Report from Dagstuhl Seminar 22512

Inter-Vehicular Communication – From Edge Support to Vulnerable Road Users II

Ana Aguiar*[1], Onur Altintas*[2], Falko Dressler*[3], Gunnar Karlsson*[4], and Florian Klingler†[5]

1 **Universidade do Porto, PT.** anaa@fe.up.pt
2 **Toyota Motor North America – Mountain View, US.** onur@us.toyota-itc.com
3 **TU Berlin, DE.** dressler@ccs-labs.org
4 **KTH Royal Institute of Technology – Stockholm, SE.** gk@kth.se
5 **Universität Paderborn, DE.** klingler@ccs-labs.org

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 21262 "Inter-Vehicular Communication – From Edge Support to Vulnerable Road Users II". Looking back at the last decade, one can observe enormous progress in the domain of vehicular networking. In this growing community, many ongoing activities focus on the design of communication protocols to support safety applications, intelligent navigation, and many others. We shifted the focus from basic networking principles to open challenges in edge computing support and, as a novel aspect, on how to integrate so called vulnerable road users (VRU) into the picture.

Seminar December 18–21, 2022 – http://www.dagstuhl.de/22512
2012 ACM Subject Classification Computing methodologies → Machine learning; Human-centered computing; Networks → Cyber-physical networks; Networks → Network protocols
Keywords and phrases 5G/6G, bicyclists, cooperative driving, edge computing, intelligent transportation systems, pedestrians, tactile internet, V2X, vehicle-to-vehicle communication, vulnerable road users
Digital Object Identifier 10.4230/DagRep.12.12.54

1 Executive Summary

Falko Dressler (TU Berlin, DE)
Ana Aguiar (Universidade do Porto, PT)
Onur Altintas (Toyota Motor North America – Mountain View, US)
Gunnar Karlsson (KTH Royal Institute of Technology – Stockholm, SE)

Looking back at the last decade, one can observe enormous progress in the domain of vehicular networking. In this growing community, many ongoing activities focus on the design of communication protocols to support safety applications, intelligent navigation, and many others. Using the terms Vehicular Ad-hoc Networks (VANETs), Inter-Vehicle Communication (IVC), Car-2-X (C2X), or Vehicle-2-X (V2X), many applications – as interesting as challenging – have been envisioned and (at least) partially realized. Very large projects have been initiated to validate the theoretic work in field tests and protocols are being standardized. With the increasing interest from industry, security and privacy have also become crucial aspects in

* Editor / Organizer
† Editorial Assistant / Collector

the stage of protocol design in order to support a smooth and carefully planned roll-out. We are now entering an era that might change the game in road traffic management. Many car makers already supply their recent brands with cellular and WiFi modems, some also adding vehicular WLAN (DSRC, ITS-G5) and C-V2X technologies.

With this latest installment of the "Inter-Vehicular Communication" Dagstuhl Seminar series, we intend to shift the focus from basic networking principles to open challenges in edge computing support and, as a novel aspect, on how to integrate so called vulnerable road users (VRU) into the picture. Edge computing is currently becoming one of the core building blocks of cellular networks, including 5G, and it is necessary to study how to integrate ICT components of moving systems. The trade-offs of computation distribution, system aspects, and the impact on end-to-end latency are still unanswered. Also, vehicular networking and cooperative driving focus almost exclusively on cars but leave out communication and coordination with, for example, pedestrians and bicyclists. And, many of the existing communication solutions for this scenario were designed without having battery constraints in mind. In the meantime, some early research has been initiated on this topic and initial projects report very interesting results on safety features for VRUs. Building upon the great success of the previous Dagstuhl Seminars – as documented, e.g., with results published in widely visible magazine articles [1, 2, 3, 4] – with this follow-up seminar, we aim to again bring together experts from all these fields from both academia and industry.

Seminars in this series focused on general vehicular communication technologies, security and safety impact, cooperative driving concepts and its implications on communication protocol design, and many more. Building upon the online-only seminar in 2021, we now shifted the focus of this seminar from basic networking principles to open challenges in edge computing support and, as a novel aspect, on how to integrate so called vulnerable road users (VRU) into the picture. Edge computing is currently becoming one of the core building blocks of cellular networks, including 5G/6G, and it is necessary to study how to integrate ICT components of moving systems. The trade-offs of computation distribution, system aspects, and the impact on end-to-end latency are still unanswered. Also, vehicular networking and cooperative driving focuses almost exclusively on cars but leaves out communication and coordination with, for ex-ample, pedestrians and bicyclists. For example, many of the existing communication solutions for this scenario were designed without having battery constraints in mind.

