Computer and Communication Systems

Lehrstuhl für Technische Informatik

Christoph Sommer, Björn Scheuermann,
Tessa Tielert, Björn Schünemann (Eds.)

Proceedings of the 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013)

Technical Report CCS-2013-01

Please cite as:
Christoph Sommer, Björn Scheuermann, Tessa Tielert, Björn Schünemann (Eds.), "Proceedings of the 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013)," University of Innsbruck, Institute of Computer Science, Technical Report CCS-2013-01, February 2013.

University of Innsbruck
Institute of Computer Science
Computer and Communication Systems

Technikerstr. 21a · 6020 Innsbruck · Austria

http://ccs.uibk.ac.at/

Proceedings of the 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication (FG-IVC 2013)

February 21st–22nd 2013
Innsbruck, Tyrol, Austria

Preface

Inter-vehicle communication (IVC), the management and control of network connections among vehicles as well as between vehicles an existing network infrastructure, is a maturing research field that is currently gaining massive momentum. The investment of European automobile manufacturers and OEMs into this idea is not only expressed in successful efforts to reserve dedicated radio spectrum harmonized across Europe, but is also reflected in numerous research ventures in cooperation with academia.

First standardization efforts across all layers, by both IEEE and ETSI, have already borne fruit, allowing researchers to gain valuable insights into both the strengths and the shortcomings of current approaches. A tremendous body of experience could be gathered in both national and international large scale field tests as well as in the domain of simulation and modeling. However, this knowledge is still fragmented, making it hard for new players to get into the game and affording even experienced groups only a restricted view on this complex field.

In February 2013 we therefore invited talented young researchers as well as their experienced colleagues to come to Innsbruck for what was to become the 1st GI/ITG KuVS Fachgespräch Inter-Vehicle Communication. Started off with a Keynote by Ilja Radusch, what followed were two days of lively discussions by a mixed crowd of 20 researchers, guided by four short and nine long talks. Discussions revolved around both the state of the art and around future directions of inter-vehicle communication research, from physical layer optimizations to novel applications of vehicular networks and from microscopic evaluation metrics to problems of scale, crime, and privacy. The Fachgespräch concluded with a half-day skiing trip to the Alps.

February 2013

Christoph Sommer
Björn Scheuermann
Tessa Tielert
Björn Schünemann

Contents

Cooperative Relaying in Vehicular Communications: Some Results from Experimental Studies

Günther Brandner
University of Klagenfurt, Mobile Systems Group, Institute of Networked and Embedded Systems, Austria
guenther.brandner@uni-klu.ac.at

***Abstract*—We analyze cooperative relaying in vehicular communications by real-world measurements and compare its performance in terms of packet delivery ratios to conventional communication schemes. Results indicate that the temporal correlation of packet delivery is a key factor on whether or not cooperative relaying is of benefit compared to time diversity, where a packet is retransmitted if the first transmission fails.**

***Index Terms*—Wireless networks, mobile networks, cooperative relaying, car-to-car communications, diversity, measurements, experimental study.**

I. Introduction

The concept of cooperative relaying in wireless systems [1] gained considerable interest within the research community throughout the last few years. Many publications address its benefits theoretically or by means of simulations (e.g., [1]–[4]). On the other hand, however, there are only few studies assessing cooperative relaying with *real-world measurements* in *realistic environments* (e.g., [5]–[8]).

The aim of our research is to assess and compare the performance of cooperative relaying in vehicular communications with respect to conventional communication schemes. In this extended abstract we present results with respect to packet delivery ratios and compare cooperative relaying to direct transmission, and time diversity. We show that the temporal correlation of packet delivery is a key factor on whether or not cooperative relaying exhibits benefits.

The results presented in this extended abstract have already been published in [9] and [10].

II. Measurement Setup and Methodology

We evaluate the performance of cooperative relaying in a vehicular communications environment. For this we compare three communication strategies:

- Conventional direct communication: The source transmits each packet *once* with *full* transmission power.
- Time-diversity direct communication: The source transmits each packet *twice*, where each transmission is made with *half* transmission power
- Cooperative relaying: The source transmits each packet *once* with *half* transmission power; the relay transmits each received packet *once* with *half* transmission power.

Note that packets of direct communication are sent at full transmission power, while packets of time diversity and cooperative relaying are sent at half power. We do this to achieve an energy-fair comparison of the schemes.

We perform the measurements in the $2.4\,\text{GHz}$ band using three WARP boards [11]. These boards are based on field-programmable gate arrays (FPGAs) and enable the programmability of low-layer protocols. Each board is assigned to a car and serves as either source (S), destination (D), or relay (R). The full (peak) transmission power is set to about $22\,\text{dBm}$, the half (peak) transmission power is $19\,\text{dBm}$. The antennas, which have a gain of $7\,\text{dBi}$, are attached to the roofs of the cars. The packet size is $1048\,\text{bytes}$, consisting of a payload of $1024\,\text{bytes}$ and a header of $24\,\text{bytes}$. The orthogonal frequency-division multiplexing (OFDM) reference design, which we employ, uses 64 subcarriers from which 48 are data-bearing. The used bandwidth is $10\,\text{MHz}$, and the data rate is $10\,\text{Mbit/s}$. Furthermore, we use quadrature phase-shift keying (QPSK) as the modulation scheme.

The following packets are transmitted cyclically (see Fig. 1):

- a full-power packet S_f from S to D,
- two half-power packets S_h and S_h^* from S to D,
- a third half-power packet S_h^{**} from S to D and R, and finally
- a half-power packet R_h from R to D.

In between these packets there is a time interval of 30 ms.

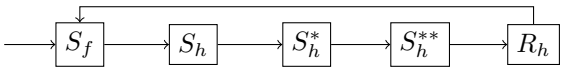
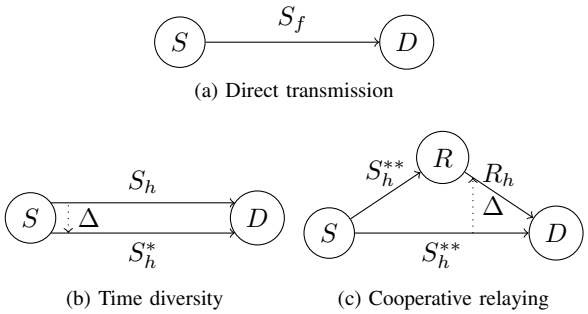


Fig. 1: Transmission cycle

At the destination we evaluate the packet delivery ratio in the following way: A packet is delivered, if it is received by the communication partner and the cyclic redundancy checks (CRCs) of both header and payload are valid. As shown in Fig. 2, a packet is delivered (a) by direct transmission if S_f is delivered to D, (b) with time diversity if at least one of the half-power packets S_h or S_h^* is delivered to D, and (c) using cooperative relaying if S_h^{**} is delivered to D, or S_h^{**} is delivered to R and R_h is delivered to D. Note that we do not employ packet combining for time diversity and cooperative relaying at the destination.

Furthermore, we evaluate three scenarios for the position of the relay: R is driving in between S and D (RM), R is driving behind D (RL), and as the third scenario we place R and D into the same car (RD).

For time diversity, but also for cooperative relaying, the length of the time period between the first and the second



(a) Direct transmission

(b) Time diversity

(c) Cooperative relaying

Fig. 2: Transmission scenarios

packet of the given scheme is of importance for its packet delivery performance. In the following we denote this time by Δ. To assess time diversity, we consider the two packets S_h and S_h^* separated by Δ. For cooperative relaying, we consider S_h^{**} and R_h separated by Δ. Packet delivery is evaluated as a function of Δ ranging from 30 ms to 30 s.

We evaluate cooperative relaying in two environments which can be classified as suburban and highway. In this extended abstract we mainly present results for the highway environment. For results regarding the suburban environment we refer to [10].

To assess the statistical significance of the measurements, we show the arithmetic mean, and its 10 % and 90 %-quantiles.

III. Temporal Correlation of Packet Reception

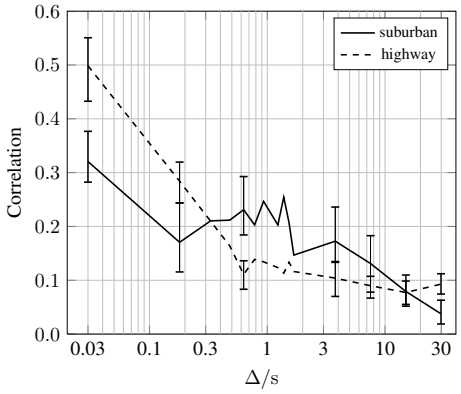


Fig. 3: Temporal correlation. Results are for the RD case, but the correlations are similar for the RM and RL cases.

The temporal correlation of packet reception of a given link is a key factor for the performance of both time diversity and cooperative relaying. For time diversity a retransmission shall be successful when the first transmission fails. This, however, will only be the case when the channel changes appropriately between first transmission and retransmission. Informally speaking, a high positive correlation means that little changes of the channel can be expected, which makes it unlikely that the second transmission succeeds if the first one fails. Thus, a high correlation will lower the performance of time diversity. Therefore, temporal correlation can be used as an indicator for the probability of successful transmission in time diversity.

Fig. 3 shows the autocorrelation for both suburban and highway environments. The autocorrelation is highly positive if the time span Δ between packets is short; it attenuates for increasing Δ. A highway exhibits a significantly higher correlation for small Δ; for $\Delta \geq 0.15$ s, the correlations of highway and suburban environments are similar. For both environments, such positive correlation will reduce the performance of time diversity.

IV. End-to-End Packet Delivery Ratio

Fig. 4 shows the percentage of packets delivered successfully from S to D as a function of Δ for all transmission schemes and relay positions. We can see that the delivery ratio of time diversity improves for increasing Δ due to decreasing correlation. In particular, we see that in all cases the packet delivery ratios of time diversity and cooperative relaying are higher than that of direct transmission.

For RM (a), cooperative relaying outperforms time diversity, mainly due to the multihop gain. For RL (b), cooperative relaying is better for small Δ on highway ($\Delta < 0.1$ s). The reason for this behavior is the correlation shown in Fig. 3, which is very high for small Δ. Thus, cooperative relaying improves the packet delivery ratios due to the lower correlation between the links $S-D$ and $S-R$ (not shown). Finally, for RD (c), cooperative relaying excels time diversity for $\Delta < 0.1$ s. For results with respect to the suburban environment we refer to [10].

V. Conclusions and Outlook

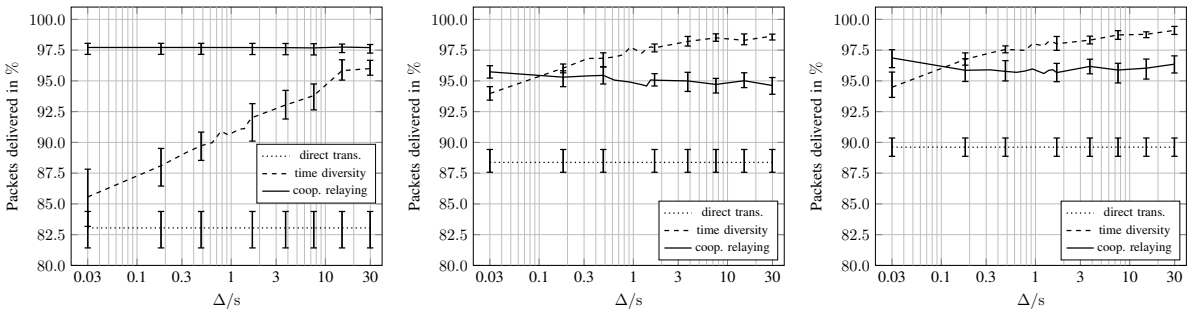
We studied the performance gains in terms of packet delivery ratios of cooperative relaying with respect to direct transmission and time diversity. Measurements have shown that the temporal correlation is a significant factor on whether or not cooperative relaying is of benefit compared to time diversity. In particular, for environments where the correlation is large cooperative relaying can be beneficial.

As future work we aim to evaluate the performance of cooperative relaying and time diversity when (sophisticated) packet combining schemes are applied at the destination. In particular, we are interested in assessing maximum ratio likelihood combining schemes. Furthermore, we also aim to evaluate cooperative relaying in single carrier systems. Here, the main research question is whether or not cooperative relaying is of higher benefit for such systems than for OFDM systems. Furthermore, we also want to perform and evaluate measurements in the 5 GHz frequency band which is specified for vehicular communications in the IEEE 802.11p standard.

References

[1] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3062–3080, Dec. 2004.

[2] E. Zimmermann, P. Herhold, and G. Fettweis, "On the performance of cooperative relaying protocols in wireless networks," *Eur. Trans. Telecomm*, vol. 16, pp. 5–16, 2005.



(a) RM (b) RL (c) RD

Fig. 4: Packet delivery ratios (highway)

[3] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Select. Areas Commun.*, vol. 24, pp. 659–672, Mar. 2006.

[4] S. S. Ikki and M. H. Ahmed, "Performance analysis of cooperative diversity with incremental-best-relay technique over Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 59, pp. 2152–2161, Aug. 2011.

[5] G. J. Bradford and J. N. Laneman, "An experimental framework for the evaluation of cooperative diversity," in *Proc. Conf. on Information Sciences and Systems (CISS)*, (Baltimore, MD), pp. 641–645, Mar. 2009.

[6] P. Kyritsi, P. Eggers, R. Gall, and J. M. Lourenco, "Measurement based investigation of cooperative relaying," in *Proc. IEEE VTC*, (Montréal, Canada), Sept. 2006.

[7] S. Valentin, H. S. Lichte, D. Warneke, T. Biermann, R. Funke, and H. Karl, "Mobile cooperative WLANs - MAC and transceiver design, prototyping, and field measurements," in *Proc. IEEE VTC*, (Calgary, Canada), Sept. 2008.

[8] F. S. González, B. Bandemer, G. Matz, C. Oestges, F. Kaltenberger, and N. Czink, "Performance of transmission-time optimized relaying schemes in real-world channels," in *Proc. Conf. on Antennas and Propagation (EuCAP)*, (Barcelona, Spain), Apr. 2010.

[9] G. Brandner, U. Schilcher, and C. Bettstetter, "Cooperative relaying in car-to-car communications: Initial results from an experimental study," in *Proc. IEEE Intern. Symp. Commun., Control and Sign. Proc. (ISCCSP)*, (Limassol, Cyprus), Mar. 2010.

[10] G. Brandner, U. Schilcher, T. Andre, and C. Bettstetter, "Packet delivery performance of simple cooperative relaying in real-world car-to-car communications," *IEEE Wireless Communications Letters*, vol. 1, pp. 237 –240, June 2012.

[11] "WARP Project: Wireless Open-Access Research Platform, Rice University," 2012 (accessed March 05, 2012). http://warp.rice.edu.

Advanced Receiver Structures For Vehicular Communications

Robert Budde; Rüdiger Kays
Communication Technology Institute
TU Dortmund University
Dortmund, Germany
{robert.budde;ruediger.kays}@tu-dortmund.de

I. INTRODUCTION

Vehicular communications are on the verge of wide-scale deployment by now. While first-day applications are designed to work in low-deployment scenarios and with unreliable network connectivity, more demanding applications have already been proposed, urging for highest communication ranges and yet unmet reliabilities.

While to a certain extent some of these challenges can be met partially by multi-hop routing, there is still need to improve single-hop communication at the physical layer.

Being a derivative of the famous IEEE 802.11 family of standards [1], which was originally targeted at indoor wireless communication, the IEEE 802.11p amendment for vehicular communication [2] still bears certain assumptions about the wireless channel which do not apply for vehicular scenarios. As IEEE standardization is finished, international harmonization of local standards is already on the way and compatibility is a key aspect. The development of more advanced receiver structures, meeting the unique challenges in vehicular communications, is an important task.

This work is structured as follows: in section II the shortcomings of the physical layer are discussed and in section III two different approaches are presented. Section IV features selected simulation results while section V concludes the paper.

II. PHYSICAL LAYER LIMITATIONS

The physical layer of IEEE 802.11p was inherited from the IEEE 802.11a physical layer. The only noticeable adjustment made was halving the channel bandwidth, effectively doubling the symbol time. While this helps when dealing with multipath echoes, as the ODFM guard interval is now doubled to be 1.6 µs, this makes the system even more susceptible to deep fades in the frequency domain. Moreover, by doubling the symbol time, the data rate was halved as well, which means wireless transmissions take longer in a vastly time-variant environment. As an OFDM system requires coherent detection it requires an up-to-date estimate of the channels' transfer function throughout packet reception.

The channel coherence time expresses how long the channel transfer function can be assumed to be correlated. Measurement campaigns have shown that this time can be in the range of 300-400 µs for certain communication scenarios [3][4], which means the channels transfer function will be uncorrelated after 40-50 OFDM symbols if the transfer function is not continuously tracked during reception. A degradation of robustness will be observed after a much smaller timespan, as the accurateness of the channel state information (CSI) decreases continuously.

For tracking the channels transfer function, four comb pilots are available in each OFDM symbol. These pilots have a frequency spacing of 2.1875 MHz, making them suitable to track variations in the frequency domain as low as 4.375 MHz. An estimate of the channel's actual frequency selectivity is given by the coherence bandwidth, which is approximately the inverse of the maximum multipath delay. This delay was reported to be up to 1 µs [3], making the coherence bandwidth as small as 1 MHz. For this reason updating the channel state information solely based on the comb pilots is not sufficient.

