WIRELESS VEHICULAR COMMUNICATIONS FOR AUTOMATIC INCIDENT DETECTION AND RECOVERY

Joaquim Ferreira[1]**, José Fonseca**[2]**, Jorge Lopes**[3]

[1]*ESTGA/IT-Universiade de Aveiro,* [2]*DETI/IT-Universidade de Aveiro,* [3]*Brisa Inovação e Tecnologia*
{jjcf,jaf}@ua.pt, jlopes@brisa.pt

Abstract: Incident detection is the process by which an incident is brought to the attention of traffic operators in order to design and activate a response plan. To minimize the detection time is crucial to mitigate the incident severity for victims as well to reduce the risk of secondary crashes. Automated incident information dissemination and traffic conditions is useful to alert in-route drivers to decide alternative routes on unexpected traffic congestion and may be also used for the incident recovery process, namely to optimize the response plan including the "nearest" rescue teams, thereby shortening their response times.
Wireless vehicular communications, notably the emergent IEEE 802.11p protocol, is the enabling technology providing timely, dependable and secure properties that are essential for the devised target application. However, there are still some open issues with vehicular communications that require further research efforts.
This paper presents an overview of the state of the art in wireless vehicular communications and describes the field operational tests proposed within the scope of the upcoming FP7 project ICSI - Intelligent Cooperative Sensing for Improved traffic efficiency. Copyright Controlo 2012.

Keywords: vehicles, security, mobile radios, real-time communication, fault-tolerant systems

1. INTRODUCTION

Transportation systems are slowly but steadily evolving towards advanced information and communication technologies (ICT). Control theory plays an important role in Intelligent Transportation Systems (ITS), since there is closed loop interaction between vehicles/drivers and the transportation infrastructure, as enabled by cooperative V2X communications and cellular networks. While some of the enabling technologies are entering their mature phase, e.g., traffic flow sensors and wireless vehicular communications, based on the IEEE 802.11p protocol, there is still the need of a complete integrated solution that can take the most benefits from a real-time analysis of the data gathered and appropriate reaction on the transportation system.
Wireless vehicular communications (VCs) require trustworthy behaviour including both security and safety attributes, since they are planned to support safety warnings in specific situations such as hard braking, intersection violation or accidents.
At a first glance, VCs do not seem to require dependable behaviour, as they do not support "closed loop" applications, i.e., no automatic action is directly made based on data gathered from the environment. However, it is well known that its pervasive adoption increases the drivers' reliance upon its connectivity, raising the level of risk when the communication fails.
Safe, secure and timely vehicular wireless communications is a research topic deserving special attention due to several factors:
- Road safety is a current concern of the European Union (EU) due to the high number of victims of accidents and its correspondent social and economical impact. VCs are a support technology for ITS (Intelligent Transportation Systems) and are being used to increase road safety.
- The high number of EU projects addressing ITS has not explored issues concerning real-time and safety guarantees at the lower layers of communication technologies that will support VCs. In particular in what concerns the IEEE802.11p and IEEE1609.X standards.
- Although the 802.11p allocation spectrum has been released in the EU just in August 2008, most probably it will become pervasive in the

new domain and will migrate to other application domains. The dissemination potential of the IEEE 802.11p can enable the use of this technology in other applications such as home automation and assistive technologies.

The state-of-the-art shows that there have not been significant research results on the deployment of safe and secure applications (with real-time behaviour) on top of V2I (vehicle-to-infrastructure) and I2V (infrastructure-to-vehicle) communications. Also, these can play an important role in the period during which a large number of "legacy" vehicles will circulate, and before vehicle-to-vehicle (V2V) communications becomes pervasive.

The rest of the paper is organized as follows. Section 2 provides an overview of related work with a special emphasis on timeliness, dependability and security. Section 3 briefly presents the supporting technologies of vehicular communications, describing also the main achievements of the HEADWAY project. Section 4 presents a application scenario of vehicular communications for automatic incident detection and recovery. The paper is concluded in Section 5, with conclusions and some hints for future work.

2. OVERVIEW OF RELATED WORK

After almost a decade of R&D, vehicular communications for cooperative systems and its enabling technologies, mostly relying on IEEE 802.11p and IEEE 1609.1-4 family of standards (ETSI standards EN 202 663 and TS 102 867) are in their trial phase (Festag, 2011), as some major field operational tests are being carried out. Nevertheless, there are still some open problems concerning the timeliness, dependability and security of IEEE 802.11p based communications.