The seminar focused intensively on discussions in several working groups. To kick-off these discussions, we invited four keynote talks:

- Vehicles and The Edge: Random thoughts and not so random Perspectives by Jörg Ott (TU Munich, DE)
- Who protects the Unprotected? ITS Services for Vulnerable Road Users by Claudio Casetti (Politecnico di Torino, IT)
- Enabling data spaces: Existing developments and challenges by Gürkan Solmaz (NEC, DE)
- Securing Cooperative Intersection Management by Subjective Trust Networks by Frank Kargl (Ulm University, DE)

We finally organized the following working groups on some of the most challenging issues related to inter-vehicular communication, edge computing, and vulnerable road users:

- Edge computing
- Vulnerable road users
- Vehicle to cloud to vehicle communication
- Sensing and analytics
- Trust

References

1 Falko Dressler, Frank Kargl, Jörg Ott, Ozan K. Tonguz and Lars Wischhof, "Research Chal-lenges in Inter-Vehicular Communication – Lessons of the 2010 Dagstuhl Seminar," IEEE Communications Magazine, vol. 49 (5), pp. 158-164, May 2011.

2 Falko Dressler, Hannes Hartenstein, Onur Altintas and Ozan K. Tonguz, "Inter-Vehicle Communication – Quo Vadis," IEEE Communications Magazine, vol. 52 (6), pp. 170-177, June 2014.

3 Onur Altintas, Suman Banerjee, Falko Dressler and Geert Heijenk, "Executive Summary – Inter-Vehicular Communication Towards Cooperative Driving," Proceedings of Dagstuhl Seminar 18202 on Inter-Vehicular Communication – Towards Cooperative Driving, Schloss Dagstuhl, Germany, May 2018, pp. 31–59.

4 Ana Aguiar, Onur Altintas, Falko Dressler and Gunnar Karlsson, "Executive Summary – Inter-Vehicular Communication – From Edge Support to Vulnerable Road Users," Proceedings of Dagstuhl Seminar 21262 on Inter-Vehicular Communication – From Edge Support to Vulnerable Road Users, vol. 11, Virtual Conference, June 2021, pp. 89–96.

2 Table of Contents

3 Overview of Talks

3.1 Who protects the Unprotected? ITS Services for Vulnerable Road Users

Claudio Casetti (Polytechnic University of Torino, IT)

In this talk we first defined what is a Vulnerable Road User (VRU) from the point of view of many international standardisation entities. We then discussed four possible approaches for ITS to protect VRUs, highlighting pros and cons. First, the use of smart infrastructure with V2X capability. Then, cooperative perception by vehicles, followed by VRU-awareness messages sent by VRUs themselves. Finally, we discussed the use of edge/cloud support and introduced some open research questions that could be addressed during the rest of the seminar.

3.2 Securing Cooperative Intersection Management by Subjective Trust Networks

Frank Kargl (Universität Ulm, DE)

In this talk, I presented results from recent and newly-starting German and European research projects SecForCARs-SAVE, CONNECT, and ConnRAD where we investigate the role which trust models can play in securing complex cooperative, connected & automated mobility (CCAM).

CCAM systems are highly complex systems-of-systems (SoS) which are composed of many layers of subcomponents. Motivated by incidents like the log4j vulnerability, supply-chain security has recently taken up the challenge to evaluate security in such SoS. In our research, we investigate how to model trust dependencies in such SoS as trust networks or trust graphs in order to allow a quantifiable analysis of the effects that security incidents in one part of the system will have on other parts.

Based on earlier works, we were able to identify Subjective Logic and Subjective Trust Networks as a very useful formalism to model such trust graphs. In the talk, I illustrated this process on the example of Cooperative Intersection Management (CIM) and showed the steps that are needed for a MEC server to establish a trust opinion on the positions that vehicles send as part of their CAM messages.

