

Internet Engineering Task Force  
Internet-Draft  
Intended status: Informational  
Expires: May 04, 2014

Georgios Karagiannis  
Geert Heijenk  
University of Twente  
Andreas Festag  
Technical University Dresden & NEC Laboratories Europe  
Alexandru Petrescu  
CEA  
Alison Chaiken  
Mentor Embedded Software Division  
November 04, 2013

Internet-wide Geo-networking Problem Statement  
draft-karagiannis-problem-statement-geonetworking-01

Abstract

This document describes the need of specifying Internet-wide location-aware forwarding protocol solutions that provide packet routing using geographical positions for packet transport.

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 <http://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 May 04, 2014.

Copyright Notice

Copyright (c) 2013 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 (<http://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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Requirements Language

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 RFC 2119 [RFC2119].

Table of Contents

1. Introduction . . . . .	3
2. Use cases and scenarios . . . . .	6
3. Requirements . . . . .	12
4. Open Design Issues . . . . .	14
5. Possible solutions . . . . .	16
6. Security Considerations . . . . .	19
7. IANA Considerations . . . . .	19
8. Acknowledgments . . . . .	19
9. Normative References . . . . .	20
10. Informative References . . . . .	20
11. Authors' Address . . . . .	22

## 1. Introduction

### 1.1 Motivation

Internet-based applications use IP addresses to address a node that can be a host, a server or a router. Scenarios and use cases exist where nodes are being addressed using their geographical location instead of their IP address. The most obvious use cases are related to Intelligent Transportation Systems (ITS) and vehicular networking, environmental monitoring, consumer electronic devices (e.g. cameras) and scientific instruments. In this document we will mainly focus on ITS and vehicular networking. An ITS use case is, for example, a traffic jam or a chain collision, where all vehicles heading towards the potential hazard should be warned. In particular, for vehicles ahead that are moving away from the hazardous location, the information is not relevant anymore. In such dangerous situation geo-networking can offer great support to applications that require geographical addressing.

Internet-wide Geo-Networking is a location-aware forwarding protocol that provides packet routing using geographical positions for packet transport over the Internet. Vehicular networking can be considered as one of the most important enabling technologies required to implement a myriad of applications related to vehicles, vehicle traffic, drivers, passengers and pedestrians. Two main types of vehicle communication networks can be distinguished. In the Vehicle-to-Infrastructure (V2I) communication network packets are exchanged among vehicles using an infrastructure that can be Internet-wide. The second type is Vehicle-to-Vehicle (V2V) communication, where packets are exchanged among vehicles without the need for a communication infrastructure. Hybrid scenarios that combine V2V and V2I communication appear reasonable.

Intelligent Transportation Systems aim to improve the operation of vehicles, manage vehicle traffic, assist drivers with safety and other information, along with provisioning of convenience applications. Prime examples of ITS services include automated toll collection systems, driver assist systems and other information provisioning systems. Over the last decade, the development of ITS services has been backed up by coordinated efforts for standardization and formation of consortia and other governmental and industrial bodies that aim to set the guiding principles, requirements, and first takes on solutions for ITS-related communication systems that primarily involve vehicles and users within vehicles.

The main challenges that are associated with Internet-wide geo-networking are:

- o) support of geo-addressing, where geographical information should be available in the addressing mechanism, such that packets can be forwarded to a target geographical area. The geographical area may either be specified by the source (application) or might not be specified at all.

- o) support of Internet-wide geo-routing, where data packets that are generated by source nodes placed anywhere in the Internet are forwarded over multiple hops by using the position of the destination node(s) and the positions of intermediate nodes for the routing decisions.
- o) creation of a forwarding method that comprises (1) a local-computer decision algorithm which can deterministically compare IP/geographical addresses present in a packet to IP/geographical addresses present in a local database, (2) a (mixed IP and geographical) database topology distribution algorithm among several computers, and (3) an IP/geographical path construction algorithm which acts on the IP/geographical database.
- o) the use of a single consensual geodesic datum which may be used by present and future GNSSs (Global Navigation Satellite Systems) by as many as possible network operators, and agreed datum conversion methods.
- o) representation of precision in IP addressing. IP addresses are precise and unique, whereas geographical coordinates involve notions of precision and accuracy.

#### Geo-addressing:

In [RFC2009], three families of solutions are described to integrate the concept of physical location into the current design of Internet that relies on logical addressing. These families of solutions are: (1) Application layer solutions, (2) GPS-Multicast solution. (3) Unicast IP routing extended to deal with GPS addresses. In particular, [RFC2009] specifies how GPS positioning is used for destination addresses. A GPS (Global Positioning System) address could be represented by using: (1) closed polygons, such as circle(center point, radius), where, any node that lies within the defined geographic area could receive a message, (2) site-name as a geographic access path, where a message can be sent to a specific site by specifying its location in terms of real-world names such as names of site, city, township, county, state, etc. [ETSI-EN-302-636-4-1] specifies geographical addressing for point-to-point and point-to-multipoint communications over short range wireless communication technologies, such as ITS-G5, for vehicle-to-vehicle communication.

Also other solutions for geo-addressing have been specified, but none of them have been applied for Internet-wide geo-networking.

#### Geo-routing:

A significant number of geo-routing protocols are available, see e.g., [KaAl11] for a survey. These protocols can mainly be divided in two categories. The first category focuses on unicast routing, and the second covers broadcast routing. [ETSI-EN-302-636-4-1] specifies a sub-IP-routing protocol with unicast and broadcast forwarding schemes for multi-hop and ad hoc communication among vehicles and between vehicles and roadside station utilizing geographical positions.

[ETSI-EN-302-636-6-1] has standardized the transmission of IPv6 packets over ETSI GeoNetworking that can be used for the forwarding of IPv6 packets using the position of the destination node(s) and the positions of intermediate nodes for the routing decisions.

