Getting the message about road safety

Chris Wright
Emeritus Professor of Transsport Management
Middlesex University, London, UK
Email: christpherwright@btinternet.com

Zory Marantz
NYC College of Technology
Brooklyn, New York 11201, USA
Email: zory@ieee.org

Penina Orenstien
Seton Hall University
South Orange, NJ 07079, USA
E-mail: orenstpe@shu.edu

***Abstract*—This paper reviews a range of problems in the road transport field, and the potential role of the vehicular ad-hoc network systems (VANETs) in helping to solve them. In reality, the communications requirements vary widely from one application to the next, in terms of range, latency, and connectivity together with vehicle and roadside hardware. Based on the nature of the wireless channel, this presents some challenges for communication to security. The paper concludes with a summary of the current state of VANET technology and presents a summary of the challenges to be found in each approach.**

***Index Terms*—vehicular, networks, mobile, ad-hoc, VANET**

I. Introduction

Much of the early research into VANET applications was driven by German car manufacturers. The FleetNet project, which started in 2001, postulated a vision for car-to-car communications as a huge MANET running mainly internet applications. The outcome was a communications platform configured to perform multi-hop unicast packet-forwarding.

European manufacturers now think in terms of specialist non-internet applications having limited distance capability, with internet access handled by infrastructure or car-to-car communication [1]. By contrast in the USA, mobile vehicle communications was always conceived as communication between vehicles and roadside infrastructure [2], [3], and to this extent, the European vision has moved towards the US model.

Currently, the technology that would be used on a large scale VANET network for practical purposes is being rolled out in today's modern vehicles in the form of sensors [4], [5]. This is being done mostly for safety purposes in avoiding automobile accidents. The result of this first step is that we are currently on the way to properly implementing a complete intelligent transportation system (ITS).

None the less, with all the research that is being done, there is still a lack of consistency in the use of terminology that the authors feel are hindering the rate of development of the technology and its rapid deployment. In addition, we investigate the many approaches and systems that have been created in achieving the ITS vision.

The rest of this paper is organized as follows. Section II will present the various types of communications that are possible within a VANET environment. In Section III we resent the various ways that information my be processed within or external to the VANET. Section IV presents the various patterns of communication and how the information makes its way from point source to destination. Section V shows the security breaches that are possible within a VANET utilizing today's current technologies. Finally, the paper concludes with a summary of the current state of VANET technology and presents a summary of the challenges to be found in each approach.

II. Applications

VANET technology has many different applications besides for safety and entertainment. We mention them to allow us a focal point on the main uses of this technology to better choose the terminology that we'll propose for it.

A. Different types of application

Reference [6] distinguishes broadly between active safety and business/entertainment, and advocate a common approach bridging across both, as do [7] in their summary of the NoW project. Reference [8] further divides applications notionally into 4 groups:

1) Active safety
2) Public service
3) Improved driving
4) Business/entertainment

However, several authors distinguish between hazards that demand immediate action, as opposed to hazards of which the driver merely needs to be aware. For example, [9] propose different strategies for handling 'Safety of life' and 'Safety' messages, although in their case the distinction is confusing because the latter term seems to refer to routine beaconing messages that other authors would not regard as safety messages as such, but rather, general-purpose messages that support a wide range of applications. One might prefer the distinction made by [10] between 'safety-critical' applications such as an imminent collision, and 'safety-related' applications such as the maximum recommended speed on a curve.

Reference [8] graduates the hazard scale differently: a potential crash is treated as a sequence of stages leading up to impact, and different applications are classified according to the stage at which they are expected to intervene (Dangerous road features, Abnormal traffic and road conditions, Danger of collision, Crash imminent, Incident occurred). [11] distinguish between 'situations' and 'events', and analyse several factors that can influence the reliability of safety information and the effectiveness of the applications that may depend on it.

B. Individual safety applications

Car manufacturers have identified many scenarios, each reflecting a specific hazard or accident type. A total of 16 applications are listed by [11]. At the same time, the US CAMP project assessed 34 safety applications and mentioned several others. Eight were chosen for more detailed analysis as representing the likely range of communication demands made on a VANET system. [2] More recently, [10] highlight four basic areas concerning highway safety: Pre-crash sensing, Cooperative collision warning, Emergency electronic brake lights, and a Lane change supervisor.