In the following discussion, we elaborated on different aspects of such trust models, for example, the role of vehicle manufacturers as possible trust brokers as they constantly monitor their vehicle fleet through their backend systems and would be in a very good position to detect intrusions or other incidents that would reduce trust in a specific vehicle.

References

1 https://www.secforcars.de/
2 https://horizon-connect.eu/

3.3 Vehicles and "The Edge": Random thoughts and not so random Perspectives

Jörg Ott (TU München, DE)

Edge computing has been considered as a promising technology direction to support low-latency applications for end users, by offloading computing-intense and energy-consuming tasks from mobile devices to close by compute resources or by pushing centralized service instances closer to the user. Edge infrastructure should similarly be able to support vehicular applications, for compute offloading or data sharing. But would it need to? And, if so, could it really? In this talk, we explore demands of mobile (vehicular) applications for different latency bounds and see how far those could, in principle, be served by regular data centers. We use Germany as an example and investigate geographic and projected network topology distances from 33M points on German roads to 200+ data centers in 41 locations within the country. We then consider another hypothetical extreme case in which each base station would also serve as an edge server and consider scaling with the number of vehicles obtained from official traffic measurement stations. We finally touch upon the implications, including the need for running, managing and arbitrating all these resources.

3.4 Enabling data spaces: Existing developments and challenges

Gürkan Solmaz (NEC Laboratories Europe – Heidelberg, DE)

This talk presents the existing developments and key technical challenges of data spaces for the future of data ecosystems. Enabling data spaces requires the three layers that are highlighted in the talk: Data connectors/infrastructure, data interoperability, and data value. In the first layer, we consider the existing developments from IDSA, Gaia-X, and FIWARE. These developments target easy and secure data sharing through access and data usage policies, federation of cloud services, and standardized data models and contextualization. The second layer provides the data interoperability to connect and harmonize various data sources through data- and knowledge-driven machine learning. Finally, the third layer focuses on the "value" generation from data by easy and efficient application of advanced data processing functions of prediction, simulation, and optimization.

As a future data space use case, we propose "Green Twin", which aims to minimize energy consumption by creating and utilizing digital twins of entities such as vehicles, buildings, network infrastructure, and people. The talk describes the proof-of-concept project toward the application of Green Twin in the smart campus, building upon the FIWARE open-source ecosystem on the networking infrastructure with 5G and applying machine learning, to improve the efficiency of the energy usage for the buildings and mobility.

4 Working groups

4.1 Sensing and analytics

Ana Aguiar (Universidade do Porto, PT), Khalil Ben Fredj (University of Twente – Enschede, NL), and Gürkan Solmaz (NEC Laboratories Europe – Heidelberg, DE)

Joint work of Carla Fabiana Chiasserini, Geert Heijenk, Klaus David, Jérôme Härri, Onur Altintas, Florian Klingler, Christoph Sommer, Lukas Stratman

The first breakout session initiated with a discussion on the relationship between IoT and intelligent mobility applications, and identification of relevant applications to make discussion more concrete. A plethora of sensing and analytics applications have been considered in research related to mobility such as pedestrian flow detection, trajectory prediction, collision risk detection, user profiling, and so on. Considering vulnerable road users (VRUs), sensing and analytics data services would make use of data such as video data, GPS trajectories, and vehicular sensing.

The sensing may have two types of goals: real-time traffic management and safety applications, or feeding urban planning. Analyzing such data in large geographical domains would bring data communication challenges as well as challenges in the computing and Artificial Intelligence (AI), where specialized algorithms in distributed analytics would be studied. Machine Learning (ML) training and inference problems can be considered for developing vehicle-specific (in-vehicle), local, cooperative and federated models. Particularly, federated and split learning are an on-going research directions that address the distribution of the more computationally expensive phase of ML models: training. These two types of algorithms address privacy constraints by avoiding centralization of the raw data. Other on-going efforts in ML that are relevant to low latency include early-exit models, which process data through the whole pipeline only when necessary, e.g. for increased confidence. This would allow light local processing, moving data out of the mobile device only for some specific (detectable) situations. The distribution of ML model training involves several challenges related to the data itself. Besides addressing the need for i.i.d samples or the bias caused by non-i.i.d samples for most models, some areas currently under-explored are the distributed data pre-processing (e.g. local statistical measures may differ from global ones), and how the annotation of the data in a distributed setting could be achieved.

