MANET Working Group
Internet Draft
Expires: May 6, 2017

Sanghyun Ahn
University of Seoul
November 14, 2016

DSR Extensions for the Resolution of Cached Route Reply Implosion
draft-ahn-manet-dsr-crri-01.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, except to format it for publication as an RFC or to translate it into languages other than English.

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 May 6, 2017.

Copyright Notice

Abstract

In DSR, a node can generate a route reply in response to a received route request if it has a fresh route to the destination in its route cache. However, this can incur the cached route reply problem and DSR just tries to mitigate this problem by reducing the possibility of cached route reply collisions. This document describes how DSR can be extended for the resolution of the cached route reply problem.

Table of Contents

1. Requirements notation

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].

2. Introduction

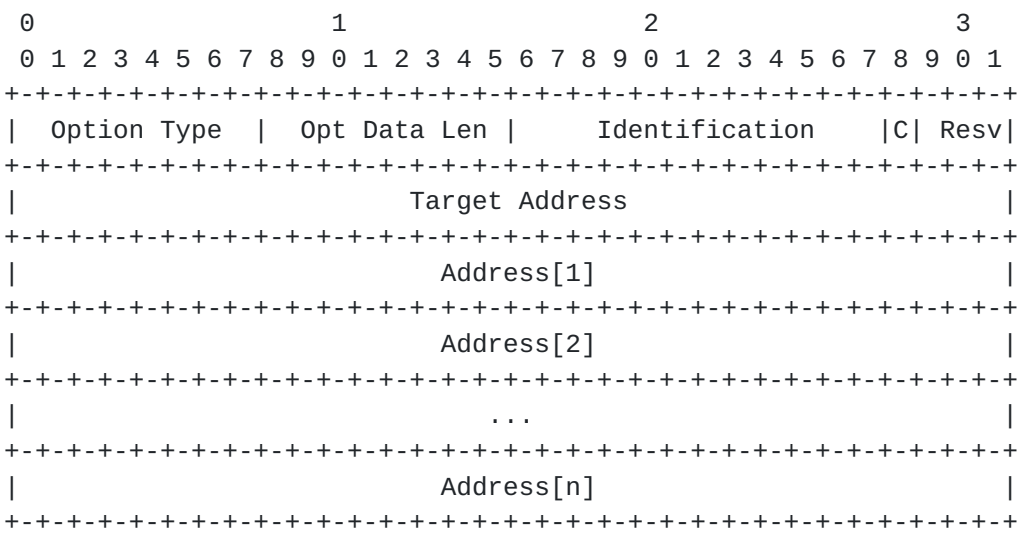
The DSR protocol [1] works based on the source routing mechanism and support multiple routes between a source and destination node pair by maintaining several routes in the route cache at the source. However, in DSR, the route reply storm problem can happen because of route replies generated by intermediate nodes with fresh routes to the destination in their own route caches (i.e., cached route replies). DSR tries to solve this route reply storm problem by reducing the possibility of route reply collisions with adding a short jitter delay before the broadcast of a route reply. However, DSR does not try to resolve the cause of the route reply storm problem.

The main reason of the route reply storm is uncontrolled generation of route replies at intermediate nodes, i.e., cached route replies. Therefore, a mechanism to control the generation of route replies at intermediate nodes is required for the effective operation of DSR. However,for the support of multipath routing, too tight restriction (control) on route reply generation may not be desirable. Therefore, when controlling the generation of route replies, both of these aspects need to be considered. In this draft, we describe how DSR Options header has to be extended to support the control of generation route replies.

3. Extensions on DSR Route Request Option

In DSR, there is no way to control the generation of cached route replies, so a C (Cached route reply) bit is inserted in the DSR Route Request option, To do that, the size of the Identification field is reduced to 14 bits from 16 bits.

The Route Request option in the DSR Options header is extended as follows:



IP fields
The same as described in [2].

Route Request fields
The same as described in [2] except for the Identification field, the C bit and the Resv field.

Identification
The definition of this field is the same as that in [2]. Only the size of this field is reduced to 12 bits.

C
C bit is used to indicate whether cached route replies are allowed or not. C bit is set to 1 if the cached route reply is allowed. The intermediate nodes can generate cached route replies only when the C bit of the received Route Request option is 1. Otherwise, only the destination node can generate route replies.

Resv
The reserved field for further extensions on DSR Route Request option.

4. Operations Related to C Flag

If a source node has to find a route to a destination, it first checks the ratio of the CRREP messages to the RREP messages received during previous route requests which can be computed by using the exponential weight moving average (EWMA). If the ratio is above the given threshold, it broadcasts an RREQ message with C = 0 to discover a route to the destination with the adaptive CRREP generation capability.

If a node, which is not the destination, receives an RREQ message with C = 0 and has the route information to the destination specified in the RREQ message, it decides the generation of a CRREP message probabilistically.

5. Other Considerations

TBD.

References

[1] D. Johnson, Y. Hu and D. Maltz, "The Dynamic Source Routing Protocol," RFC 4728, February 2007.

Author's Address

Sanghyun Ahn
University of Seoul
90, Cheonnong-dong, Tongdaemun-gu
Seoul 130-743
Korea
Email: ahn@uos.ac.kr