Since the presentation of IEEE 802.11p and 1609.1-4 protocols, valuable work has been done to assess the 802.11p MAC performance. Eichler (Eichler, 2007) made a performance evaluation of IEEE 802.11p and concluded that the protocol can prioritize messages, but in dense high load scenarios the throughput decreases and the delay increases significantly. In (Bilstrup, 2008), periodic V2V communication was assessed in terms of channel access delay and it was found that the CSMA mechanism is not suitable for time-critical communications. Gallardo *et al* (Gallardo *et al.*, 2009) studied the EDCA mechanism over the control channel of IEEE 802.11p, focusing on messages transmitted with different priorities. Performance of V2I communication was evaluated by Wang *et al.* (Wang *et al.*, 2008) and an adaptive back-off window adjusting scheme was proposed to enhance the non-safety critical traffic, but without guaranteeing fairness. Du *et al.* (Du *et al.*, 2010) presented a simulation study on the periodic heartbeat beacon frames broadcasting the status of each vehicle to assess the fairness deterioration of the heartbeat beacons. Simulation results have shown that, for high vehicle density, more beacon frames are lost and that

fairness cannot be guaranteed. Shie-Yuan *et al.* (Shie-Yuan *et al.*, 2008) highlighted the bandwidth waste in 802.11p and proposed fragment and best-fit schemes to reduce it, but without considering real-time requirements.

Several 802.11p MAC layer enhancement strategies have been proposed in literature. A polling-based MAC-layer protocol was proposed in (Choi, 2007) but the scheme does not guarantee fairness among vehicles since the polling is still based on CSMA. Ferreira *et al.* (Ferreira, 2008) proposed a slotted-based channel access scheme for re-broadcasting safety message on the control channel to meet the fairness and timing requirements of safety-critical traffic. A super-frame consisting of a collision-free phase and a contention-based phase was presented by Bohm and Jonsson (Bohm, 2008)(Bohm, 2008) to provide determinism for safety-critical traffic and a best-effort service for non-safety critical traffic. However this proposal is not compliant with the 802.11p standard.

At the security side, the work of Aijaz *et al.*, (Aijaz, 2006) and Plossl *et al.*, (Plossl, 2006) discussed general security issues such as attack models, security requirements and properties of IVC systems. Most of the current research (Raya, 2007)(Rahman, 2007) dealing with security and anonymity issues for VANETs propose the use of Public Key Infrastructure (PKI) based security schemes. Moreover, some research effort has also been made trying to gain knowledge about attackers (Leinmüller, 2008). For this purpose, some proposals for using honey pots in VCs have been proposed (Verendel, 2008). From Schütze (Schütze, 2011) and Festag *et al.* (Festag, 2011) it can be concluded that IEEE 1609.2 deployment is facing some impairments either due to high performance requirements of C2X security mechanisms and due the lack of consensus on which protocol layer the cryptographic protection should be applied. According to Schütze (Schütze, 2011) current COTS automotive processors cannot deliver the required performance, however, with specialized hardware the performance problems can be solved.

Timely and secure communications are important properties that cooperative systems must secure to attain dependable behaviour. However, additional mechanisms must be considered to improve the dependability of vehicular communications, namely its resilience to physical and MAC layer attacks and the replication of critical components. There is not much published work in these areas for the specific case of IEEE 802.11p, in contrast with the numerous publications on this area for the general case of IEEE 802.11 protocol. Some replication techniques used in wired networks can be adapted to the case of V2X communications. Silva *et al.* (Silva, 2009) proposed an integrated solution to replicate both the nodes and the communication channels. Although dual transceivers are already considered in the European standard EN 202 663, the challenge of an efficient multi-channel operation scheme still remains (Festag, 2011).

An analysis of related work shows the lack of a holistic approach accommodating a balanced harmonization among dependability, security and timeliness.

3. ENABLING TECHNOLOGIES

The IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE) defines an architecture and a standardized set of services and interfaces that collectively enable secure V2X wireless communications. These standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management and many others Additionally, the IEEE 1609 standards rely on IEEE 802.11p that specifies the extensions to IEEE 802.11 necessary to provide wireless communications in a vehicular environment.