The trade-offs between different degrees and type of distribution, convergence speed, networking costs and model accuracy are yet in the realm of research. Modelling such trade-offs was identified as a valuable research direction. Distributed computing should make use of cloud and edge resources efficiently, such that the quality-of-service requirements, e.g. latency, from both the communication (network latency) and computation (virtualization and AI latency) angles would be satisfied. One may consider the networking as "in-vehicle" where wired communication would be utilized whereas the information that goes out of the vehicle should be transferred through wireless communication. For the computing side, edge computing may be applied in-vehicle, road-side, or edge data centers that are in the vicinity, materializing the vehicular edge computing paradigm. A brief call of attention was made to the different semantics of the fog, edge and cloud nomenclature in different communities, namely the Internet of Things.
Distributed sensing data collection and analytics are of utmost importance for improved

safety applications for cars, bikes, and pedestrians. For instance, cooperative sensing and perception has the potential to greatly improve the VRU safety in various areas of traffic in and out of cities such as traffic intersections, pedestrian crossings, or blind spots. On the other hand, there is a challenging decision making process between data offloading for improving application performance and keeping critical data in-vehicle for privacy and liability reasons. Especially, liability and accountability concerns are likely to play a determinant role on these scenarios. Other than the safety, there can be various mobility applications. A few of these applications, which can be enabled by distributed sensing and analytics, are listed below.

- Digitalization of the cities: e.g. for improving navigation, transportation and parking services
- Pothole or obstacle detection: Enabling comfort and efficiency.
- Dynamic infrastructure: making dynamic changes to the infrastructure for cost and energy efficiency, e.g. pop-up bike lanes.

The above-mentioned sensing and analytics applications mostly involve dealing with personal and sometimes confidential information, thus privacy-aware system design is a key aspect. The privacy-aware design would have particularly more importance when the new systems evolve from research-level prototypes towards real deployments. Trade-offs between utility and privacy are not well understood, and privacy by design should become the state-of-the-art. Yet, a quantification of the trade-offs would be valuable.

The future of Cooperative-Intelligent Transportation Systems (C-ITS) and the challenges for integration of VRU into the picture was widely discussed. It was consensual that to a large extent the technical problems have been covered in previous research, and the biggest hurdles to actual implementation are of societal, legal, political and economic nature. Nevertheless, several open research directions were identified.

- Improved large scale simulation models and digital twins enabled by high performance computing will enable a better understanding of behaviours. Current simulation solutions are often closed, proprietary, expensive, and of limited access. Lowering the cost for such solutions, e.g. using open source to facilitate evolution, expansion and integration of different simulation environments, enabling this integration on multiple-locations, etc would be of great value to a broad research community. Current status is assessed as very early infancy.
- Sensing and analytics plays a key role to build these models: mobility micro-models for traffic participants, especially VRUs, behavioural models (operational, tactical and strategical) in complex and safety relevant situations, traffic light models. It is of special relevance to study and model unexpected behaviours or behaviour/ intention change, as these are more likely to cause hazardous traffic situations. The metrics to validate such models are also in their infancy.
- Little data exists about accidents and their analysis, and access to existing data is a challenge for collaborative research, e.g. accident analysis databases like GIDA require very strict NDAs. User interface research for interaction with VRUs is another research direction with significant gaps.

Much of this research is strongly inter-disciplinary, and disciplines like transportation, urban planning and human factors need to be involved.

4.2 Edge computing

Falko Dressler (TU Berlin, DE) and Gürkan Solmaz (NEC Laboratories Europe – Heidelberg, DE)

The breakout discussion on edge computing started with the discussion for relevance and applicability of edge computing in terms of the communication and cost of resource usages. There are several questions raised for the applicability of the edge computing:

- Who should manage the edge servers?
- Which computations should happen at the edge?
- What are the communication requirements of mobility applications?

Starting with the first question, there is a question on whether mobile service providers or original equipment manufacturers (OEMs) should deploy and host the edge servers. For instance, mobile service providers may not have interest to realize dense deployments but OEMs can build edge servers on the cars and loads of data can start coming from the cars. For the second question, high-definition map building through video could be considered. Such application would cause high demand in terms of computation cost, bandwidth, and latency due to transfer of videos and the tasks of high-definition map building. There are, however, many more lightweight applications, which intelligent transportation systems applications could benefit from.