Only the last three are common to all the publications cited. It appears that different research teams have different perceptions of which hazards are worth taking on, not least because applications are identified using a reductive approach, that is to say, hazards are broken down into narrowly defined categories, and applications are conceived to deal with them individually. Two possible exceptions are the ‘Virtual warning signs’ put forward by [12] and [8], and the Cooperative Intersection Collision Avoidance System (CICAS) featured in [13] together with its close cousin ‘Vehicle-to-vehicle anti-crash warning’ that appears in [11]. Hence there is no ITS-based equivalent of the safety belt and airbag that in the past have yielded appreciable casualty savings in relation to a wide range of hazards under different road and traffic conditions.

C. Non-safety applications

The CAMP project [2] report assessed eleven ‘non-safety’ applications and mentioned several others. [14] regard non-safety applications as the key to market penetration. Other interesting proposals featured in other publications are Traffic jam detection [15] and Detecting vacant parking spaces [3], [16]. Before information and delay sensitive information is sued for safety purposes on a VANET, it is these non-safety applications that will be the gateway tests to prepare VANETs for more processing and communication intensive applications such as cooperative collision mentioned in Section II-B.

D. Performance requirements

Wireless radio technology by itself does not make the road a safer place, but it does enable a range of applications that rely on communications. In particular, it can be used to measure separation between vehicles equipped with accurate GPS units, by exchanging location data. Crucially, it does not require unobstructed line of sight. A single wireless radio on-board unit (OBU) is expected to have a range of up to 1 km, compared with 120 m for 77 GHz radar [14], and the range can be extended via multi-hop forwarding over an ad hoc network.

The snag is that vehicular traffic density varies enormously between different sections of road, and between different times of day on any given section of road. Wireless nodes are sometimes densely packed, leading potentially to ‘broadcast storms’ and interference, while at the other extreme, vehicles may be too far apart to communicate at all [7]–[9], [17].

For safety applications, where events on the road can change in a fraction of a second, fast communication is vital. A maximum latency figure of 100 ms has been cited as a basic requirement [2], [18]. Non-safety applications are less demanding, but they do have specific requirements in economic, functional, performance and deployability terms [19].

Most of the research done in VANET works with off-the-shelf technology, specifically the IEEE 802.11 standard compliant devices. Since that technology was designed with a base station in mind, the protocols used for medium access result in various issues such as broadcast storms and hidden nodes which are active areas of research. [20]–[24] In that research there seems to be different set of terminologies compared to what the VANET society is using.

III. Information processing

Information processing is a major consideration when dealing with safety applications. The information obtained from the environment before, during, or after an incident needs to be processed and a decision made whether to send out any notifications of the incident. These notifications may be sent to the surrounding vehicles and processed by them explicitly, i.e. either braking or swerving to avoid collision. The other option is to have the nearest neighbors closest to the scene of the event pass on any information that may be relevant to the proper authorities, i.e. sending the information to emergency services to have arrive at the scene and/or insurance companies so that they can log the event properly.

A. In-network processing

While some authors see regular beaconing as an auxiliary function essential to hazard warning applications [25], others see it as an application in its own right. A receiving vehicle (call it vehicle B) keeps track of the messages by storing their contents in a location table [9], otherwise known as the ‘neighbour table’ [16]. From the contents of its table at any particular moment, vehicle B can infer the speeds and positions of the vehicles closest to it, in other words it can identify its nearest neighbours and track their movements. If vehicle B deduces that it is on a collision course with vehicle A, its on-board unit can be programmed to issue an audible warning. In addition, vehicle A can broadcast threshold information from its sensors, for example, such as ‘I am braking’, or ‘my ABS has activated,’ implying that the road surface might be slippery. To which Vehicle B would react accordingly. Such categories of information are richer but less objectively reliable. Accordingly, any vehicle B that receives the beacon can add information to it (‘my ABS has activated too’) before passing it on to its neighbors to notify them of an imminent accident about to occur. Irrelevant information is dropped. In this scenario, broadcast messages may be propagated from vehicle to vehicle over large distances, at the cost of some delay at each node, a process that has been described as single-hop with in-network processing [7], [19], [25]. It allows vehicles to collaborate by evaluating, sharing and filtering information in such a way as to improve reliability and at the same time, reduce the number of transmissions and hence the load on the wireless network.