However, these geo-routing protocols are not designed for Internet-wide geo-networking.

## 1.2 Goal

Internet-wide geo-networking targets at IP-layer extensions that allow source nodes anywhere in the Internet to geo(broad/any)cast packets to all/any node(s) with geo-location awareness within an arbitrary, source-specified destination area.

## 1.3. Terminology

### On Board Unit (OBU)

a processing and communication feature that is located in a vehicle, which provides an application runtime environment, positioning, security and communications functions and interfaces to other vehicles including human machine interfaces. OBU is also known as OBE (On-Board Equipment).

### Road Side Unit (RSU)

equipment located along highways, at traffic intersections and other type of locations where timely communications with vehicles are needed. Each RSU includes DSRC (Direct Short Range Radio, e.g., IEEE 802.11p) radio, a positioning system and a router to route packets back through the infrastructure network. RSU is also known as RSE (Road Side Equipment)

### Vehicle-to-Vehicle (V2V)

(same as in [draft-ietf-mext-nemo-ro-automotive-req]): a generic communication mode in which data packets are exchanged between two vehicles, either directly or traversing multiple vehicles, without involving any node in the infrastructure.

### Vehicle-to-Infrastructure (V2I)

generic communication mode in which data packets sent by a vehicle traverse a communication infrastructure.

### Infrastructure-to-Vehicle (I2V)

generic communication mode in which data packets received by a vehicle traverse a communication infrastructure.

### Host vehicle

a vehicle that uses the ITS application.

### Traffic safety application

application that is primarily applied to decrease the probability of traffic accidents and the loss of life of the occupants of vehicles.

Geographically-scoped broadcast (or geocast), see [C2C-CC\_Manifesto]

forwarding mechanism that is used to transport data from a single node to all nodes within a target area that is specified by geographical positions, e.g. defined by a geographic region. The geographic region is determined by a geometric shape, such as circle and rectangle.

Geographical Unicast (or geounicast) see [C2C-CC\_Manifesto]

Forwarding mechanism that is used for unidirectional data transport from a single node (source) to a single node (destination) by means of direct communication or by multiple hops based on geographic specific addresses that include node identifier, geographical position, and time information.

Geographically-scoped anycast (or geoanycast), see [C2C-CC\_Manifesto]

forwarding mechanism that transports data from a single node to any of the nodes within a geographically area. Compared to geographically-scoped broadcast, with geographically-scoped anycast after a packet reaches one vehicle located in the specified geographic area, it stops being forwarded to other vehicles located in the same area.

#### 1.4. Organization of This Document

This document is organized as follows. Section 2 describes several Geo-networking use cases and scenarios. Section 3 describes the requirements that need to be fulfilled by the Internet-wide Geo-networking solution. The open design issues are discussed in Section 4. Section 5 describes possible solutions of realizing the Internet-wide Geo-networking solution. Section 6 describes the security considerations. The acknowledgement section is provided in Section 8.

## 2. Use cases and scenarios

### 2.1 Scenario

The scenario that is considered in this document for the support of Internet-wide geo-networking is shown in Figure 1. This scenario shows a source node, which can be located anywhere, and is interconnected with access routers via the Internet. The packets generated by the source are routed through the Internet using the typical destination address based routing up to the access routers. Geo-routing is then used to forward the packets towards the destination area where the recipients are located. In the destination area the packets are geo-broadcasted to all the recipients within the destination area.

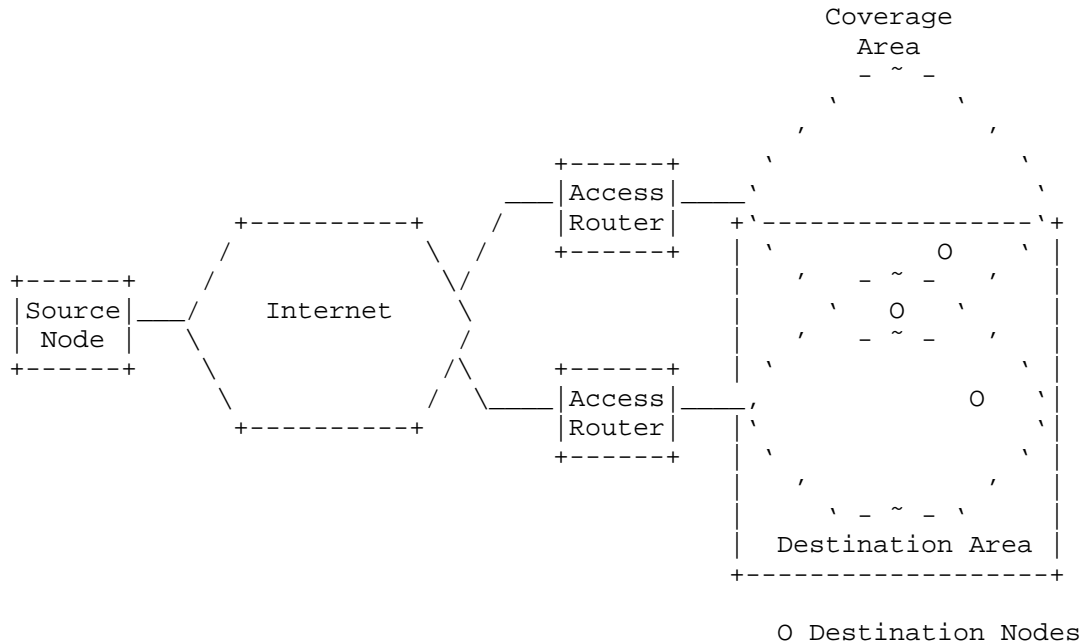


Figure 1: Internet-wide geo-networking scenario

## 2.2 Use cases

The use cases considered in this section are vehicular networking use cases. However, Internet-wide geo-networking can be applied to any use case that is similar to these vehicular use cases where source nodes anywhere in the Internet are able to geo(broad/any)cast packets to all/any node(s) with geo-location awareness within an arbitrary, source-specified destination area.