As a benefit of edge computing, the edge layer can serve as a buffer, where various computation tasks such as preprocessing could be performed on the edge; and extracted information could be shared with the cloud. Considering the other way around, the edge servers might share data with the vehicle for the internal computation and actuation of the vehicle. However, such critical scenarios will need to be carefully designed to avoid security vulnerabilities. For instance, steering a vehicle by bringing data from edge or cloud might create vulnerabilities to attacks. Furthermore, as vehicles move, they will occasionally be in out-of-coverage areas of the service providers. Thus, basic services and decisions such as steering can stay in the vehicle itself, whereas certain information that could not be collected through in-vehicle sensors may enable a smoother ride.

Edge computing would enable various applications, some of which are discussed during the breakout meeting. These applications include "cooperative" applications that require multiple vehicles as opposed to having a single vehicle behaving independent from other vehicles. At the initial phases of edge computing, a pragmatic approach would be to start with a "minimum viable edge". The minimum viable edge would have services that are beneficial and easily applicable. For instance, assisting consensus building or creating local dynamic maps based on information collected from various vehicles could be implemented on the edge. For the latter, information can include traffic congestion, obstacles (e.g., potholes), disasters (e.g., water pipe burst), and other unexpected events (e.g., animal nearby). Moreover, applications that are not safety critical such as parking services could be more efficient through the application of edge computing.

One important aspect is the physical placement of the edge computing – if realized on cars. Several possible options exist for the physical placement:

- Intersections, where many vehicles pass by regularly
- Parked vehicles, where the computing platform could be made available
- Charging stations, where vehicles wait for relative long times.

The final part of the breakout discussion focused on the business models for future mobility use cases in terms of edge computing. Recently, vehicle manufacturers have become more like "data" companies as they collect mobility data from the vehicles and users. For the data ecosystem aspects, developments in the fields data contextualization (e.g., FIWARE, smart data models), for understanding data and creating value, as well as data spaces (e.g., Gaia-X, IDSA) for data sharing and exchanges between different parties are becoming highly relevant.

4.3 Trust

Frank Kargl (Universität Ulm, DE) and João P. Vilela (University of Porto, PT & INESC TEC – Porto, PT & CISUC – Coimbra, PT)

Trust can be considered a key aspect of resilient systems, reliably assessing a systems trustworthiness enables informed decisions with respect to, for example, safety- or security-critical functions. This working group discussed trust in cooperative, connected & automated mobility (CCAM) starting with looking at different dimensions of trust. We distinguished a technical, human, and regulatory notion of trust. The technical perspective is based on a notion of functional trust, i.e., the trust that one entity puts in another entity to perform a specific function in a trustworthy way. Alternatively, this can also mean that named other entity can provide certain data accurately. For example, this can refer to another vehicle correctly reporting its position in a CAM message where a receiving node has to rely on this data to predict collision risks. Modeling such trust relationships between components in an automotive system of systems leads to a trust graph that could be modelled using a formal logic to quantify the amount of trust and reason over trust relationships. Subjective logic trust networks are one suitable formalism which was illustrated in the plenary talk of Frank Kargl. With such an approach, a functional model of a system could be augmented with a trust model that allows to reason about technical trust in the system both at design and at run-time. Subjective logic provides the appealing property to allow reasoning under uncertainty with incomplete evidence. Open questions here include how and where to find the initial evidence for trustworthiness to feed the trust model with concrete data. This could come from looking at trust- or node-related trust as distinguished in a survey on misbehavior detection [1]. Furthermore, the structure of trust networks and reasoning approaches and the expected and required levels of trust require further investigation.

