Individual Submission
Internet-Draft
Intended status: Informational
Expires: August 25, 2010

G. Karagiannis
University of Twente
R. Wakikawa
J. Kenney
Toyota ITC
C. J. Bernardos
Universidad Carlos III de Madrid
F. Kargl
University of Twente

February 25, 2010

Traffic safety applications requirements
draft-karagiannis-traffic-safety-requirements-02.txt

Abstract

This document describes a number of communication performance requirements that are imposed by traffic safety applications on a network layer. These traffic safety applications and requirements have been derived by the USA VSC (Vehicle Safety Communications)and VSC-A (VSC-Applications) projects and by the European Car to Car Communication Consortium (C2C-CC) and the ETSI TC ITS standardization body. The goal of this document is to stimulate the discussion on judging whether these performance requirements could or could not be supported (currently and in the future) by IP based network solutions.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

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, which are not specifically used to decrease the probability of traffic accidents and/or the loss of life of the occupants of vehicles.

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. This document describes a number of communication performance requirements that are imposed by traffic safety applications on a network layer.
These traffic safety applications and requirements have been derived by:

- the USA VSC (Vehicle Safety Communications) and VSC-A (VSC-Applications) projects.
- the European Car-to-Car Communication Consortium (C2C-CC) [C2C-CC] and the ETSI TC ITS [ETSI TC ITS], 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 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 goal of this document is to stimulate the discussion on judging whether these communication performance requirements could or could not be (currently and in the future) supported by IP based network solutions.

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.

2. Terminology

The following terms are used in this document :

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 radio, a positioning system and a router to route packets back through the infrastructure network. RSU is also know 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

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

infrastructure-to-vehicle

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

Host vehicle

a vehicle that at a certain moment in time uses the traffic safety 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 geographically target area. The scope is defined by the 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 C2C Communication 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 a packet is not forwarded inside of the geographic area when the packet has reached the area.

3. Overview of VSC and VSC-A traffic safety applications

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]):

- 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.

- Curve speed warning - Rollover Warning: aids the driver in negotiating and choosing appropriate curve speeds.

- 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.

- Pre-crash sensing: it prepares the driver for an unavoidable and imminent collision.

- 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.

- 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.

- Lane Change Warning: it warns the driver if an intended lane change may cause a crash with a nearby moving vehicle.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- Control Loss Warning: this is an application that was not investigated in the VSC project. It is intended to enable the host vehicle to autonomously 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.

4. Overview of the European Car to Car Communication Consortium traffic safety applications

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]:

- Cooperative Forward Collision Warning: this use case tries to provide assistance to the driver. Vehicles share 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%).

- 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.

- 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.

5. Overview of traffic safety communication performance requirements

5.1 VSC and VSCA Traffic safety communication performance requirements

The VSC consortium specified several performance communication requirements derived from the traffic safety applications, see Figure 1 and Figure 2 and [VSC]. The communication parameters used in Figure 1 and Figure 2 where specified in [VSC]. These are:

- Type of Communication: considers the (1) source-destination of the transmission (infrastructure-to-vehicle, vehicle-to-infrastructure, vehicle-to-vehicle), (2) direction of the transmission (one-way, two-way), and DSRC (IEEE 802.11p), see [DSRC], [IEEE 802.11p], communication, (3) source-reception of communication (point-to-point, point-to-multipoint). Note that the protocol suite that is used in the VSC and VSC-A projects is the WAVE protocol suite, which is composed by the combination of IEEE 1609 protocol suite, see [IEEE 1609.1], [IEEE 1609.2], [IEEE 1609.3], [IEEE 1609.4] and the IEEE 802.11p.

- Transmission Mode: Describes whether the transmission is triggered by an event (event-driven) or sent automatically at regular intervals (periodic)

- Minimum Frequency: defines the minimum rate at which a transmission should be repeated (e.g., 1 Hz).

- Allowable latency: defines the maximum duration of time allowable between when information is available for transmission (by the sender) and when it is received by the receiver (e.g., 100 msec).

