Network Working Group
Internet-Draft
Intended status: Informational
Expires: 25 Nov 2026

J. Chen
Independent Researcher
21 Nov 2025

Dynamic No-Entry Zone Dissemination in IPv6 Vehicular Networks
draft-jun-chen-ipwave-dynamic-no-entry-zone-00

Abstract

This document defines the Dynamic No-Entry Zone (DNEZ) information element and its dissemination mechanism using IPv6-based vehicular networks. A DNEZ is a temporary lane-level polygonal area generated by a stopped or faulty vehicle to indicate a region that surrounding vehicles may need to avoid. The primary use case is to provide redundancy when roadside perception systems fail due to occlusion, weather, or infrastructure limitations.

The DNEZ is disseminated using geographically-scoped IPv6 multicast (GeoBroadcast) as defined in RFC 9366. Receiving vehicles or Road Side Units (RSUs) may rebroadcast the message to extend coverage. Local interpretation and usage of the DNEZ is implementation-specific and outside the scope of this document.

Table of Contents

1. Introduction

When an automated or highly automated vehicle stops unexpectedly due to a critical fault, surrounding vehicles must be informed promptly and accurately to prevent secondary collisions. Traditional roadside perception systems may fail in tunnels, heavy rain, fog, or due to occlusion.

This document defines the Dynamic No-Entry Zone (DNEZ) as a temporary lane-level polygonal area generated by the stopped vehicle. The DNEZ is disseminated using IPv6 geographically-scoped messages defined in [RFC9366]. The mechanism provides a fully distributed, infrastructure-independent redundancy channel that complements existing Collective Perception and Decentralized Environmental Notification services.

How a receiving vehicle or RSU reacts to a DNEZ is deliberately left out of scope.

1.1. Requirements Language

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.

2. Terminology

Dynamic No-Entry Zone (DNEZ)
: A temporary polygonal area indicating a region that surrounding vehicles may need to avoid.

RSU
: Road Side Unit equipped with IPv6 and V2X communication capabilities.

3. Dynamic No-Entry Zone (DNEZ) Definition

A DNEZ is encoded as a sequence of geographical points defining a closed polygon together with associated metadata.

3.1. Polygon Construction

A stopped vehicle SHOULD construct the polygon as follows:

- Obtain its current position and heading using GNSS and/or sensor fusion.
- Retrieve lane-level geometry from a local high-definition map or recent MAP messages.
- Define the polygon with a rear boundary typically 50-200 m behind the vehicle and a front boundary at or slightly in front of the vehicle.

The polygon MUST be closed and use WGS84 coordinates.

3.2. DNEZ Attributes

The following attributes SHOULD be included:

- Generation timestamp
- Expiration timestamp or duration (maximum recommended 10 min)
- Cause code (e.g., vehicle breakdown, accident)
- Confidence level

- Originating vehicle temporary identifier

4. Dissemination Using IPv6 GeoNetworking

The DNEZ SHALL be disseminated using the GeoBroadcast mechanism defined in [RFC9366] with a destination area that fully covers the polygon plus a safety margin (typically 300-1000 m).

The originating vehicle SHALL broadcast immediately and MAY repeat with decreasing frequency until expiration.

Any receiving RSU or vehicle inside or near the destination area MAY rebroadcast the message once. Duplicate detection based on originator identifier and sequence number SHALL be implemented.

5. Local Relevance and Polygon Inclusion Check

Receivers SHOULD test whether their position lies inside the DNEZ polygon using the odd-even ray casting algorithm or equivalent.

Usage of the result is implementation-specific and outside the scope of this document.

6. Security Considerations

DNEZ messages carry safety-of-life implications and MUST be secured using existing V2X security mechanisms such as IEEE 1609.2 or ETSI ITS security. Receivers MUST verify signatures, certificate validity, and geographical/temporal relevance before processing.

Misbehavior detection and position plausibility checks SHOULD be applied.

7. IANA Considerations

This document has no IANA actions.

8. 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>.

[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>.

[RFC9366] Jeong, J. and Y. Shen, "IPv6 GeoNetworking Address Configuration", RFC 9366, DOI 10.17487/RFC9366, October 2023, <https://www.rfc-editor.org/info/rfc9366>.

Author’s Address

Jun Chen
Independent Researcher
Email: bot@botrun.cn