Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 12, 2011

K. Uehara
M. Sato
Keio Univ.
K. Shima, Ed.
IIJ II

November 8, 2010

The Message Format for Decentralized Probe Applications for Vehicles
draft-uehara-dtnrg-decentralized-probe-message-00

Abstract

(This document is a description of the decentralized viechle to viechle probe mechanism currently being prototyped. The main purpose of disclosing this -00 document is to introduce the application idea and start discussion within the DTNRG. Because of this, the current mechanism described in this docment does not conform to the protocols defined in the DTNRG at this moment. The mechanism should be updated based on the discussion in this group.)

This document describes the application message format used for the decentralized probe system for vehicles. The probe system exchanges the application messages between vehicles using the transport protocol defined in the separate specification.

Table of Contents

1. Introduction

Thanks to the the advance of the Internet and the wireless communication technology, it becomes possible to equip communication mechanisms for vehicles for various purposes, such as for safety applications, entertainment applications, and so on. Recently, approaches utilizing the DTN (Delay Tolerant Network) technology for inter-vehicle communication are attracting people from both academy and industry. One of the application of the approaches is decentralized probe system for traffic information. It is considered that by combining the existing centralized approach for traffic monitoring and the proposed decentralized approach, more detailed information exchange is possible and wider area can be covered. This document proposes a standard message format for the traffic information dissemination application, and proposes a reference message dissemination strategy.

2. Application Behavior

2.1. Message Generation/Storing/Forwarding

The mechanism described in this document proposes a decentralized approach of message exchange for car traffic monitoring. The similar purpose is of course provided by the ITS (Intelligent Transport System) framework with the centralized approach. However, since such systems require a large amount of investment for the road side units and their management system, they are usually deployed only on highways and main lines of urban areas. The decentralized approach is one way to extend the area of the ITS service coverage, because the decentralized mechanism does not need to build any road side units, and each vehicle autonomously organizes the transport information network.

This document defines a general format of the message exchanged in the decentralized approach. Each vehicle monitors its activity, creates a message that indicates the activity, and distribute the message to other vehicles nearby based on the dissemination strategy defined in Section 2.2. A vehicle that receives messages from other vehicles stores the messages in its own message storage, and distribute again using the dissemination strategy specified in the message body.

For example, in the traffic jam information distribution case, a vehicle periodically monitors its speed and detects a traffic jam based on a traffic jam detection algorithm. Once a jam is detected, the vehicle creates a message with an application identifier that indicates it is a traffic jam detection application, and distributes

the message. Every message includes the time when the message is generated, the location where the message is created, the valid lifetime of the message, and the algorithm how/where to distribute the message. The transport mechanism of the messages is defined in other document [decentralized-probe-transport].

To avoid a malicious vehicle to inject faked messages, applications can sign the messages based on the identifier of the vehicle if necessary. If the message validation procedure fails when a vehicle receives a message, the message is discarded.

2.2. Dissemination Strategy

The dissemination strategy determines how to distribute a message. This document only defines a simple round dissemination strategy. The more complicated strategy is also possible and will be defined in separate documents.

The round-shape dissemination strategy specifies the destination location (with latitude/longitude values) and the distribution radius.

If a vehicle receives a message (regardless of the value of the dissemination identifier), it first looks up the same message in its message storage. A message can be identified by a node identifier, application identifier, and application sequence number. If the same message has already been stored in the storage, the received message is just ignored and discarded. If the message is not found in the storage, then the vehicle stores the received message.

A vehicle periodically checks its message storage to find messages which lifetime are expired. Any messages with expired lifetime are marked as deleted and removed when the amount of the free space of the storage becomes low.

A message will not be re-distributed until the dissemination conceal period has passed since the time when the message was received or re-distributed previously to avoid too frequent message exchange.

In the round-shape dissemination strategy, a vehicle compares its current location and the region specified in the dissemination parameter fields in the message. If the current location is covered by the region specified, the vehicle distribute the message to other vehicles nearby.

If the vehicle is out of the dissemination target region, the message is not distributed and kept in the storage.

3. Message Format

The application message consists of three parts. Each part is concatenated in the order listed below and passed to the packet sender module. The detailed description of the packet sender and receiver are found in [decentralized-probe-transport].

The first part contains the basic information of the application message. The second part contains the parameters for message dissemination strategy. The final part contains the security information.

3.1. Basic Information Part

Figure 1 shows the basic information part of the message.