- Data to be transmitted and/or received: describes the contents of the communication (e.g., vehicle location, speed and heading). Design considerations include whether or not vehicles make periodic broadcasts to identify their position on the roadway and how privacy is best maintained.

- Maximum required range of communications: defines the communication distance between two units (e.g., two vehicles) that is required to effectively support an application.

	Commun. Type	Trans. Mode	Min. Freq. (Hz)
Traffic Signal violation warning	* infrastructure -to-vehicle * one-way * point-to-multipoint	Periodic	~10
Curve Speed warning	* infrastructure -to-vehicle * one-way * point-to-multipoint	Periodic	~1
Emergency Electronic Brake lights	* vehicle-to-vehicle * one-way * point-to-multipoint	Event driven	~10
Pre-Crash Sensing	* vehicle-to-vehicle * Two-way * Point-to-point	Event driven	~50
Cooperative Forward Collision warning	* vehicle-to-vehicle * One-way * point-to-multipoint	Periodic	~10
Left Turn Assistant	* vehicle-to-infrastructure and infrastructure-to-vehicle * One-way * point-to-multipoint	Periodic	~10
Lane change warning	* vehicle-to-vehicle * One-way * point-to-multipoint	Periodic	~10

Stop Sign Movement Assistance	* vehicle-to-infrastructure and infrastructure-to-vehicle * One-way * point-to-multipoint	Periodic	~10	

Figure 1: Preliminary application scenario communication requirements (part A), from [VSC]

	Latency (msec)	Data to be transmitted and/or received	Max. Req'd comm.. range (m)
Traffic Signal violation warning	~100	* traffic signal status * Timing * Directionality * position of the traffic signal stopping location * Whether condition (if available) * Road surface type	~250
Curve Speed warning	~1000	* Curve location * Curve speed limits * Curvature * Bank * Road surface type	~200
Emergency Electronic Brake lights	~100	* Position * Heading * Velocity * Deceleration	~300

Pre-Crash Sensing	~20	* Vehicle type * Position * Velocity * Acceleration * Heading * Yaw rate	~50
Cooperative Forward Collision warning	~100	* Position * Velocity * Acceleration * Heading * Yaw rate	~150
Left Turn Assistant	~100	* Traffic signal status * Timing * Directionality * Road shape and intersection information * Vehicle position * Velocity * Heading	~300
Lane change warning	~100	* Position * Heading * Velocity * Acceleration * Turn Signal status	~150
Stop Sign Movement Assistance	~100	* Vehicle position * Velocity * Heading * Warning	~300

Figure 2: Preliminary application scenario communication requirements (part B), from [VSC]

From these requirements, see also Section 4.6 of [VSC], the most significant ones are:

- Message packet size: for all 8 scenarios, a message size of 200 to 500 bytes is needed.

- Maximum required range of communication: for all 8 scenarios, a maximum required range of communication of 50 to 300 meters is

needed.

- During 7 of the 8 scenarios, one-way, point to multipoint broadcast messages were used.
- During 1 of the 8 scenarios, Two-way, point to point messages
- During 6 or 7 of the 8 scenarios, the periodic transmission mode is used.
- During 1 or 2 scenarios, Event-driven transmission mode is used.
- During 6 of the 8 scenarios an allowable latency of 100 milliseconds is needed.
- During 1 of the 8 scenarios an allowable latency of 20 milliseconds is needed.
- During 1 of the 8 scenarios an allowable latency of 1 second is needed.

In addition to these communication performance requirements the VSC project derived the network constraints, depicted in Figure 3, see Appendix H of [VSC].

Constraint type	Constraint value
Aggregate bandwidth	6 Mb/s
Maximum received packets/sec	4000
Maximum allowable latency	100 ms
Maximum network latency	10 ms
Maximum packet size	200 bytes

Figure 3: Network constraints, from appendix H of [VSC]

The VSC-A project, relaxed some of these network constraints. In particular, the security related network constraints were derived, see Figure 4 and [VSC-A_1609.2]. In addition to these network security constraints, the VSC-A uses for the traffic safety application Do Not Pass Warning, a Maximum required range of communication, of 700 meters as a target.