III. ADVANCED RECEIVER STRUCTURES

A vast number of concepts exist to address the shortcomings of the IEEE 802.11p standard [5]. Nevertheless, all concepts requiring the standard to be modified, as it would be the case for non-coherent detection, more bandwidth or

TABLE I. CHANNEL PARAMETRIZATION

Parameter	Channel	
	CM1	***CM2***
Fading	Rayleigh	Rice
Rice Factor K	-	15.3 dB
Delay spread	200 ns	26.1 ns
Vehicle speed	100 km/h	120 km/h
Doppler spectra	Classical (Jakes)	Flat
Maximum Doppler frequency	1093 Hz	1311 Hz

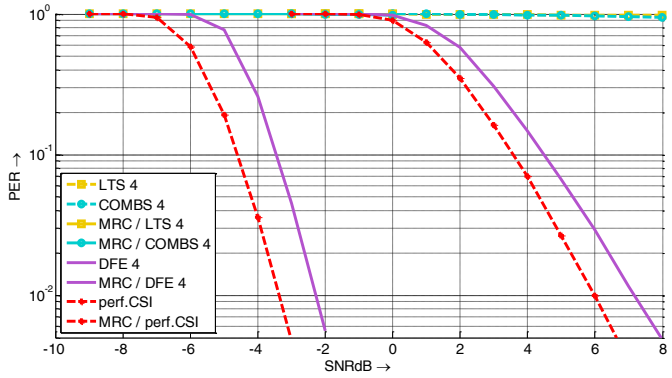


Figure 1. CM2: 3Mb/s, BPSK, 1/2, 128 Byte (43 OFDM symbols)

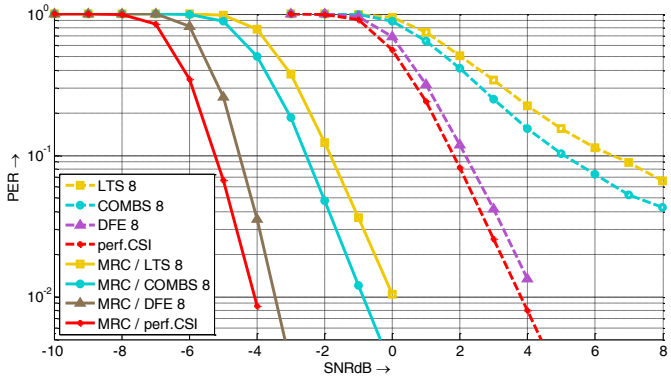


Figure 2. CM1: 3 Mb/s, BPSK, 1/2, 128 Byte (43 OFDM symbols)

other pilot patterns, are unfeasible at this late deployment stage. For this reason, the adaption of advanced receiver techniques structures is the only option.

A. Decision Feedback Equalization

Decision Feedback equalization, sometimes referred to as iterative decoding or pseudo pilots, is a key concept to allow for continuous channel tracking. It exploits the fact, that by demodulating and decoding channel noise and errors are removed from the data. By assuming the decoded data to be free of errors, the original symbol can be reconstructed by re-encoding and -modulating the data. This in turn allows for computation of the channels transfer function by a zero-forcing estimator, as it is done for the training symbols.

B. Spatial Diversity Combining

While the decision feedback equalization enables continuous channel tracking, the wireless system will still suffer from the high frequency selectivity and the overall fast fading behavior of vehicular channels in certain scenarios. For this reason, exploitation of spatial diversity is promising, especially with the assumption that there will be always more than one antenna deployed on a car's body to avoid slow-fading caused by shadowing. While Selection Combining chooses the presumably strongest antenna signal at the beginning of the transmission, Equal Gain Combining adds up all received signals with equal weight. As a drawback, this amplifies channel noise in deep fades. This drawback motivates the application of Maximum Ratio Combining (MRC). MRC is the optimum combining technique, as it weights every carrier estimate with its amplitude, suppressing noise from highly attenuated carriers. A more detailed description is given in [6].

IV. Simulation Results

A wide range of numerical simulations were carried out to investigate the effectiveness of the proposed structures in demanding vehicular channels. Two exemplary channels were chosen to test the receiver structures. The parameters of these channel models are given in Table I. For a more detailed discussion on the channel model, the reader is referred to [7].

In all simulations, the channel estimate was further filtered for noise reduction in both frequency and time-domain [8]. The channels are supposed to be completely uncorrelated, which is optimum for the diversity combining. In real scenarios, the channel will be correlated somehow, leading to smaller improvements when using MRC [9].

For reference, the results for a receiver having perfect state information were also computed.

In Fig. 1, the results for the Rayleigh-fading channel and the lowest available data rate (BPSK, R=½) are shown. It is obvious, that the channels transfer function varies so fast that receivers, which solely rely on the long training sequences (LTS) or track the channels transfer function by using the Comb Pilots (COMBS), reach no useful packet error rate (PER) in this setup. Contrary to this, the DFE receiver can successfully track the channel. It yields only about 0.8 dB penalty at 10% packet error rate compared to perfect channel state information for both SISO and MRC. Comparing the results for SISO and MRC, a huge difference of about 7.7 dB at 10% can be observed. This difference has to be explained. For AWGN channels MRC converges towards an equal gain combining (EGC) and by just adding up four AWGN signals, a SINR gain of 6 dB is indisputable. By exploiting constructive interferences in non-AWGN channels on a subcarrier level by using MRC, an even higher gain, as observed here, is plausible.

The same simulations were re-run for a less demanding Rician-fading channel. The results are shown in Fig. 2. In this setup, the naive LTS receiver even succeeds to a certain extent. Compared to this, the exploitation of Comb Pilots (COMBS) gives an advantage in terms of SINR of about 1.3 dB for SISO and 0.8 dB for MRC at 10% PER respectively. Yet an error floor well above 1% PER is observable for both receivers, indicating that besides the SINR the receiver structures still suffer from the high time variance of the channel.

In Fig. 3, the channel setup was kept constant, while a higher data rate was chosen. By choosing the mandatory rate of 12 Mb/s, a modulation scheme with multiple amplitudes can be investigated. Because of the higher data rate, the packet duration is almost quartered when considering the same payload size. The impact of the channels' time variance should consequently be less dominant.

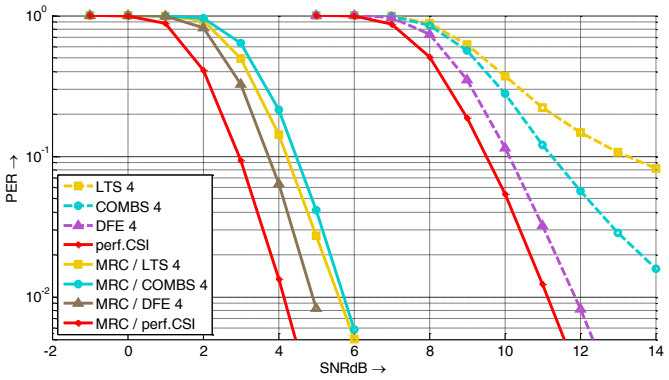


Figure 3. CM2: 12 Mb/s, 16QAM, 1/2, 128 Byte (11 OFDM symbols)

Compared to the lower data rate (Fig. 2), the average required SINR increases by about 8 dB when focusing on the results obtained by perfect channel state information (perf.CSI). Considering the SISO results, the LTS receiver loses slightly less compared to perfect CSI, which can be explained by the shorter packet duration. For the same reason, the COMBS receiver performs better as well. Yet both receivers approach an error floor. This is especially obvious for the LTS receiver. Considering the results obtained by MRC simulations, we see big improvements for both LTS as well as COMBS receiver. Because of the short packet duration, channel tracking is less important. Moreover, due to the multiple channels when using ratio combining, it is likely for the receiver to get hold of at least one channel which hardly changes at all. This is especially true for the LTS receiver, which consequently even outperforms the COMBS receiver for this specific setup.

V. CONCLUSION

This work summarizes the key weaknesses of the IEEE 802.11p physical layer. It points out, that especially in demanding vehicular environments, channel tracking capability is inevitable and needs to be improved by the deployment of advanced receiver structures.

Two advanced receiver concepts are presented, which can be applied individually or complementary, depending on desired hardware costs and computing complexity. Simulation results are presented for all relevant combinations of such.

More detailed research has been conducted for optimizing the parameterization of both concepts for specific vehicular channels. The layout of the applied noise-filters both in frequency- and time-domain also greatly impacts the overall system performance.

Further research will include the application of turbo-concepts to the receiver structure as well as more advanced filter algorithms. As these concepts lead to a high computing complexity, adaptive strategies for enabling the appropriate receiver structures on demand are also a topic for research.

REFERENCES

[1] IEEE Standard 802.11-2012, Wireless LAN Medium Access Control and Physical Layer Specifications, Mar. 2012.

[2] IEEE Standard 802.11p-2010, Wireless Access in Vehicular Environments, Jul. 2010.

[3] C.F. Mecklenbräuker et al, “Vehicular Channel Characterization and Its Implications forWireless System Design and Performance”, Proceedings of the IEEE, vol. 99, no. 7, pp.1189-1212, 2011.

[4] L. Cheng et al, “Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frequency Band”, IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp.1501-1516, 2007.

[5] R. Budde, R. Kays, “Challenges and Improvement Strategies for the Physical Layer in Vehicular Communications”, European Wireless 2012, Poznan, Poland, 2012.

[6] J. Nuckelt, H. Hoffmann, M. Schack, T. Kuerner: “Linear Diversity Combining Techniques Employed in Car-to-X Communication Systems”, IEEE 73rd VTC Spring 2011, Budapest, Hungary, 2011.

[7] S. Nowak, R. Budde, R. Kays, “Channel Tracking in Vehicular OFDM systems based on IEEE 802.11p”, 16th International OFDM-Workshop, Hamburg, Germany, 2011.

[8] H. Schmidt, V. Kühn, K. Kammeyer, R. Rückriem, S. Fechtel: “Channel Tracking in Wireless OFDM Systems,” Multi-Conference on Systemics, Cybernetics and Informatics, Orlando, USA, 2001.

[9] J. Nuckelt, Th. Kürner: “MRC performance benefit in V2V communication systems in urban traffic scenarios”, 6th European Conference on Antennas and Propagation (EUCAP), Prague, Czech Republic, 2012.

A Methodology to Evaluate the Optimization Potential of Co-ordinated Vehicular Route Choices

Daniel Cagara Björn Scheuermann

Computer Engineering Group
Humboldt University of Berlin, Germany
{cagarada, scheuermann}@informatik.hu-berlin.de

Ana L. C. Bazzan

Instituto de Informática
Univ. Federal do Rio Grande do Sul, Brazil
bazzan@inf.ufrgs.br

***Abstract*— A car navigation system's job is to plan a good route from an origin to a destination. There are many different options how this can be accomplished. Path choices can be calculated based on static road map representations, or they can take into account dynamic information like, e. g., known road blocks or the current traffic situation. More recently, the idea has gained ground that navigation systems could even cooperate in order to co-ordinate route choices so as to proactively avoid the formation of traffic jams. While several heuristics for algorithms to improve the vehicles' route choices have been proposed, little is known about the potential benefit of such optimizations. How much can we gain if dynamic information exchange and/or co-ordination between vehicles are used? Answering this question requires to obtain information on the travel times realized by "best possible", globally co-ordinated route choices—and therefore the solution of a highly complex optimization problem. Here, we propose a method to accomplish this. We use genetic algorithm optimization to jointly evolve the route choices of all cars in a street network iteratively towards an optimal solution, where the quality of each intermediate optimization step is assessed using a road traffic simulation.**

I. Introduction

Car navigation systems get increasing attention and popularity. The navigation system helps the user to find his best route from an origin to a destination. The selection of this optimal route is, in essence, the solution of a shortest path problem in directed graphs, and can thus be solved by algorithms like Dijkstra's algorithm, the A* algorithm [1] or the Bellman-Ford algorithm. Static map data forms the foundation for this functionality, but most modern devices use multiple sources of information and take various dynamic variables like the current traffic situation or historical traffic data into account when finding an optimal path. As of today, though, the decision in practice is generally a local one: the route choice is optimized per vehicle, minimizing the anticipated travel time of this one driver.

Such a local optimization from each driver's perspective, though, does not necessarily mean that an optimal point for the system as a whole is reached. In fact, it could mean that all drivers choose one route and a major traffic jam forms, while with proper distribution across multiple routes each single driver would be better off. Even with perfect information for all drivers, selfish route choices can lead to a highly suboptimal global situation—the *price of anarchy* is potentially high [2]. While several heuristic approaches to optimize route choices by cooperation between the individuals have been proposed [3], [4], there is no way to tell how far away from globally optimal routes (in whatever sense) those solutions actually are: if 5 % improvement is the best that can be reached, a heuristic which results in a 4 % improvement would be considered very good; if 20 % improvement are possible, the same heuristic would appear in a different light. The question how much improvement can be achieved in different kinds of road networks, if all the optimization potentials are fully used, has, so far, not been assessed in sufficient depth.

Here, we therefore do not aim for a route selection method that is directly applicable to the selection of routes in a real, live traffic scenario. But we discuss a methodology which is able to jointly optimize the route choices of all vehicles in a given scenario, in order to assess the optimization potential. To this end, we employ genetic algorithms [5]. Genetic algorithms have often be used very successfully to solve complex optimization problems. We argue that they are also well-suited to the structure of our problem. We employ a genetic algorithm in combination with microscopic traffic simulation in order to evaluate the quality ("fitness") of candidate solutions ("individuals"). Thereby, the set of routes for all vehicles is jointly evolved, so as to optimize the choices with regard to a global target function.

Besides their utility as a benchmark, we expect the obtained globally optimized routes to also provide valuable hints on how to *design* good heuristics: by analyzing the chosen optimal routes in different scenarios, we hope to identify patterns which can be taken up in the design of future cooperative routing algorithms.

This paper is structured as follows. After reviewing related work in Sec. II, we formally define the optimization problem in Sec. III. In Sec. IV, we then introduce the genetic algorithm which we use for optimization. In Sec. V, we present and discuss first results and experiences that we obtained from applying the proposed methodology to simple scenarios. Finally, in Sec. VI, we conclude this paper with a summary of our results and insights, along with a discussion of intended directions for future work.

II. Related Work

In recent years, there have been numerous papers that focused on improving route choices in road traffic networks. For example, [4] introduces an approach to optimize traffic flow using a genetic algorithm. This approach is targeted to practical use in a real world traffic information system by periodically repeating short-time forecasts of the traffic situation. We, in contrast, do not want to optimize routes online based on limited knowledge. We rather aim to quantify how much can be gained by searching for the best solution given perfect knowledge.

In [6], the authors' goal is again finding the optimal distribution of traffic in road networks. Their approach is to use an evolutionary game, Minority Game. They show that near-optimal traffic distribution can be achieved even when drivers choose their routes independently and without communication. However, they are working in a simple scenario with several highly simplified abstractions, whereas we use microscopic traffic simulations and therefore operate on a much more realistic view of road traffic.

In [7], a mathematical approach to optimizing traffic from the systems perspective is pursued. Again, do the complexity of the problem, several abstractions are made—for instance, static traffic flows are assumed. By using our genetic algorithm based optimization strategy, we are able to avoid such simplifications.

The existing body of work on traffic flow improvement in a more general sense includes, for example, approaches like [3], where an ant-hierarchical fuzzy system is applied. Yet, it is generally unknown how far those approaches are from an optimal solution—and this is just the question we are targeting here.

III. Problem Formulation

Assume the road map being represented by a graph $G = (V,E)$, consisting of a set of vertices V which represent the intersections of the road network, and a set of directed arcs $E \subset V \times V$ which describes the existing roads as directed connections between pairs of vertices. Further assume that there are z cars $c_1,\ldots,c_z$ in the road network, with car c starting its journey at time t_0^c. The route of car c is a sequence of k_c links, i. e., $R^c = (l_1^c,\ldots,l_{k_c}^c)$, where $\forall i \in \{1,\ldots,k_c\} : l_i^c \in E$ and for $i \in \{2,\ldots,k_c\}$ it holds that the i-th link starts at the vertex where the $i-1$-st link ended.

Each link $l \in E$ is associated with a function f_l; $f_l(t)$ is the travel time that it will take a vehicle entering link l at time t to traverse the link. This function depends on the traffic density and the characteristics of the respective road segment. It relates to the fundamental diagram used in traffic engineering. The functions f_l are therefore, in turn, influenced by the route choices of the cars in a non-trivial way. This is what makes the optimization problem so complex.

Consequently, the time at which car c has traversed the i-th link along its route is

$$t_i^c = t_{i-1}^c + f_{l_i^c}(t_{i-1}^c), \tag{1}$$

and the car's total travel time is given by

$$T_c = \sum_{i=1}^{k_c} f_{l_i^c}(t_{i-1}^c) = t_{k_c}^c - t_0^c. \tag{2}$$

In order to find the "best" routes for all cars, it is first necessary to define by which measure this decision is to be made. There are many possible choices for the target function. It is for example conceivable to minimize the mean of the absolute travel times, or the average (or maximal) level of congestion on the road networks links. Here, we propose to optimize the route choices in such a way that the mean relative improvement in the cars' individual travel times is maximized. The relative improvement is measured compared to the situation in which each car is individually and egoistically driving the shortest path. That is, for each individual car we determine the travel time if no optimization is in place; for car c, we denote this travel time by $\widehat{T}_c$. We then consider the ratio $T_c/\widehat{T}_c$, which describes the relative improvement (or deterioration) for car c: a ratio smaller than one means that the car's travel time has improved (i. e., it has reduced), a ratio larger than one corresponds to a deterioration for the individual car. Our target function is the mean relative gain of the cars, i. e., we minimize the expression

$$\sqrt[z]{\prod_{i=1}^{z} \frac{T_{c_i}}{\widehat{T}_{c_i}}}. \tag{3}$$

By using the relative changes instead of the absolute ones, we prevent longer routes from being favored during the optimization at the cost of ignoring shorter routes. Other target functions are equally well usable in our framework, so that this choice is not critical for the applicability of the method in general.