Vehicular networking can be considered as one of the most important enabling technologies needed to support various types of traffic applications, such as infotainment type of applications, traffic efficiency & management and traffic safety applications.

Traffic safety applications are those that are primarily applied to decrease the probability of traffic accidents and the loss of life of the occupants of vehicles. Note that VSC and VSC-A projects focus on vehicle-to-vehicle safety. Another project called CICAS-V (Cooperative Intersection Collision Avoidance Systems - Violation) discuss the traffic safety application over vehicle-to-infrastructure communication.

Traffic efficiency & management applications are focusing on improving the vehicle traffic flow, traffic coordination and traffic assistance. Moreover, traffic efficiency & management applications are focusing on providing updated local information, maps and in general messages of relevance limited in space and/or time.

Infotainment types of applications are the applications that are neither traffic safety applications nor traffic efficiency & management applications. Such applications are supported by e.g., media downloading use cases.

Such vehicular applications are defined by several initiatives:

- o the USA VSC (Vehicular Safety Communications) and VSC-A (VSC-Applications) projects.
- O the European Car-to-Car Communication Consortium (C2C-CC) [C2C-CC] and the ETSI TC ITS [ETSI TC ITS], [ETSI-TR-102-638] with the additional support of some EU funded research projects, such as SEVECOM [SEVECOM], SAFESPOT [SAFESPOT], CVIS [CVIS]. PREDRIVE-C2x [PREDRIVE-C2x], GEONET [GEONET].

The USA Vehicle Safety Communications (VSC) consortium, see [VSC], is supported among others by CAMP (Crash Avoidance Metrics Partnership). CAMP is a partnership that has been formed in 1995 by Ford Motor Company and General Motors Corporation. The objective of CAMP is to accelerate the implementation of crash avoidance countermeasures to improve traffic safety by investigating and developing new technologies. VSC has been realized in two phases.

The descriptions of the relevant traffic safety applications are taken from [draft-karagiannis-traffic-safety-requirements].

The first phase, denoted as VSC started in 2002 and ended in 2004. The second phase started in 2006 and ends in 2009. VSC focused and is focusing on traffic safety related applications. In 2006, The VSC 2 consortium in cooperation with USDOT initiated a three-year collaborative effort in the area of wireless-based safety applications under the Vehicle Safety Communications - Applications (VSC-A) project, see [VSC-A]. The VSC2 consortium consists of the following members; Mercedes-Benz, Ford, General Motors, Honda & Toyota. The main goal of this project is to develop and test communications-based vehicle safety systems to determine whether vehicle positioning in combination with the DSRC at 5.9 GHz can improve the autonomous vehicle-based safety systems and/or enable new communication-based safety applications.

The WAVE Short Message Protocol [IEEE 1609.3] was designed specifically to offer a more efficient (smaller size) alternative to TCP or UDP over IP, for 1-hop messages that require no routing.

The European Car-to-Car Communication Consortium (C2C-CC) is an industry consortium of car manufacturers and electronics suppliers that focuses on the definition of an European standard for vehicular communication protocols.

The European Telecommunications Standards Institute (ETSI) Technical Committee (TC) Intelligent Transport Systems (ITS) was established in October 2007 with the goal of developing and maintaining standards, specifications and other deliverables to support the development and the implementation of ITS service provision.



It is foreseen that ETSI ITS will be the reference standardization body of the future European ITS standards, and actually the C2C-CC provides recommendations to the ETSI TC ITS.

The following subsections describe use cases that can be implemented using either V2I or V2V. When V2V is applied, the use of Internet-wide Geo-networking solution is not required.

#### 2.2.1 Traffic safety use cases

In VSC, see [VSC] 34 vehicle application scenarios have been identified, evaluated and ranked. From this evaluation, a subset of eight significant near- and mid-term traffic safety applications have been selected: (1) cooperative forward collision warning, (2) curve speed warning, (3) pre-crash sensing, (4) traffic signal violation warning, (5) lane-change warning, (6) emergency electronic brake light, (7) left turn assistant, (8) stop sign movement assistant. A brief description of these applications is given below (for more details, see [VSC]):

- o Traffic signal violation warning: it informs and warns the driver to stop at a legally prescribed location in the situation that the traffic signal indicates a stop and it is estimated that the driver will be in violation.
- o Curve speed warning - Rollover Warning: aids the driver in negotiating speeds at appropriate curves.
- o Emergency Electronic Brake Lights: it is used to inform vehicles that a vehicle brakes hard. In particular in this situation a warning message is sent to the vehicles moving behind the vehicle that brakes hard.
- o Pre-crash sensing: it prepares the driver for an unavoidable and imminent collision.
- o Cooperative Forward Collision Warning: aids the driver in mitigating or avoiding collisions with the rear-end vehicles in the forward path of travel through driver notification or warnings of an unavoidable collision. This application does not attempt to control the vehicle to avoid an unavoidable collision.
- o Left Turn Assistant: it informs the driver about oncoming traffic in order to assist him in making a left turn at a signalized intersection without a phasing left turn arrow.
- o Lane Change Warning: it warns the driver if an intended lane change may cause a crash with a nearby moving vehicle.
- o Stop Sign Movement Assistance: it warns the driver that the vehicle is nearby an intersection, which will be passed after having stopped at a stop sign.

In the VSC-A project an additional investigation has been performed, on traffic safety applications that can be used in crash immitment scenarios, see [VSC-A]. The following 7 traffic safety applications have been selected for implementation in the VSC-A test bed.

