Car-to-Car Communication

Stephan Eichler[#], Christoph Schroth[§] and Jörg Eberspächer[#]
[#] Institute of Communication Networks, Technische Universität München, München, Germany
[§] Institute of Media and Communication Management, SAP Research CEC, University of St. Gallen, Switzerland

Abstract

Car-to-car communication aims at increased driving comfort and safety. Moreover, it changes the role of vehicles from mere transportation means to "smart objects". Despite many R&D activities in the last years, this technology still poses multiple challenges on the wireless transmission and network protocols. Aspects like efficient message dissemination, network scalability, and information security mechanisms are still major research areas in the area of vehicular ad hoc networks. In this paper we present the potential of future car-to-car and car-to-environment communication systems, introduce the major research challenges in this field, and provide a selection of current research results.

1 Introduction and Motivation

In the last couple of years communication between vehicles has attracted the interest of many researchers around the world [1], [2]. In the European Union some research projects look into the potential of reducing road fatalities under the eSafety initiative (e.g. GST, PreVent). The same is true in other countries like the USA or Japan. Car-to-car communication (C2CC), often referred to as vehicular ad hoc networks (VANETs), enables many new services for vehicles and creates numerous opportunities for safety improvements. Communication between vehicles can e.g. be used to realize driver support and active safety services like collision warning, up-to-date traffic and weather information or active navigation systems. However, besides enabling new services VANETs pose many challenges on technology, protocols, and security which increase the need for research in this field.

VANETs have similar characteristics as mobile ad hoc networks, often in the form of multi-hop networks. Due to the high mobility of nodes network topology changes occur frequently. All nodes share the same channel leading to congestion in very dense networks. The decentralized nature of VANETs leads to the need for new system concepts and information dissemination protocols. In addition, new approaches for data and communication security have to be designed to fit the specific network needs and to guarantee reliable and trustworthy services.

Technologically, a number of more general questions have to be answered. These include decision on the wireless communication standard to be used and message dissemination schemes capable of exchanging messages in many different network scenarios. Not independent from this, issues like quality of service (QoS) and high speed real-time communication will have to be tackled to enable on-the-fly collision warning or autonomously driving vehicles. The second important area of interest is the services and applications enabled through C2C communication. As will be shown later, the design and provisioning of attractive car-to-environment or car-to-infrastructure services is crucial for the successful market introduction of C2CC systems.

2 Choice of Technology and Services

In spite of huge remaining technological challenges that are to be tackled in the field of C2CC, the definition of a sound business case is one of the most critical question to be solved: Technology allows for a multitude of different telematics services, but the end-users' demands and preferences must be thoroughly investigated to make the market introduction of C2CC an economic success.

Services and applications which are based on mere inter-vehicle communication and do not involve any infrastructure only provide value to the customer in case a sufficient penetration rate of C2CC-enabled vehicles has been reached. In the case of a road crossing collision warning application that triggers cars to periodically broadcast their exact positions to all neighbors within communication range, for example, a reduction of traffic incidents can only be realized if a high percentage of vehicles approaching the crossings are equipped with a module allowing for transmitting and receiving data. Due to the long vehicle lifecycles, however, a relevant penetration rate can only be reached after several years, even if all newly produced cars were adequately equipped from now on. For this reason, car manufacturers have to think about gradual market introduction strategies.

We therefore do not solely focus on mere inter-vehicular communications systems in this paper, but also take into account applications that rely on wireless enabled road side units (RSUs), services that leverage common Internet portals, and also briefly introduce the potential of integrating vehicles into backend business processes. So-called infrastructure-based services (e.g. car-to-home data exchange, car-to-garage communications for remote diagnosis, Floating Car Data or Location Based Services) provide clear customer benefit and motivate drivers to invest in additional wireless equipment for their vehicles. Eventually, after a longer period of time – it is expected that this process will take up to 10 years – high enough penetration rates can be reached to allow for mere inter-vehicular communication services such as intersection collision warning, local danger warning, and the de-central dissemination of real-time traffic flow information.

