Considerations for ID/Location Separation Protocols in IP-based Vehicular Networks
draft-kjsun-ipwave-id-loc-separation-01

Abstract

ID/Location separation protocols are proposed for scalable routing, enhancing mobility and privacy in IP based internet infrastructure. When we consider IP based vehicular networks, ID/Location separation architecture is expected to offer benefits. In this draft, we analyze whether ID/Location separation protocols can adjust into IP based vehicular networks and solve requirements.

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 https://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 January 3, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
1. Introduction

For vehicular networks, it is required to provide connection to the Intelligent Transport System (ITS) for the driver’s safety, efficient driving and entertaining with fast mobility management. Other scenarios besides V2I communication, like V2V and V2X communication are also considered. Link layer protocols such as IEEE 802.11 OCB are already defined for low-latency and alternative networks, and it is designed for enabling IPv6 as a network layer protocol. Nevertheless, for using IPv6 in the vehicular network, there are some requirements for optimization as described in [ietf-ipwave-vehicular-networking]. These issues are classified into neighbor/service discovery, mobility management, security and privacy.

In IETF, there are several ID/Location separation protocols such as LISP [RFC6830] and ILNP [RFC6740] for scalable routing, enhancing privacy and mobility management. Currently ID/Location separation concept is useful not only for decomposing ID/Location from an IP address, but also for control/data plane separation which is a major evolution of the internet infrastructure. For the vehicular network, ID/Location separation protocols can be expected to meet requirements and solve problem statements discussed in IPWAVE WG. In this draft, we describe use cases for applying ID/Location separation architecture into IP-based vehicular network, and analyze whether such protocols can meet requirements for IPv6 in vehicular networks.
2. 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]. This document uses the terminology described in [ietf-ipwave-vehicular-networking], [RFC6830], [RFC6740].

3. Use Cases for ID/Location Separation Protocols

3.1. LISP

Traffic Control Center in Vehicular Cloud

*-----------------------------------------*
*                                          *
*                                           *
*             +----------------+              *
*              | Mapping System |               *
*              +----------------+               *
*              ^                       ^ *
*              MS/MR                  MS/MR *
*-----------------------------------------*

RLOC1 v v RLOC2 v v RLOC3

+---------+ Ethernet +---------+ Tunneling +---------+
| RSU1 |<--------| RSU2 |<--------| RSU3 |
| (xTR) |        | (xTR) |        | (xTR) |

+---------+ Ethernet +---------+ Tunneling +---------+
| Vehicle1|<------| Vehicle2|<------| Vehicle3|<------| Vehicle4|<------|
| (EID)  |       | (EID)  |       | (EID)  |       | (EID)  |

+---------+ V2V +---------+ V2V +---------+ V2V +---------+

LISP Site-1 LISP Site-2

<----> Wired Link <....> Wireless Link ===> Moving Direction

Figure 1: LISP Use Case Scenario in IP-based Vehicular Network Architecture
Figure 1 describes a vehicular network architecture with the LISP protocol. A single LISP site can have multiple RSUs with xTR function to communicate with other LISP sites. In the figure, we assume that Vehicle 1, 2 and 3 belong to LISP site 1 and Vehicle 4 to LISP site 2. IPv6 addresses for wireless interfaces of each vehicle are mapped to unique EIDs, which can communicate with other EIDs in the same LISP site same as a legacy IPv6 operation. That is, vehicles are able to communicate with RSU as V2I communication at the same time with other vehicles in the same LISP site as V2V communication.

Traffic control center in the vehicular cloud is appropriate to deploy a mapping system, since it is a point accessible from all RSUs. When vehicles enter each LISP site and attach to the RSU, RSU sends Map-Register message to the mapping system including vehicle’s EID and RLOC of attached RSU. After registration, the vehicle can be provided reachability from other LISP sites or non-LISP sites. In the figure, for communication between vehicle 4 and vehicle 3, RSU 3 which is the attachment point of vehicle 4 should request for the RLOC of vehicle 3 from the mapping system by sending Map-Requests message. After receiving mapping information of vehicle 3’s EID and its RLOC in Map-Reply message, RLOC 3 can forward packets via the IP tunnel between xTR (e.g. RSU 2 in this figure) assigned to vehicle 3. Note that several data plane protocols (e.g. SRv6, etc.) can be used with LISP control plane functions.

3.2. ILNP

In the ILNPv6, IPv6 address is replaced with an I-LV value. The I-LV has a 128-bit length allowing it to be applied to the current IPv6 header without modification. [RFC6740] describes in detail how I-LV value can replace an IPv6 address at the same time how can it works in current IPv6 based infrastructure. In [RFC6741], the details of the ILNPv6 packet header, locator subnetting and new DNS resource record type for mapping I-LV values are defined.