Human aspects

A purely technical treatment of trust would deny the fact that such vehicles are meant to transport humans safely and that those humans ultimately also need to trust the technical system to have a comfortable ride. This human aspects focused on the human perception of trust, which is challenging due to the fact that different people reason differently about the trust levels of different entities, be it automated vehicles or other users in the system. This is a highly subjective assessment that depends on many different personal notions of trust. For this, mental models of trust could be devised, as was done previously in privacy research [2], as well as creating user profiles that represent different user perspectives of trust. The generation of such profiles can be helpful to effectively predict user's preferences based on

their perspectives on trust. The human aspect of trust perception is not sufficiently explored, in particular not in the context of technical systems and their objective trustworthiness. Open challenges here include being able to convey technical and regulatory trust mechanisms to users in an effective manner, as well as assessing the effect of such functional and regulatory mechanisms on the human perception of trust. Moreover, due to the subjectiveness of trust notions stemming from the distinct risk-perception of users, user profiles may be useful to accurately model an individual's perceptions of trust. However, such profiles must be created while also respecting privacy principles. This can come from federated learning mechanisms to predict users' preferences through user profiles in a privacy-preserving manner [3].

Regulatory aspects

The impact of regulations on trust is another relevant dimension that has an impact on both the technical solutions developed, as well as the human factor of trust perception. On the one hand, regulations define minimum requirements that technical solutions must abide to and thereby guarantee a certain level of safety. This is both a source of trust for us humans, as we assume these regulations to be in place and enforced and thus providing our safety. From a technical perspective, such regulations also provide us with certain assumptions about the trustworthiness of automotive systems and products that we can reflect in our trust models. The challenge here is to translate from regulatory requirements to the trustworthiness reflected, for example, in a Subjective Trust Network. Such a translation is by no means straightforward and defining such a quantification requires additional research. On the other hand, we having precise trust models would allow us to assess trustworthiness and trust requirements for automotive systems in a well-defined way, something that regulations might mandate one day, similar to safety and security analyses are mandated today. With respect to the human aspect, regulations can improve the perception of trust by users, if there is awareness that regulations are strictly enforced and there are visible consequences to institutions that do not comply. A set of challenges arise in this context, namely having auditing mechanisms that are effective in assuring compliance, otherwise a risk assessment may lead to conclusions that the risk and consequences of not being compliant may be worth it. Another challenge lies in the effect of regulations on users' interactions with services. It is known from privacy research that users exchange privacy for small benefits [4]. Additional research is needed to assess if the same holds with respect to trust.

Perceptions of Trust

The discussion group then dived deeper into trust perception. We identified that the perception of trust can be affected by technical solutions and regulatory aspects. With respect to the technical solutions, there are two relevant factors having effect on the trust level achieved:

- The effectiveness of technical solutions in conveying a feeling of trust to the users. For example, are users able to understand what measures a system takes to actually be trustworthy? This requires the ability to translate complex technical solutions into a common language that can be easily communicated to and understood by the average user.
- The usability of the technical solutions. A good technical solution can be easily compromised if it is not usable or affects the level of service that users expectto obtain. The challenge here lies in being able to develop technical solutions that are effective to increase trust, yet without being intrusiveor compromising usability.

A well-known example of a technically sound but not widely adopted trust mechanism is that of Pretty Good Privacy (PGP) to increase security and trust on email communications. It is recognized that PGP is an effective technical solution to increase security and trust of email, but failed from a usability perspective by putting the burden of managing part of the system on users. Users expect technical solutions to be as transparent and automated as possible, although providing visual cues that the system is compliant (e.g., the lock that represents an effective secure HTTP connection when browsing websites). This challenge of devising effective technical solutions that are usable remounts to early days of email, but still holds nowadays. An opposite example is that of trust in avionics. Although the general user/client is not aware of the specifics of regulations that rule the sector, there is a general feeling of trust in such system, instilled by a perception that there are tight regulations and inspections in place, as well as well-defined procedures to adopt in case of incidents. In this case, the user easily accepts tight restrictions and the burden of security controls, in exchange for a more secure system. This is also a natural consequence of the possible impacts of non-compliance: if on the previous example of PGP, the consequence may just be the impersonation of the sender of emails, in this later case it may be a question of life or death. Sousers are likely more willing to accept more complex security- and trust-enhancing mechanisms if their goal is to protect critical assets. Whenever the goal is to protect less tangible or not so critical assets, users expect trust-enhancing mechanisms that are transparent/automated to cause as little disturbance as possible to their operations/usability. Moreover, regulations can have a positive effect on perception of trust, but mostly if there is evidence that such regulations are known to have consequences (e.g.security checks at airports, or auditing of institutions for non-compliance).