IEEE 1609.3 defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange. It also defines Wave Short Messages (WSMs), providing an efficient WAVE-specific alternative to Internet Protocol version 6 (IPv6) that can be directly supported by applications. This standard also defines the Management Information Base (MIB) for the WAVE protocol stack.

Brisa, Instituto Superior de Engenharia de Lisboa and Instituto de Telecomunicações (Aveiro site), have been involved in the HEADWAY project, funded by Brisa (HEADWAY-Highway Environment ADvanced WArning sYstem). This project addresses two broad ranges of applications that will be provided in the near future in ITS: safety applications and comfort/infotainment applications.

Safety applications are meant to improve driving safety, meaning they can possibly reduce the number of accidents and consequently the number of injured persons. A brief list of safety services can be thought of: Emergency Electronic Brake Light, Lane Change Assistance, Post-crash Warnings, Sign Extension Services, Wrong Way Warning, Road Blocked Warning, Intersection Collision Warnings, etc.

Comfort and infotainment applications can provide some commodity to travelling car passengers while becoming a source of revenue to motorway and/or telecommunication operators: Tolling Services, Internet Access, Online Games, Location Based Services (e.g. traffic routing, tourist information), GPS Map Update, E-mail Servers, other multimedia services (e.g. instant messaging, movies and music downloads), Parking Spot Locator, etc.

In order to have full access to WAVE technology, an IEEE 802.11p transceiver is being designed and implemented from scratch. Most of the implementation efforts have been concentrated on the WSMP part of the WAVE standards and supporting 802.11p MAC and PHY layers. The IPv6 can be added later if required.

The approach used to implement the defined subset of the WAVE standard explores a mix of hardware (analogue components and multiple processors, both general purpose and specialized) and software to achieve the required performance and flexibility levels. Fig. 1 shows the global structure of our implementation, while Fig. 2 depicts the current 802.11p HEADWAY board. Please refer to Matos *et al.* (Matos, 2010) for further implementation details.

The HEADWAY IEEE 802.11p transceiver board will be integrated in a WAVE communication box together with a single board computer. This box can either be used as OBU or as RSU. Each communication box requires several interfaces (with both the vehicle devices and the user/driver), namely:
- Power supply
- Antenna connector
- OBD-II interface
- USB and/or Bluetooth interface

Driver interface may rely on a specific display with touch capabilities or through an Embedded or Portable Navigation Device (PND), using an USB interface, since a Bluetooth interface would provide the required level of determinism.
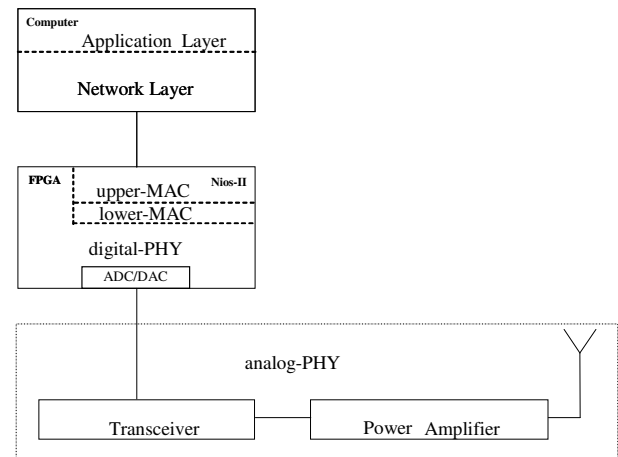

Fig. 1 – Block diagram of the current implementation. Source (Matos, 2010).

Fig. 2. HEADWAY IEEE 802.11p transceiver board.

3.1 Some open issues in vehicular communications

Strict real-time behaviour and safety guarantees are typically very difficult to attain in ad-hoc networks. However, we believe that the presence of the infrastructure, e.g. road-side units and the underlying cabled network, adds a degree of determinism that will very useful to enforce real-time and safety at the wireless end of the network.

The current trend of using wireless networks for embedded system interconnection places new challenges with respect to the predictability of the network infrastructure. However, in some extent, these problems are similar to those classically found in wired networks. Thus, one fundamental idea is to investigate how the methods used to enforce real-time operation in wired networks could be applied to the wireless world and to define a unified approach securing fundamental properties in both wired and wireless network infrastructures.