- o Emergency Electronic Brake Light: is a traffic safety application that is the same as the Emergency Electronic Brake Light application defined in the VSC project, see above.
- o Forward Collision warning: is a traffic safety application that is the same as the Cooperative Forward Collision Warning application defined in the VSC project, see above.
- o Intersection Movement Assist: is a traffic is intended to warn the driver of a vehicle when it is not safe to enter an intersection due to high collision probability with other vehicles. It is similar to the Stop Sign Movement Assistance application defined in the VSC project, see above.
- o Blind Spot Warning & Lane Change Warning: it is similar to the Lane Change Warning application defined in the VSC project, see above. In the Blind Spot Warning application the driver of a host vehicle is informed that another vehicle is moving in an adjacent lane and that this vehicle is positioned in a blind spot zone of the host vehicle.
- o Do Not Pass Warning: this is an application that was not investigated in the VSC project. It is intended to warn the driver of a host vehicle during a passing maneuver attempt when a slower vehicle, ahead and in the same lane, cannot be safely passed using a passing zone which is occupied by vehicles with the opposite direction of travel. In addition, the application provides advisory information that is intended to inform the driver of the host vehicle that the passing zone is occupied when a passing maneuver is not being attempted.
- o Control Loss Warning: this is an application that was not investigated in the VSC project. It is intended to enable the driver of a host vehicle to generate and broadcast a control- loss event to surrounding vehicles. Upon receiving this information the surrounding vehicle determines the relevance of the event and provides a warning to the driver, if appropriate.

The Car to Car Communication Consortium specified a number of traffic safety use cases. The following three are considered as being the main traffic safety use cases, see [C2C-CC\_Manifesto]:

- o Cooperative Forward Collision Warning: this use case tries to provide assistance to the driver. Vehicles share (anonymously) information such as position, speed and direction. This enables the prediction of an imminent rear-end collision, by each vehicle monitoring the behavior of its own driver and the information of neighboring vehicles. If a potential risk is detected, the vehicle warns the driver.

This use case requires: the ability for all vehicles to share Information with each other over a distance of about 20 to 200 meters, accurate relative positioning of the vehicles, trust relationships among the vehicles and a reasonable market penetration (at least 10%).

- o Pre-Crash Sensing/Warning: this use case is similar to the previous one, but in this case the collision is identified as unavoidable, and then the involved vehicles exchange more precise information to optimize the usage of actuators such as airbags, seat belt pre-tensors, etc...  
This use case requires basically the same abilities that the previous one, restricting the needed communication range to 20 to 100 meters, and adding the requirement of a fast and reliable connection between the involved cars.
- o Hazardous Location V2V Notification: this use case is based on the share of information that relates to dangerous locations on the road, among vehicles, and also among vehicles and the road infrastructure.  
On one hand, vehicles may detect the dangerous locations from sensors in the vehicle or from events such as the actuation of the ESP (Electronic Stability Program).  
On the other hand, recipients of this information may use it to properly configure active safety systems and/or warn the driver.  
This use case requires: vehicles to trust other vehicles and roadside units, reasonable market penetration, the ability of vehicles to share information about a specific geographic location over multiple-hops and the ability to validate information propagated through multiple hops.

#### 2.2.2 Traffic efficiency and management use cases

Such applications are focusing on improving the vehicle traffic flow, traffic coordination and traffic assistance and provide updated local information, maps and in general, messages of relevance bounded in space and/or time. Two typical groups of this type of applications are speed management and co-operative navigation are two typical groups of this type of applications [ETSI-TR-102-638], [KaAl11].

##### o) Speed management:

Speed management applications aim to assist the driver to manage the speed of his/her vehicle for smooth driving and to avoid unnecessary stopping. Regulatory/contextual speed limit notification and green light optimal speed advisory are two examples of this type.

##### o) Co-operative navigation

This type of applications is used to increase the traffic efficiency by managing the navigation of vehicles through cooperation among vehicles and through cooperation between vehicles and road side units. Some examples of this type are traffic information and recommended itinerary provisioning, co-operative adaptive cruise control and platooning.

### 2.2.3 Infotainment Applications

Such applications are neither traffic safety applications nor traffic efficiency & management applications and are mainly supported by e.g., media downloading use cases, see [CVIS], [C2C-CC\_Manifesto], [ETSI-TR-102-638], [PREDRIVE-C2x], [KaA111]:

#### o) Co-operative local services

This type of applications focus on infotainment that can be obtained from locally based services such as point of interest notification, local electronic commerce and media downloading.

#### o) Global Internet services

In this type of applications the focus is on data that can be obtained from global Internet services. Typical examples are Communities services, which include insurance and financial services, fleet management and parking zone management, and ITS station life cycle, which focus on software and data updates.

## 3. Requirements

This section includes the requirements that need to be fulfilled by Internet geo-networking solutions and are based on [ETSI-EN-302-636-1].

### 3.1 Functionality requirements

This section describes the functionality requirements that need to be supported by the Internet-wide geo-networking solution.

#### 3.1.1 No changes to existing routing infrastructure

The Internet geo-networking solution **MUST NOT** impose any changes on the existing Internet-wide routing infrastructure.

#### 3.1.2 Minimal changes to the IP layer in source nodes

The changes on the IP layer used by the source nodes, i.e., the nodes that are making use of Internet-wide geo-networking **SHOULD** be minimized.

#### 3.1.3 Communication mode

The geocast, geounicast and geobroadcast communication modes **MUST** be supported by the Internet-wide geo-networking solution.

#### 3.1.4 Geo-addressing

Geographical information **MUST** be available in the addressing mechanism, such that packets can be forwarded to a target geographical area.

### 3.1.5 Internet-wide geo-routing

The Internet geo-networking solution MUST enable the forwarding of packets over multiple hops by using the position of the destination node(s) and the positions of intermediate nodes for the routing decisions. The Internet geo-routing solution SHOULD be able to operate without predefining the set of possible destination areas.

### 3.1.6 Internet-wide geo-networking and IPv6

The Internet geo-networking solution MUST support transparently the routing of IPv6 packets.