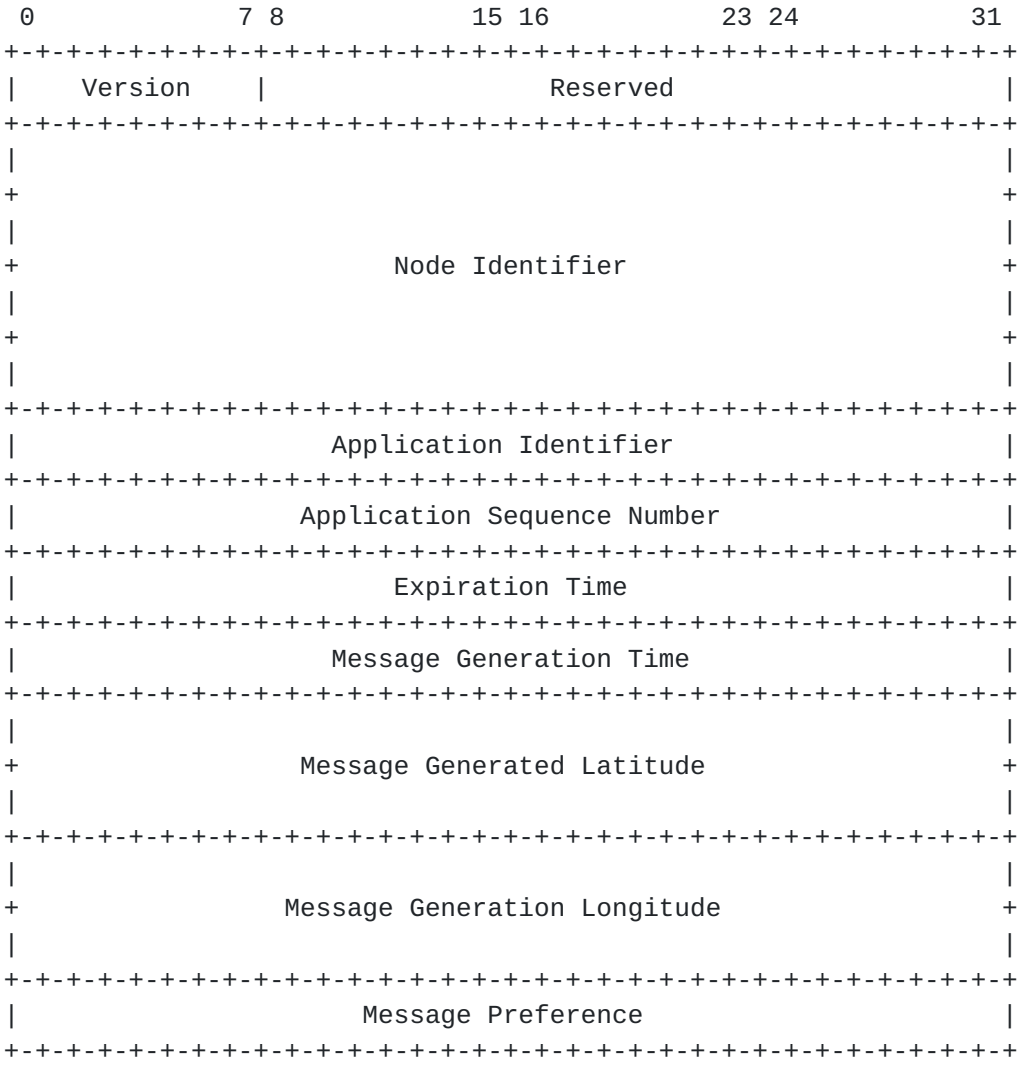

Figure 1: Basic Information Part

Version: 1

The version number of the message format. Currently version 1 is the only version defined.

Reserved: Reserved for future use

The field is reserved to support future extension. The sender of the message should fill 0 in this field and the receiver of the message must ignore the field.

Node Identifier: The unique identifier of the node

Application Identifier: The unique identifier of the application

Application Sequence Number: The unique number of the message generated within the node and application specified by the previous two fields

Expiration Time: The message expiration time in second from the epoch

Message Generation Time: The time from the epoch when the message was generated

Message Generation Latitude/Longitude: The location information of the message where it was generated

The values are represented in IEEE 754 double precision number format. The WGS 84 is used as a geodetic system.

Message Preference: A 32-bit ordered value indicating the preference within the application specified by the Application Identifier field.

3.2. Dissamination Parameters Part

Figure 2 shows the dissemination part of the message.