IV. The Genetic Algorithm

Due to the complex codependencies, the optimization problem is very difficult. Here, we tackle it by using a genetic algorithm. Genetic algorithms are a way to probabilistically search for an optimum regarding a predefined optimization criterion. The underlying model is borrowed from the evolution of living organisms. They operate by iteratively refining a fixed-size *population* of solution candidates, which are called *individuals*. In our case, an individual corresponds to a set of route choices: a specific driving route for each single car. These route choices are encoded in a bit field, termed the individual's *chromosome*.

The first generation of individuals is generated randomly. For all the individuals, the target function is evaluated; in the context of genetic algorithms, the value of the target function is also called *fitness*. A number of operations (selection, crossover, and random mutation) are then executed on the population, taking into account the determined fitness values. These operations generate new individuals forming a new generation. The intention is to preserve the beneficial properties of good individuals, while adding sufficient randomness in order to find yet better points in the optimization space.

Consequently, properties of individuals with high fitness values are more likely to end up in the newly generated individuals. The fitness of all individuals in the new generation is assessed again, and the process is repeated.

In order to encode the cars' route choices for an individual into a chromosome without generating a too complex solution space, we limit the number of possible route choices for each car to a fixed set of k alternative routes. This seems appropriate, since most routes that are theoretically conceivable (huge detours, routes with cycles,...) are not viable options anyway. We obtain the k path alternatives for a given car by an iterative penalty method [8]: Dijkstra's algorithm is applied k times. Initially, a road segment's cost is set to its length divided by the maximum allowed speed on the segment. Whenever a segment is used on a path, its weight is increased by multiplying it by a constant factor y. This makes the segment less likely to be chosen again on alternative routes. y has to be chosen in such a way that a segment is re-used only in cases where no suitable alternative exists. In the road network used in our evaluations, $y = 4$ has shown to give good results.

In a practice, one should choose k as a power of two (we use $k = 8$ here), so that the route choice for a car can be encoded in $\log_2 k$ bits, and each combination of bit values is a valid entry. Consequently, a chromosome is a bit string of length $z \cdot \log_2(k)$ bits. The bits $[(i-1) \cdot \log_2(k), \ldots, i \cdot \log_2(k)[$ represent the route choice for car c_i.

In order to obtain the resulting travel times of all cars in different configurations, we use the microscopic traffic simulator SUMO [9]. Before starting the optimization process, we once run a simulation where cars drive along their individually and independently chosen shortest paths. From this simulation run, we obtain the baseline travel time values $\widehat{T}_c$ used in the target function. During the optimization, in order to evaluate the fitness of a given individual, we run simulations in which cars choose the routes as determined by the chromosome under evaluation. Thereby we obtain the values T_c, so that we can determine the fitness according to (3). In order to reduce the simulation time per generation, our implementation distributes the simulations for assessing the individuals in a populations across the machines in a cluster.

The crossover operation generates new individuals for the next generation. To do so, it picks two candidates using the Roulette Wheel Selection method [10], which prefers individuals with good fitness. The chromosomes of these individuals are cut at a random point. By concatenating the left part of the first individual's chromosome and the right part of the second individual's, a new one is formed. After an individual has been sampled in this way, a mutation operation flips each bit in the chromosome with some probability (we use $p = 0.001$ here), causing random route changes for a small fraction of the cars.

V. Results

For our results presented here, we use a street map of the German city of Eichstädt grabbed from the OpenStreetMap [11] project. We imported it into SUMO using netconvert, SUMO's map conversion tool.

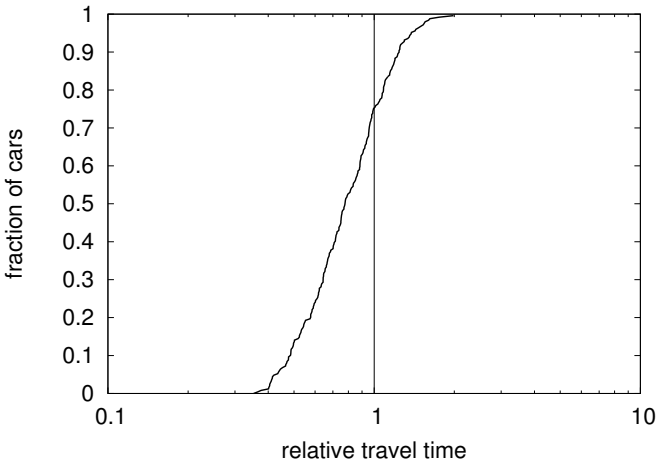


Fig. 1. CDF of the relative travel times in the congested scenario, after ten generations.

In order to test our methodology, we concentrated on two extreme cases. In both scenarios, the simulations include 250 cars, and we simulate a duration of 250 minutes. The scenarios differ in the distributions of the cars' starting times and their origin-destination pairs, though. In the congested case, scenario *A*, there is highly concentrated traffic, where all cars drive along the same route. Moreover, all cars enter the simulation close to its beginning, with 1 s fixed spacing. In the other case, scenario *B*, sources and destinations are chosen uniformly over the whole road network, and vehicles enter at uniformly distributed points in time. In this scenario, no congestion builds up and traffic flows smoothly even if each cars individually chooses the best route.

For the initial results presented here, we use a population size of 100 individuals for the genetic algorithm. On our machines, each simulation run takes ca. 5 min; distributed over six machines, an evolution over ten generations takes approximately 14 hours. The time for the operations of the genetic algorithm itself is negligible.

In Figure 1, we plot the per-car relative travel time gains in scenario *A* after ten generations. The plot shows the cumulative distribution of these values. As discussed above, values below one mean that the car has improved its travel time. As can be seen, this is the case for the majority of cars; improvements of up to 65 % are reached for individual cars. For some cars, the travel time deteriorates. This may indicate that a globally good solution indeed requires some cars to actually drive longer than if they entered the traffic jam. If this picture is confirmed once we obtained more results with our simulation methodology, an interesting research question arises: how could drivers be incentivized to voluntarily accept a deterioration, in order to improve the global outcome?

During the simulation we have found that the genetic algorithm converges very quickly to a virtually optimal point. The reason for this behaviour can be seen in the nature of this scenario: due to very high congestion, the possible travel speed

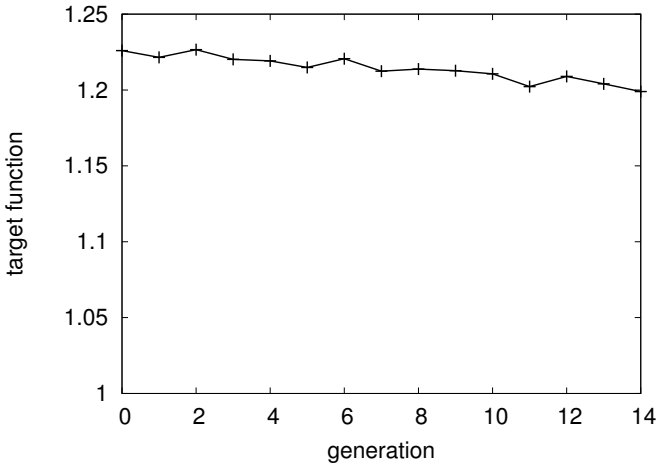


Fig. 2. Progress of the target function in the non-congested scenario.

on the shortest path gets so low that picking almost any other alternative route leads to an improvement in the cars' travel times. In fact, since alternative routes are virtually free (recall that all vehicles concentrate on the same origin-destination pair), a randomized choice between one of the k alternative paths distributes vehicles well and is thus not unlikely to yield a good result. This is just what happens when individuals for the first generation of the genetic algorithm are sampled—so, the existence of a very good individual from the very beginning is a likely event.

As one might expect, the results in the non-congested scenario B are quite different. Clearly, if there is no noteworthy congestion, there is not much optimization potential: if every car follows its individually calculated shortest path route, we will be very close to the optimal point. Therefore, it is to be expected that the target function converges to one over the generations. Indeed, we notice that the genetic algorithm does by far not as quickly converge to a stable level as in the congested scenario. In contrast to the congested situation, initial random choices may be expected to be quite far off the ideal—which is again just what we observe.

Figure 2 shows the progress of the target function over 14 generations. The y axis shows the target function of the best individual in the respective generation, which, slowly, moves towards the anticipated long-term limit of 1—which, in essence, means that each car will again choose its individually shortest path. Over the generations evaluated here, there is continuous improvement, but the results are still far off the ones obtained with individually optimized routes. Many cars are still worse off. Due to limited available computation time, we were not yet able to verify the long-term evolution, and leave this for future work.

VI. Discussion and Conclusion

In summary, the first results provided here clearly underline that the potential for optimization heavily depends on the traffic situation: if there is no substantial congestion, then very obviously the possible gain of coordinated route choices is close to zero. If, on the other hand, there is substantial congestion and if viable alternative paths are available, much can be gained. In this case, though, our observations corroborate the suspicion that a randomized choice between some reasonable route alternatives might indeed not be far off the optimal strategy. Moreover, our results already raise the problem how to deal with those drivers who's travel times increase—and a plethora of follow-up questions related to the acceptance of such route choices, or appropriate incentive or compensation mechanisms. Using our methodology, we now have the tools to assess these issues in more depth.

Our future work, consequently, will first focus on obtaining more results with larger simulation scenarios, more generations, different target functions, and a greater variety of different traffic situations. We plan to use computing clusters in order to simulate more complex city scenarios, like for instance the TAPASCologne scenario with realistic origin-destination matrices [12].

We also hope to learn about the structure of "good" route choices from our results. Even if our approach is not directly usable for route choices in real navigation systems—because it requires global knowledge, even about cars entering in the future—we intend to extract hints about how optimal routing can be done from a global systems perspective.

References

[1] P. E. Hart, N. J. Nilsson, and B. Raphael, "A formal basis for the heuristic determination of minimum cost paths," *IEEE Transactions on Systems Science and Cybernetics*, vol. 4, no. 2, pp. 100–107, 1968.

[2] T. Roughgarden, *Selfish Routing and the Price of Anarchy*. MIT Press, 2005.

[3] H. M. Kammoun, I. Kallel, A. M. Alimi, and J. Casillas, "Improvement of the road traffic management by an ant-hierarchical fuzzy system," in *CIVTS '11: Proceedings of the IEEE Symposium on Computational Intelligence in Vehicles and Transportation Systems*, Apr. 2011, pp. 38–45.

[4] Y. Shigehiro, T. Miyakawa, and T. Masuda, "Road traffic control based on genetic algorithm for reducing traffic congestion," *Electronics and Communications in Japan*, vol. 95, no. 4, pp. 11–19, 2012.

[5] M. Srinivas and L. Patnaik, "Genetic algorithms: a survey," *IEEE Computer*, vol. 27, no. 6, pp. 17–26, June 1994.

[6] S. M. Galib and I. Moser, "Road traffic optimisation using an evolutionary game," in *GECCO '11: 13th Annual Genetic and Evolutionary Computation Conference*, July 2011, pp. 519–526.

[7] O. Jahn, R. Möhring, A. Schulz, and N. Stier-Moses, "System-optimal routing of traffic flows with user constraints in networks with congestion," Massachusetts Institute of Technology (MIT), Sloan School of Management, Working papers 4394-02, 2004.

[8] V. Akgun, E. Erkut, and R. Batta, "On finding dissimilar paths," *European Journal of Operational Research*, vol. 121, no. 2, pp. 232–246, 2000.

[9] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz, "SUMO – simulation of urban mobility: An overview," in *SIMUL '11: Proceedings of the Third International Conference on Advances in System Simulation*, Oct. 2011.

[10] J. Zhong, X. Hu, M. Gu, and J. Zhang, "Comparison of performance between different selection strategies on simple genetic algorithms," in *CIMCA-IWATIC '05: Proceedings of the International Conference on Computational Intelligence for Modelling Control and Automation / International Conference on Intelligent Agents, Web Technologies and Internet Commerce*, Nov. 2005, pp. 1115–1121.

[11] M. Haklay and P. Weber, "Openstreetmap: User-generated street maps," *IEEE Pervasive Computing*, vol. 7, no. 4, pp. 12–18, Oct. 2008.

[12] "Tapascologne project," http://sf.net/apps/mediawiki/sumo/index.php?title=Data/Scenarios/TAPASCologne.

Privacy and Surveillance: Concerns About a Future Transportation System

David Eckhoff
Computer Networks and Communication Systems
Dept. of Computer Science, University of Erlangen, Germany
eckhoff@cs.fau.de

***Abstract*—Intelligent Transportation Systems (ITS) are envisioned as the next step in the evolution of road traffic. They are enablers for visionary technologies such as autonomic driving or traffic light free intersection handling. Furthermore drivers can directly benefit from them in the near future, as they are believed to improve road safety, increase the passengers' comfort and also reduce emissions through dynamic and more accurate route planning. The technology for this is currently being tested and standardized. But what are the drawbacks of such a system? In this article we look into the European and American systems and discuss privacy matters and to what degree they could turn into a surveillance system. We find that the possibilities to do so are manifold and without proper legal and technical aid. Building ITS can very well mean to build the infrastructure to aid an Orwellesque society.**

I. Introduction

According to the World Health Organization there were over 1.2 million road traffic fatalities (and 20-50 million non-fatally injured) in 2009, and even higher numbers have been announced for 2013 [1]. Passive safety systems such as airbags can only reduce this number to a certain degree, making active safety systems such as radars for pre-crash warnings more important.

One promising approach is to enable vehicles to communicate wirelessly to form vehicular networks. The ability of vehicles to communicate with each other and/or the infrastructure allows for many applications to increase road safety in general. By periodically sending the current position, speed, and heading receiving vehicles can automatically detect impending collision and therefore take precautionary steps and warn the driver. While safety is certainly the major advantage of these systems, drivers are envisioned to also benefit from other applications, e.g., dynamic route planning based on information collected by and received from other vehicles or even comfort systems such as video streaming or traffic light assistance systems [2].

Potential downsides of these Intelligent Transportation Systems (ITS) could be insufficient measures to protect drivers' location privacy, i.e., information about current and past whereabouts [3]. This can result to the disclosure of private information and thereby reduce the feeling of freedom of individuals.

It can be argued that it is even possible that these systems allow for overly restrictive law enforcement and thereby even affect the quality of life for the people in it, who may not even have a real choice whether to participate or not. In this article we want to pessimistically discuss possible issues that come with this technology by taking a closer look at the current version of the ETSI and WAVE standards upon which the operation of ITS in Europe, and the USA respectively, will be based.

The remainder of this paper is organized as follows: in Section II we outline why we believe that location privacy is important and is worthy of being protected. We then discuss current approaches and their efficiency as well as their applicability in vehicular networks (Section III). In Section IV we give an outlook on how ITS could be exploited for automated traffic supervision, followed by a discussion about the possibilities to reveal a driver's identity (Section V). We identify open challenges in the field of which we believe – if solved – can substantially help protect drivers' location privacy (Section VI). We conclude this article in Section VII.

II. The Necessity of Location Privacy

Economically, there is a large demand for personal data. Many online services that seem to be free of cost require the individual to disclose personal information in order to work. The users can then evaluate which is more valuable: the data they publish or the benefits they receive from the service, making privacy some kind of currency. So naturally, location privacy has a value attached to it and each person should be able to decide individually what that value is.

While in the industry there is a growing interest to collect personal information in order to generate profit, people seem to accept this and rather pay with their privacy instead of real money. Studies show that location information has only little value to many persons, and a majority of it would sell one month of location data to be used commercially for as little as US$ 35 [4], [5]. Furthermore, the desire of an individual not to be trackable by a third party does not seem to be too big as tracking is already done by mobile phone operators, even though some discuss selling customer location information to retailers.[1] This suggests that from a provider's point of view, preservation of location privacy might not be a critical feature for the design of ITS as it could not even have a significant impact on the financial success.

[1]The Spanish mobile phone operator Telefonica revealed plans to sell customer location information in Spain, England and Germany: http://www.bbc.co.uk/news/technology-19882647

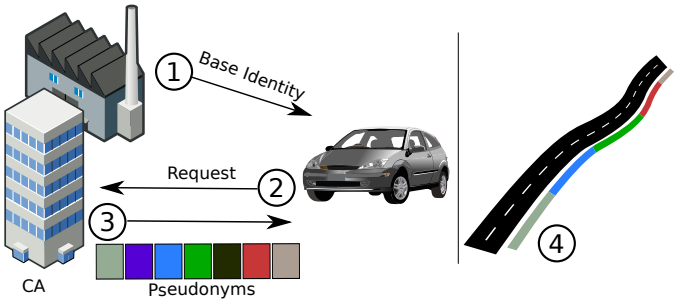


Figure 1. Principles of a PKI in vehicular networks: (1) The vehicle is pre-equipped with a base identity (2) The vehicle requests the signing of pseudonyms (3) The CA signs the pseudonyms if they have been created using the base identity (4) The vehicle uses the pseudonyms as its address.