### 3.1.7 Data congestion control

Data congestion control functions SHOULD be supported in order to keep network load at an acceptable level and eliminate unnecessary duplicates of packets with limited control overhead.

### 3.1.8 Security and privacy

The Internet-wide geo-networking solution MUST support security objectives for all supported communication modes. Security objectives particularly include integrity, privacy and non-repudiation and SHOULD protect the network and transport layer protocol headers. In addition the Internet-wide geo-networking solution MUST also protect privacy, i.e. provide confidentiality to personal data such as relation between node identifier and location.

## 3.2 Performance requirements

This section describes the performance requirements that need to be supported by the Internet-wide geo-networking solution.

### 3.2.1 Low-latency communications

The Internet geo-networking solution SHOULD support low latency communications. This requirement mainly applies to traffic safety and traffic efficiency applications.

### 3.2.2 Reliable communications

The Internet geo-networking solution SHOULD support reliable communications with the highest reliability for traffic safety messages.

### 3.2.3 Low signaling, routing and packet forwarding overhead

The signaling, routing and packet forwarding overhead SHOULD be minimized.

#### 3.2.4 Priority support

The Internet geo-networking solution SHOULD support packets with different priorities with the highest priority for critical traffic safety packets.

#### 3.2.5 Scalability

The Internet geo-networking solution SHOULD be able to maintain its performance to acceptable levels even when it is applied to:

- o) global coverage with small geocast areas
- o) large traffic volumes (large flows)
- o) large number of active sources

### 4. Open Design Issues

This section describes the Internet wide geo-networking open design issues that can be addressed by the IETF.

#### 4.1 Geo-addressing in the wired Internet

The Standard Internet routers are not aware of geo-networking functionality. Therefore, the used addresses used must be regular addresses that route to / via the Access Router.

In particular, regarding unicast and multicast addresses the following issues can be identified.

- o) Using unicast addresses for all destination areas: does not scale well and packets are sent multiple times on the wireless interface
- o) Unicast addresses of relevant access routers: can be realized by using e.g., tunneling.
- o) Using multicast addresses to specify destination areas: A standard router should be able to route packets that are using predefined multicast addresses. This implies that an arbitrary, source-specified destination area cannot be coded this way. Alternatively, packets could be sent to a set of predefined areas which together include the source-specified destination area (further filtering at destination). However, consider that one multicast address per access point is needed. Consider also that each access point provides radio coverage to an area of 300m x 300m, which is approximately equal to  $10^5 \text{ m}^2$ . This would require that on a global scale we will need:  $5 * 10^{14} / 10^5 = 5 * 10^9$  multicast addresses to cover the earth, which will need to be maintained by the routing table of a router. This is far too many addresses that can be maintained by nowadays routers in their routing tables. A solution could be to define larger predefined areas. In this case however, many useless packet transmissions will need to be supported. It can be, therefore, deduced that the normal use of multicast addresses does not scale. Meaning that other solutions are needed, such (1) aggregation of multicast addresses into "larger" multicast addresses, (2) support of a routing hierarchy for geocasting.

#### 4.2 Exchanging destination area information

Until all routers in the Internet are geo-aware, or until a sufficient level of multicast address aggregation has been achieved to have a manageable total number of multicast addresses, we need a way for the source node to reach the (right) first geo-aware access router, e.g., RSU, (over the standard Internet). In addition to that the destination area specification needs to be exchanged at this first geo-aware access router. This can be achieved only if there is precise knowledge about the location of this destination node. The destination area specification has to be carried in the packet, using one of the following options:

- o) Specify this information in the IP destination address (tunneled in wired Internet)
- o) Use IP header extensions (not processed by standard Internet routers)
- o) Carry this information in the application layer header

#### 4.3 Lookup and translation of destination area to IP address

When a source needs to disseminate information in a destination area it should lookup and translate the destination area into a standard IPv6 address of the first geo-aware access router, e.g., RSU, which is routable in the standard Internet. The destination area can be specified by an application at the source, and does not have to coincide with known (predefined) areas, e.g., corresponding with the coverage area of an AR (e.g., RSU), or with the area covered by a predefined multicast address. This can be realized using location databases that provide the mapping between the destination area and the IPv6 address of the first geo-aware access router, e.g., RSU. Examples of such location databases are:

- o) Application specific location database
- o) DNS extended with location records and queries
- o) Table of known multicast addresses

#### 4.4 Updating the location database

The location databases that stores the mapping between the destination areas and the IPv6 addresses of the first geo-aware access router, e.g., RSU, need to be dynamically maintained and be up to date. Meaning that whenever new destination areas are identified or when the mapping between the stored destination areas and the associated IPv6 addresses change the location database needs to be updated.

#### 4.5 Support of Internet-wide geo-routing

By using Internet-wide geo-routing the data packets that are generated by source nodes placed anywhere in the Internet are able to be forwarded over multiple hops by using the position of the destination node(s) and the positions of intermediate nodes for the routing decisions.

Several geo-routing protocols have been defined by other standardization bodies, e.g., ETSI ITS, however, these geo-routing protocols are not designed for Internet-wide geo-networking.

## 5. Possible solutions

This section presents two possible ways of how the Intern-wide geo-networking solution can be designed. These solutions are the extended DNS and GeoServer. The extended DNS solution uses GPS coordinates to address geo-location. However, also other types of coordinates, such as the Galileo coordinates could be used for this purpose.

### 5.1 Extended DNS

One of the ingredients for Internet-wide geo-networking is a (distributed) database, able to resolve a geographical area to relevant IP addresses. Source nodes wishing to send geo-networking packets can then resolve the destination area of (a flow of) packets to a number of IP addresses, and send the packets to these destination addresses.