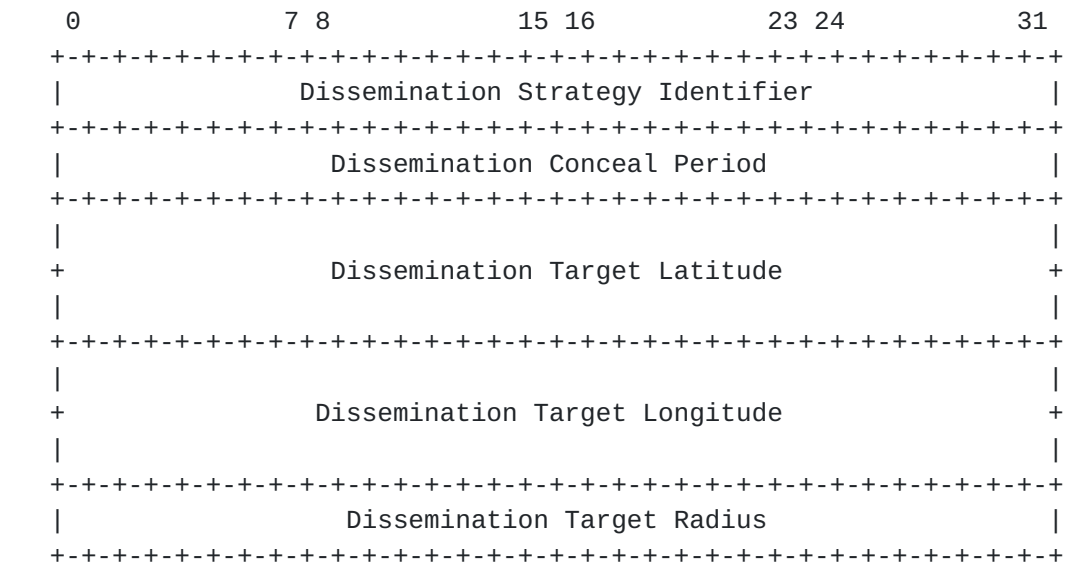

Figure 2: Dissemination Parameter Part

Dissemination Strategy Identifier: The dissemination strategy identifier specified in Section 2.2

Dissemination Conceal Period: The time in second to stay in the node without being disseminated

Dissemination Target Latitude/Longitude: The final target area of the message to be delivered

The values are represented in IEEE 754 double precision number format. The WGS 84 is used as a geodetic system.

Dissemination Target Radius: The radius in units of meter that indicates the size of the final target area

3.3. Security Part

Figure 3 shows the security part of the message.

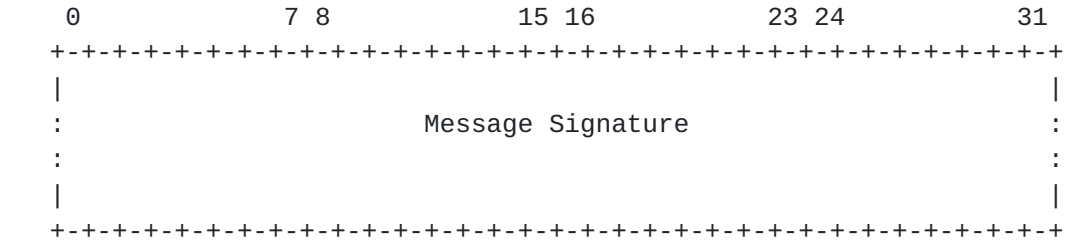

Figure 3: Security Part

Message Signature: PKCS #7 based message signature

The message contents may be signed by the message creater using creater's private key associated with the node identifier of the creater. The name space of the common name field is defined hierarchically (TBD) and its character code is utf-8. The key length and the algorithm is RSA2048.

4. Security Considerations

Sender verification and message integrity are provided by the upper layer mechanism, by using PKCS#7 based mechanism.

5. Protocol Constants

General

DCP_VERSION: 1

Application identifiers

DCP_APP_ID_RESERVED: 0

DCP_APP_ID_TRAFFICJAM: 1

Dissemination strategy identifiers

DCP_DISS_ID_RESERVED: 0

DCP_DISS_ID_ROUNDSHAPE: 1

6. Normative References

[decentralized-probe-transport]
Uehara, K., Imaike, M., and K. Shima, Ed., "The Transport Protocol for Decentralized Probe Applications for Vehicles", 2010.

Authors' Addresses

Keisuke Uehara
Keio University
5233 Endo
Fujisawa-shi, Kanagawa 252-8520
Japan

Email: kei@wide.ad.jp

Masaaki Sato
Keio University
5233 Endo
Fujisawa-shi, Kanagawa 252-8520
Japan

Email: saikawa@sfc.wide.ad.jp

Keiichi Shima (editor)
IIJ Innovation Institute Inc.
1-105 Kanda-Jinbocho
Chiyoda-ku, Tokyo 101-0051
Japan

Email: keiichi@iijlab.net