However, information needs to be interpreted in context [6]. Suppose that vehicle A detects that vehicle B is approaching on a collision course. If their paths intersect at a 'give way' junction, it would be a good idea to warn the respective drivers what could happen. But if vehicle A is travelling along a freeway and vehicle B is crossing the freeway on an overpass, the interpretation changes completely. An ontological approach to organising this kind of information in a machine-readable manner so that it can be shared across a range of applications is proposed by [6].

The problem is expressed in a more direct way by [11]. The evaluation of incoming safety messages may be affected by circumstances, a phenomenon they call 'situation dependency'. Important sources of variation are (a) driver-related determinism (for example, if drivers respond to an icy road warning by driving more cautiously, they will collectively be less likely to confirm the presence of the hazard, being less liable to skid) and (b) configuration dependency, for example, condition of tyres. Judging the implications of (a) or (b) is difficult, especially in a continuously changing situation. Events that can be detected objectively and deterministically are the most promising candidates for VANET safety applications.

B. *Outcome and response*

The alternative responses generated by a VANET safety system can be classified into three groups [11]:

- Autonomous action, e.g. the system applies the vehicle brakes without reference to the driver
- A warning is issued to the driver that immediate action is required
- An 'awareness' alert is issued to the driver.

Interestingly, few consider application in the first category. Almost all applications work in the same way, by producing a computer-generated alert that is intended to spur the driver into doing something (or not doing it as the case may be).

The ergonomics of the driver interface must be considered. The question arises as to whether warning messages can be made sufficiently intelligible and timely to be acted on by the driver. [11] If only a small proportion of these applications appeared on the market, drivers could be inundated with alerts. Experience in the airline industry suggests that repetitive alerts are ignored, and in an emergency, they can be distracting and even counter-productive. [26]

IV. Patterns of communication

Road traffic can be regarded as a system in which not only drivers but also highway authorities and commercial agencies participate. Different VANET applications call for radio messages to be instigated by and delivered to different groups of participants in different ways: beaconing, unicasting, multicasting, etc. An example of different applications matched with different communication schemes appears in [8].

In particular, safety applications and non-safety applications tend to require quite distinct patterns of communication. Like any message sent over the internet, a non-safety message is composed of data packets [19] that are independently directed towards a target that could be several kilometres away, but the target has a known address. The data packets are routed and delivered without reference to their contents. In other words, non-safety messages are unicast multi-hop [7].

By contrast, safety messages are warnings delivered either to vehicles that happen to be nearby or vehicles in a defined geographical area. Here, it is the relative position of the 'target' vehicle that matters, not who is driving it. Several papers refer to the gathering of 'state information' with 'processing at network level', the information being 'consumed where it is generated' [19].

Awareness beaconing is a safety message that can be pictured as a short-range status message broadcast at frequent and regular intervals to any vehicle that happens to be in radio range: 'awareness beaconing' [7], [16]. The idea is for every equipped vehicle to bombard neighbouring vehicles with messages announcing its speed and position on the road. Such messages are not addressed to any particular vehicle and recipients do not acknowledge receipt, so the sender cannot be sure whether anyone is taking any notice.

Unicast and multicast, on the other hand, refer to messages intended for pre-identified targets, and they are used mainly for non-safety applications. These are the modes that would be used for downloading/uploading information from neighbors or utilizing the neighbors as relays for communication with an infrastructure backbone.

A. *Routing and forwarding*

In a conventional mobile ad-hoc network (MANET) message handling is organised around the data packet as the unit of communication. Similarly, non-safety communications are transmitted across a VANET in data packets [19]. Each packet has a specific destination, and is relayed to its destination intact irrespective of its content or meaning, an approach referred to as 'address-centric routing' [25], or alternatively 'Packet-Centred Forwarding' (PCF) [9].

By contrast, in 'data-centric routing' [25], also referred to as 'Information-Centric Forwarding (ICF)' [9], the forwarding process takes into account whatever information the data is intended to convey. At each node, the contents are evaluated and modified according to context where appropriate before any information is passed on. As a result, duplicate or redundant information is systematically discarded, which helps to reduce pressure on the wireless network and avoid potential 'broadcast storms' in congested city traffic.

B. *Store-and-forward*

Store and forward is an essential part of any VANET system because at any time, traffic density can fall below the threshold level necessary to sustain wireless connections [7], [8], [11]. In sparse traffic conditions, it is necessary for vehicles to hold and re-broadcast a hazard message at intervals to ensure that it is passed on. Such messages will need to be accompanied by 'Time of validity' and 'Area of validity' information [9] so they do not bounce around the road network indefinitely. Alternatively, roadside units (elsewhere referred to as 'message boxes') could be used to store and pass on messages to vehicles approaching remote locations, but [27] cite three reasons why store-and-forward might not be easy to implement in practice, the main reason being delays introduced by edge nodes that would have to process all the packets in the queue and then transmit them causing a bottleneck.