Constraint type	Constraint value
Certificate size	< 300bytes
Authentication generations per second	10
Authentication verifications per second	1000
Time delay (authentication + + verification)	< 20ms
Over-air-bandwidth overhead introduced by security mechanisms (including certificates); certificates with each message	1,810 bytes/s

Figure 4: Network security constraints, from [VSC-A_1609.2]

5.2 C2C-CC and ETSI TC ITS traffic safety communication performance requirements

The performance requirements associated with the C2C-CC traffic safety applications are listed in the [ETSITR102638] ETSI specification.
These performance requirements are listed in Figures 5 and 6.

	Commun. Type	Trans. Mode	Min. Freq. (Hz)
Cooperative Forward Collision warning	* vehicle-to--vehicle * Broadcast * Geocast	Periodic	~10
Pre-Crash Sensing	* vehicle-to--vehicle * Unicast *	Periodic	~10

Hazardous location notification	* vehicle-to--vehicle * Broadcast * Geocast *	Time limited Periodic	~10	

Figure 5: Preliminary application scenario communication requirements (part A), from [ETSITR102638]

	Latency (msec)	Data to be transmitted and/or received	Max. Req'd comm.. range (m)
Cooperative Forward Collision warning	~100	* Position * Velocity * Acceleration * Heading * Yaw rate	20 to 200
Pre-Crash Sensing	~100	* Vehicle type * Position * Velocity * Acceleration * Heading * Yaw rate	20 to 100
Hazardous location notification		* events and * characteristics * of road	300 to 20000

Figure 6: Preliminary application scenario communication requirements (part B), from [ETSITR102638]

6. Discussion and conclusions

This document described a number of communication performance requirements that are imposed by traffic safety applications on a network layer.

These traffic safety applications and requirements have been derived by the USA VSC (Vehicle Safety Communications)and VSC-A (VSC-Applications) projects and by the European Car to Car Communication Consortium (C2C-CC) and the ETSI TC ITS standardization body. The goal of this document is to stimulate the discussion on judging whether these performance requirements could or could not be supported (currently and in the future) by IP based network solutions.

Comparing the traffic safety applications derived by European and by USA projects and consortia the following conclusions can be derived:

- the traffic safety applications and the use cases derived by European and USA projects and consortia are quite identical.

- the performance requirements derived by European and USA projects and consortia are similar. The main difference between the requirements derived by European projects and consortia and the ones derived by USA projects and consortia is that the European derived traffic safety applications consider multi-hop communication, i.e., geocasting forwarding, while the USA derived ones use only single hop broadcast solutions. The multi-hop communication requires geocast related forwarding mechanisms, such as: geographical unicast, geographically-scoped broadcast (also referred to as geo-broadcast) and geographically-scoped anycast (also known as geo-anycast). The C2C-CC currently assumes that IP is not suitable for safety and traffic efficiency applications (too much overhead, lack of geocast forwarding features, etc.). There are however initiatives, like the GeoNet project [GEONET] working on the design of mechanisms to integrate IP on top of the C2C-CC architecture.

It is however important to note that according to the VSC-A project the following points are important to be mentioned:

1. A general point is that the requirements of the target applications are intended to be somewhat representative of the expected requirements discussed in the VSC and VSC-A projects, but over time it is expected that new application ideas to come forward and the communication requirements may broaden as a result. For example, most applications today are designed to treat safety messages as self-contained such that the decision to warn a driver can be made purely based on the contents of the most recent message. In the future, we may see applications that require correlation of data over multiple messages from a given sender, or between multiple senders.

