

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 14, 2013

A. Petrescu
C. Janneteau
M. Boc
CEA
W. Klaudel
Renault
July 13, 2012

Scenarios and Requirements for IP in Intelligent Transportation Systems [draft-petrescu-its-scenarios-reqs-01.txt](#)

Abstract

This draft describes scenarios of vehicular communications that are considered pertinent to Intelligent Transportation Systems. In these scenarios, the necessity of using IP networking technologies and protocols is exposed.

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 January 14, 2013.

Copyright Notice

Copyright (c) 2012 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.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Scenarios	4
3.1.	Intra-Vehicular (V)	5
3.2.	Vehicle-to-Infrastructure (V2I)	7
3.3.	Vehicle-to-Vehicle (V2V)	7
3.4.	Vehicle-to-Vehicle-to-Infrastructure (V2V2I)	8
3.5.	Infrastructure Support	9
4.	Requirements	9
5.	Acknowledgements	10
6.	IANA Considerations	10
7.	Security Considerations	10
8.	References	10
8.1.	Normative References	10
8.2.	Informative References	10
Appendix A.	ChangeLog	10
	Authors' Addresses	11

1. Introduction

The field of vehicular communications is encompassing a large number of wired and wireless technologies. In particular, the breakthrough advancements in wide-area cellular telecommunications, the advent of inexpensive hardware, impressively high bandwidth and low-cost data subscription plans make possible new paradigms which put the vehicle at the center of a communications ecosystem. It can be observed that whereas only in the recent past linking vehicles in a robust manner to a fixed infrastructure represented endeavors available only to top categories, more and more middle category vehicles are announced to take advantage of data connectivity.

Communication protocols used in the fixed and mobile (terminal) Internet can be applied in the scenarios employing vehicles which communicate. A number of particular aspects make vehicular communications different, not least being the that mobility is the norm, rather than the exception. At the same time, several protocols developed at IETF are good candidates to form basis of further development of IP protocols for vehicular communications.

The use of Internet protocols in the vehicular scenarios may prove advantageous from several standpoints:

- o immediate availability of a large number of applications with an established customer base.
- o scalability: large numbers of inter-communicating vehicles can be accommodated across large distances.
- o accessing heterogeneous, mixed and multiple-standard link layer technologies.

The context of vehicular communications considers the use of several classes of Internet protocols for vehicular applications. One particular family of protocols is Mobile IP. Its salient features

characterize well several mobility aspects such as reachability at permanent addresses, seamless handovers and group mobility management. Earlier documents at IETF identified a number of scenarios and potential requirements for further work towards improving the Mobile IP protocols for a better adaptation in vehicular environments (see for example the draft titled "Automotive Industry Requirements for NEMO Route Optimization" edited in 2009 [[I-D.ietf-mext-nemo-ro-automotive-req](#)].)

A Vehicle-to-Infrastructure scenario (V2I) is a typical setting in which a vehicle uses a long-range wireless interface (cellular, satellite) to connect to a fixed infrastructure. As a separate

matter, scenarios of Vehicle-to-Vehicle (V2V) communications consider direct communications between vehicles, without, or with minimal, assistance from the infrastructure. In areas where wireless coverage is absent, Vehicle-to-Vehicle-to-Infrastructure communications are scenarios where covered vehicles offer access to non covered vehicles, in a multi-hop manner.

[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 [RFC 2119](#) [[RFC2119](#)].

[3.](#) Scenarios

Several scenarios of vehicular communications are described. We choose a set of illustrative scenarios, described next, and then followed by a list of high-level topologies which may be considered in terms of IP communications (V2V, V2I, etc.)

Scenario 1: A rented car (for instance a autolib as in Paris) is (will be) equipped with the car manufacturer network (sensors, CAN bus monitoring, infotainment), the car rental owner network (accidents detection, geolocation, etc.), the insurer network for behavior detection (speed, location, distance, etc.), and other stakeholders network such as highway company, municipality public service company (detection of free parking for instance), etc. Those

sub-networks may be interconnected together by one (mobile) router that ensures stable IP connectivity.

Scenario 2: Because of the wide variety of available wireless technologies, the vehicle should dispose of more than one wireless interface towards the infrastructure. In city center, Wi-Fi hotspots may provide Internet access at crossing roads stops. In the suburbs, Internet Access may only be available with LTE or 3G.

Scenario 3: An ambulance may need to stream video to the main hospital requesting minimum bandwidth during the whole operation. The mobile router should consider this requirement and prevent other less important traffic from the vehicle to have a negative impact on the stream.