IEEE 802.11p inherits most of the characteristics from IEEE 802.11 including the medium access protocol (MAC), Carrier Sense Multiple Access (CSMA), where collisions may indefinitely occur. As a result, native IEEE 802.11p alone does not support real-time communications. The probability of collisions occurrence may be reduced if the load of the network is kept low, which is difficult to guarantee in vehicular communications, or if some extended MAC protocol restricts and controls the medium access to provide a deterministic behaviour.

Disturbances in the physical medium, caused by electromagnetic interference or malicious attacks, may compromise the temporal guarantees provided by the MAC level or even fully disrupt the communications capabilities of the nodes.

Since network availability is a fundamental design goal of VANETs, solutions to increase the network availability may include replicating critical RSU nodes according to a (possibly) semi-active replication mechanism.

Although dual transceivers are already considered in the European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band (EN 202 663), the challenge of an efficient multi-channel operation scheme still remains.

The IEEE 1609.2 standard for wireless security services in vehicular communications provides detailed documentation including the format of the security messages and the choice of the cryptosystem. IEEE 1609.2 uses anonymous public keys to sign and verify messages and use short-lived anonymous certificates to automatically revoke keys.

An open issue of the IEEE 1609.2 standard is the implementation of a cryptographic engine, that could either be software or hardware based. State of the art indicates that current automotive processors are not able to process as many cryptographic operations as required by operational scenarios.

An important design goal of security services is to achieve efficient resource utilization, knowing that such requirements are frequently in trade-off with each other, e.g. increased dependability may lead to decreased performance. In such cases, the proposed solutions have to accommodate a balanced harmonization among dependability, security, and real-time aspects. This means, that in a failure situation, when resources become scarce, one must prioritize certain applications/users/services over others to be able to retain the most critical applications.

Since most error scenarios and scheduling conditions are very difficult to be tested in a real environment, fault injectors, either software or hardware based, are a promising solution.

Some of these issues will be addressed in the upcoming FP7 project ICSI - Intelligent Cooperative Sensing for Improved traffic efficiency. Trustworthy vehicular communications will be tested in field operational tests, coordinated by Brisa, to deploy project technologies and solutions for the exploitation of project results, in the A5 highway, in the region of Lisbon.

4. AUTOMATIC INCIDENT DETECTION AND RECOVERY – FIELD OPERATIONAL TEST

Incident detection is the process by which an incident is brought to the attention of traffic operators in order to design and activate a response plan. To minimize the detection time is crucial to mitigate the incident severity for victims as well to reduce the risk of secondary crashes. Automated incident information dissemination and traffic conditions is useful to alert in-route drivers to decide alternative routes on unexpected traffic congestion and may be also used for the incident recovery process, namely to optimize the response plan including the "nearest" rescue teams, thereby shortening their response times.

The 25 km long inter-urban A5 motorway section between Lisbon and neighbouring Cascais in the West-coast of Portugal is an intensively used road corridor. In the morning rush hours, traffic in this highway heading to Lisbon typically experiences high levels of congestion, due to the high demand on the network, which acts as the main exogenous factor. A5 includes 14 intersections with 64 ramp connections. In the heaviest congestion area, ramps are located 300 meters apart. This configuration represents a major endogenous factor imposing additional strong pressure over the overall performance.

Average weekdays daily traffic for this highway reaches 65,000 vehicles and twice as much in the first 8 km stretch, towards the city of Lisbon. For the entire trip, daily commuters' experiences travel times from 12 minutes off peak, up to 60 minutes during the rush hour that goes from 7:30 to 9:30 AM.

The A5 highway is widely equipped with telematics systems for tolling and traffic management and control. Primarily, telematics installations on the roadway regarded toll collection systems for open tolling service, where tolls fees are levied at certain

points on the highway, once on the main carriageway and other at interchanges. Since 1991, the high acceptance of Via Verde – the nation-wide electronic toll collection service, based on dedicated short-range communications (DSCR), A5 toll plazas, located between kilometre 11 and 19, are fully equipped with such electronic toll collection (ETC) systems.

A5 is also covered with cameras and variable message signs controlled by the Brisa Operational Centre, where the accident recovery process is coordinated. Currently the accident detection is not automatic and relies in human operators to process these events.