One direction for solutions is to extend the DNS system for this purpose, see [FiHell]. Rather than modifying the DNS protocol, requiring new top level domains or requiring changes in the routing behavior of today's Internet, this proposal is relying on the use DNS LOC (location) resource records defined in the [RFC1876]. Through the use of LOC records, geographical information about hosts, networks, and subnets can be stored in the DNS files. By performing then forward DNS lookups, geographical information about hosts or domains can be obtained. Current implementation of DNS, such as NSD, support LOC records to be inserted in the master file. This LOC record can then be used to specify the location of an end-host, the coverage area of an access router or access point, or the area in which the members of a multicast group are spread.

The key point in this proposal is the use of LOC records as primary key in the forward DNS lookup in order to return IP addresses associated with geographical locations. In other words, we introduce a new primary key into DNS besides the already existing ones (hostnames and IP addresses). The extended version of DNS extends the DNS server with capabilities to handle queries for an area within a domain. Upon receiving a query with such a specified area, the extended DNS server should return resource records for all names for which the area specified in a LOC record overlaps with the area specified in the query, and are also sub-domains of the domain specified in the query.

These addresses can then be used by the source as destination address for its geocast packets.

A possible format for a query is to replace the lowest-level subdomain by a location description:

```
("dlat [mlat [slat [mslat]]] "N"|"S" dlon [mlon [ slon [ mslon]]]
"E"|"W" alt["m"] size["m"])"
```



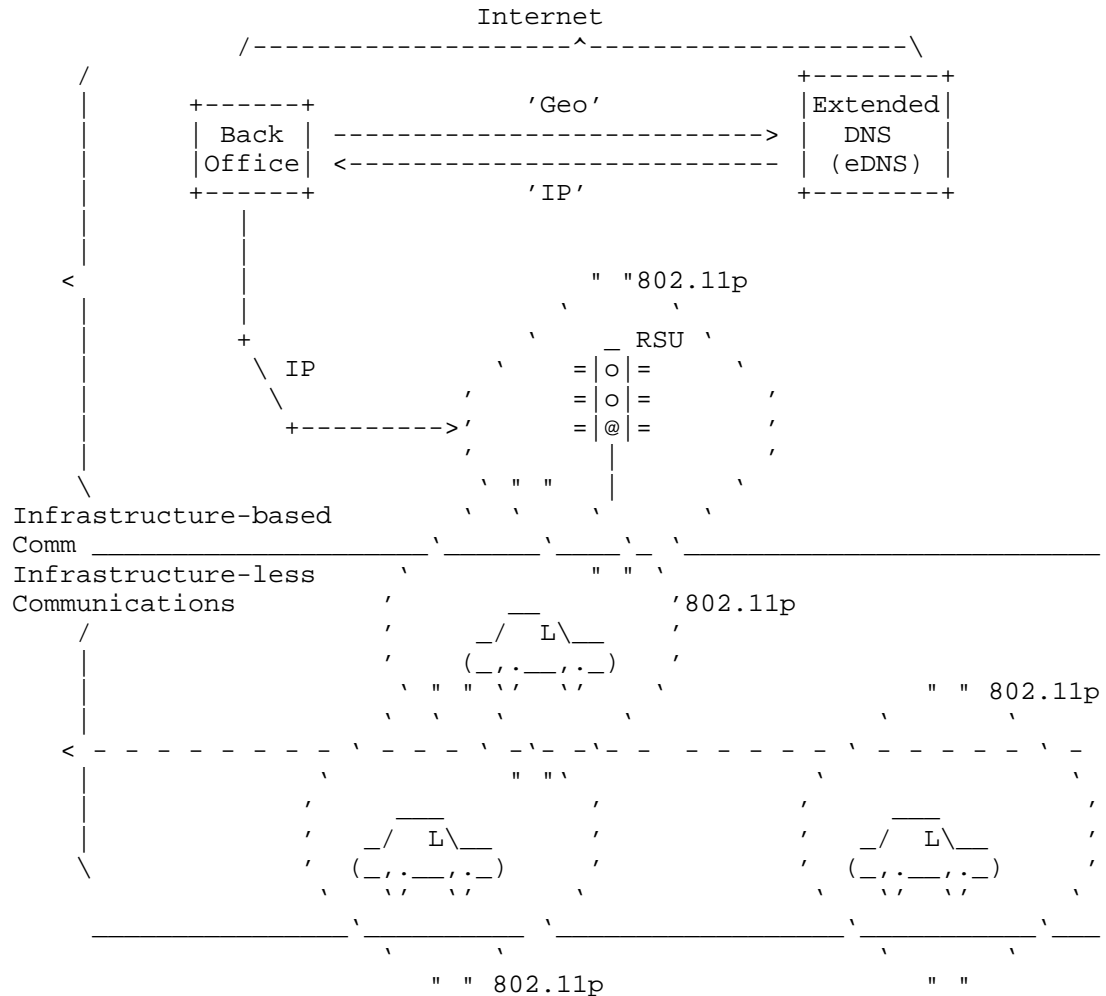


Figure 2: The extended DNS scenario

Here, dlat, mlat, slat and mslat specify the latitude of the center of the destination area in degree, minute, second, and millisecond, North ("N") or South ("S") respectively. Similarly, dlon, mlon, slon and mslon specify the longitude of the center of the destination area in degree, minute, second, and millisecond East ("E") or West ("W") respectively. Further, alt is the altitude in meters; size the (radius) size of the destination area in meters and domain specifies the domain to search in. Such an approach scopes geographical queries to a certain domain. In order to allow for name servers to delegate location queries to servers responsible for subdomains, for each delegated subdomain the latter servers must maintain a bounding box of their subdomains and make sure that also their parent server has its up-to-date bounding box. To this end, a new record type (Bounding Box) BND is used in this proposal.

Dynamic DNS update, as specified in [RFC2136] can be used to update BND and LOC records. Different levels of granularity are possible w.r.t. location representation in DNS.