Scenario 4: 802.11p may support the broadcast of alerts to vehicles. If the mobile router hosts a 802.11p interface, such alerts should be handled accordingly and routed to the right subnetworks.

Scenario 5: The vehicle may have a large amount of data to transfer to another vehicle but have only an Edge connection with the infrastructure. The transmission of the data may be delayed until a WiFi, 3G, or LTE connection becomes available.

Scenario 6: MANET routing between vehicles may be inefficient if the two communicating vehicles are not in vicinity. By using geographical information, the mobile router may know how to route data towards the destination efficiently.

Scenario 7: The insurer (generic term), the car manufacturer, and other stakeholder do not want to share their (private) data. The insurer do not want to let data coming from a network where the driver is active to have an influence on the reported behavioral information.

[3.1.](#) Intra-Vehicular (V)

Within one particular vehicle, an entire network may and will be deployed. This network is constituted of routers, hosts and other entities configured each with one or several IP addresses. Devices within vehicles are reachable to other vehicles and to Internet at

large.

One illustration of an intra-vehicular network is depicted in the next figure:

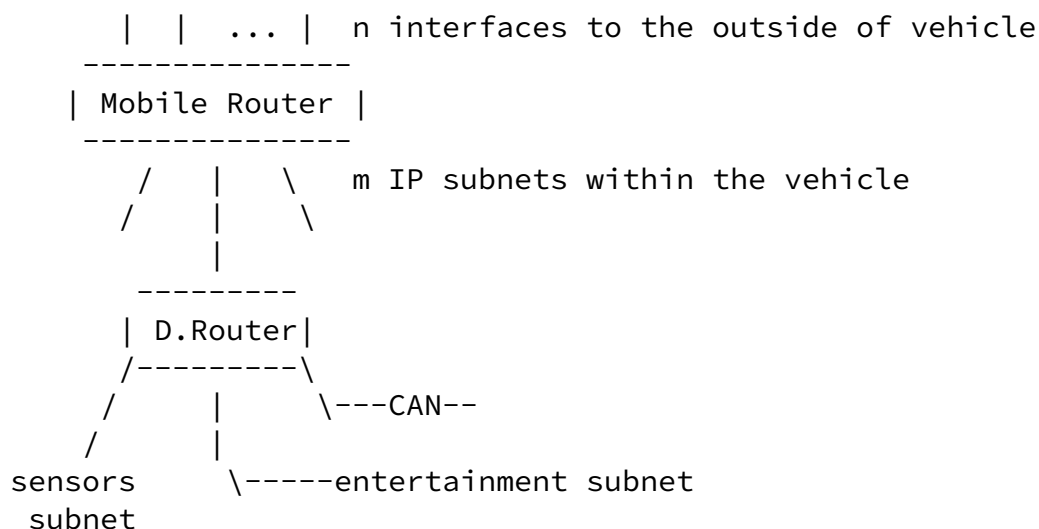


Figure 1: Topology for Vehicle-to-Infrastructure V2I Communications

This figure tries to illustrate the complexity of a intra-vehicular network. Even though the first deployments of intra-vehicular

networks were being constructed using a single IP subnet, the most recent advancements propose the use of multiple subnets within one vehicle.

In this example deployment, the moving vehicle holds on-board a Mobile Router. The MR is in charge of communicating to the outside world. It is equipped with one or several wireless interfaces towards the outside world (the world 'wireless' should be understood largely as 'without wires'; near-field contact-less communications are proposed for vehicular communications as well).

Within a vehicle, a dedicated router (D.Router) is in charge of subnets whose purpose is more application specific. The applications are typical vehicular, like the applications communicating on CAN (Car Area Network). This router may also be forwarding packets of

less importance (less constrained in terms of real time) which are related to entertainment (e.g. video stream to a screen built into a front seat).

Within one vehicle, there may thus be deployed several IP subnets, with traffic separated, dedicated to particular applications. The network within a vehicle may be formed by Routers, Switches and Hosts. It is also very probable that mobile devices carried by passengers connect to the vehicle's network, in a dynamic manner (users would expect an IP session ongoing on their personal terminal to continue working when getting into and outside of a vehicle).

The IP addressing scheme for deployment in a vehicle is not straightforward. The addresses should follow the pattern of use of applications: constrained applications may need to be separated from the entertainment applications right at the addressing level. For example, it may be needed to assign ULAs to some devices dedicated to some applications, Global addresses to other devices and link-local addresses on links where communication is local.

The topology of the intra-vehicular network may be interpreted as a multi-stage deployment; the multiplicity of stages is serving to protect against external attacks from the Internet to the inherent mechanisms of the vehicle dedicated CAN.