After presenting the state-of-the-art of wireless transmission standards, an overview of both mere inter-vehicular and vehicle-to-infrastructure communication based services is provided in this section, closing with the integration of vehicle-based services into the business processes.

2.1 Wireless transmission and multiple access

Many different wireless technologies are currently discussed to be used for car-to-car communication. Conventional IEEE 802.11 wireless LAN (WLAN), dedicated short range communication (DSRC), and GPRS/ UMTS are just some selected technologies. Due to its success in the area of data communication, the IEEE 802.11 technology family is most likely to emerge as the prevailing communication standard implemented in future cars, specifically in the variant 802.11p, which is currently defined by an IEEE working group. The European Car-to-Car Communication Consortium (http://www.car-to-car.org/) is heavily involved in the standardization process of the IEEE 802.11p automotive communication standard, which is equivalent to the DSRC technologies used in the US. Both standards use a communication frequency band around 5.9 GHz and rely on the OFDM modulation scheme. The preferred medium access method is the so-called *random access*, which does not need a global scheduler. The IEEE 802.11e standard defines Quality of Service mechanisms for the current WLAN technology. Its concepts can also be used to improve message dissemination in VANETs and improve the channel usage even in combination with the IEEE 802.11p standard.

The WLAN-based technology proved to be usable for the general task of exchanging messages between vehicles in an ad hoc fashion, however, for services with specific quality or time constraints, as well as for very large networks (»500 nodes) this technology is not applicable as is [3].

2.2 Inter-vehicle Services

Vehicle-to-vehicle communication can be used to disseminate messages of multiple services generating their content using sensors within the vehicle. These services can include accident warning, information on traffic jams or warning of an approaching rescue vehicle. In addition, information on road or weather conditions can be exchanged. More elaborate inter-vehicle services are direct collision warning or intersection assistance with information on cross traffic.

2.3 Services of Road Side Units

Communication between vehicles and RSUs can also increase safety. Traffic lights or road signs could be equipped with a communication device to actively inform vehicles in the vicinity. Hence, drivers can receive information on traffic flow, road conditions or construction sites directly from the respective RSU. In addition, static hazard areas, e.g. construction sites, could be equipped with a RSU to warn surrounding vehicles. RSU-based services will play an important role during the introduction phase, since they are almost unaffected by the penetration rate.

2.4 Portal-based Services

Besides the safety related services, many other services related to the vehicle or providing entertainment to the passengers can be brought to future vehicles. The on board unit (OBU) inside the vehicle collects all incoming messages and sensor information. In addition, it relies on a server-based infrastructure providing many additional services. These can include information on parking or hotels as well as sightseeing information. One example for such a system is the Virtual City Portal presented in [4]. The telematics platform needed to realize the portal-based services should be a standardized solution used by all vehicle manufacturers. A promising approach is the Global System for Telematics (GST) developed in the EU FP6 project GST (http://www.gstforum.org/). A standardized solution opens the market to multiple service providers and reduces the time to market for service applications.

2.5 Integration of vehicles into backend business processes

In an interconnected world of "*things that think*" (http://ttt.media.mit.edu/), vehicles will certainly play a major role in every day business processes that are currently handled by enterprise IT systems. Two different ways of integrating cars into business processes are considered valuable: First, data such as geographical position, covered distance or average speed may be transmitted to a company's backend system to allow for mobile asset management services. Logistics providers, for example, who nowadays run complex IT systems to manage their fleet, could feed real-time information into their applications to improve flexibility and adaptivity of their business processes. If such a system was enabled to receive the current, geographical position of all vehicles, the firm could react to customer demands more agilely due to better capacity forecasting mechanisms. Insurance companies and their customers might also be interested in connecting vehicles to backend IT services. Initiatives such as "*Pay-as-you-drive*" currently investigate the market potential of such applications. Drivers who only cover short distances and drive carefully would have to pay less than someone driving long distances.

Besides the transmission of data from the car to backend IT application landscapes, the provisioning of car drivers with access to external data is a promising possibility of applying vehicular communications as well. Business people, which are always "on the move", such as sales persons or consultants, may be highly interested in leveraging their cars' onboard systems as a conventional workplace. Via speech input, drivers could trigger their cars to remotely access a company portal and to download crucial information for their next customer visit, for example.