If LOC records are stored for individual end-hosts, a significant load for dynamic updates of LOC records may be caused by mobile nodes. Alternatively, (stationary) access routers or access points may store a LOC record specifying their coverage area, and forward geocast packets to their coverage area. As a third alternative, multicast addresses may be used to represent areas, allowing host to subscribe to an area-specific multicast address ([GEONET]).

Note: if the destination location is somehow specified in the packet, additional packet filtering can be done by destination hosts, using their exact, current location.

#### 5.1.1 Dynamic IP address-to-geographical Address Resolution

A method similar to the name resolution (DNS) method can be provided. The user of this method may query a server in this way: it provides an IP address and it obtains in return the geographical coordinates of where the interface assigned that IP address is situated, or vice-versa. The method should also work for groups of IP addresses (prefixes) and three-dimensional regions.

#### 5.2 GeoServer

A design approach for Internet-wide geo-networking is to introduce a new network element that serves as a message reflector to facilitate the communication among vehicles. This network element functions as a server. It processes incoming messages from each vehicle, aggregates these messages when appropriate, and redistributes the messages to other vehicles. Since this server is typically responsible for a geographical area, it is termed GeoServer. The main functionality of a GeoServer is to provide vehicles with geographical-related services such as for traffic safety and traffic efficiency & management and infotainment-type of applications. The GeoServer is linked to an application server; both might be co-located. The application scenario is illustrated in Figure 3.

Applications may work vehicle or AppServer-triggered. In a typical vehicle-triggered scenario, the vehicle may detect road works or an obstacle by any means (local sensors, communication over other media or user input), triggers a message and sends it to the GeoServer.

The GeoServer can either forwards the messages directly to the destination area or involve the AppServer for information aggregation before forwarding the data. In the GeoServer-triggered scenario, the application server acts as originator of a message, based on data aggregation or information from a traffic management center or static configuration.

The scenario requires three main communication tasks [ITSWC2012], [WANG2013]: location updates, event reporting and geographical messaging (GeoMessaging). Location updates are periodically sent from the vehicle to the GeoServer. Their transmission can be triggered query-based, time-based, distance-based, grid-based (or a combination) (see [ITSWC2011]). If the driver or the vehicle detects an event, then the event will be reported to the GeoServer.

The GeoServer enables the distribution of messages to vehicles in a geographical area. The GeoServer also takes care of periodic re-transmission of the warning during the lifetime of the event, i.e. the repetition of the messages in order to keep the information alive in the destination area when vehicles start their journey or enter the area.

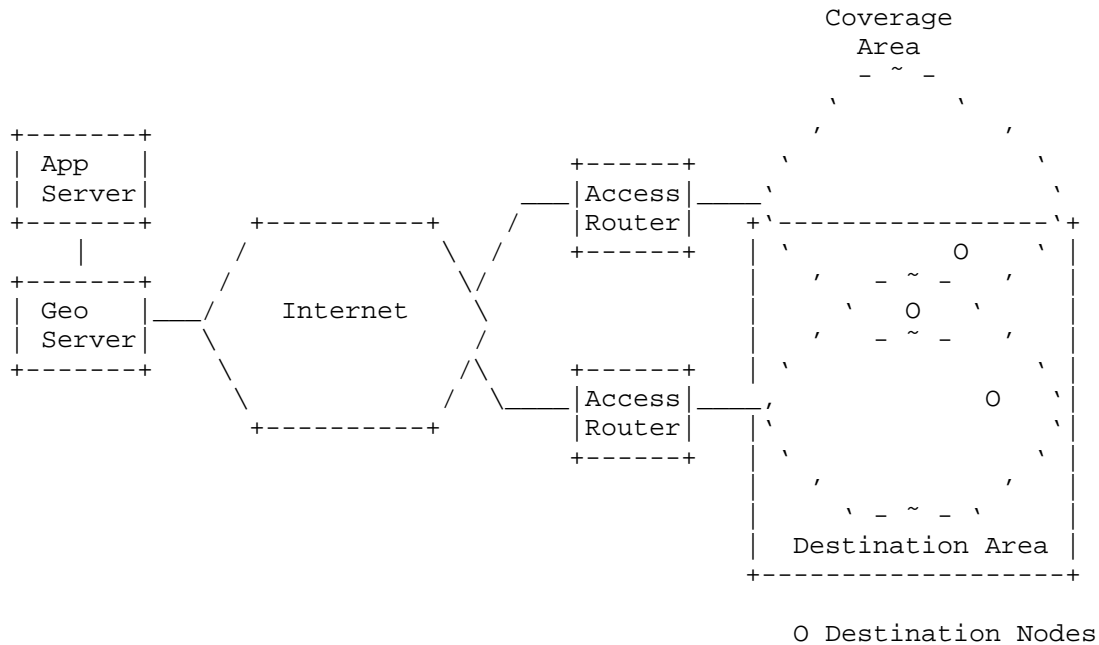


Figure 3: GeoServer scenario

## 6. Security Considerations

According to requirement 3.8.1, the Internet-wide geo-networking solution MUST support security objectives for all supported communication modes. Security objectives particularly include integrity, privacy and non-repudiation and SHOULD protect the network and transport layer protocol headers. In addition the Internet-wide geo-networking solution MUST also protect privacy, i.e. provide confidentiality to personal data such as node identifier and location.

## 7. IANA Considerations

No IANA considerations are considered in this document.

## 8. Acknowledgments

We would like to thank the members of the IETF ITS community for their comments and discussions. Furthermore, we would like to thank the authors of the Internet draft [draft-karagiannis-traffic-safety-requirements], G. Karagiannis, R. Wakikawa, J. Kenney, C. J. Bernardos and F. Kargl, since some parts of the traffic safety application descriptions are taken from the mentioned draft.

## 9. Normative References

## 10. Informative References

[C2C-CC] C2C-CC official website, <http://www.car-2-car.org/>, (visited in October 2009).