2. We now expect typical safety messages to be on the order of 300 to 400 bytes (including all layers of overhead), rather than the 200 bytes given as the upper limit cited in Appendix H of [VSC].It is expected that the security overhead will be between about 200 bytes and about 90 bytes, depending on whether a full certificate or a hashed certificate digest is included (the full certificate will be included at some reduced rate, probably 1 Hz to 3 Hz). There is also some additional, sub-rate safety information to communicate the sending vehicle's path history, its predicted path, and some of its raw GPS data. The latter is for purposes of computing precise relative positioning. Furthermore, it is expected that in some congested-channel scenarios we might expect to see more than 10 msec of network latency. This is exacerbated under the current multi-channel operation standard (IEEE 1609.4) [IEEE 1609.4], which calls for time to be divided into 50 msec intervals, with switching between a "control channel interval" and a "service channel interval", and then back again. Safety messages are only sent during the control channel interval. It is possible for a given message that is enqueued in one control channel interval to have to wait for the next one if it is still in backoff when the first interval ends, thus incurring up to 50 more msec of latency.

   That is highly undesirable however, and in any case we're hoping to change the standards to avoid this channel-switching paradigm for safety messages.

3. Furthermore, the requirement on "maximum allowable latency" is difficult to be interpreted when the communication takes place over an inherently unreliable medium. The fact is that the applications built on DSRC (Dedicated Short Range Communications) will have to be somewhat robust to lost broadcast messages. We often talk about the delay between successfully delivered messages, and it is expected that safety applications can generally tolerate at least 300 msec of such delay (i.e. two successive lost packets).

7. Security Considerations

As safety applications operate in dangerous situations, it is generally accepted that secure operations of vehicular networks are of paramount importance. Attackers must not be able to subvert operation of applications, e.g. to trigger false warnings or easily suppress real ones. Therefore, both US and European research activities on vehicular networks have worked on security solutions right from the start.

IEEE 1602.2 [IEEE 1609.2] provides an early solution taking into account many requirements. The European SeVeCom project [SEVECOM] has also published a design for a complete security subsystem for vehicular networks [SEVECOM-D2.1,SEVECOM-D2.1-APPA]. Furthermore, the PRECIOSA project is focusing dedicatedly on privacy-friendly design of Intelligent Transportation Systems, including vehicular networks [PRECIOSA].

Analyzing security requirements in vehicular networks, one can refer to classical security goals: confidentiality, integrity, and availability.

Confidentiality: One can note that for all safety applications, listed earlier, confidentiality is not a primary requirement. Information contained in safety-related messages should be received by all neighbors and can be considered public. So encryption of data is not a primary concern. If so, one could analyze the applicability of ESP headers for this purpose. However, note that there are privacy requirements (see below).

Integrity: It is of great import to ensure correctness of communicated data and to prevent attackers from sending forged or modified messages that could trigger application warnings or other reactions. One first step suggested by above mentioned solutions is to establish an identity management system that uses digital certificates and signatures by which receivers can verify that messages have been sent by valid vehicles. These solutions are very similar to AUTH headers of IPsec, however, size limitations suggest to use suitable cryptosystems like ECDSA. Restricting communication to valid vehicles is not sufficient, as those vehicles could still send false information (e.g. wrong position data). Additional mechanisms for data-consistency checking are proposed to detect and discard such information.

Availability: protecting the vehicular network from all kind of jamming and overloading attacks is important but beyond the scope of this paper, as security mechanisms usually address physical and datalink layer attacks. If multi-hop forwarding schemes like Geocast are used, protection from Denial-of-Service attacks targeting the network layer also need to be taken into consideration. Because of the broadcast nature of vehicular communication, mechanisms to protect e.g. from DDoS attacks in the Internet will likely be not portable.

Beyond those security requirements, it is also important to protect privacy of drivers. Foremost, it should be impossible to find the location of a vehicle or track its itinerary based on recorded

vehicular communications. Solutions generally apply pseudonymous identifiers to prevent a certain degree of unlinkability.

To prevent tracking vehicles, those identifiers need to be changed regularly (e.g., in each minute). This creates additional challenges to communication layers that can e.g. be addressed using MobileIP/NEMO technologies.