Assuming a high penetration rate of wireless enabled cars, one could even imagine that cars act as network nodes that are able to both offer and consume Web Services in a completely decentralized way. Peer-to-peer load balancing technologies [5], Web Service description, publishing and discovery mechanisms (WSDL) and novel, wireless communication standards that are able to cope with the instable connectivity and the high speeds of the vehicles would then have to be brought together to allow for real intelligent road traffic.

3 Research Challenges for Car-to-Car Communication

Previous research initiatives like Fleetnet [6] or the ongoing project Networks on Wheels [7] already looked into several aspects of C2CC. However, many different aspects of car-to-car communication still need ideas and results from research. They include high performance and efficient physical layer transmission schemes, fair and scalable medium access (MAC) schemes, efficient data dissemination protocols, security, routing protocols, to name the most critical ones. Some selected research aspects will be presented in the following sections.

3.1 Scalability of Protocols

The term scalability means that the number of users and/or the traffic volume can be increased with reasonably small performance degradation or even network outage and without changing the system components and protocols. Especially due to the distributed nature of car-to-car networks (multi-hop communication) the complexity of protocols for routing or message dissemination is rather high. Using security mechanisms further increases this overhead and the protocol complexity. Unfortunately, the network capacity in multi-hop networks is rather limited [3]. Moreover, in large networks a multitude of events will be generated and sent across the network, resulting in a network overload or even complete breakdown. Using ad hoc routing protocols, to allow for direct unicast transmissions rather than mere broadcast, usually adds complexity to the network and increases both the data overhead and the message latency. Simple flooding-based message distribution mechanisms most likely lead to network overload due to the Broadcast Storm problem [8]. Hence, better routing protocols and strategies have to be developed to tackle the scalability issue in VANETs. An overview on existing routing strategies for C2CC can be found in [9]. Promising are the routing protocols relying on position information, the so-called geo-routing protocols (e.g. GPSR).

3.2 Introduction of Security

The use and integration of security mechanisms for warning messages and safety services is absolutely necessary within VANETs [10]. Car-to-car communication and its services will only be a success and accepted by the customers if a high level of reliability and security can be provided. The most crucial security service for VANETs is the introduction of trust and the provisioning of trustworthy services. However, this is a great challenge for the distributed VANET. Conventional cryptographic mechanisms rely on e.g. a public key infrastructure (PKI) which is a centrally organized trust scheme. Thus, the use of a PKI in a distributed network is not feasible without new concepts and mechanisms. Especially the exchange and management of certificates in VANETs is a challenging task.

Besides the introduction and management of trust also the reliability of message content is a big issue for car-to-car communication. The content of a received message has to be verified within a short time to be able to use the information as soon as possible. Since vehicles will encounter each other maybe only once in their lifetime certificate-based reliability is not very efficient. New schemes based on reputation of nodes or even messages will have to be defined to solve this issue.

Integrating security is a big challenge for high speed communication as well as group communication. Since most security schemes include some cryptographic calculations the latency will be increased, thus limiting the speed for data exchange. Moreover, if a key agreement needs to be done further delay will be added. Depending on the operations, an additional delay of around 50 ms will be added for each node due to the cryptographic mechanisms. For secure group communication (e.g. for platooning) the group key agreement is the biggest bottleneck [11].

3.3 High-Speed Real-Time Communication

Since no global scheduling scheme is likely to be used in future car-to-car communication schemes, high speed communication with guaranteed low latency times is a great challenge. Especially for direct back-to-back collision warning very low latency times are required. A vehicle traveling at a speed of 50 km/h travels around 1.4 m/100ms. Hard deadlines are necessary for specific services. However, these quality-of-service requirements are hard to be met in a best effort-based network. Therefore, new approaches have to be defined to fulfill these requirements. The mentioned WLAN QoS standard (IEEE 802.11e) may be one approach to solve this issue. The same is true for concepts like using priority queues.
In this respect research related to the lower layers of the OSI layer model, e.g. new wireless radio systems, use of beam forming techniques or new medium access schemes appear to be very promising to increase data rate while reducing interference and latency [12].