4.1 Towards automatic accident detection and recovery in motorways

The impact of events on traffic conditions has not been effectively accounted, which results in inefficient guidance and management. A semi-automatic accident detection and recovery system involving the main stakeholders (motorway operator, police and emergency services) may contribute to more efficient guidance and management in parallel with increased safety. A fully automated accident detection and recovery system is out of the scope of ICSE project, since core algorithms and technologies need to be fully assessed in terms of safety and security prior to full deployment. However, the envisaged field operational test is an important step towards this ultimate goal.

Beyond unforeseen congestion caused by incidents, there is an additional serious problem: the risk of secondary crashes, those that occur at the end of the queue as high-speed traffic approaches an unexpected stopped or slow-moving backup. Data collected from Brisa's highway network from 2008 to 2011 accounted for a total of 15521 accidents, of which 438 (2.8%) have been directly related with previous incidents. Fig. 3 shows the distribution of previous causes for serious accidents collected. Moreover, about 11% of the 10,078 minor accidents (without injuries or serious damages to vehicles or infrastructures) during the same time period were related with previous incidents. In this context, one objective of this operational test is to assess the impact of semi-automatic accident detection and recovery in decreasing the number of secondary crashes.
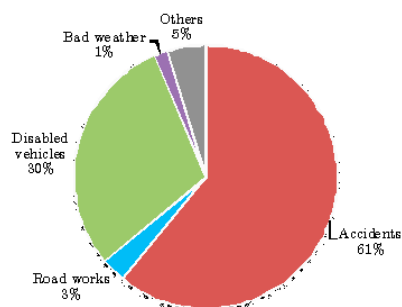

Fig. 3. Causes of secondary accidents in Brisa network. Source (Lopes, 2012).

We plan to cover A5 highway with full V2X communications and equip some probe vehicles with on-board units. The exact number of OBUs will depend on their market price at deployment time, with an estimated minimum number of 30 OBUs. The backhauling communication infrastructure will also be adapted according to the ICSI' project requirements.

Actual raw data will be collected for further analysis purposes and detailed validation of system

5. CONCLUSIONS AND FUTURE WORK

This paper presented an overview of the state of the art in wireless vehicular communications, identifying some open problems, and describes the field operational tests proposed within the scope of the upcoming FP7 project ICSI - Intelligent Cooperative Sensing for Improved traffic efficiency. These field operational tests present both technical and management challenges and will contribute to validate the achievements of the research project.

The paper has also presented the current status of the HEADWAY project and has briefly described the IEEE 802.11p transceiver board designed by the HEADWAY research team.

Plans for future work include the implementation of an enhanced 802.11p transceiver with simultaneous multi-channel operation and increased resilience to physical and MAC layer attacks. In parallel, a real-time MAC protocol and mechanisms to support replication and enforcement of fail-silent failure mode of critical nodes will also be developed. A fundamental design goal of providing these enhanced properties at the MAC level is to establish a solid foundation to simplify the design of the entire real-time wireless protocol stack.

Strict real-time behaviour and safety guarantees are typically difficult to achieve in ad-hoc networks. However, the presence of road-side units adds a degree of determinism that will very useful to attain real-time, safety and security. RSUs should be connected together with a deterministic network (e.g., TTEthernet, EtherCAT, Profinet or FTT-SE), capable of providing traffic isolation between real- and non-real- time traffic. The RSUs could then coordinate the OBUs access to the control channel of IEEE802.11p, possibly using a master- slave approach. In this scope, another ST objective is the holistic end-to-end analysis of both V2X and backhauling communications in terms of real-time and dependability

REFERENCES

Aijaz A., B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh and T. Leinmuller, "Attacks on Inter Vehicle Communication Systems - an Analysis", 3rd International Workshop on Intelligent Transportation (WIT 2006), March, 2006.

Bilstrup, K., Uhlemann E., Strom E.G. and Bilstrup U, "Evaluation of the IEEE 802.11p MAC Method for Vehicle-to-Vehicle Communication," IEEE VTC Fall 2008, 21-24 Sept. 2008, pp. 1-5.

Bohm, A., and Jonsson M., "Position-Based Data Traffic Prioritization in Safety- Critical, Real-Time Vehicle-to-Infrastructure Communication," IEEE Int. Conf. on Communications (ICC) Workshops, June 2009, pp. 1-6.