The Mobile Router deployed in a vehicle is in charge of communications to the outside world. One example application on the MR is the following: in case that two versions of the IP protocol need to be deployed and interoperable, then the MR may run a proxy HTTP function to allow IPv6 clients on-board to query IPv4 servers in the fixed Internet.

Some scenarios considered for vehicle communications need to take

into account that the vehicle is powered by very complex schemes which include power-saving mechanisms as well as eventual power distribution. It is important to consider mechanisms to wake-up the vehicle by messages coming from the outside network (IP Router Alert, or SMS of LTE).

[3.2.](#) Vehicle-to-Infrastructure (V2I)

This section describes the communication scenario in which one mobile vehicle connects to a fixed infrastructure.

Topology:

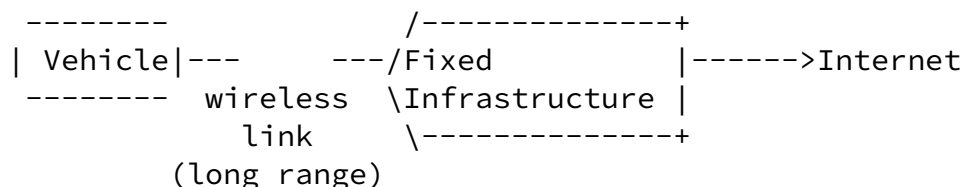


Figure 2: Topology for Vehicle-to-Infrastructure V2I Communications

In this figure, the wireless link used between the vehicle and the fixed infrastructure is of type 'long range' - typically a cellular link terminal-infrastructure, alternatively named a Wireless Metropolitan Area Network. A vehicle-to-infrastructure scenario considers often that the vehicle uses a cellular interface attached to an on-board router.

A different V2I scenario involves the use of short-range wireless links between the vehicle and the infrastructure. For example, it is possible to use interfaces of type IEEE 802.11b, or 802.11p to connect to a fixed infrastructure, which is itself connected to the Internet. The first IP hop between the vehicle and the infrastructure is using a short-range communication link.

[3.3.](#) Vehicle-to-Vehicle (V2V)

Topology:

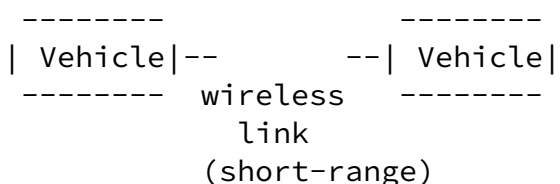


Figure 3: Topology for Vehicle-to-Vehicle V2V Communications

In this figure, the wireless link is of type short range. One

vehicle uses a interface of kind IEEE 802.11b, for example, and communicates to another vehicle using same kind of interface. Contrary to cellular links, the short-range wireless links are active in smaller areas (in terms of square meters of area). Typical examples of short-range wireless links are IEEE 802.11b, or IEEE 802.11p.

There are several possibilities of using short-range wireless between vehicles. In one scenario, the link uses the ad-hoc mode of operation between the egress interfaces of on-board vehicles. This works without the use of a fixed infrastructure. In another scenario, the link may use the 'managed' mode of operation between the egress interfaces of on-board vehicles; an Access Point is necessary for this to operate; the Access Point may be elected among one of the vehicles, or it may be deployed in a fixed manner along the road.

A distinctive factor may be constructed between the V2V and the V2I scenarios with respect to fixed infrastructure. At one extreme, the presence of fixed infrastructure is completely disallowed for V2V communications, and the short-range communications are completely disallowed between vehicles which perform V2I. Along the spectrum of scenarios, one scenario is possible where fixed infrastructure is deployed with the goal to support V2V communications but without offering Internet access; this is often the case with the scenarios currently described with IEEE 802.11p. At another extreme, V2I communications may be realized by building a complete infrastructure with moving vehicles.

[3.4.](#) Vehicle-to-Vehicle-to-Infrastructure (V2V2I)

Topology:

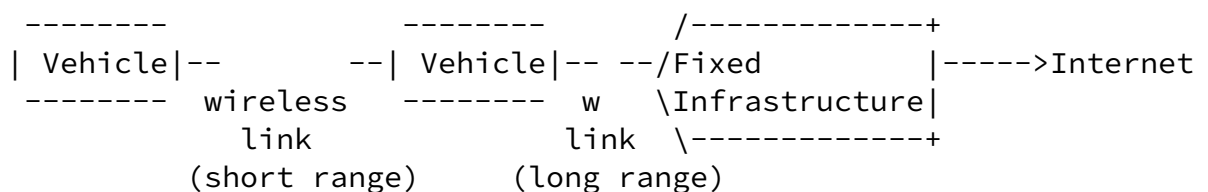


Figure 4: Topology for Vehicle-to-Vehicle-to-Infrastructure V2V2I Communications

In Vehicle-to-Vehicle-to-Infrastructure (V2V2I) communications a mix is realized between V2V communications and V2I communications. For example, a subnet is established between two vehicles in a V2V manner (e.g. using the ad-hoc mode between egress interfaces of on-board

routers of vehicles), and one of the vehicles is simultaneously connected to the fixed infrastructure (and to the Internet) using a V2I cellular link.