C. Interference, redundancy and overload

Although wireless radio signals do not require clear line of sight, they are subject to degradation from various sources. Since the VANET signals broadcast by neighbouring vehicles share the same frequency, on crowded roads they can interfere with one another sufficiently to prevent reception, a process referred to as packet 'collision' [1], [27]. In the case of a traffic jam on a 4-lane highway, where each car may in theory have 120 others within transmission range, it is possible to trigger a 'broadcast storm' in which the number of attempted transmissions arising from a single incident grows explosively to swamp the medium [27].

The likelihood of a broadcast storm increases with the size of road network. For a VANET system to be 'scalable', it is necessary to eliminate duplicate messages where possible, and this is partly the motivation for in-network processing: content must be 'evaluated at every node' [11], but of course there is then the trade-off with delay, as mentioned in Section IV-B

V. Security

To preserve privacy, a vehicle must not have a globally unique recognisable permanent identifier [11]. Among others, [7] have recommended encryption together with frequent interchange of pseudonyms which triggers substitution of addresses on all protocol layers in a node. The pseudonymity concept, certification authority, pseudonymous authentication, and signed beacons are all discussed in more detail by [18], who conclude that available encryption techniques push existing on-board processors to their limits. But by far the biggest threat to a VANET system is jamming of the GPS radio signals, whose signal is necessary to a VANET for knowing the locations of its members. This can be done with a device being made in China and sold for $30 [28].

VI. Conclusions

In a conventional network, the endpoints of a message are defined in advance. The originator and recipient(s) of unicast and multicast messages have fixed digital addresses, so that the communication layers in the protocol stack can handle dissemination independently of the contents of the message, but safety applications are different. The OBU has no idea who to talk to. It must first identify a target.

Awareness beaconing makes practical sense. For two vehicles to avoid a collision it is the relative trajectory of the vehicles that is important. There may be several vehicles in the vicinity. The most important ones are the vehicles immediately upstream and downstream, together with any other vehicles that happen to be on a collision course with yours. Of course, the threat changes from moment to moment, and the OBU must keep tally so it can identify the ones that matter most at any particular time.

Other safety messages are targeted towards vehicles further away, but the target is a geographical area rather than a set of addresses. News of an icy patch in the road is relevant to any vehicle that happens to be approaching the ice. Again, the emphasis is on position, but here interest focuses not on a single point but a section of road that may or may not happen to contain vehicles at the time. The intended destination, mode of forwarding and message content are all determined by the safety application software rather than the communications software. And if the message is determined by the application software, it follows that the applications software and communications software must interact somehow. The implication is that a cross-layered solution is necessary. This is typically observed by the custom pieces of software that are made for each vehicle/system independently.

Moreover, information is subject to uncertainty. The communications layer in a protocol stack understands nothing of road surface friction. Ice is diagnosed indirectly through the triggering of the ABS or stability enhancement system of a vehicle passing over it: the wheels lose some of their grip, and this shows up in the vehicle electronics. But the diagnosis is not very precise, and the reliability of a warning can be improved by combining information from several different vehicles.

This implies a degree of 'in-network processing'. When an OBU receives a message, it does not pass it on straight away, but sends it up to the application layer for evaluation, where it may be combined with the information contained in several other messages before they are all replaced with a single transmission. Not only does this improve reliability, it also reduces the communications load on the network, which can easily be overwhelmed in a 'broadcast storm' when the road is congested.

These complications may explain why in Europe, research has moved away from multi-hop IP towards the single-hop model that has dominated throughout in the US and Japan. But there are misgivings. [27] claim that single hop is not sufficiently reliable for safety-critical applications because (a) single-hop messages are not acknowledged and (b) a single-hop message can be destroyed in a 'collision'. In particular, single-hop does not work in heavy traffic, where an explosion of messages can easily overload the system.