Table I
EXCERPT FROM THE COOPERATIVE AWARENESS MESSAGE (CAM) [12] AND BASIC SAFETY MESSAGE (BSM) [13] FORMAT

field	comment
direction	direction of the vehicle
position	current (GPS) position
movement	current speed
acceleration	longitudinal and latitudinal acceleration
steeringWheelAngle	(optional) angle of the steering wheel
vehicleLength	length of the vehicle
vehicleWidth	width of the vehicle
exteriorLights	turn signals, headlights, etc.
pathHistory	a history of the last positions

In many cases, the choice not to use a location based service or to not reveal personal information to some service provider will preserve a user's (location) privacy to a certain degree. There is, however, a difference when it comes to vehicular networks as one of the benefits of these networks is safety, something that most users will probably value higher than location privacy. If ITS do not guarantee location privacy they all but force drivers to trade their location information for the sake of personal safety. This situation becomes worse, when Car-2-Car systems are mandatory for new vehicles as shown by tendencies in current discussions.

A violation of location privacy can lead to unwelcome effects – from obtrusive advertisements to disclosure of information that causes embarrassment or humiliation [6]. This disclosure of a person's location information can lead to the violation of other types of privacy. Knowing an individual visits the hospital three times a week could indicate a medical condition and, for example, make the person less interesting for potential employers. In order to avoid this a system has to provide anonymity, the precondition for location privacy. Anonymity is interpreted by Pfitzmann and Köhntopp [7] as the "state of being not identifiable within a set of subjects [...]". Only when an individual cannot be identified or re-identified, it can preserve its location privacy.

There have been numerous publications on methods and algorithms to preserve location privacy in vehicular networks. As the standardization progresses, it will be interesting to see which approaches will be realized and to what extent location privacy can be protected in ETSI ITS G5 and IEEE WAVE. In the following we examine the current progress and its implications on privacy for drivers. We also discuss how in a worst case scenario a surveillance society may exploit such a system.

III. LOCATION PRIVACY IN VEHICULAR NETWORKS

In both the European (ETSI ITS G5) and American (IEEE WAVE) systems, all vehicles will periodically emit broadcast messages including information about their current state. A small excerpt from the message format can be found in Table I. The frequency of these messages is envisioned to be at least 1 Hz and at most 20 Hz, depending on the current traffic situation.

To prevent unauthorized users from joining the network a Public Key Infrastructure (PKI) can be deployed. Vehicles have one pre-installed base identity which must never be used to sign messages, but is only used to generate or request pseudonyms from some kind of (possibly governmental) Certificate Authority (CA). Pseudonyms are also certificates and only valid when signed by the CA. Each vehicle maintains a pool of pseudonyms and uses them as its visible address, that is, to sign and send messages. A message is only valid if it has been signed with a pseudonym that was previously signed by the CA. While it would be beneficial for the anonymity of a driver to use a different pseudonym for each message, it would very likely compromise safety applications of other vehicles, as these can no longer link two messages to the same vehicle. Therefore, pseudonyms are only changed according to some pseudonym change strategy. A common approach is to change the pseudonym from time to time to complicate linking messages with different pseudonyms to each other and hence to prevent the tracking of vehicles.

While this approach does not allow unauthorized users to send valid messages, it does not preclude them from receiving and analyzing this data, because safety messages are not encrypted.

It was shown that pseudonym changes (even with high frequencies of 2 Hz) can be tracked without correlation of additional data [8], if a theoretical attacker was able to overhear all messages. Efficient countermeasures include random silent times, that is, not sending safety messages for a random amount of time after changing a pseudonym [9]. Another approach is context based pseudonym switching, that is, changing pseudonyms when it is believed to cause confusion for possible attacker, e.g. when vehicles with similar states (speed, direction) are close by [10], [11]. However, these approaches possibly interfere with safety applications and are therefore unlikely to be deployed.

Tracking becomes more difficult for an attacker when he is unable to overhear all messages but, for example, only monitors certain areas of a city. Once a vehicle leaves a monitored area and changes its pseudonym before it enters another one, there is good chance to avoid re-identification by an attacker [14]. However, data included in safety messages, such as vehicle

width and height could be used to correlate messages and therefore increase the chance to re-identify a vehicle. The more information a vehicle discloses, the easier it becomes to link two pseudonyms and therefore to track it. It is an open challenge to identify how often and which additional data can be included in messages to avoid this problem and how accurate it has to be to still allow proper operation of safety applications without making vehicles more or less unique. Because even if some data is marked *optional*, the decision whether to include this information will not be made by driver but by the on-board unit.

IV. Automated Surveillance

Even if pseudonyms cannot be linked to each other, the problem remains that each pseudonym can still be resolved to base identities by the authority that signed it, meaning that complete location privacy cannot be ensured.

Although there are different approaches to prevent this (pseudonym swapping [10], blind signatures [15]), they will likely not be a part of future ITS as they possibly violate accountability. It is therefore of utmost importance to lawfully control when and for what cause pseudonyms are allowed to be resolved, for example by the means of knowledge splitting, making it only possible to resolve a pseudonym when multiple institutions cooperate [16].

Accountability in ITS comes with the possibility to resolve a pseudonym to a single unique base identity and thereby to a certain vehicle. Theorteically, this not only allows the identification of vehicles that (deliberately or unintentionally) send false messages, the recovery of stolen vehicles, or the detection of hit-and-run offenses but could also change traffic supervision as we know it.

A vehicle that continuously broadcasts its current velocity will also do so when the driver is speeding. These messages could be received by provider operated road side units for automated ticketing. The formats of safety messages in both ETSI ITS G5 and WAVE make it possible to not only monitor speeding but basically almost all traffic offenses. Turning or lane changing without indication through a turn signal and the violation of traffic lights, right of way or stop lines can all be detected by only evaluating one or few periodic safety messages emitted from a vehicle for example by examining the *exteriorLights*, *pathHistory* or even *steeringWheelAngle* fields.

Tendencies in both academia and industry show that Car-2-X enabled vehicles will be equipped with both ad-hoc 802.11p-based and cellular radio technology, so even in scenarios where no road side unit is nearby to supervise traffic there are possibilities to detect traffic offenses. Receiving vehicles could act as *witnesses* and report traffic offenses directly to some kind of authority over the cellular link. If no cellular connection is available the vehicle could also follow a store-and-forward approach and report to a road-side unit once one is within transmission range. Based on the certainty of the report (potentially derived from the number of vehicles that observed the violation) the misbehaving vehicle could be fined.

We are well aware that from today's view such a scenario certainly seems far-fetched, however, ITS (as currently envisioned) give the operator or the government the ability to deploy these or similar methods in the future. These "features" will most likely not be part of ITS from the beginning, but once on-board-units are widely deployed or even legally mandated, the penetration rate of equipped vehicles will increase – making this kind of traffic supervision far more interesting for certain institutions.

V. Driver Identification

The aforementioned scenarios involve tracking and automated surveillance of vehicles, but not of drivers, that is, individuals. Automated ticketing presumably requires an almost certain identification of the driver or some kind of incontestable proof. Fortunately, this is not a trivial task. However, location information of drivers does not have these strict requirements to be of value. Instead, it suffices if the collected data is likely correct.

Usually, a vehicle is only driven by a very small set of persons, and by only looking at a two week GPS-trace it was shown that, with an accuracy of 60 m, the home address of the driver could be determined, as Krumm showed in 2007 [17]. He also showed that with a simple white page search this was enough to disclose the identity of a driver with an accuracy of 5 %. We expect that with today's presence of social networks this number would be much higher.

With the aid of additional knowledge such as home/work location pairs (city block granularity), Golle et al. were able to identify a large amount ($> 50\,\%$) of drivers [18]. Access to this data is widely available, not only to governmental institutions, but to a variety of parties. Customer location information can be obtained through location based services, social networks, synchronized address books, white pages or public data sets, and even by laws that allow registration offices to sell information on its residents.[2]

The more information can be correlated with a transmitting vehicle, the easier it becomes to identify the actual driver. For example, communicating personal devices such as mobile phones or tablet computers can be traced back to an individual. The use of location based services as well as payment systems that require user identification can also disclose the identity of the driver. More obviously, traffic or surveillance cameras can be directly used to clearly identify a driver and therefore serve as proof that a certain individual was in fact behind the steering wheel.

Lastly, advanced driver assistance systems, including their numerous sensors, are already discussed to be used beyond their main purpose, for example, as a countermeasure against vehicle related crime [19]. In a worst case scenario, fatigue warning systems or dash board cameras could be exploited to

[2]In Germany a law was passed that allows the sale of address data collected at registration offices for commercial purposes: http://www.dw.de/protest-grows-over-german-registration-law/a-16084893

identify drivers and make vehicles support what amounts to automated traffic surveillance.

VI. Open Challenges

In order to build privacy preserving ITS it has first to be fully understood how privacy measures affect other applications such as safety or comfort. Especially the privacy/safety trade-off needs to be investigated more closely to comprehend the exact requirements of safety applications and to draw a reasonable line at the amount and accuracy of information included in periodic safety messages.

On the other hand, it also needs to be easier to evaluate privacy in vehicular networks. Privacy metrics do not only have to be applicable, but also meaningful and easy to understand to allow for the comparison of different approaches, that is, the ability to decide whether one approach is *more private* than another. Furthermore, Open Source simulation frameworks to assess different algorithms are necessary for the integration of privacy methods in future ITS.

Finally, there has to be a stronger emphasis on privacy in ongoing standardization efforts, recommending practices for the technical protection of users' location information and measures to prevent institutions to easily access trusted data and resolve pseudonyms. Retrofitting privacy is bound to fail; therefore field operational tests all over the world should understand privacy as an integral part to serve as an example for future implementations.

VII. Conclusion

Communicating vehicles will change road traffic as we know it and help create Intelligent Transportation Systems. The fact that this technology is mostly beneficial is without controversy; however, certain implications of such a system may raise concerns.

In both ETSI ITS G5 and WAVE vehicles are envisioned to periodically transmit messages containing a considerable amount of information about the vehicle and its current state.

In this paper we showed that this can compromise the location privacy of drivers and that strict legal regulations are needed to control when and by whom this data can be accessed.

Theoretically, these periodic messages could even be used to deploy a fully automated traffic surveillance system and control drivers and vehicles in an overly restrictive fashion. The coverage and accuracy of such a surveillance system could be aided by a high penetration rate and the correlation of data from other systems.

As both families of standards are currently under development, we suggest that these issues are discussed to avoid building an infrastructure that could be exploited in the future. Institutions from both academia and industry should therefore address the open challenges in the field to enable the integration of applicable privacy measures before the roll-out phase, as retrofitting them afterwards is nearly impossible.

References

[1] World Health Organization, "Global Status Report on Road Safety: Time For Action," World Health Organization, Tech. Rep., April 2009. [Online]. Available: http://www.who.int/violence_injury_prevention/road_safety_status/2009/en/

[2] R. Braun, F. Busch, C. Kemper, R. Hildebrandt, F. Weichenmeier, C. Menig, I. Paulus, and R. Presslein-Lehle, "TRAVOLUTION – Netzweite Optimierung der Lichtsignalsteuerung und LSA-Fahrzeug-Kommunikation," *Strassenverkehrstechnik*, vol. 53, pp. 365–374, June 2009.

[3] F. Dötzer, "Privacy Issues in Vehicular Ad Hoc Networks," in *5th International Workshop on Privacy Enhancing Technologies (PET 2005)*, vol. LNCS 3856. Cavtat, Croatia: Springer, May 2005, pp. 197–209.

[4] D. Cvrcek, M. Kumpost, V. Matyas, and G. Danezis, "A study on the Value of Location Privacy," in *13th ACM Conference on Computer and Communications Security (CCS '06). 5th Workshop on Privacy in Electronic Society (WPES)*. Alexandria, VA, USA: ACM, October 2006, pp. 109–118.

[5] G. Danezis, S. Lewis, and R. Anderson, "How Much is Location Privacy Worth?" in *Fourth Workshop on the Economics of Information Security (WEIS'05)*, Cambridge, MA, USA, June 2005.

[6] B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," *Computer*, vol. 36, no. 12, pp. 135–137, December 2003.

[7] A. Pfitzmann and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity - a Proposal for Terminology," in *International Workshop on Design Issues in Anonymity and Unobservability*, ser. LNCS, vol. 2009. Berkeley, CA, USA: Springer, July 2000, pp. 1–9.

[8] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough," in *7th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS 2010)*, Kranjska Gora, Slovenia, February 2010.

[9] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing Wireless Location Privacy Using Silent Period," in *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, New Orleans, LA, March 2005.

[10] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "SlotSwap: Strong and Affordable Location Privacy in Intelligent Transportation Systems," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 126–133, November 2011.

[11] M. Gerlach and F. Guttler, "Privacy in VANETs Using Changing Pseudonyms - Ideal and Real," in *65th IEEE Vehicular Technology Conference (VTC2007-Spring)*, Dublin, Ireland, April 2007, pp. 2521–2525.

[12] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," ETSI, EN 302 637-2 V0.0.9, November 2012.

[13] SAE Int. DSRC Committee, "DSRC Message Communication Minimum Performance Requirements: Basic Safety Message for Vehicle Safety Applications," SAE, Draft Std. J2945.1 Revision 2.2, April 2011.

[14] L. Buttyán, T. Holczer, and I. Vajda, "On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs," in *4th European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS 2007)*. Cambridge, UK: Springer, July 2007.

[15] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for Conditional Pseudonymity in VANETs," in *IEEE Wireless Communications and Networking Conference (WCNC 2010)*. Sydney, Australia: IEEE, April 2010.

[16] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure Revocable Anonymous Authenticated Inter-Vehicle Communication (SRAAC)," in *4th Conference on Embedded Security in Cars (ESCAR 2006)*, Berlin, Germany, November 2006.

[17] J. Krumm, "Inference Attacks on Location Tracks," in *5th International Conference on Pervasive Computing (PERVASIVE 2007)*, ser. LNCS, vol. 4480. Toronto, Canada: Springer, May 2007, pp. 127–143.

[18] P. Golle and K. Partridge, "On the Anonymity of Home/Work Location Pairs," in *7th International Conference on Pervasive Computing*, ser. LNCS, vol. 5538. Nara, Japan: Springer, May 2009, pp. 390–397.

[19] P. Knapik, E. Schoch, M. Müller, and F. Kargl, "Understanding Vehicle Related Crime to Elaborate on Countermeasures based on ADAS and V2X Communication," in *4th IEEE Vehicular Networking Conference (VNC 2012)*. Seoul, Korea: IEEE, November 2012, pp. 86–93.

A Study on Highway Traffic Flow Optimization using Partial Velocity Synchronization

Markus Forster, Raphael Frank, Thomas Engel
Interdisciplinary Centre for Security, Reliability and Trust,
University of Luxembourg, 1359, Luxembourg
firstname.lastname@uni.lu

***Abstract*—In this paper we present a study of highway traffic flow optimization using Partial Velocity Synchronization (PVS). PVS is a *Cellular Automaton* (CA) model that is extended by a communication layer providing the ability to exchange relevant information between vehicles. We show that it is possible to enhance traffic flow on highways significantly with a small number of velocity recommendations computed from the traffic conditions ahead. Furthermore we show that only a limited number of hops in an information chain is necessary to reschedule the vehicles on a given highway segment to avoid the formation of shockwaves. Our results show that traffic flow will be increased while travel time and emissions will be reduced dramatically.**

***Index Terms*—Traffic Modeling, Congested Flow, Cellular Automaton, Vehicular Ad Hoc Networks**

I. Introduction

Over recent decades, traffic demand on highways has increased significantly and is still doing so. In many regions the existing infrastructure has reached a capacity limit and cannot be extended easily [1]. This results in more and more drivers being stuck in congestion, causing billions of dollars worth of economic and ecological damage [2]. Besides the time loss, frequent switching between acceleration and deceleration makes driving very tedious and wastes energy as well increasing emissions.

In this paper we present a study on a new *Advanced Driver Assistance System* (ADAS) that is extended by a *Vehicular Ad Hoc Network* (VANET) to propagate additional information upstream in the traffic flow with the ability to react much earlier than is possible by relying solely on information from within the line of sight. The protocol presented here can be used to set individual speed limits. Compared to a spatially-fixed system such as information panels a more dynamic velocity adaptation is possible.

The simulations are performed on the basis of a *Cellular Automaton* (CA) model that is extended by a communication layer. The new protocol, *Partial Velocity Synchronization* (PVS), aims to give non-intuitive velocity recommendations to drivers to prevent shockwaves from forming and to reduce the formation of *phantom jams*. We show that only a small number of velocity recommendations is necessary to redistribute the upstream traffic in a way that can disperse congestions before the traffic inflow arrives.

The remainder of this paper is organized as follows. In Section II we describe the base model and our extension. In section III, we discuss the results obtained from the simulations. Finally, a conclusion is drawn in Section IV.

II. Partial Velocity Synchronization

This section provides an overview of the *Partial Velocity Synchronization* (PVS) protocol. For a complete description please refer to the original paper [3]. PVS is an extension of the well-established *Velocity Dependent Randomization* (VDR) model [4]. It specifies a communication channel between vehicles to enable the transfer of recent traffic metrics.