[3.5.](#) Infrastructure Support

[4.](#) Requirements

- o R0. IP addressing within each vehicle.
- o R1. IP addressing on the interface between vehicles.
- o R2. Sub-networks support: Mobile router support several sub-networks hosting stakeholder networks,
- o R3. Support of multiple interfaces: The vehicle (not restricted to the MR physically) should support several interfaces towards the infrastructure.
- o R4. Quality of Service: One stakeholder may request for a minimum bandwidth for its applications. QoS should ensure those minimums are taken into accounts.
- o R5. Broadcasted Alerts support: Along the highway, the MR may receive alerts about accident through 802.11p.
- o R6. Store, Carry and Forward: Improve communication efficiency by delaying transfer of information.
- o R7. Geographic information support: Efficient inter-vehicular routing may take advantage of geographic information (not restricted to geonetworking).
- o R8. Security: MR must prevent routing of packets between sub networks and ensure protection of those data within the vehicle.
- o R9. Continuity of ongoing sessions: it is desirable that ongoing sessions between one device within the vehicle and one device in the Internet is maintained ongoing during vehicle movements, and upon handovers between heterogeneous access points.
- o R10. Reachability at permanent home addresses: it is desirable that each device connected inside a vehicle to be reachable at a permanent fixed address, for all other IP devices deployed in the Internet.

- o R11. It is desirable that devices connected in one vehicle to be able to communicate directly to other devices in a vehicle nearby, even when the infrastructure is absent, and without using artificially long IP paths.

[5.](#) Acknowledgements

The authors would like to acknowledge colleagues who commented and thus helped improving this document.

[6.](#) IANA Considerations

No particular requirements to IANA.

[7.](#) Security Considerations

Connecting a vehicle to the Internet poses a number of significant problems related to security: new attacks are possible and the vehicle should be protected.

[8.](#) References

[8.1.](#) Normative References

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

[8.2.](#) Informative References

[I-D.ietf-mext-nemo-ro-automotive-req]
Baldessari, R., Ernst, T., Festag, A., and M. Lenardi,
"Automotive Industry Requirements for NEMO Route
Optimization", [draft-ietf-mext-nemo-ro-automotive-req-02](#)
(work in progress), January 2009.

[Appendix A](#). ChangeLog

The changes are listed in reverse chronological order, most recent changes appearing at the top of the list.

From [draft-petrescu-its-scenarios-reqs-00.txt](#) to -01:

Petrescu, et al.	Expires January 14, 2013	[Page 10]
------------------	--------------------------	-----------

Internet-Draft	Scenarios and Reqs for IP in ITS	July 2012
----------------	----------------------------------	-----------

- o Added requirements from R2 and up.
- o Better description of V2V, V2I terms. Introduction of the intra-vehicular scenario.
- o Enumeration of scenarios.
- o Expanded authorship.

From -- to [draft-petrescu-its-scenarios-reqs-00.txt](#):

- o First version of draft issued.

Authors' Addresses

Alexandru Petrescu
CEA
Communicating Systems Laboratory, Point Courier 173
Palaiseau, F-91120
France

Phone: +33(0)169089223
Email: alexandru.petrescu@cea.fr

Christophe Janneteau
CEA
Communicating Systems Laboratory, Point Courier 173
Palaiseau, F-91120
France

Phone: +33(0)169089182
Email: christophe.janneteau@cea.fr

Michael Mathias Boc
CEA, LIST
Communicating Systems Laboratory, Point Courier 173
Palaiseau, F-91120
France

Phone: +33 (0) 169083976
Email: michael.boc@cea.fr

Petrescu, et al.	Expires January 14, 2013	[Page 11]
------------------	--------------------------	-----------

Internet-Draft	Scenarios and Reqs for IP in ITS	July 2012
----------------	----------------------------------	-----------

Witold Klaudel
Renault
1 Av. du Golf
Guyancourt, F-78288
France

Phone: +33(0)176845680
Email: witold.klaudel@renault.com