To make real progress, strong government leadership is required, although the manufacturers do not seem to want it. [14] In principle at least, high market penetration is possible with stand-alone units installed under mandatory vehicle manufacturing regulations. Initially, like safety belts and airbags, they would be expensive. But with political will, a cooperative ITS system could reduce road casualties drastically by wrapping each vehicle in a very thick security blanket. Collisions would become impossible, because cars would behave like bees in a swarm, adjusting autonomously to each others' behaviour.

To sum up:

- Different 'safety' applications call for different kinds of

VANET. There is no single model that works under all road conditions.

- In conventional MANET technology, nodes have fixed, recognisable addresses. But in a VANET application such as collision avoidance, this is not the case. Targeting is not explicit.
- Almost all safety applications proposed so far refer to a narrowly-defined hazard scenarios. There are dozens of them. In each case, output is generated in the same way, by warning the driver of a threat. If only a small proportion of these applications ever made it onto the market, drivers could be inundated with warnings.
- On the other hand, the most ambitious applications rely on 95-100% market penetration, which will require considerable political will to bring about, yet manufacturers don't want government intervention.
- Retro-fitting is difficult, but not impossible. The question is not whether it can be done, but how much will it cost.
- Once installed, by far the biggest security threat to a VANET system is jamming of the radio signals.

References

[1] H. F§ğler, S. Schnaufer, M. Transier, and W. Effelsberg, "Vehicular ad-hoc networks: From vision to reality and back," in *4th Annual IEEE/IFIP Conference on Wireless On Demand Network Systems and Services (WONS)*, Obergurgl, Austria, January 2007.

[2] F. G. N. T. The CAMP Vehicle Safety Communications Consortium consisting of BMW, DaimlerChrysler and VW., "Vehicle safety communications project task 3 final report identify intelligent vehicle safety applications enabled by dsrc," U.S. Department of Transportation National Highway Traffic and Safety Administration, 400 Seventh Street, S.W. Washington, D.C. 20590, Tech. Rep. DOT HS 809 859, March 2005.

[3] Cable, "Free 4g and a freed up parking spot in nyc," *Cable*, vol. 38, no. 5, pp. 26 – 27, 2011. [Online]. Available: http://cable.poly.edu/sites/default/files/download/cable_winter_2011_web.pdf

[4] T. B. Mello. (2011, September) Collision-avoidance systems can save lives. Bankrate.com. [Online]. Available: http://www.bankrate.com/finance/auto/collision-avoidance-systems-can-save-lives.aspx

[5] D. Sedgwick. (2011, July) Study links low-speed collision-avoidance system to fewer accidents. [Online]. Available: http://www.autoweek.com/article/20110719/CARNEWS/110719886

[6] R. Eigner and G. Lutz, "Collision avoidance in vanets - an application for ontological context models," in *Proceedings of the 5th IEEE Workshop on Context Modeling and Reasoning*, Hong Kong, China, March 2008.

[7] A. Festag, G. Noecker, M. Strassberger, A. L§bke, B. Bochow, M. Torrent-Moreno, S. Schnaufer, R. Eigner, C. Catrinescu, and J. Kunisch, "Õnow Ð network on wheelsÕ: Project objectives, technology and achievements," in *Proceedings of 5rd International Workshop on Intelligent Transportation (WIT)*, Hamburg, Germany, March 2008, pp. pp. 211–216.

[8] E. Schoch, F. Kargl, T. Leinm§ller, and M. Weber, "Communication patterns in vanets," *IEEE Commun. Mag.*, vol. 46, pp. 119 – 125, November 2008.

[9] M. Torrent-Moreno, A. Festag, and H. Hartenstein, "System design for information dissemination in vanets," in *Proceedings of 3rd International Workshop on Intelligent Transportation(WIT)*, Hamburg, Germany, March 2006, pp. 27 – 33. [Online]. Available: http://www.network-on-wheels.de/downloads/WIT2006_InfoDissem_Torrent-Moreno_etal_wConfInfo.pdf

[10] A. K. K. Aboobaker and S. Wolthusen. (2010) Analysis of authentication protocols in vehicular networks. [Online]. Available: http://media.techtarget.com/searchSecurityUK/downloads/RHUL_Aboobaker_2010.pdf

[11] F. Dotzer, M. Strassberger, and T. Kosch, "Classification for traffic related inter-vehicle messaging," in *Proceedings 5th IEEE International Conference on ITS Telecommuncations*, June 2005.

[12] R. Eberhardt and C. Maihofer, "Virtual warning signs: a geocast enabled service for ad hoc networks," in *Proceedings of the 3rd Workshop on Applications and Services in Wireless Networks (ASWN)*, Bern Switzerland, 2003, pp. 135 – 147.