Bohm, A., and Jonsson M., "Supporting real-time data traffic in safety-critical vehicle-to-infrastructure communication," IEEE Int. Conf. on Local Computer Networks (LCN), October 2008, pp. 614-621.

Choi, N., Sungjoon Choi, Yongho Seok, Taekyoung Kwon, Yanghee Choi, "A Solicitation-based IEEE 802.11p MAC Protocol for Roadside to Vehicular Networks," Mobile Networking for Vehicular Environments, May 2007, pp. 91- 96.

Du, Y., Lin Zhang, Yufei Feng, Zhanyang Ren, Zi Wang , "Performance analysis and enhancement of IEEE 802.11p/1609 protocol family in vehicular environments," Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on , vol., no., pp.1085-1090, 19-22 Sept. 2010.

Eichler, S., "Performance Evaluation of the IEEE 802.11p WAVE Communication Standard", IEEE 66th Vehicular Technology Conference, Sept. 30 – Oct. 3 2007, pp. 2199-2203.

Ferreira, N., Fonseca J.A., and Gomes J.S., "On the adequacy of 802.11p MAC protocols to support safety services in ITS," IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA), September 2008, pp. 1189- 1192.

Festag, A.; Long, L.; Goleva, M., Field Operational Tests for Cooperative Systems: A Tussle between Research, Standardization and Deployment, Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, 2011, pp 73-78.

Gallardo, J.R., Makrakis D. and Mouftah H.T., "Performance Analysis of the EDCA Medium Access Mechanism over the Control Channel of an IEEE 802.11p WAVE Vehicular Network," IEEE Int. Conf. on Communications (ICC) 2009, June 2009, pp. 1-6.

Leinmüller, T., Robert K. Schmidt, Elmar Schoch, Albert Held, and Günter Schäfer, "Modeling Roadside Attacker Behavior in VANETs", Proceedings of the 3rd IEEE Workshop on Automotive Networking and Applications (AutoNet 2008), New Orleans, LA, USA, December 4, 2008.

Lopes, J.; "Traffic Prediction for Unplanned Events on Motorways"; Doctoral Thesis; Instituto Superior Técnico – Technical University of Lisbon; Portugal; 2012

Matos, J. N.; Oliveira, A.O.; Meireles, T.; Ferreira, N. F.; P.M. Mar; D. C. Carona; Serrador, A.;"Emergent Vehicular Communications: Applications, Standards and Implementation", Proc URSI Seminar of the Portuguese Committee, Lisboa, Portugal, Vol. 1, pp. 1 - 1, September, 2010.

Plossl, K., T. Nowey and C. Mletzko. "Towards a Security Architecture for Vehicular Ad Hoc Networks". The 1st International Conference on Availability, Reliability and Security (ARES2006), pp. 374 -381, April, 2006.

Rahman, S. U., and U. Hengartner. "Secure Crash Reporting in Vehicular Ad hoc Networks". In Proceedings of the 3rd International Conference on Security and Networks". In Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm2007), Nice, France, September, 2007.

Raya, M. and J. P. Hubaux. "Securing Vehicular Ad Hoc Networks". Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, pp. 39 - 68, 2007.

Schütze, T., Automotive Security: Cryptography for Car2X Communication, Embedded World Conference, 2011, Germany.

Shie-Yuan, W., Hsi-Lu Chao, Kuang-Che Liu, Ting-Wei He, Chih-Che Lin, and Chih-Liang Chou, "Evaluating and improving the tcp/udp performances of IEEE 802.11(p)/1609 networks," Proceedings of IEEE Symposium on Computers and Communications, July 2008, pp. 163-168.

Silva, V., Paulo Bartolomeu, Joaquim Ferreira, José Fonseca. "Assessment of multi-bus fault-tolerant communications", Proceedings of the 7th IEEE International Conference on Industrial Informatics 24-26th June 2009, Cardiff, Wales.

Verendel, V., Nilsson, D.K., Larson, U.E., Jonsson, E., "An Approach to using Honeypots in In-Vehicle Networks," Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th , vol., no., pp.1-5, 21-24 Sept. 2008.

Wang, Y., Ahmed A., Krishnamachari B. and Psounis K., "IEEE 802.11p performance evaluation and protocol enhancement," IEEE Int. Conf. on Vehicular Electronics and Safety (ICVES) 2008, 22-24 Spet. 2008, pp. 317-322.