3.4 Simulation of Vehicular Ad Hoc Networks

New protocols and wireless transmission schemes for VANETs can not be implemented in large testbed systems due to complexity and costs. Therefore, simulation of VANETs is a crucial method to evaluate new approaches. But the specific characteristics of vehicular networks also require specific simulation models. New road-based mobility models including the behavior of potential drivers are one example for a specific simulation model [13]. In addition, new more accurate and realistic physical channel models are required. One example for a sophisticated channel model can be found in [14], [15]. These models however, need many resources for the simulation (memory and CPU cycles).
Another challenge for VANET simulation is simulation scalability. The full-stack simulation of very large networks is currently impossible [16]. Hence, more efficient simulation techniques and strategies have to be defined to be able to evaluate large scale VANET scenarios. The promising approach is to split the simulation according to the system layering.
The credibility of simulations is also an important issue besides the feasibility of simulations [17]. Therefore, future simulations of VANET scenarios have to be based on reliable and "*standardized*" simulation parameters which are reproducible and verifiable.

4. Selected Research Results

4.1 Telematics Service Platform

Many of the aforementioned services need some kind of OBU and a supporting backend infrastructure. This platform concept should be standardized between multiple vehicle manufacturers to generate a mass market and ease the market entry for new service providers. A standardization approach for a system platform has been developed within the European Project GST backed by the major car manufacturers. In Figure 1 the open high level platform architecture is shown, detailing the system entities and their interactions.

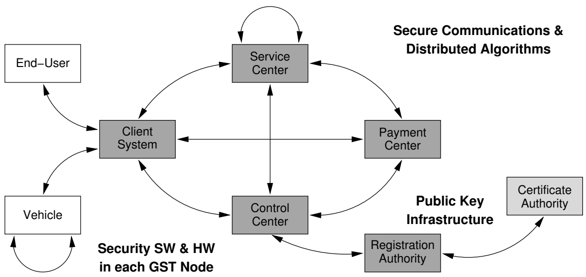

Figure 1 - The GST high level architecture diagram

Security is a crucial aspect for a platform concept, especially if commercial services are included and subscription and billing have to be conducted over the platform. In [18] the security concepts of the GST platform are presented in detail. The trust is based on a PKI with certificates. In addition, each entity is equipped with a hardware security module which is tamper proof. This module is the key component for all security related operations, since it stores, handles, and uses the keys and certificates.

4.2 Security in Vehicular Ad Hoc Networks

As mentioned above, in the decentralized MANETs, the use of a PKI and certificates to introduce trust is not an obvious choice. Especially the continuously changing connectivity to different neighbors and the not guaranteed access to an Internet gateway node make the use of certificates a challenge. Our security framework LKN-ASF is a first approach using certificates to secure VANETs. The performance evaluation proved the feasibility of the approach [19]. However, simply installing a PKI to introduce trust is not sufficient. A certificate management is needed which can validate and revoke certificates. With the limited access to the Internet and hence the PKI backend servers, this management is difficult to realize in VANETs. Two approaches to solve this challenge have been presented in [20]. Both a conventional certificate revocation list approach and a concept using validation tickets proved to be quite efficient for the certificate management in distributed network environments.

Many solutions have been published concerning secure routing protocols [21]. A secure version of the popular AODV routing protocol is AODV-SEC. Our evaluation of AODV-SEC [22] was based on simulations using the network simulator ns-2 implementing the full protocol with all cryptographic extensions. This evaluation demonstrated the feasibility of secure routing, however it also pointed out several scalability and performance limits.