[13] C. Maihöfer, T. Leinmüller, and E. Schoch, "Abiding geocast: time–stable geocast for ad hoc networks," in *Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, ser. VANET '05. New York, NY, USA: ACM, 2005, pp. 20–29. [Online]. Available: http://doi.acm.org/10.1145/1080754.1080758

[14] K. Matheus, R. Morich, and A. L§bke, "Economic background of car-to-car communications," in *Informationssysteme f§r mobile Anwendungen (IMA 2004)*, October 2004. [Online]. Available: http://www.network-on-wheels.de/downloads/IMA2004_Matheus_Paper.pdf

[15] B. Kerner, S. Rehborn, and H. Palmer, "Using probe vehicle data to generate jam warning messages," *Traffic Engineering & Control*, vol. 45, no. 3, pp. 141 – 148, 2011.

[16] M. Torrent-Moreno, "Inter-vehicle communications: Assessing information dissemination under safety constraints," in *4th Annual IEEE/IFIP Conference on Wireless On Demand Network Systems and Services (WONS)*, Obergurgl, Austria, January 2007. [Online]. Available: www.network-on-wheels.de/downloads/TorrentMoreno_WONS07_AssessingInfoDissem.pdf

[17] H. Fubler, M. Torrent-moreno, M. Kruger, M. T. Rol, H. Hartenstein, and W. Effelsberg, "Studying vehicle movements on highways and their impact on ad-hoc connectivity," ACM SIGMOBILE Mobile Computing and Communications Review, Tech. Rep., 2005.

[18] P. Papadimitratos, G. Callandriello, J.-P. Hubaux, and A. Lioy, "Impact of vehicular communication security on transportation safety," in *IEEE MOVE*. IEEE Computer Society, 2008.

[19] R. Baldessari, A. Festag, and J. Abeille, "Nemo meets vanet: A deployability analysis of network mobility in vehicular communication," in *7th International Conference on ITS Telecommunications (ITST 2007)*, 2007, p. pages 375Ð380.

[20] M. K. Ajay Dureja, Aman Dureja, "Ieee 802.11 based mac improvements for manet," *IJCA Special Issue on MANETs*, no. 2, pp. 54–57, 2010, published by Foundation of Computer Science.

[21] H. Gossain, N. N, K. An, and D. P. Agrawal, "Supporting mac layer multicast in ieee 802.11 based manets: Issues and solutions," in *In 29th Annual IEEE International Conference on Local Computer Networks (LCNÕ04*, 2004, pp. 172–179.

[22] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," in *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking*, ser. MobiCom '99. New York, NY, USA: ACM, 1999, pp. 151–162. [Online]. Available: http://doi.acm.org/10.1145/313451.313525

[23] G. Korkmaz, E. Ekici, F. Özgüner, and U. Özgüner, "Urban multi-hop broadcast protocol for inter-vehicle communication systems," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, ser. VANET '04. New York, NY, USA: ACM, 2004, pp. 76–85. [Online]. Available: http://doi.acm.org/10.1145/1023875.1023887

[24] M. Sharma and G. Singh, "Evaluation of proactive, reactive and hybrid ad hoc routing protocol for ieee 802.11 mac and 802.11 dcf in vanet using qualnet," in *CCSEA*, e. a. D.C. Wyld, Ed. CS & IT-CSCP, 2011, p. 209Ð220.

[25] H. Fubler, M. Torrent-moreno, M. Transier, A. Festag, and H. Hartenstein, "Thoughts on a protocol architecture for vehicular ad-hoc networks," in *2nd Int. Workshop on Intelligent Transportation (WIT 2005)*, March 2005.

[26] (2010, June) Pilots in polish air disaster ignored warnings, transcripts reveal. Associated Press. [Online]. Available: http://www.guardian.co.uk/world/2010/jun/01/pilots-polish-ignored-warnings

[27] S. Schnaufer, H. Fuğler, M. Transier, and W. Effelsberg, "Vehicular ad-hoc networks: Single-hop broadcast is not enough," in *Proceedings of 3rd International Workshop on Intelligent Transportatio (WIT)*, Hamburg, Germany, March 2003, pp. 49 – 54.

[28] D. Hambling. (2011, March) Gps chaos: How a $30 box can jam your life. [Online]. Available: http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html