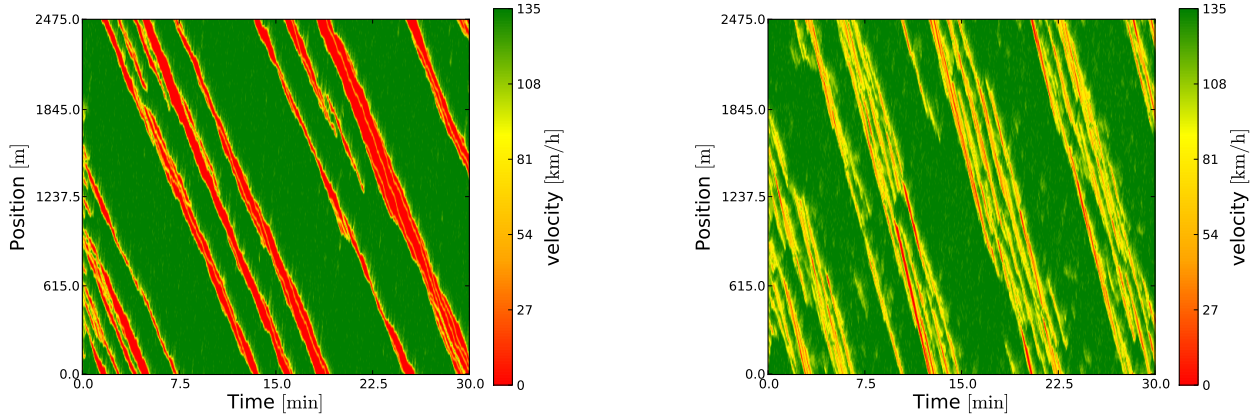
The VDR model is a *Cellular Automaton* (CA) model based on simple rules, executed in fixed time steps. This models are particularly applicable for highway traffic. The most popular model in this class is the *Nagel-Schreckenberg* (NaSch) model, introduced by Kai Nagel and Michael Schreckenberg [5].The VDR model is based on the NaSch model but extends it with a probabilistic factor to represent the human tendency to dally. More precisely, this tendency is represented by a probabilistic factor that depends on the actual velocity. In fact only two cases are distinguished, namely a moving driver having a much lower probability of dallying (p_m) compared to a stationary one (p_s). This probabilistic extension is necessary to model the so-called *phantom jams* that are caused mainly by human inefficiency [6]. The model equation for driver inattention depends on the actual velocity:

$$P_d(v_\alpha(t)) := \begin{cases} p_s & \text{if} v_\alpha(t) = 0 \\ p_m & \text{else} \end{cases} \quad \text{where } p_m \ll p_s \qquad (1)$$

The main principle of these traffic models is to ensure collision-free driving. In the VDR model this is ensured by the fact that drivers will adapt their velocity to the preceding vehicle if its distance is less than would be covered at the demanded velocity in the next time-step. This implies, however, that the maximum distance for reactions and hence the line of sight is given by the maximum allowed velocity.

The communication channel introduced with PVS extends the awareness horizon of the motorists far beyond the line of sight. The objective of the protocol is to use the additional information to redistribute the traffic upstream in such a way that the already decelerating or stationary vehicles will have enough time to leave the critical region downstream before the new inflow arrives.

In practice, the communication protocol adds two new rules to the VDR model, namely *notification* and *anticipation*:



(a) Space-Time diagram for VDR

(b) Space-Time diagram for PVS

Fig. 1: comparison of space-time diagrams for 330 cells and $\rho = 33$ vehicles/km

a) Notification: A vehicle that has to decelerate, or is not allowed to accelerate, under the rules of the VDR model, sends a message m upstream to the following vehicle containing its actual position $x_\alpha(t)$, the actual time t and velocity $\hat{v}(t)$. A modification to this rule is that vehicles with velocities less or equal to 1 km/h always send this message, which is given by the vector:

$$m_\alpha(t) = [x_\alpha(t), t, \hat{v}_\alpha(t+1)]$$

b) Anticipation: Vehicles receiving the *notification* message from the preceding vehicle calculate an anticipated velocity as follows:

$$v_{\alpha,\mathrm{ant}}(t+1)^{(1)} = \max\left[\lceil (d_\alpha(t) + \hat{v}_{\alpha+1}(t))/2 \rceil, 1\right] \qquad (2)$$

where $v_{\alpha,\mathrm{ant}}(t+1)$ is the anticipated velocity considering the estimated distance $d_\alpha(t)+\hat{v}_{\alpha+1}(t)\cdot\Delta t$ to the preceding vehicle $\alpha+1$ after its current move. The multiplication by the time-step Δt can be ignored because it is generally set to $1s$. If the anticipated velocity is smaller than the desired velocity (by VDR rules) the system notifies the driver to adapt his velocity to $v_{\alpha,\mathrm{ant}}(t+1)$.

Algorithm 1 PVS model algorithm

```
1: procedure PVS( )
2:     p=P_d(v_α(t))
3:     d(t) = x_{α+1}(t) − x_α(t) − 1
4:     v_α(t+1) = min(v_α(t)+1, v_max, d(t))
5:     if RECEIVE( ) then
6:         v_{α,ant}(t+1) = max(⌈d(t) + v_{α+1}(t)/2⌉, 1)
7:         v_α(t+1) = min(v_{α,ant}(t+1), v_α(t+1))
8:         p = P_d(κ(t), v_α(t))
9:     end if
10:    if RANDOM(0,1)≤ p then
11:        v_α(t+1) = v_α(t+1) − 1
12:    end if
13:    if v_α(t+1) < v_α(t) ∨ v_α(t+1) ≤ 1 then
14:        SEND(v_α(t+1))
15:    end if
16: end procedure
```

The idea is to adapt the actual velocity to cover half of the estimated distance after the current step. This must be done to ensure a minimal distance that allows one additional move considering the worst case, namely that the preceding car stops immediately in the next time step.

Further, we extend the velocity-dependent randomization function to take into account two input parameters, namely the velocity $v_\alpha(t)$ and an action event parameter $\kappa(t) \in \{0, 1\}$. Two states are possible for $\kappa(t)$: 0 if no message is received, and 1 otherwise.

$$P_d(\kappa(t), v_\alpha(t)) = \begin{cases} p_n & \text{if } \kappa(t) = 1 \\ P_d(v_\alpha(t)) & \text{else} \end{cases} \qquad (3)$$

where p_n is the probability of dallying for a notified motorist. It holds true that $p_n < p_m \ll p_s$.

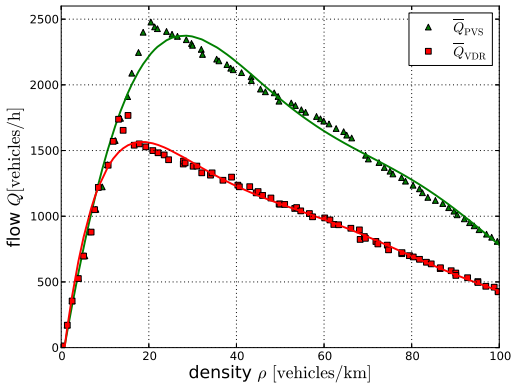
The PVS protocol is designed to improve the actual situation on highways. This means that we have to deal with humans and their imprecision. Although PVS is intended to be an *Advanced Driver Assistance System* it is also applicable to fully-autonomous vehicles, which are accommodated by setting the probabilistic factors to zero, resulting in completely deterministic behavior.

The model behavior for one vehicle performing a distinct simulation round is given as pseudo code in Algorithm 1. For more information we refer to our original paper [3].

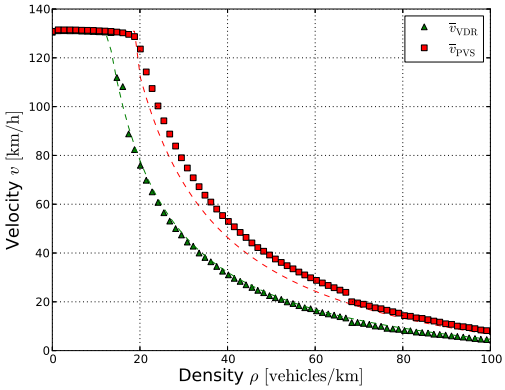
III. Evaluation

In the simulations performed, only single-lane traffic has been considered. Furthermore, the simulated traffic environment is a closed loop, meaning there are neither inflows nor outflows to disturb the simulated traffic. These constraints, as a first step, allow us to investigate an upper bound for traffic flow optimization.

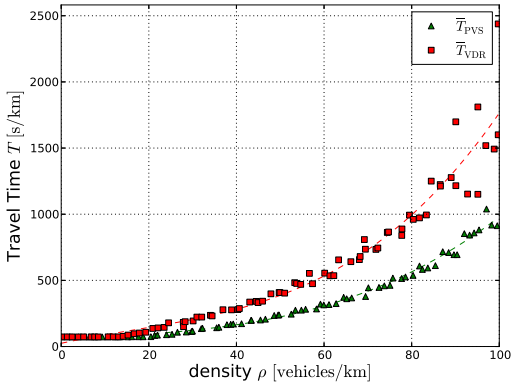
The simulation parameters are as follows:
The cell size is $|x_\alpha| = 7.5$ m, which represents the standard length of a vehicle plus a safety gap. For all simulation runs, the length of the observed road segment is given as $L = 1330$ cells $= 9.75$ km. The maximum allowed velocity



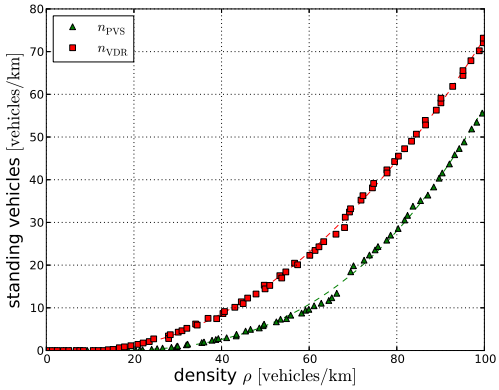
(a) flow-density diagram



(b) average velocities VDR vs. PVS



(c) average travel-time



(d) number of non-moving vehicles

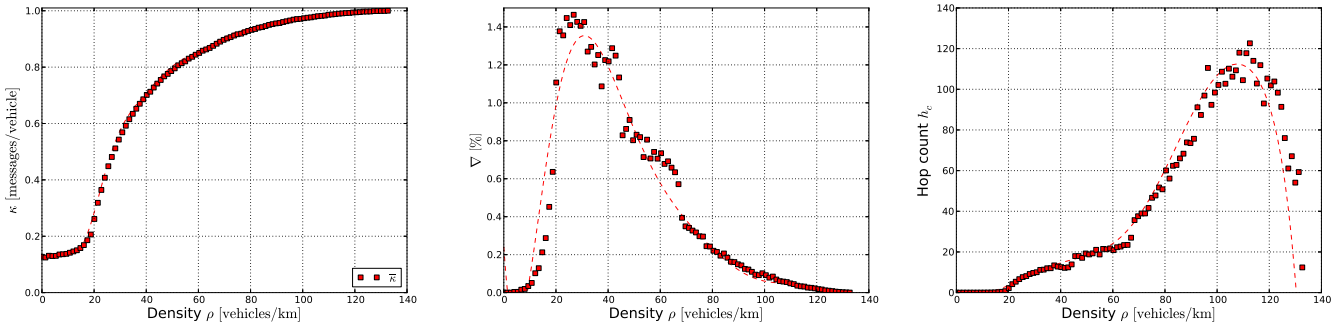
Fig. 2: Comparison of macroscopic results for VDR versus PVS

is set to $v_{\max} = 5$ cells/s ≈ 135 km/h. Simulations where performed for densities starting at $\rho = 1$ veh/km up to $\rho = 134$ veh/km and statistical values are taken from 10800 simulation rounds for each density, resulting in an overall simulation time $T_{\mathrm{overall}} = 300$ h. The probabilistic values for human behavior are set to $p_n = 0.05$, $p_m = 0.15$ and $p_s = 0.5$. This means that a motorist alerted by PVS has a probability of 5% of not obeying the recommendation. The other probabilistic factors state that a moving driver tends, with a probability of 15%, to dally whereas a stationary one has a probability of 50% not to accelerate even if he could.

Figure 1 represents the velocity distribution on a time-space diagram for a constant overall density $\rho = 33$ vehicles/km. The red zones in Figure 1a depict the propagation of the slowdowns upstream, whereas with Figure 1b it becomes obvious that the strategy of PVS almost completely absorbs the shockwaves and so limits the number of slow-downs. There are still congested regions, but nearly no standing vehicles. One major result is that the traffic is better distributed over the available road section, so avoiding unnecessary decelerations and accelerations.

Figure 2 depicts comparisons of flow density, average velocity, average travel time and average number of non-moving vehicles for simulations with the VDR model versus the PVS model for single-lane traffic. The graphs can be divided into two distinct regions, where the first, reaching from zero density to the inflection point of the flow-density diagram is called the *free-flow phase* and the region thereafter is called the *congested phase*. The metastable branch of the VDR model in Figure 2a is caused by two completely different behaviors in the same density regions [4], [7]. This is caused by the fact that inflow to, and outflow from, congested areas are controlled by different probabilities. The results of the average velocity (Figure 2b) and travel time (Figure 2c), clearly show that we are able to increase the average speed and hence reduce the average time needed to pass the given road segment by up to 30%. In Figure 2d we see that with PVS we also have up to 60% fewer standing vehicles and for densities below 40 vehicles/km there are nearly none.

In Figure 3 some properties of the proposed PVS message protocol are shown. Like the graphs for the macroscopic traffic metrics, given in Figure 2, the results for the messages can be divided into two branches. These segments are the *free-flow phase* before the inflexion point, and the *congested phase* thereafter. The information hop-count, given in Figure 3c, is the average length of a continuous velocity



(a) messages per vehicle (b) recommendations per vehicle and message (c) hop-count.

Fig. 3: Communication Protocol evaluation

recommendation chain upstream against density. This means the value is increased if a vehicle receives a message from the preceding vehicle and computes the necessity for a velocity recommendation to the driver and of whether to send the information further upstream. Figure 3a depicts the average number of messages per vehicle over density. In the free-flow phase, there are nearly no messages emitted and hence, the driver receives no recommendations and the information hop-count is zero. The average number of broadcast messages per vehicle increases asymptotically towards 1 very rapidly. Due to the increasing density, more vehicles have to perform a braking maneuver, releasing a message. In the region of maximal density only a very low number of vehicles are able to move because only a low number of cells are not occupied. In this situation nearly every road user broadcasts a message. The number of recommendations per vehicle and message (Figure 3b) jumps from zero to 1.4% at the inflexion point and remains stable until approximately one third of the maximum density. This region is to be considered the sensitive range of the PVS protocol. The decrease in recommendations after this point is caused by the shortening of distances between vehicles with increasing density. This means that most decelerations happen within drivers' awareness horizon. They are controlled by the deceleration rule of the VDR model itself and are not triggered by a PVS recommendation.

IV. Conclusion

In this paper we show that it is possible to set up an *Advanced Driver Assistance System* (ADAS) with limited network capabilities, provided by a VANET, to increase traffic flow as well as the average travel velocity and so reduce average travel-time and emissions.

A system based on *Partial Velocity Synchronization* (PVS) will be able to provide individual velocity recommendations to motorists (or operate in a fully automated vehicle) to avoid hard braking maneuvers. This will certainly improve driving convenience and road safety. Another advantage of such a system will be the reduction of fuel consumption and all its drawbacks.

Though the use of *Partial Velocity Synchronization* (PVS), only a low number of velocity recommendations are adequate to improve highway traffic flow significantly. Distributing only relevant traffic information upstream in the traffic flow over a limited number of hops is sufficient to redistribute the approaching traffic such that forming shockwaves can be absorbed.

Future work will focus on the proportion of the participants needed to achieve a significant improvement in highway traffic flow.

Acknowledgment

The authors would like to thank the National Research Fund of Luxembourg (FNR) for providing financial support through the CORE 2010 MOVE project (C10/IS/786097).

References

[1] M. Shinkman, M. Buchanan, and E. I. U. G. Britain), *Driving change: how policymakers are using road charging to tackle congestion*. The Economist Intelligence Unit, 2006. [Online]. Available: http://books.google.lu/books?id=1dW3HAAACAAJ

[2] Schrank, D. and Lomax, T. and Eisele, B., "2011 Urban Mobility Report," http://tti.tamu.edu/documents/mobility-report-2011.pdf, Last Accessed in February 2012.

[3] M. Forster, R. Frank, M. Gerla, and T. Engel, "Improving Highway Traffic through Partial Velocity Synchronization," *2012 IEEE Global Communications Conference (GLOBECOM)*, pp. 5795–5800, December 2012.

[4] R. Barlovic, L. Santen, A. Schadschneider, and M. Schreckenberg, "Metastable states in cellular automata for traffic flow," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 5, no. 3, pp. 793–800, 1998. [Online]. Available: http://www.springerlink.com/index/CAKA40V8B9Q41XQJ.pdf

[5] K. Nagel and M. Schreckenberg, "A cellular automaton model for freeway traffic," *Journal de Physique I*, vol. 2, no. 12, pp. 2221–2229, 1992. [Online]. Available: http://hal.archives-ouvertes.fr/docs/00/24/66/97/PDF/ajp-jp1v2p2221.pdf

[6] C. J. M. Tampère, S. P. Hoogendoorn, and B. Van Arem, "A Behavioural Approach to Instability, Stop and Go Waves, Wide Jams and Capacity Drop." *Proceedings of the 16th International Symposium on Transportation and Traffic Theory*, pp. 205–228, 2005. [Online]. Available: http://www.mech.kuleuven.be/cib/verkeer/dwn/pub/P2005F.pdf

[7] A. Schadschneider, "Cellular Automaton Approach to Highway Traffic: What do we Know?" pp. 19–34, 2009. [Online]. Available: http://www.springerlink.com/index/u881651358378j51.pdf

Misbehavior Detection in Vehicular Ad-hoc Networks

Rens van der Heijden, Stefan Dietzel, Frank Kargl
Institute of Distributed Systems
University of Ulm, Germany
{rens.vanderheijden, stefan.dietzel, frank.kargl}@uni-ulm.de

In this paper we discuss misbehavior detection for vehicular ad-hoc networks (VANETs), a special case of cyber-physical systems (CPSs). We evaluate the suitability of existing PKI approaches for insider misbehavior detection and propose a classification for novel detection schemes.