[C2C-CC\_MANIFESTO] Car to Car Communication Consortium, "Car to Car Communication Consortium Manifesto: Overview of the C2C-CC System", C2C-CC, version 1.1, 2007.

[CVIS] CVIS EU FP6 project website, [http://www.cvisproject.org](http://www.cvisproject.org/), (visited in October 2009).

[draft-ietf-mext-nemo-ro-automotive-req] Baldessari, R., Ernst, T., Festag, A., Lenardi, M., "Automotive industry requirements for NEMO Route Optimmmization", draft-ietf-mext-nemo-ro-automotive-req-02, (Work in progress), 2009.

[draft-karagiannis-traffic-safety-requirements] Karagiannis, G., Wakikawa, R., Kenney, J., Bernardos, C.J., Kargl, F., "Traffic safety applications requirements, IETF Internet draft (work in progress), draft-karagiannis-traffic-safety-requirements-02.txt, February 2010;

[ETSI TC ITS] ETSI official website, <http://www.etsi.org/>, (visited in October 2009).

[ETSI-TR-102-638] ETSI TR 102 638, "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Definition", ETSI specification TR 102 638, v.1.1.1, June 2009.

[ETSI-EN-302-636-1] ETSI TS 102 636-1 V1.1.1, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements", ETSI Specification ETSI TS 102 636-1 V1.1.1, March 2010

[ETSI-EN-302-636-4-1] ETSI TS 102 636-4-1, "Intelligent Transport Systems (ITS); Vehicular communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality", ETSI specification ETSI TS 102 636-4-1 V1.1.1, June 2011

[ETSI-EN-302-636-6-1] ETSI TS 102 636-6-1 V1.1.1, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols", ETSI specification ETSI TS 102 636-6-1 V1.1.1, March 2011

[FiHell] Fioreze, T. and Heijenk, G.J. (2011) Extending the Domain Name System (DNS) to Provide Geographical Addressing Towards Vehicular Ad-Hoc Networks (VANETs). In: 2011 IEEE Vehicular Networking Conference (VNC), 14 - 16 Nov 2011, Amsterdam, The Netherlands. pp. 70-77. IEEE. ISBN 978-1-4673-0047-6

[GEONET] GeoNet EU FP7 project website, <http://www.geonet-project.eu>, (visited in October 2009).

[IEEE 1609.3] IEEE Std P1609.3, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services", 2007.

[KaAll11] Karagiannis, G. Altintas, O., Ekici, E., Heijenk, G.J., Jarupan, B., Lin, K., Weil, T., "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions", IEEE Communications Surveys & Tutorials, 13 (4). pp. 584-616. ISSN 1553-877X, 2011.

[ITSWC2012] A. Festag, M. Wiecker, N. Zahariev: "Safety and Traffic Efficiency Applications for GeoMessaging over Cellular Networks", 19th ITS World Congress and Exhibition, Vienna, Austria, October 2012

[ITSWC2011] G. Jodlauk, R. Rembarz, Z. Xu: "An Optimized Grid-Based Geocasting Method for Cellular Mobile Networks", in Proc. 18th ITS World Congress, Orlando, USA, Oct. 2011

[WANG2013] S. Wang, L. Le, N. Zahariev, and K. K. Leung: "Centralized Rate Control Mechanism for Cellular-Based Vehicular Networks", accepted for IEEE Global Communications Conference GLOBECOM) 2013, Dec. 2013.

[PREDRIVE-C2x] Pre-Drive C2X EU FP7 project website, <http://www.pre-drive-c2x.eu>, (visited in October 2009).

[RFC2009] T. Imielinski and J. Navas, "GPS-Based Addressing and Routing", RFC 2009, November 1996.

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

[RFC1876] C. Davis, P. Vixie, T. Goodwin, I. Dickinson, "A Means for Expressing Location Information in the Domain Name System", RFC 1876, January 1996.

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[SAFESPOT] SAFESPOT EU FP6 project website, <http://www.safespot-eu.org>, (visited in October 2009).

[SEVECOM] SEVECOM EU FP6 project website, <http://www.sevecom.org>, (visited in October 2009).

[VSC] Vehicle Safety Communications Project, Final Report, DOT HS 810 591, April 2006.

[VSC-A] Vehicle Safety Communications - Applications (VSC-A) Project, Final Annual Report, DOT HS 811 073, January 2009.

[VSC-A\_1609.2] VSC-A presentation, "Security in VSC-A", slides presented at IEEE 1609 meeting on August 26 - 28, 2008, to be found via: [http://vii.path.berkeley.edu/1609\\_wave/aug08/presentations/VSCA-1609\\_080827.pdf](http://vii.path.berkeley.edu/1609_wave/aug08/presentations/VSCA-1609_080827.pdf)

#### 11. Authors' Address

Georgios Karagiannis  
University of Twente  
P.O. Box 217  
7500 AE Enschede,  
The Netherlands  
EMail: [g.karagiannis@utwente.nl](mailto:g.karagiannis@utwente.nl)

Geert Heijenk  
University of Twente  
P.O. Box 217  
7500 AE Enschede,  
The Netherlands  
EMail: [geert.heijenkg@utwente.nl](mailto:geert.heijenkg@utwente.nl)

Andreas Festag  
Technical University Dresden & NEC Laboratories Europe  
Germany  
Email: [andreas.festag@ifn.et.tu-dresden.de?;](mailto:andreas.festag@ifn.et.tu-dresden.de?;)

Alexandru Petrescu  
CEA  
Communicating Systems Laboratory, Point Courrier 173  
Palaiseau, F-91120  
France  
Phone: +33(0)169089223  
Email: [alexandru.petrescu@cea.fr](mailto:alexandru.petrescu@cea.fr)

Alison Chaiken  
Mentor Embedded Software Division  
46871 Bayside Parkway  
Fremont, CA 94538  
USA Email: [alison@she-devel.com](mailto:alison@she-devel.com)