As discussed in Section 5, vehicular networks create a very challenging environment for a security system. Due to the broadcast and periodic nature of communication, vehicles might have to send some dozens of packets per second while at the same time receiving up to a few thousand packets per second from neighboring nodes. This corresponds to some dozens of signature generations per second and some thousands of signature (plus certificate) verifications per second. OBU hardware is not likely able to cope with this cryptographic load, so usage of dedicated crypto-coprocessors is likely. [SCHOCH-EFF-2010] outlines some other strategies to reduce cryptographic load.

Cryptographic payload in messages (signatures, certificates, metadata) must also not overload the communication medium. Based on information from [REF 1602.2] security payload will increase packet size by at least 181 bytes even when using space-efficient ECDSA. Assuming message sizes of 200 bytes, this almost doubles the size of a message. [SCHOCH-EFF-2010] also analyzes this and proposes mitigation strategies.

Using standard IPsec techniques (ESP/AUTH headers and X.509 certificates) would aggravate this problem. However, work on space-efficient IPsec variants, e.g. from the Wireless Sensor Network domain, could be considered for adoption in IP-based vehicular networks.

Overall, if one would adopt IP as a protocol for safety-related messages in vehicular-networks, one would need to take into account the issues raised above. This would require at least a modification of IPsec plus introduction of additional security mechanisms like pseudonymous identifiers and data-consistency checking. Note that for communication with backend infrastructures via RSUs, IPsec can be considered a mature solution to be applied.

8. IANA considerations

No IANA considerations apply to this document.

9. References

9.1. Normative References

9.2. 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/, (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 Optimmization", draft-ietf-mext-nemo-ro-automotive-req-02, (Work in progress), 2009.

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

[ETSITR102638] ETSI TR 102 638, "Intelligent Transport System (ITS); Vehicular Communications; Basic Set of Applications; Definition, ETSI specification TR 102 638, v.1.0.5, 2009

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

[IEEE 802.11p] IEEE P802.11p/D3.0, "Draft Amendment to Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks- Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications- Amendment 7: Wireless Access in Vehicular Environment", 2007.

[IEEE 1609.1] IEEE P1609.1, "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Resource Manager", 2006.

[IEEE 1609.2] IEEE P1609.2, "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) Security Services for Applications and Management Messages", 2006.

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

[IEEE 1609.4] IEEE P1609.4, "Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", 2006

[DSRC] Dedicated Short Range Communications (DSRC), USA ITS Standards advisory, http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm

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

[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

[SEVECOM-D2.1] A. Kung (ed.), "Security Architecture and Mechanisms for V2V / V2I", SeVeCom Deliverable 2.1 v3.0, February 2008.

[SEVECOM-D2.1-APPA] F. Kargl (ed.), "Baseline Security Specification", SeVeCom Deliverable 2.1 Appendix A v1.2, April 2009.

[PRECIOSA] PRECIOSA EU FP7 project website, http://www.preciosa-project.org/, (visited February 2010).

[SCHOCH-EFF-2010] E. Schoch, F. Kargl, "On the Efficiency of Secure Beaconing in VANETs", ACM Conference on Wireless Security (WiSec '10), 03/2010.

Authors' Addresses

Georgios Karagiannis
University of Twente
P.O. BOX 217
7500 AE Enschede
The Netherlands

Email: g.karagiannis@ewi.utwente.nl

Ryuji Wakikawa
TOYOTA InfoTechnology Center, U.S.A., Inc.
465 Bernardo Avenue
Mountain View, CA 94043
USA

Email: ryuji@jp.toyota-itc.com

John Kenney
TOYOTA InfoTechnology Center, U.S.A., Inc.
465 Bernardo Avenue
Mountain View, CA 94043
USA

Email: johnkenney@alumni.nd.edu

Carlos Jesus Bernardos
Universidad Carlos III de Madrid.
Avda de la Universidad, 30
E-28911 Leganes (Madrid)
Spain

Email: cjbc@it.uc3m.es

Frank Kargl
University of Twente
P.O. BOX 217
7500 AE Enschede
The Netherlands

Email: f.kargl@utwente.nl