Cyber-physical systems (CPSs) are digital systems that are closely embedded into the physical world with which they interact through sensors and actuators. In contrast to classical embedded systems, they often form networks with a large number of sensor or actuator devices. These devices sense information, process it in a distributed system, and then influence the physical world using actuators. Notable examples of CPS are wireless sensor networks (WSNs), smart factories, distributed e-Health systems, and VANETs. In this paper, we focus on VANETs, which are a prime example for CPS and will soon be deployed on a large scale.

Vehicular ad-hoc networks (VANETs) are networks that are created by equipping vehicles with wireless transmission equipment. VANETs offer great potential to improve road safety and to provide information and entertainment applications for drivers and passengers. Due to the unique properties of VANETs, this type of network has attracted many researchers, including those in the domain of security. The security challenges in VANETs include the requirement for strong privacy, the computationally constrained environment, and the ephemeral nature of connectivity.

VANETs and other CPSs share a number of characteristics that require fundamentally new approaches for security, which differ from existing IT security requirements.

- **Critical usage scenarios.** CPSs often control systems where failure or malfunction may have severe consequences, including massive financial loss or loss of lives. Often, these systems fall under the term critical infrastructures (CI). VANETs are one example where failure or malfunction may lead to massive congestion with subsequent delays and financial losses or even to accidents with loss of lives in a worst case.
- **No clear security perimeter.** In many of these systems, there is no clear boundary between insiders and outsiders. Instead, the logically and physically distributed nature of CPSs leads to unclear security perimeters and possible insider attacks. VANETs are again a core example, as such networks are cooperatively formed by vehicles and road-side equipment. As vehicles are under distributed ownership and control, it needs to be assumed that some of the vehicles are under full control of attackers.
- **Limited physical security.** As nodes in CPSs are often distributed in a potentially hostile environment, they may be subject to hijacking, analysis, and reprogramming by attackers. Due to cost constraints, the protection against such hijacking is often limited. A typical example is a Wireless Sensor Network for environmental monitoring, where nodes may be scattered randomly in the environment. Due to the long lifetime of vehicles, similar challenges can be found in both VANETs and in-vehicle networks.
- **Sensor values as security assets.** The primary security assets in CPS are the sensor values and the actuators controlled based on this input. Spoofing and manipulation of sensor data are thus primary attack vectors. For instance, in a VANET that is used for detecting traffic jams, an attacker may want to suppress certain sensor readings that would indicate a traffic jam, or inject sensor values that indicate a traffic jam where none exists.

In summary, CPSs, and VANETs in particular, will likely attract attackers that try to manipulate sensed data and influence the resulting actions taken by the system. Such attackers may participate as regular network entities either because attackers can easily join the VANET or hijack already participating nodes. Once an attacker has entered the VANET, she can easily inject spoofed infor-

mation into the VANET and trigger incorrect behavior. From the perspective of the VANET, this attacker can be seen as a misbehaving node that is sending incorrect data. In addition to information injection and manipulation, other attack types are conceivable, such as compromising routing efficiency by not forwarding information for other nodes. In this paper, we focus on detection of information manipulation. Note we cannot necessarily distinguish whether information manipulation is due to malicious intent or due to faulty hardware. However, from an information quality perspective, the resulting countermeasures should arguably often be the same.

Classical IT security mechanisms, like encryption, signatures, access control, (signature-based) intrusion detection systems, and so forth, are not suitable to thwart such insider attacks. Instead, we need security mechanisms that can identify misbehavior, identify the misbehaving node, and react either by filtering out the incorrect data or excluding the misbehaving node from further participation in the VANET. Research on security in VANETs has already developed several novel ideas for these tasks, many of which align with the goals of other CPSs.

Golle et al. [1] propose a method to detect misbehavior as we defined it above in the context of VANETs. Instead of placing *trust* in nodes – as often done by classical cryptographic authentication mechanisms –, the proposed approach is to gain *confidence* in correctness of data by analyzing the local information base and deriving most probable explanations. During the following years, more research was done that proposes comparable misbehavior detection mechanisms for VANETs. Examples of these include [2], [3], [4], [5], [6], [7], and [8].

There are fundamentally different approaches to misbehavior detection that can be used for a categorization of different mechanisms as shown in Figure 1. A first distinction is whether mechanisms focus on data values contained in messages or on the node sending the messages. *Node-centric* mechanisms require authentication mechanisms to reliably distinguish between different nodes. Many systems achieve this by assuming a trusted third party like a PKI that issues credentials, which are then used to authenticate messages and the corresponding information, using a security mechanism like digital signatures. Node-centric mechanisms can further be divided into *behavioral* and *trust-based* mechanisms.

Behavioral mechanisms inspect a node's observable behavior (but not the information it is sending) and try to derive a metric that identifies how well a node behaves. For instance, a behavioral mechanism may inspect rates at which a neighboring node sends packets and decide whether a node significantly exceeds a "normal rate,"

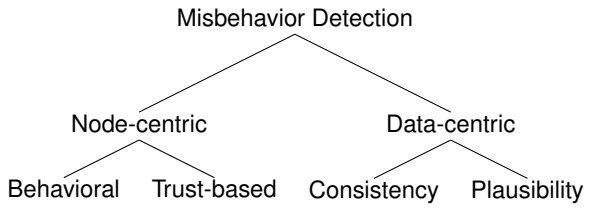


Fig. 1. Taxonomy of misbehavior detection.

which would then be considered as misbehavior. This approach is particularly common in WSNs, and is sometimes referred to as a Watchdog mechanism. However, attempts have been made to distribute these ideas in such a way that the need for a trusted node is removed, with the goal that a Watchdog mechanism can be used in VANETs [9].

On the other hand, *trust-based* mechanisms inspect the past and present behavior of a node and use this to derive a probability for future misbehavior. The assumption is that a node who behaved correctly in the past is more likely to behave correctly in the future. Essentially, this boils down to some form of reputation management scheme where correct behavior increases the reputation while misbehavior reduces it. These mechanisms are commonly used for reporting and local revocation of nodes in a VANET, for example through LEAVE [10].

In contrast to those node-centric mechanisms, the second major category, namely *data-centric* misbehavior detection, subsumes all mechanisms that directly inspect the disseminated information to detect potential misbehavior. While *data-centric* mechanisms do not primarily care about the identities of individual nodes, they often still require some form of linking between messages to be able to reliably distinguish between different hosts. However, these mechanisms do not depend on the linkability of messages, which makes them highly valuable for the detection of Sybil attacks. Sybil attacks are a type of attack where a node replicates itself arbitrarily to undermine the honest majority assumption. Due to the strong privacy requirements in VANETs compared to other cyber-physical systems, which makes linkage between different messages more difficult, concerns for Sybil attacks are particularly relevant. In response to this, many VANET researchers have developed novel schemes to perform data-centric misbehavior detection; these can be divided further into *consistency* and *plausibility* mechanisms.

Of these two types, *consistency* mechanisms rely more strongly on protection against sybil attacks. The purpose of consistency mechanisms is to compare measurements from different entities to detect and, where possible, resolve conflicts between these measurements. For in-

stance, in a VANET, a single vehicle could report a severe traffic jam while other vehicles report free flow of traffic. A consistency-based mechanism would use such information to conclude that there is likely no traffic jam and that the single vehicle may have misbehaved or be faulty.

Finally, *plausibility* checking mechanisms are all mechanisms that have some implicit or explicit model of the real world and check whether incoming information is plausible within this model. For instance, in VANETs, speed reports of 700 km/h are not very plausible and may be filtered out. However, plausibility should be applied with caution in VANETs, as part of the focus of such networks is to detect outliers that indicate important, but rare, events, such as collisions between vehicles.

Note that no single mechanism alone will likely provide a convincing misbehavior detection mechanism that detects all forms and types of misbehavior. Instead, mechanisms will likely be combined. For instance, consider the following as an example for a combined approach. First, a number of data-centric mechanisms work on the same knowledge base to jointly detect incorrect data. Results are then augmented using behavioral mechanisms that check whether nodes behave according to protocol specifications. All these mechanisms are then used as input to a node-centric reputation management system that determines whether nodes show long-term misbehavior. These misbehaving nodes can then be reported to a central authority, which can determine whether nodes should be removed from the network; meanwhile, the nodes can be revoked temporarily by the nodes that detected the misbehavior. In the case of VANETs, the latter is particularly important, as this provides protection against determined attackers that may not be discouraged by high fines.

Based on our categorization, we are currently preparing a broad literature study on misbehavior detection in both VANETs and other CPSs. Our goal is to identify general patterns for misbehavior that work across specific application domains and scenarios, and can be re-used for a generic misbehavior detection architecture. This will allow application of security mechanisms developed for VANETs to be applied to a broader spectrum of problems, and could lead to security mechanisms developed for other CPSs to be applied to VANETs, furthering the safety and security of both.

REFERENCES

[1] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. Philadelphia, PA, USA: ACM, 2004, pp. 29–37.

[2] N. Biß meyer, J. Njeukam, J. Petit, and K. M. Bayarou, "Central misbehavior evaluation for VANETs based on mobility data plausibility," in *Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications - VANET '12*. New York, New York, USA: ACM Press, 2012, pp. 73–82.

[3] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. J.-P. Hubaux, "On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks," in *2008 IEEE INFOCOM - The 27th Conference on Computer Communications*. Ieee, Apr. 2008, pp. 1238–1246.

[4] J. Grover, V. Laxmi, and M. Gaur, "Misbehavior detection based on ensemble learning in vanet," in *Advanced Computing, Networking and Security*, ser. Lecture Notes in Computer Science, P. Thilagam, A. Pais, K. Chandrasekaran, and N. Balakrishnan, Eds. Springer Berlin / Heidelberg, 2012, vol. 7135, pp. 602–611.

[5] H. Stübing, J. Firl, and S. A. Huss, "A two-stage verification process for Car-to-X mobility data based on path prediction and probabilistic maneuver recognition," in *2011 IEEE Vehicular Networking Conference (VNC)*. IEEE, Nov. 2011, pp. 17–24.

[6] J. Hortelano, J. Ruiz, and P. Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in vanets," in *Communications Workshops (ICC), 2010 IEEE International Conference on*, may 2010, pp. 1 –5.

[7] M. Mahmoud and X. Shen, "Stimulating cooperation in multihop wireless networks using cheating detection system," in *INFOCOM, 2010 Proceedings IEEE*, march 2010, pp. 1 –9.

[8] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of the 4th Workshop on Vehicle to Vehicle Communications (V2VCOM 2008)*, 2008.

[9] Z. Li, C. Chigan, and D. Wong, "AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs," in *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*. IEEE, 2008, pp. 1–6.

[10] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-p. Hubaux, "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

Open Issues in Inter Vehicle Communication and the Question: How to Address Them?

Bernhard Kloiber
Institute of Communication and Navigation
German Aerospace Center (DLR)
82234 Wessling, Germany
Email: bernhard.kloiber@dlr.de

***Abstract*—Despite intensive research activities on the field of Inter Vehicle Communication (IVC) for quite some time, a lot of open issues still remain. Some of them are of fundamental importance, some require high urgency and others will only show up one day in the future.**

In this paper we introduce three relevant problems in IVC: *evaluation metrics*, *downward scalability* and *upward scalability*. We map these problems according to the type of issue and we present concepts how these issues are addressed by DLR.

I. Introduction

Future vehicular safety applications depend on reliable information exchange in cooperative Vehicular Ad-hoc NETworks (VANETs). Although the vehicular communication standard in Europe called ITS-G5 [1], which is based on IEEE 802.11(p) [2], has been adapted to the challenging vehicular environment, it has not been adapted to the stringent communication requirements imposed by vehicular applications.

The most common VANET applications by now are based on the exchange of Cooperative Awareness Messages (CAMs) [3] or Decentralized Environmental Notification Messages (DENMs) [4]. Since CAM based applications are dependent on up-to-date information about the status of the neighbouring vehicles, a reliable 1-hop broadcast is required to provide correct application functionality. For DENM based applications it is important to disseminate information about a certain event to all relevant vehicles in time. Since the event is not necessarily located within the immediate vicinity, a reliable multi-hop dissemination is required to make these type of applications working correctly.

The following sections shortly describe three types of important open issues in inter vehicle communications and how they are addressed by DLR.

II. Evaluation metrics

The fist problem arising is a *fundamental* one: how to analyse and evaluate the communication performance correctly? As the requirements of vehicular applications have changed completely, the default metrics like throughput, latency, packet delivery/loss ratio, etc. are no longer suitable for evaluating the applications reliability. As introduced above, the dissemination of information is the key objective of current vehicular applications. Hence, new information-centric metrics are required, which are able to analyse the reliability of vehicular applications from a communications perspective.

In a first step, we are focusing on CAM based safety applications. They make use of established knowledge about the surrounding environment by receiving CAMs from other vehicles in the vicinity, usually referred to as *Cooperative Awareness*. The more frequently CAMs are received, the more up to date the information about the appropriate vehicles is, which is also known as *Awareness Quality*.

The Awareness Quality is time as well as space dependent and typically varies from application to application. From an information-centric point of view, its behaviour in time is similar to the behaviour of an information fusion filter, regarding the Prediction step and the Update step: As long as a CAM is not received, the vehicle's state can be predicted by using an appropriate prediction model. When a CAM is received, the prediction is updated again, using the information provided by the received CAM. Since prediction adds uncertainty to the current status information and hence reduces the Awareness Quality, each update step typically reduces the uncertainty, which in turn improves Awareness Quality.

As the Awareness Quality heavily depends on the used information fusion filter, the *Update Delay* - also known as *Packet Inter Arrival Time* [5] - on network-level can be analysed. The Update Delay principally represents the duration of the prediction step between two consecutive update steps for estimating the Awareness Quality. Hence, a strong correlation between these two metrics exists.

However, the exact mapping between Update Delay on network level and Awareness Quality on application level is a complicated task and still up to future work.

Another important aspect is the representation of metrics. In just presenting average values a lot of information is getting lost. We prefer to present the Update Delay as a *Complementary Cumulative Distribution Function (CCDF)* which keeps all the information gathered from the measurements. Further details on that can be found in [6].

III. Upward scalability

The *scalability problem* is well known within the VANET community. It typically shows in a degradation of the communication performance, if the number of transmitting vehicles is increased and so the data traffic [5], [7]–[10]. All participating vehicles must share one common communication medium (e.g. G5A-CC of 10 MHz bandwidth) with each other. The

more vehicles participate in communication, the more vehicles contend for channel access and more data traffic is generated, which typically leads to increasing delays and even packet losses due to packet collisions. The scalability problem in the upward direction is not an imminent issue by now but still *pending*. It only appears if many vehicles are equipped with ITS-G5 technology, which is not the case in the early phase of market introduction. However, due to its complexity, it is important to think about it even now.

Since the original IEEE 802.11 protocol was optimized for Internet-type applications and especially vehicular safety applications show totally different patterns and requirements, the poor performance, typically observed when the medium becomes congested, may be explained by the use of a MAC protocol not adapted to the specific vehicular application requirements.

Instead of focusing on a completely new design of an appropriate access mechanism for VANETs, we are in favour of making use of the IEEE 802.11 protocols flexibility, to tweak and adapt the current technology for vehicular application requirements. One proposal is to add a touch of *randomization in the selection of the transmit powers* by randomly selecting it from a given probability distribution for each CAM transmission and vehicle. The beneficial effects of that approach are described and shown in [11]. There, the use of a simple uniform TX power distribution was analysed in a first step. Future investigations will also include other probability distributions, depending on the applications communication requirements. This concept is also compatible with current TX power control algorithms. Instead of adapting the current TX power value, the mean and moments of higher order can be controlled to keep the beneficial effects of random TX power selection.

IV. Downward scalability

Although the *scalability problem* is more common for the upward direction as described above, it also shows in the downward direction. It deteriorates information dissemination for the multi-hop use case, if the number of forwarding vehicles is too low. Due to the limited communication range of ITS-G5, a certain density of vehicles is required to be able to forward messages beyond the communication range or to keep it alive, via multi-hop. If the vehicle density is too sparse, messages can starve or can be not delivered in time.

Especially in the early phase of market introduction, the low penetration rate of ITS-G5 equipped vehicles will result in a low density of forwarding vehicles, which makes this issue an *urgent* one. Within the SafeTRIP project, we have investigated the benefit of *heterogeneous networks* by integrating ITS-G5 with an additional satellite communication link. In this case both technologies have completely different characteristics. ITS-G5, for instance, has a limited communication range, but because of its fully decentralized network structure, the latencies are very low. Whereas the satellite link can provide transnational coverage but suffers from high signal propagation delays. We have shown, that both can really benefit from each other, even if only a few of ITS-G5 equipped vehicles will be additionally equipped with a satellite communication link. Further information and results can be found in [12].

A satellite communication link is one possibility for enhancing VANETs. In future work, also other communication technologies, like UMTS, LTE, WiMAX, etc. should be investigated for integration with common ITS-G5.

Acknowledgement

The author of this paper would also like to thank the following colleagues, for their strong contributions to the concepts described above: Jérôme Härri (EURECOM), Cristina Rico-Garcia (DLR), Thomas Strang (DLR) and Hanno Spijker (University of Twente).

References

[1] ETSI, "Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band," ETSI TC ITS, European Standard 202 663, november 2009, version 1.1.0.

[2] IEEE, "802.11-2012 - IEEE 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," IEEE Computer Society, IEEE Standard 802.11-2012, 2012.

[3] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," ETSI TC ITS, Technical Specification 102 637-2, march 2011, version 1.2.1.

[4] ——, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service," ETSI TC ITS, Technical Specification 102 637-3, september 2010, version 1.1.1.