Vehicular network architecture design for supporting ILNP is shown in Figure 2. Most of the components are similar with architecture described in [ietf-ipwave-vehicular-networking]. Every vehicle can have more than one NID to connect to a network, and the IPv6 address for communication is represented as a combination of NID and Locator. Site Border Router (SBR) can be implemented in the RSU or border of ILNP subnet site, which should have a routing table mapped with I-LV values for forwarding packets. A DNS server can be deployed in the vehicular cloud which is accessible from both in ILNP site and external internet.
4. Gap Analysis

4.1. Neighbor Discovery

In both cases of LISP and ILNP, usage of existing neighbor discovery message defined in [RFC4861] is possible without modification. In LISP, vehicles and RSUs in the same LISP site can exchange ND/NA messages for routing via EID configured as IPv6 format. Also, ILNP can operate Neighbor Discovery for configuration of I-LV value as the I-LV for ILNPv6 occupies the same bits as the IPv6 address in the IPv6 header[RFC6740]. Thus, for vehicular networking, we expect that
the same solutions already mentioned in [ietf-ipwave-vehicular-networking] (e.g. new ND option [ID-Vehicular-ND]) also can be applicable in ID/Location separation architecture.

4.2. Mobility Management

One of the advantages for using LISP is that mobility management can be provided efficiently, when a device is roaming across different LISP sites while maintaining its EID. Existing IP mobility management schemes such as MIP or PMIP required an anchor function (e.g. Home Agent, Local Mobility Anchor) to maintain the IP address of mobile node when the mobile node moves so that it occurs non-optimized forwarding path between anchor and current attachment point of mobile node. In LISP, however, forwarding path can be optimized by updating EID-RLOC mapping information and establishing IP tunnel between xTR of corresponding node and xTR of current mobile node’s attachment point. This provides advantages for easily optimizing forwarding path especially in the vehicular network where connection point of the mobile node can be fastly moved away from its initial attachment point. In the vehicular network, EID will roam much faster and it means that the mapped RLOC will be changed more frequently. For faster RLOC assignment, a predictive RLOC algorithm for roaming-EID is proposed in LISP WG [draft-ietf-lisp-predictive-rlocs]. Using this algorithm, it predicts moving direction of roaming-EID, registers predictive RLOCs as a list to the mapping system, and replicates packets to each RLOC in the list. It can minimize packet loss while maintaining transport session continuity.

In ILNP, mobility management is classified into host mobility and network(site) mobility. For a vehicular network, host mobility scenario is suitable [RFC6740]. When the vehicle moves to its network attachment point and locator, it is changed to belong to new site, it may send Locator Update (LU) message to the Corresponding Node (CN) and also send a request to the DNS server to change its entry. Even though LU procedure is necessary, it causes delay and packet loss during handover, and it may become a more critical issue in the vehicular network which changes locator of vehicle faster and more frequently. Therefore, ILNP needs to minimize LU process including DNS updates for seamless mobility management in vehicular networks. For example, [ILNP-Sol-Wireless-Net] may be one possible solution that defines a geological information server, which gives information of attachment points nearby to devices to prepare handover, deliver its predictive locator to the CN so that it reduces packet loss and latency for updating DNS.
4.3. Security and Privacy

ID/Location separation architecture can enhance privacy. It is difficult to track a device using single RLOC or locator value since its locator changes with movement across sites. Nevertheless, since EID or identifier is defined as permanent, additional methodologies may be considered for enhancing access security of device identifier information. For example, [draft-ietf-lisp-eid-anonymity] defines Ephemeral-EID which is frequently changed by the device. For ILNP, identity privacy supports using IPv6 privacy extensions for stateless address autoconfiguration[RFC4941] and Locator Rewriting Relay (LRR) component for locator privacy[RFC6748], can be solutions for enhancing privacy in vehicular network.

In [draft-nordmark-id-loc-privacy], they raised two issues of privacy in ID/Location separation environment. One is location privacy which is related to geographic location of device reachable at some IP address coupled identifier, and other is movement privacy which is derived from changing locator of point of attachment at different times even without knowing particular locators and by possible correlation with other information. From that issues, [draft-xyz-pidloc-ps] described some use cases for privacy in vehicular network. [draft-xyz-pidloc-reqs] gave requirements for solving that challenges.

5. Informative References

[draft-ietf-lisp-eid-anonymity]

[draft-ietf-lisp-predictive-rlocs]

[draft-nordmark-id-loc-privacy]
Nordmark, E., "Privacy issues in ID/locator separation systems", draft-nordmark-id-loc-privacy-00 (Expired) (work in progress), July 2018.

[draft-xyz-pidloc-ps]
[draft-xyz-pidloc-reqs]
Iannone, L., von Hugo, D., and B. Sarikaya, "Requirements to Secure End to End Privacy in IdLoc Systems", draft-xyz-pidloc-reqs-00 (working on progress) (work in progress), May 2019.

[ID-Vehicular-ND]

[ietf-ipwave-vehicular-networking]

[ILNP-Sol-Wireless-Net]


Authors’ Addresses

Kyoungjae Sun  
School of Electronic Engineering  
Soongsil University  
369, Sangdo-ro, Dongjak-gu  
Seoul, Seoul 06978  
Republic of Korea  
Phone: +82 10 3643 5627  
EMail: gomjae@dcn.ssu.ac.kr

Younghan Kim  
School of Electronic Engineering  
Soongsil University  
369, Sangdo-ro, Dongjak-gu  
Seoul, Seoul 06978  
Republic of Korea  
Phone: +82 10 2691 0904  
EMail: younghak@ssu.ac.kr