4.3 Improving Scalability using Message Evaluation Schemes

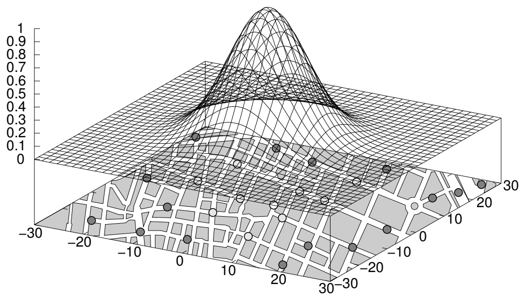

Figure 2 - Benefit value changing over distance

A relatively new approach to improve scalability is to reduce the number of messages to be transmitted by evaluating the relevance of the respective message content. This message selection, which is based on the content relevance, uses context information of the vehicle and the message to calculate the benefit which the message will give to surrounding vehicles. If all vehicles use this approach the overall utility can be maximized, leading to somewhat globally optimized network utilization. In Figure 2 a benefit curve of an event is plotted. The benefit decreases over the distance to the information source, limiting the dissemination area.

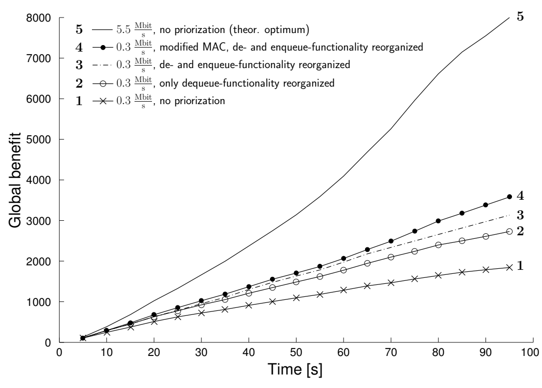

Figure 3 - The global benefit improvement through utility maximization

A detailed presentation of the benefit-based message dissemination has been presented in [23]. The improvement potential of this approach can be seen in Figure 3. Graph 5 shows the theoretical maximum for the global benefit. The graph 1 is the plot for a system using no benefit evaluation at all, while the graphs in between show the results using different combinations of queue resort mechanisms and channel contention adaptation based on the calculated local benefit values.

4.4 Simulation Environments

Several VANET-specific simulation environments have been published in the last couple of years. GrooveSim [24] and CARISMA [13] are just two examples. Most of these simulators use digital maps as a basis for the node mobility model. In Figure 4 a VANET simulation on a real map can be seen. The figure shows both wireless equipped and regular vehicles as well as the wireless communication links. The information on node positions and wireless links are used as input to either an included or an external network simulator (e.g. ns-2). The effects of car-to-car communication on city traffic have been evaluated in [13].

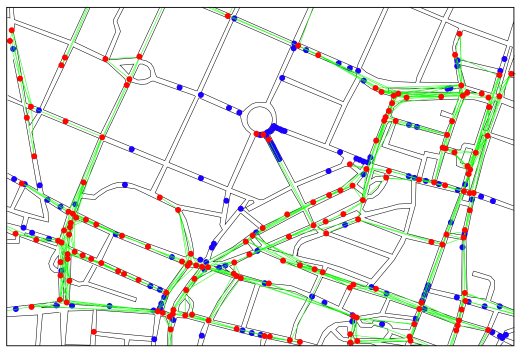

Figure 4 - Street-based mobility model for VANET simulations

This publication also presents some detailed information how to couple the simulators for mobility and the wireless network efficiently while generating reliable simulation results based on realistic mobility patterns.

5 Conclusion

Car-to-car communication is an interesting and challenging new field in communication network research. While many creative and powerful new solutions have already been proposed, still many open issues exist. In addition to technical breakthroughs, the phase of market introduction is critical for the success of this new technology. VANETs will only become a commercial and technological success as long as its services and capabilities are of high value to potential users during all phases of the introduction phase. Hence, services and technology have to be adaptable to the different levels of market penetration. Quality of Service (especially concerning latency) and security for VANET systems are crucial aspects of car-to-car communication that need to be integrated to ensure the success of this promising technology.

6 Bibliography

[1] D. W. Franz, "Car-to-car Communication – Anwendungen und aktuelle Forschungsprogramme in Europa, USA und Japan", in *Kongressband zum VDE-Kongress 2004 – Innovationen für Menschen*, VDE, October 2004.

