establishing the connection between the Primary node and the Backup nodes and establishing the connection between the backup nodes. For the first process, the Destination sends its neighbors a Discovery Reply message that contains the above options and the rank of the Destination. If the rank of a neighbor is smaller than the rank contained in the option, the neighbor continues forwarding the reply message to its neighbor. Otherwise, this message is discarded. After the second-packet-broadcasting process occurs in the Destination's neighbor, if a node in the Primary path receives this message, based on the rank contained in each message, the node will choose the node with a greater than its rank, making it the smallest rank among the satisfying ranks. If multiple nodes satisfy the above condition, one of them is randomly chosen. For the second process, a DIO message that contains the Backup Path Confirming option (which is defined in the next section) is sent back to the chosen backup node. Then, this

process is repeats to choose the next backup node. The entire process stops when it reaches the Source.

In the above process, the Source has to clarify the following information:

- The IPv6 address of the Destination: This address could be a unicast or multicast address.
- The forwarding mechanism: hop-by-hop.

In addition, one of the most important factors is the distance between the Source and the Destination, which determines whether the Destination should establish a path to the Source. If this distance is too great, energy is wasted forming a path from the Source to the Sink and from the Sink to the Destination.

After setting up the paths, except the interactive links, other links are unnecessary, and nodes do not keep those connections. Then, the DAG is released.

Finally, the data packets are forwarded along the Interactive path and adhere to the following rule: The Source sends data along the Primary path. If there is a broken link in this path, the intermediate node will redirect the data to the node in the Interactive path. At this node, the data are forwarded to the next hop in the Primary path if the link is available. Otherwise, the data are forwarded to the next-hop in the Interactive path.

5. Message Format

5.1. Backup Path Establishing Option

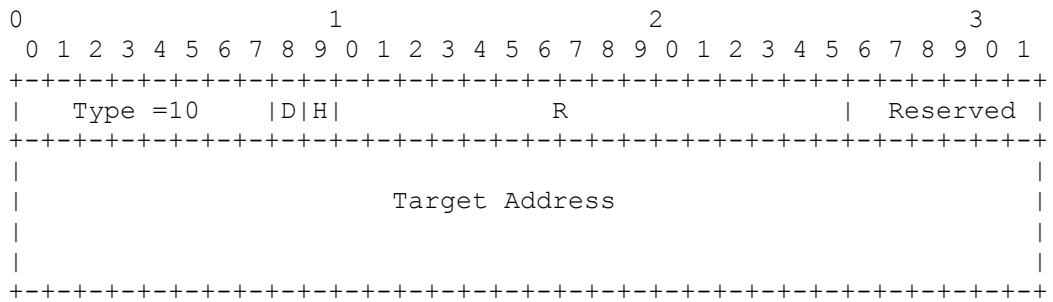

Figure 1: Format of the Backup Path Establishing Option

The Backup path Establishing Option is an alternative to the Discovery Reply Object in establishing the path between the backup and primary nodes.

- Option Type = 0x10 (to be confirmed by IANA).
- Target Address: The IPv6 address of the target node.
- D: A 1-bit field that indicates the direction of the desired routes.
  - D = 0x0: Forward from the primary node to the backup node.
  - D = 0x1: Backward from the backup node to the primary node.
- H: Limit the scale of sending message within one hop
- R: Rank of the sending node

5.2. Backup Path Confirming Option

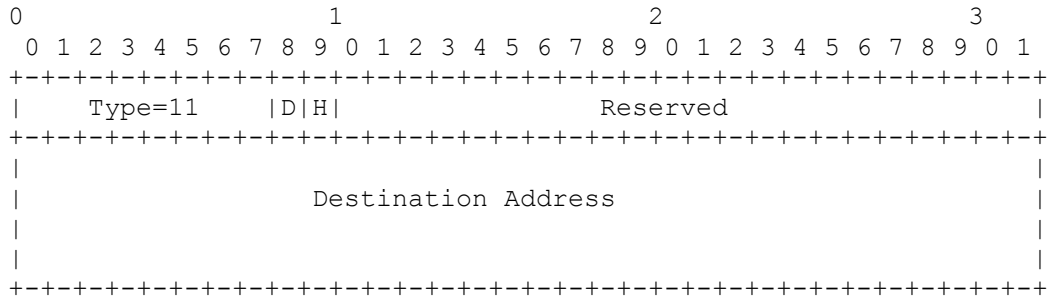

Figure 2. Format of the Backup Path Confirming Option

- Option Type = 0x11 (to be confirmed by IANA).
- Target Address: The IPv6 address of the selected node.
- D: A 1-bit field that indicates the direction of the desired routes:
  - D = 0x0: Forward from the primary node to the backup node.
  - D = 0x1: Backward from the backup node to the primary node.
- H: Limit the scale of sending message within one hop

[RFC6550] Winter, T., Thubert., P, and R. Team, "RPL: IPv6 routing protocol for low power and lossy networks, "RFC 6550, March 2012.

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, March 2011.

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

[1] Goyal, M., Baccelli, E., Philipp, M., Brandt, A., and J. Martocci, "Reactive Discovery of Point-to-Point Routes in Low Power and Lossy Networks, "draft-ietf-roll-p2p-rpl-15 (work in progress), October 2012.

Authors' Addresses

Dinh-Sy Do
Soongsil University
Huyngnam Enginerring Building 424, Soongsil Univ, Sangdo-do,
Dongjak-Gu, Seoul, Korea 156-743

Phone: 00828200841
Email: sydodinh@dcn.ssu.ac.kr

Ngoc-Thanh Dinh
Soongsil University
Huyngnam Enginerring Building 424, Soongsil Univ, Sangdo-do,
Dongjak-Gu, Seoul, Korea 156-743

Phone: 00828200841
Email: ngocthanhdinh@dcn.ssu.ac.kr

Younghan Kim
Soongsil University
Huyngnam Enginerring Building 424, Soongsil Univ, Sangdo-do,
Dongjak-Gu, Seoul, Korea 156-743

Phone: 00828200841
Email: younghak@ssu.ac.kr