[5] T. ElBatt, S. K. Goel, G. Holland, H. Krishnan, and J. Parikh, "Cooperative collision warning using dedicated short range wireless communications," in *Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, ser. VANET '06. New York, NY, USA: ACM, 2006, pp. 1–9. [Online]. Available: http://doi.acm.org/10.1145/1161064.1161066

[6] B. Kloiber, C. R. Garćia, J. Härri, and T. Strang, "Update delay: A new information-centric metric for a combined communication and application level reliability evaluation of cam based safety applications," oct. 2012, ITS World Congress.

[7] S. Eichler, "Performance evaluation of the ieee 802.11p wave communication standard," in *Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th*, 30 2007-oct. 3 2007, pp. 2199 –2203.

[8] A. Brakemeier, "White Paper on Network Design Limits and VANET Performance," Car2Car Communication Consortium, White Paper, Nov. 2008, version 0.5.

[9] R. Stanica, E. Chaput, and A.-L. Beylot, "Comparison of csma and tdma for a heartbeat vanet application," in *Communications (ICC), 2010 IEEE International Conference on*, may 2010, pp. 1 –5.

[10] M. van Eenennaam, A. Remke, and G. Heijenk, "An analytical model for beaconing in vanets," in *Vehicular Networking Conference (VNC), 2012 IEEE*, nov. 2012, pp. 9 –16.

[11] B. Kloiber, J. Härri, and T. Strang, "Dice the tx power - improving awareness quality in vanets by random transmit power selection," nov. 2012, VNC.

[12] B. Kloiber, T. Strang, H. Spijker, and G. Heijenk, "Improving information dissemination in sparse vehicular networks by adding satellite communication," in *Intelligent Vehicles Symposium (IV), 2012 IEEE*, june 2012, pp. 611 –617.

The Use of Vehicle-to-X Communication to Combat Vehicle Related Crime

Peter Knapik
Volkswagen AG, 38440 Wolfsburg, Germany, Email: peter.knapik@volkswagen.de

***Abstract*—Vehicle related crime is a pervasive occurrence leading to economic losses and personal injury. Existing countermeasures are mostly concentrated on the own vehicle and do not involve other vehicles, infrastructure or other potential technologies to counteract crime. However, new technologies such as vehicle-to-X (V2X) communication are on the rise and provide the opportunity to be used to tackle criminal activities directed against the vehicle and occupants.**

I. Introduction

Vehicle related crime has constantly constituted over 10% of the overall crime in Germany during the last 10 years [1]. The occurrence is not limited to Germany but is a worldwide ongoing phenomenon. The probably mostly known criminal offense is vehicle theft which is typically committed in order to gain temporary transportation, to commit another crime, to joyride, to strip down the vehicle for resale of parts or to resell the entire vehicle [2]. Apart from theft of whole vehicles, further types of crime exist such as theft of vehicle parts, theft from vehicles and vandalism. The term vehicle related crime also includes any attacks, such as physical attacks or robbery, against the driver as well as passengers while entering, using and exiting the vehicle. All these crimes occur in a wide spectrum of different forms and ways. So, in a nutshell, any malicious attacks directed against occupants and the vehicle causing any sort of damage, injury or property loss and being in a broad sense in relation with a vehicle are considered as vehicle related crime.

Vehicle-to-X communication is on the advance and not limited to vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Also communication between vehicles and mobile devices, such as smartphones and tablets, which are continuously becoming more important in our daily lives, gains in importance. Thus, step by step connected mobility becomes a part of our life. Additionally, the number of vehicles equipped with advanced driver assistance systems (ADAS), such as emergency brake assistants and lane assistants, increases. ADAS also penetrate lower class vehicles leading consequently to a high availability of sensors and actuators in a wide range of vehicles.

Industry and academia are mainly focusing on the use of the aforementioned new technologies to realize safety functions, to improve traffic efficiency and to provide occupants with infotainment features. However, in our opinion these technologies also provide the potential to elaborate on security functions.

By our definition, security functions make use of new technologies to tackle vehicle related crime. They aim to predict, warn about and prevent such crime as well as help to investigate and reduce the impact of vehicle related crime. Additionally, security functions pursue the goal to increase occupants' feeling of security.

To be able to elaborate on security functions, first, the frame of new technologies being involved needs to be determined. Second, a basic overview of existing measures tackling vehicle related crime is necessary. Third, a crime analysis must be conducted in order to get a deeper understanding of crime occurrence and people's fear of crime. In the last step, a systematical approach needs to be used to slip in the previous insights and generate ideas for security functions.

The next four sections will briefly summarize our achieved results, until now, according to the aforementioned steps. Before concluding our work and giving an outlook to future actions, we present two conceptual ideas for security functions making use of new technologies.

II. New technologies

To elaborate on security functions, we will concentrate on three groups of new technologies, which already entered or have the potential to enter into the market in the near future.

A. Advanced Driver Assistance Systems

Due to the increasing penetration of ADAS, several sensors and actuators are available in vehicles. For example, lane and parking assistants come along with a front and partly with a rear camera. Systems even exist that provide a 360° top view based on additional cameras build in the side mirrors. Moreover, night vision systems working at night also exist. Adaptive cruise control (ACC) makes typically use of either a LIDAR (light detection and ranging) or radar sensor to measure the distance to the vehicle in front. Another prominent example are dynamic cornering lights, which actively adjust to light into corners.

B. Consumer Electronics (CE)

We are surrounded by consumer electronics at work, at home and even underway. Especially mobile devices such as smartphones have become constant companions in our daily life so that we mainly focus on these devices. However, due to the fast development and continuous penetration of CE in the daily routine, we constantly keep an eye on new CE which have the potential to be a part of security functions.

C. Vehicle-to-X Communication

According to our definition, V2X communication includes also communication with (mobile) devices (V2D) besides V2V and V2I communication. As a wide spectrum of communication technologies exist and the standardization as well as harmonization process, referring especially to V2V communication, is still in progress, we simply imply in the beginning that wireless communication is available. Thus, we make the choice for a specific communication opportunity dependent on our use case.

III. Existing Countermeasures

To combat vehicle related crime, several security measures exist. We suggest to separate them in 4 categories:

- *Preventive measures*, e.g., preventive navigation, awareness campaigns and vehicle choice: prevent the occurrence of a malicious attack
- *Protective measures*, e.g., locking systems, armored vehicles and electronic immobilizer: intervene when a malicious attack is in progress
- *Detecting measures*, e.g., alarm systems, bait vehicles and automatic number plate recognition: detect a malicious attack and forward or store information about the attack
- *Reactive measures*, e.g., vehicle tracking systems and remote disabling: intervene after the attack happened to reduce the damage or investigate the attack

However, most security measures combating vehicle related crime work in isolation, focus on physical target hardening and neither involve other participants nor make use of new technologies.

IV. (Fear of) Vehicle Related Crime Analysis

To gain a deeper understanding of vehicle related crime, we started an analysis based on 4 areas. First, we evaluated statistical crime data as they provide an objective view of crime occurrence. Second, we evaluated crime surveys and also conducted our own survey to get a subjective view of crime and fear of crime. Third, we analyzed research projects which explored specific vehicle related crimes. In the fourth step, we started to collect information about criminals' approach (modus operandi) to commit a crime.

A. Statistical Analysis

We evaluated statistical data referring to vehicle related crime for several countries. We used data which is provided to the public by according statistical institutions and federal / state police offices. Data quality and variety of data decreases from industrial through emerging to developing countries. Additionally, directly comparing the data is not possible since data collection often underlies different definitions of crime and other methodological differences. Nevertheless, general trends are evident and indicate that vehicle related crime, especially vehicle theft, was continuously decreasing over the last 10 years but reached in the last few years a bottom line and even increased again a little in some countries. Due to the continuous introduction of security measures mainly crime committed by casual criminals was reduced. Organized crime has become more professional in order to bypass introduced security measures.

B. Survey Analysis

We conducted an anonymous online survey in Germany, the USA and Mexico focusing on the fear of crime and the need for security systems. To be able to provide an extensive analysis, we also collected data from participants about the vehicle and demographic information. The online questionnaire was spread via personal contacts, Facebook, internet forums and several websites. After filtering incomplete and false data sets we achieved response rates between 100 to 200 answers per country. Presenting all the results of the survey is beyond the scope of this report, however some results are worth mentioning. The majority of Mexicans is worried of becoming victim of vehicle related crime, whereas the majority of Germans is not worried at all. The fear of US respondents looks nearly like a normal distribution. So, the feeling of fear is completely different in all countries. However, looking at the importance of the criteria when buying a new car, the results look nearly similar for all countries. Quality is most important and off-road capability is least important. Security systems are in the lower middle of the field.

C. Research Projects

Clarke [3] researched thefts of and from cars in parking facilities and estimated contributing factors such as car security, regional location, car make and model as well as parking lot design. He provides both recommended countermeasures and countermeasures with limited effectiveness. Among others, parking attendants, improved surveillance, CCTV installation and monitoring, improved lighting as well as access control, e.g. via chip cards, is seen as effective. In contrast, lock-your-car campaigns, car alarm promotion as well as the use of bait cars are evaluated to have limited effectiveness. According to [4], the introduction of a bicycle-mounted patrol on a Vancouver commuter lot led to a reduction of vehicle theft.

D. Modus Operandi

The expression describes the crime procedure and contains information about the methods, habits, used tools and actions the criminal went through to commit the crime. The MO can be determined for example by analyzing a crime afterwards or interviewing offenders. According to [3], interviews with offenders indicate that vehicles with alarms are avoided, but the decision depends on the offender's skills. Professional thieves specialized in particular vehicles are able to invest more effort to overcome the system. Tuchscherer [5] also interviewed offenders and additionally concluded that offenders generally try to avoid to face the owner while stealing a vehicle.

V. SYSTEMATICAL APPROACH

Surveying the literature, two criminological approaches, Rational Choice Perspective and Situational Crime Prevention, together provide a conceptual framework to systematically analyze criminal acts [6]. The former approach suggests a separation of the crime process in detailed events which the offender goes through to commit the crime. The latter approach provides 25 techniques to combat crime. Based on the knowledge from our vehicle crime analysis shown in section IV, we researched some specific crimes and used the 25 techniques to generate ideas for security functions. The interested reader can find detailed information about the approach in [6]. In the next section, two ideas for security functions will be conceptually presented.

VI. SECURITY FUNCTIONS

A. Electronic Decal

In the 1990s, several states in the USA introduced a program called *Watch Your Car* to combat vehicle theft [7], [8], [9]. The vehicle owner registers his vehicle with an according state authority and confirms that the vehicle is normally not driven between the hours of 1 a.m. to 5 a.m.. Hence, the police has permission to stop the vehicle during program hours and check whether the vehicle is legally operated or not. To indicate that a vehicle participates in the program, a program specific decal is placed on the front or rear windshield.

The electronic decal partly transfers the idea of the physical decal into the world of connected mobility. Instead of a visibly placed decal on a windshield of the vehicle, the vehicle uses the onboard communication unit (OCU) for two purposes as soon as the vehicle is illegally moved. First, the vehicle informs the owner via smartphone about a potential misuse. This way, the opportunity for quick reaction is enabled either to deactivate the electronic decal due to a false alarm or to report the vehicle stolen. Second, the vehicle continuously broadcasts a message with the request to be checked by the police. Passing police vehicles are initiated to stop and check the suspect vehicle. Moreover, the broadcasted message can be evaluated by infrastructure such as police stations and border crossings. Other vehicles and infrastructure in range but not of interest simply discard the message.

We propose a control of the electronic decal function in three ways. First, the owner or authorized persons transfer a detailed schedule to the OCU including information about times the vehicle is allowed to move. Data transfer can be realized via smartphone, from any computer via internet or basically through direct input in the vehicle, which of course needs to be secured properly. Second, the activation as well as deactivation go hand in hand with the immobilizer whereas the functionality is implemented in a separate electronic control unit (ECU), namely the OCU. Third, the smartphone is used to control the electronic decal. As soon as the smartphone gets paired with the vehicle, for example via near field communication or a wireless short range communication such as Bluetooth, the electronic decal functionality is disabled. Vice versa, when the smartphone is out of range, the function is enabled. Of course, each smartphone which is intended to control the function needs to be enrolled once with the system. In case that the smartphone is not available, for example due to an empty battery, the user falls back on direct input within the vehicle which is secured by a personal identification number (PIN).

The electronic decal introduces extended opportunities and advantages compared to the physical decal. First, the owner or any other authorized person is informed as soon as the vehicle is moved outside of predefined times. This way, a quick theft report is possible. Second, the function can be realized with hardware that is or will be available anyway in the course of connected mobility. Third, the electronic decal is not limited to static times. Next, as there is no visible decal which informs the offender about this function, the offender never knows if the electronic decal function is supported or even enabled by the targeted vehicle. However, one drawback needs to be mentioned. If the function is controlled by a schedule, a motivated and self-disciplined driver who regularly updates the schedule is necessary. Otherwise, police could stop an "innocent" vehicle due to an outdated schedule. Nevertheless, it is still in police's discretion whether to stop a vehicle or not.

B. Cooperative Extended Coming / Leaving Home Light

Currently, so called coming / leaving home functions (CHF / LHF) exist. When leaving the car (CHF), the low beams, taillights and other available lights keep on lighting during darkness for a specific period of time in order to light the driver the way "home". The duration can be adjusted by the vehicle owner. Referring to the LHF, the aforementioned light sources start lighting as soon as the driver remotely opens the car. However, this described functionality has the drawback to be static. The lighting duration can only be adjusted in the vehicle and it is independent of the drivers position. That means, if the duration is to short, the illumination would turn off before the driver even reaches the vehicle and vice versa respectively. Furthermore, the vehicle turns on all light sources although some light sources are probably unnecessary since the driver approaches the vehicle from one direction.

Our idea is to extend the existing CHF / LHF by the opportunities of dynamic light assistants. We suggest to use the opportunity that the low beams can be swiveled vertically and horizontally to light the driver's direct route to the vehicle, of course within the mechanical limits of the beams. Additionally, only light sources are turned on which directly influence the illumination of the route.

To realize the extended CHF / LHF (ECHF / ELHF), a bidirectional communication between the vehicle and a device, such as a smart key or smartphone, being with the driver while exiting or entering the vehicle is assumed. Additionally, position estimation of the key relatively to the vehicle is necessary. It is irrelevant whether the position is estimated on the key (smart key / smartphone) or in the vehicle

since position data is continuously synchronized between both participating partners due to bidirectional communication.

The ELHF is activated as soon as the doors are remotely unlocked. Both, the two-way communication between the key and the vehicle as well as the location estimation of the key starts. The position of the key is updated at regular intervals, so that the vehicle can evaluate the position. The movable low beams are aligned in the mechanical limits of the yaw and tilt angle in the direction of the driver. The other non-moveable light sources are turned on only when they illuminate the direct path of the driver. Since the driver of the vehicle is moving, the possible direct route to the vehicle is constantly changing. Therefore, the low beams are continuously tracked. Turned off light sources are switched on if they are relevant for the direct path of the driver to the vehicle. In return, turned on light sources can be switched off if they lose the relevance for illuminating the direct path. There is no need to consider time to switch off the lights because the lighting is switched off with reaching the vehicle or even only with the opening of the door. Nonetheless, a long run-time can be defined as a fallback option.

When exiting the vehicle (ECHF), the direct path of the driver is illuminated analogously to the ELHF. The duration of illuminating can be done with a defined delay time. However, there is also the possibility to deactivate the illumination after the driver has left a certain radius around the vehicle. An organic surface around the vehicle is also possible since the effectiveness of involved light sources is different. Of course, it is also possible to disable the function with the key (smartphone).

Both, the ECHF and ELHF can use V2V or V2I communications to be enhanced to a cooperative ECHF / ELHF (CECHF / CELHF). Due to the physical and mechanical constraints, the own vehicle is not always in a position to illuminate the direct path of the driver. Therefore, vehicles or infrastructure in the area are included to illuminate the direct path to the host vehicle. The own vehicle initiates the communication with the other participants and shares the driver's position with them.

VII. Conclusion and Future Work

The main goal of this work was to illustrate our idea and approach to systematically design innovative security functions based on new technologies, since the frame for new functions is not limited to road safety, traffic efficiency and infotainment features. We determined the frame of new technologies to be used to realize security functions, examined existing countermeasures in the automotive field and conducted a crime analysis to get a deeper understanding of vehicle related crime and fear of crime. Slipping in the previous insights we used a criminological approach to generate ideas for security functions, and lastly we conceptually drew two security functions.

In the future, we are going to design selected security functions to investigate feasibility, effectiveness and user acceptance. This involves in detail the implementation of prototypes or the use of simulations. Additionally, user surveys seem to be unavoidable since we also aim to estimate user acceptance. Of course, we will also consider privacy issues with respect to our security functions. However, fundamental privacy issues will have to be solved by according institutions in order to provide a frame to introduce and make use of new technologies such as V2X communication.

In the end, we hope that our work extends the portfolio of functions making use of new technologies as well as paves the way to reduce vehicle related crime and to increase the feeling of security.

References

[1] BKA. (2011) Polizeiliche Kriminalstatistik 1997 - 2010. Bundeskriminalamt. [Online]. Available: http://www.bka.de/pks/

[2] T. Keister, "Thefts of and from cars on residential streets and driveways," U.S. Department of Justice, Problem-Oriented Guides for Police Series - Problem Specific Guide Series 46, Feb. 2007. [Online]. Available: http://www.popcenter.org/problems/

[3] R. V. Clarke, "Thefts of and from cars in parking facilities," U.S. Department of Justice, Problem-Oriented Guides for Police Series - Problem Specific Guide Series 10, Jan. 2002. [Online]. Available: http://www.popcenter.org/problems/

[4] P. Barclay, J. Buckley, P. J. Brantingham, P. L. Brantingham, and T. Whinn-Yates, "Preventing auto theft in suburban vancouver commuter lots: Effects of a bike patrol," in *Preventing Mass Transit Crime*, ser. Crime Prevention Studies, R. V. Clarke, Ed. Monsey, NY: Criminal Justice Press, 1996, vol. 6, pp. 133–161.