[2] A. Lübke, "Car-to-car Communication – Technologische Herausforderungen", in *Kongressband zum VDE-Kongress 2004 - Innovationen für Menschen*, VDE, October 2004.

[3] P. Gupta and P. R. Kumar, "The capacity of wireless networks", *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388-404, March 2000.

[4] R. Bogenberger et al., "Virtual city portal - a multi-network personal information system for automobile users", in *Proceedings of Workshop on Multiradio Multimedia Communications, Communication Technology for Vehicles*, February 2003.

[5] B. Godfrey et al., "Load balancing in dynamic structured p2p systems", in *Proceedings of the 23rd Conference of the IEEE Communications Society (Infocom)*, March 2004.

[6] Fleetnet Project Homepage, http://www.et2.tu-harburg.de/fleetnet/

[7] Network on Wheels Project Homepage, http://www.network-on-wheels.de/

[8] S.-Y. Ni et al., "The broadcast storm problem in a mobile ad hoc network", in *Proceedings of the 5th International Conference on Mobile Computing and Networking*, 1999.

[9] H. Füßler et al., "A comparison of Routing Strategies for Vehicular Ad Hoc Networks", Technical Report TR-02-003, Department of Computer Science, University of Mannheim, July 2002.

[10] J. P. Hubaux et al., "The security and privacy of smart vehicles", IEEE Security & Privacy, vol. 4, no. 3, pp. 49-55, May/June 2004.

[11] Y. Amir et al., "On the performance of group key agreement protocols", in ACM Transactions on Information and System Security, vol. 7, no. 3, pp. 457-488, August 2004.

[12] R. Vilzmann and C. Bettstetter, "A Survey on MAC Protocols for Ad Hoc Networks with Directional Antennas", in *Proceedings of the 11th EUNICE Open European Summer School*, July 2005.

[13] S. Eichler et al., "Simulation of car-to-car messaging: Analyzing the impact on road traffic", in *Proceedings of the 13th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, September 2005.

[14] J. Maurer et al., "A new inter-vehicle communications (ivc) channel model", in *Proceedings of the 61st Vehicular Technology Conference (VTC)*, September 2004.

[15] J. Maurer, "Strahlenoptisches Kanalmodell für die Fahrzeug-Fahrzeug Kommunikation", *Ph.D. Dissertation*, Universität Karlsruhe (TH), May 2005.

[16] R. M. Fujimoto et al., "Large-scale network simulation: How big? how fast?" in *Proceedings of the 11th Annual Meeting of the IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, October 2003.

[17] S. Kurkowski et al., "Manet simulation studies: the incredibles", *SIGMOBILE Mobile Computing Communications Review*, vol. 9, no. 4, pp. 50-61, October 2005.

[18] S. Eichler et al., "On providing security for an open telematics platform", in *Proceedings of the 5th International Conference on ITS Telecommunications*, June 2005.

[19] C. Schwingenschlögl and S. Eichler, "Certificate-based key management for secure communications in ad hoc networks", in *Proceedings of the 5th European Wireless Conference: Mobile and Wireless Systems beyond 3G*, February 2004.

[20] S. Eichler and B. Müller-Rathgeber, "Performance analysis of scalable certificate revocation schemes for ad hoc networks", in *Proceedings of the 30th Conference on Local Computer Networks (LCN)*, November 2005.

[21] P. G. Argyroudis and D. O'Mahony, "Secure routing for mobile ad hoc networks", *IEEE Communications Surveys & Tutorials*, vol. 7, no. 3, pp. 2-21, 2005.

[22] S. Eichler and C. Roman, "Challenges of secure routing in MANETs: A simulative approach using AODV-SEC", in *Proceedings of the 3rd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS)*, October 2006.

[23] S. Eichler et al., "Strategies for context-adaptive message dissemination in vehicular ad hoc networks", in *Proceedings of the 2nd International Workshop on Vehicle-to-Vehicle Communications (V2VCOM)*, July 2006.

[24] R. Mangharam et al., "GrooveSim: A topology-accurate simulator for geographic routing in vehicular networks", in *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks*, September 2005.