[5] S. Tuchscheerer, "Human factors in automotive crime and security," Ph.D. dissertation, University of Technology Chemnitz, 2011.

[6] P. Knapik, E. Schoch, M. Müller, and F. Kargl, "Understanding vehicle related crime to elaborate on countermeasures based on ADAS and V2X communication," in *Proceedings of the IEEE Vehicular Networking Conference 2012*. IEEE, Nov. 2012.

[7] Maryland - Watch Your Car. (2008) Make your car tough to steal. Maryland Vehicle Theft Prevention Council. [Online]. Available: http://www.mdautotheft.org/wyc/

[8] Utah - Watch Your Car. (2012) Make your car tough to steal. State of Utah. [Online]. Available: https://secure.utah.gov/wyc/whatis.html

[9] Arizona - Watch Your Car. (2009) The watch your car program. Arizona Automobile Theft Authority. [Online]. Available: https://www.aata.az.gov/watch_your_car/default.asp

Novel Communication Strategies for Platooning and their Simulative Performance Analysis

Michele Segata*†
*Computer and Communication Systems, Institute of Computer Science, University of Innsbruck, Austria
†Systems and Networks, Dept. of Information Engineering and Computer Science, University of Trento, Italy
segata@ccs-labs.org

***Abstract*—Platooning, the act of a car autonomously following its leaders to form a road train, is a hot topic in research. It has the potential to improve traffic flow on freeways, improve safety, and enhance the driving experience. A lot of effort has been put in several projects in order to implement and test systems capable of performing close car following. While the problems related to control theory seems to be solved, some questions regarding communication are still open. Wireless networking is fundamental for this application, as it is needed to manage and maintain the platoons and, clearly, has strict requirements in terms of frequency update and delay constraints. This paper surveys the literature about platooning systems and related research, identifies some open challenges, presents a simulation framework which can be used to tackle them, and outlines promising approaches.**

I. Introduction

Since the advent of Vehicular Ad Hoc Networks (VANETs) hundreds of applications have been proposed, analyzed and tested. Among these applications, platooning is often cited as one of the most visionary. It has been investigated since the eighties within the California PATH project [1] and it is still under current research.

The reasons behind such a huge investment and interest by the community are most probably the benefits that this application could provide once deployed and the challenging problems it arises.

Platooning could improve the driving experience in different ways. First of all, it has the potential to reduce, if not solve, big traffic jams on freeways and highways by improving the traffic flow [2]. The close following performed by computer-driven vehicles results in a more efficient utilization of the road, where most of the space is wasted because drivers must keep a safety distance from the vehicle in front. Such close following also reduces the fuel consumption, because the air drag is lower [3]. Lower fuel consumption clearly results in lower emissions of greenhouse gases. Secondly, platooning could improve drivers' safety, if a system fault is less likely than a human error, which is the major cause of accidents [4]. Last but not least, a vehicle which autonomously follows its leaders permits the driver to relax, read a newspaper or the emails, as shown by the recent SARTRE project [5]. Driving time would not be wasted time anymore.

From the research point of view platooning has always been extremely challenging, as it involves control theory, traffic engineering, vehicle dynamics and information technology. The controller designed for supporting platooning, namely Cooperative Adaptive Cruise Control (CACC) [6, Chapter 7], needs indeed frequent and up-to-date information about vehicles in the platoon in order to avoid instabilities which might lead to collisions. This is where the networking community comes into play: a platooning system requires an information update frequency of at least 10 Hz [7]. Whether such communications requirements can be satisfied by the plain DSRC/WAVE stack [8] is still unclear. The aim of this paper is thus to study the current state of the art concerning communication strategies and protocols for platooning and highlight the challenges that are still open, giving some ideas on how they could be tackled.

II. Related Work

The platooning research community focused firstly on the problems connected to the automated control of vehicles. This is due to the fact that the design of a system able to maintain a constant distance between the vehicles independently from the speed is a non-trivial task. The characteristic which makes a CACC different from a standard Adaptive Cruise Control (ACC) is indeed the capability of performing a close following (in the order of roughly 5 m) independently from the speed the vehicles are currently traveling at. This is not possible with ACC, as the platoon would not be string stable, i.e., a spacing error occurring at the head of the platoon might be amplified and lead to a collision [6][1]. An ACC, in order to be string stable, must keep a headway time from the vehicle in front strictly higher than 1 s, translating into a distance not smaller than 36 m at 130 km h^{-1}. This is exactly what a human driver should do in order to respect the safety distance.

A CACC instead obtains the information about the leader and the vehicle in front by means of wireless communications: in this way a vehicle can know in advance what is happening at the head of the platoon and react quicker [6]. This kind of controllers have been investigated since the beginning by the pioneering platooning projects PATH and Auto21 CDS [1], [9], but they are still under continuous improvement either by academic research [7] or by car manufacturers, as in the case of the SARTRE project [5].

What differentiates pioneering projects from recent studies is the philosophy. In the case of PATH or Auto21 CDS, platoons were designed to run on dedicated highways, managed by a

[1] An example of a stable and an unstable behavior is shown in Section III.

centralized system [10]. The idea in SARTRE instead, is that platoons form autonomously, and they can travel on public motorways mixed with human driven vehicles. In both cases, network conditions are still a major concern. It is well known that 802.11-based networks can suffer of high packet loss ratios even in moderate channel load conditions. Given the frequent updates needed by the CACC in order to ensure string stability, the impact of the network performance on the safety of the overall system is non-marginal.

Due to this reason, the VANET community recently started to investigate the impact of communication characteristics on platooning performances. As an example, Lei et. al. [11] showed the impact of different packet loss rates on the performance of the CACC. Bergenhem et. al. [12] and Karlsson et. al. [13] instead focused on real world measurements, showing first the impact of the antenna positioning on the packet error rate, and then the impact of Non Line of Sight (NLOS) communications caused by obstructing vehicles. Fernandes and Nunes [14] started to investigate strategies to improve communications reliability by analyzing five different communication algorithms, all based on a slotted TDMA. Furthermore, they propose a dynamic adaptation of CACC parameters, in order to cope with different situations.

These works provide a solid foundation which made it possible to raise challenging questions that we have identified.

- Under which channel conditions a reliable communication can still be ensured?
- How many platoons can co-exist without interfering?
- How does platooning cope with other applications?
- What is the effect of background traffic?
- How can we cope with bad wireless channel conditions?

These are some of the questions that still remain open and that we intend to investigate in the near future.

III. Simulation Framework

The investigation of platooning systems under challenging conditions (i.e., high network and road traffic) can be performed by means of simulations, reducing costs and providing deeper insights. Due to this, starting from the Veins simulator [15], we have developed a platooning simulation framework [16] which enables researchers to define highway scenarios, high level applications, and communication protocols. In such a way it is possible to investigate platooning strategies, for instance understanding what is the better way of organizing the vehicles, or determine networking metrics, such as packet loss rate, delays, experienced channel load, etc.

Fernandes and Nunes [17] developed such a simulator to investigate a completely automated and dedicated highway as in the idea of the PATH project. We developed one which generalizes this idea to the SARTRE philosophy: it is indeed possible to simulate automated vehicles, together with vehicles controlled by well-known car following models, enabling the possibility of studying mixed scenarios.

We further enhanced the level of details by coupling the mobility simulator with a detailed network simulator, as we focus more on the investigation of networking related questions.

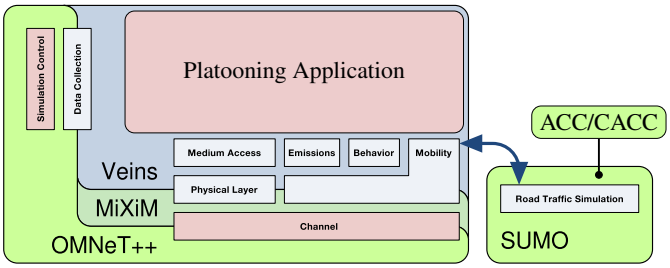


Figure 1. The Veins simulation tool extended by the platooning framework.

The Veins framework natively comes with an IEEE 802.11p and IEEE 1609.4 model [18], [19], permitting a detailed simulation of a DSRC/WAVE system.

The structure of the simulator is shown in Figure 1. Veins relies on SUMO [20] for traffic simulation and on OMNeT++/MiXiM [21] for network simulation. We extended Veins by implementing the automated controllers (ACC and CACC) described in [6] as new car following models in SUMO. The models are then made accessible from within Veins; in this way it is possible to enable/disable the controllers and change their parameters, such as the desired speed or the information received via wireless communication.

The definition of the logic of the applications and the protocols can be then easily implemented like usual OMNeT++ modules, permitting the collection of data to the purpose of successive analysis. As a simple example we compared stability properties of ACC and CACC. Figure 2 shows the headway error each car has to the vehicle in front when the leader changes its speed in a sinusoidal trend. For the sake of clarity, a positive headway error means that a car is farther from its direct leader than expected. As clearly shown in Figure 2a, the ACC is unstable, as the error is being amplified through the platoon. The CACC instead (Figure 2b) is able to react in a quicker way and the oscillatory effects are being attenuated: the last vehicles in the platoon are perfectly maintaining the desired distance.

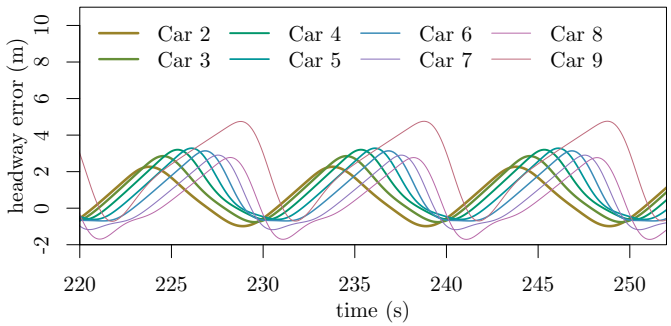
As performed in this paper, it is also easy to make network or application layer analysis, like the one shown in [16].

IV. Research Questions and Possible Solutions

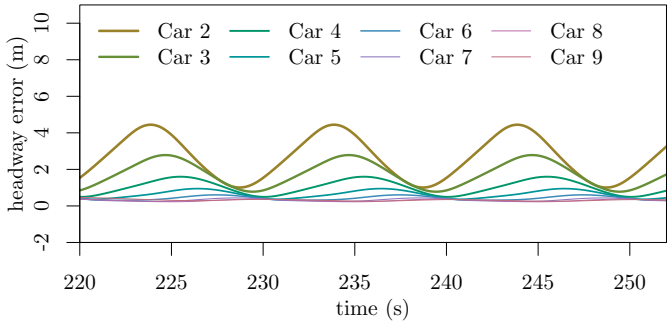
Once the state of the art has been surveyed and the simulation framework has been implemented, some research questions arise.

In a first step we are interested in identifying to which extent the plain IEEE 802.11p is able to support platooning. This can be done by performing some network stress tests, either by simulating a highway with several platoons or taking into account background traffic. In this way it will be possible to understand how many of the expected packets are received by platooning vehicles and with how much delay.

Secondly, it would be interesting to make an analysis of the communication requirements needed to keep the CACC safe, for example by making the leader perform an emergency



(a) ACC



(b) CACC

Figure 2. Comparison of spacing errors of ACC and CACC under sinusoidal variation of leader's speed, showing an instable behavior for ACC and a stable behavior for CACC.

braking and see what happens to the platoon by changing the beaconing frequency.

Once these steps are performed, it would be possible to analyze different communication protocols and strategies, in order to determine which one is best suited for platooning. For example, comparing static beaconing using pure CSMA/CA with TDMA approaches (as in [14]), as well as transmission power control algorithms.

As a final step, even if the best of such approaches could not guarantee safety in all possible network conditions, it might be possible to determine network capabilities and react upon that, for instance by adapting the inter-vehicle distance.

V. Conclusion

In this paper we have surveyed the current state of the art regarding platooning, describing the main projects, the technologies, and the research involving wireless networking. We have highlighted the potential that platooning has and how it could enhance the driving experience.

Still, some issues remain open and they must be carefully investigated and understood before the actual deployment of such system. We outlined these issues and have described the simulation framework that we have developed, which enables the analysis of vehicles' dynamics, application logic and network protocols. Such tool will be used for tackling the problems and for replying to the questions that are still lacking an answer. This enables the means of addressing the highlighted issues for which we have provided some first potential approaches.

References

[1] S. Shladover, "PATH at 20 – History and Major Milestones," in *IEEE Intelligent Transportation Systems Conference (ITSC 2006)*, Toronto, Canada, September 2006, pp. 22–29.

[2] B. van Arem, C. van Driel, and R. Visser, "The Impact of Cooperative Adaptive Cruise Control on Traffic-Flow Characteristics," *IEEE Transactions on Intelligent Transportation Systems*, vol. 7, no. 4, pp. 429–436, December 2006.

[3] A. Davila and M. Nombela, "Platooning - Safe and Eco-Friendly Mobility," in *SAE 2012 World Congress & Exibition*. Detroit, Michigan: SAE, April 2012.

[4] ——, "Reducing Fuel Consumption through lower Aerodynamic Drag Coefficient," in *SAE Brazil*, Sao Paolo, Brazil, October 2011.

[5] C. Bergenhem, Q. Huang, A. Benmimoun, and T. Robinson, "Challenges of Platooning on Public Motorways," in *17th World Congress on Intelligent Transport Systems*, Busan, Korea, October 2010.

[6] R. Rajamani, *Vehicle dynamics and control*. Springer, 2006.

[7] J. Ploeg, B. Scheepers, E. van Nunen, N. van de Wouw, and H. Nijmeijer, "Design and Experimental Evaluation of Cooperative Adaptive Cruise Control," in *IEEE International Conference on Intelligent Transportation Systems (ITSC 2011)*, Washington, DC, October 2011, pp. 260–265.

[8] "Wireless Access in Vehicular Environments," IEEE, Std 802.11p-2010, July 2010.

[9] S. Hallé, B. Chaib-draa, and J. Laumonier, "Car Platoons Simulated As A Multiagent System," in *4th Workshop on Agent-Based Simulation*, Montpellier, France, April 2003, pp. 57–63.

[10] L. Baskar, B. De Schutter, J. Hellendoorn, and Z. Papp, "Traffic Control and Intelligent Vehicle Highway Systems: a Survey," *IET Intelligent Transport Systems*, vol. 5, no. 1, pp. 38–52, March 2011.

[11] C. Lei, E. van Eenennaam, W. Wolterink, G. Karagiannis, G. Heijenk, and J. Ploeg, "Impact of packet loss on CACC string stability performance," in *11th International Conference on ITS Telecommunications (ITST 2011)*, Saint Petersburg, Russia, August 2011, pp. 381–386.

[12] C. Bergenhem, E. Hedin, and D. Skarin, "Vehicle-to-Vehicle Communication for a Platooning System," in *Transport Research Arena*, Athens, Greece, April 2012.

[13] K. Karlsson, C. Bergenhem, and E. Hedin, "Field Measurements of IEEE 802.11p Communication in NLOS Environments for a Platooning Application," in *76th IEEE Vehicular Technology Conference (VTC2012-Fall)*. Quebec City, Canada: IEEE, September 2012, pp. 1–5.

[14] P. Fernandes and U. Nunes, "Platooning With IVC-Enabled Autonomous Vehicles: Strategies to Mitigate Communication Delays, Improve Safety and Traffic Flow," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 1, pp. 91–106, March 2012.

[15] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2011.

[16] M. Segata, F. Dressler, R. Lo Cigno, and M. Gerla, "A Simulation Tool for Automated Platooning in Mixed Highway Scenarios," in *18th ACM International Conference on Mobile Computing and Networking (MobiCom 2012), Poster Session*. Istanbul, Turkey: ACM, August 2012, pp. 389–391.

[17] P. Fernandes and U. Nunes, "Platooning of autonomous vehicles with intervehicle communications in SUMO traffic simulator," in *IEEE International Conference on Intelligent Transportation Systems (ITSC 2010)*, Madeira Island, Portugal, September 2010, pp. 1313–1318.

[18] "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation," IEEE, Std 1609.4, February 2011.

[19] D. Eckhoff and C. Sommer, "A Multi-Channel IEEE 1609.4 and 802.11p EDCA Model for the Veins Framework," in *5th ACM/ICST International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2012), Poster Session*. Desenzano, Italy: ACM, March 2012.

[20] D. Krajzewicz, G. Hertkorn, C. Rössel, and P. Wagner, "SUMO (Simulation of Urban MObility); An open-source traffic simulation," in *4th Middle East Symposium on Simulation and Modelling (MESM 2002)*, Sharjah, United Arab Emirates, September 2002, pp. 183–187.

[21] A. Köpke, M. Swigulski, K. Wessel, D. Willkomm, P. T. K. Haneveld, T. E. V. Parker, O. W. Visser, H. S. Lichte, and S. Valentin, "Simulating Wireless and Mobile Networks in OMNeT++ – The MiXiM Vision," in *1st ACM/ICST International Conference on Simulation Tools and Techniques for Communications, Networks and Systems (SIMUTools 2008)*. Marseille, France: ACM, March 2008.