Trust in Automated Driving

We then continued to discuss how these insights could be transferred to trust in automated driving compared to trust in today's manually driven vehicles. Regarding the human perception, people tend to desire to at least feel in-control. Therefore, it is important to keep human passengers informed and involved even in a human vehicle. On the other hand, given too much control back to humans, like allowance to make the car speed, might also introduce human error again and might make driving more unsure. So this needs to be investigated and balanced for automated driving. As evidenced by the avionics industry, tight regulations and inspections can instill trust in a system even though the passengers are not in control at all. If trustworthiness of a system can be assessed appropriately, this might even lead to some product certification like, e.g., NCAP or produce some online display of trust status to passengers. If this is helpful or damaging to trust requires investigation. The question should also be if trust assessment is confined to the single vehicle only. As vehicles start to form cooperative systems, the trustworthiness of the overall system should move into focus. Automated driving surely poses many challenges to safety. One involves the fact that it is hardly possible to predict every possible driving situation an automated car might be exposed to beforehand. Therefore, a continuous self-assessment of a vehicle might become a very important feature for autonomous vehicles. First simple self-assessment features are already implemented with today's cars. In such a self-assessment, a sound trust model might be a vital part, as the ultimate question the vehicle has to answer is whether it is still operating trustworthy.

In summary, in order to increase trust in automated driving, we recommend the following steps:

- deepen our understanding how to quantify trust in a complex automotive system-of-systems,
- precisely define what levels of trust are required,
- analyze sources of trust-related information, for example misbehavior detections systems, hardware security mechanisms, or certification,
- investigate how to interface an automated trust management with the driver,
- identify what action to take if insufficient trust is detected, e.g., initiation of a minimum risk maneuver.

References

1 Van der Heijden, R.W., Dietzel, S., Leinmüller, T. and Kargl, F. (2019). Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. In IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 779-811, doi: 10.1109/COMST.2018.2873088.
2 Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., and Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In Proceedings of the 2012 ACM conference on ubiquitous computing, pages 501–510.
3 Brandão, A., Mendes, R., and Vilela, J. P. (2022). Prediction of mobile app privacy preferences with user profiles via federated learning. In Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy.
4 Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, vol 347, issue 6221, pages 509–515.

4.4 Vulnerable road users

Gunnar Karlsson (KTH Royal Institute of Technology – Stockholm, SE), Khalil Ben Fredj (University of Twente – Enschede, NL), Klaus David (Universität Kassel, DE), and Marie-Christin Hannah Oczko (Paderborn, DE)

Overview and problem formulation

New technologies in motorized vehicles provide active collision avoidance that reduces both the risk of accidents as well as their severity. In addition, drivers and passengers are protected by their cars and trucks. Hence, their safety in traffic is progressing; a vision of zero fatalities might be reached eventually with autonomous vehicles. In contrast to that, traffic safety for vulnerable road users is decreasing as more and more persons switch from transportation by automotive vehicles to walking or to riding bicycles, scooters and other light and unprotected motorized vehicles. The topic of discussion in this breakout groups has targeted how modern computing and communication technologies might be used to improve the safety of vulnerable road users (VRUs). We noted that most developments regarding VRU safety are for heavier vehicles to detect pedestrians crossing roads and bicycles at right turns, and other dangerous situations. Alas, there is little attention to technology support for avoiding collisions among VRUs: bikers with other bikers, bikers with pedestrians who stray into bicycle lanes, and other equally well-known and contentious situations. It is clear by design that developments for autonomous driving have little use for road users who are in direct control of their vehicles, or for pedestrians who do not use a vehicle at all. The system support must hence aim at raising awareness of other road-users and of potential dangers in the infrastructure, such as slippery road conditions, ongoing road works and missing or inconsistent signs and directions.

The group discussed the categorization of vulnerable road users and concluded that it may be broad, considering both pedestrians and runners, people on horseback or in wheelchairs, and users of any two- or three-wheeled vehicle. We decided to focus on three common categories: pedestrians (including runners), bikers (with and without electric motoring), and scooter drivers. As stated, a general problem is lacking awareness of other road users such as bikers approaching pedestrians and faster, overtaking bikers from behind, as well as approaching but visually obstructed bikers. Here the transmission of radio beacons could be used to alert the surrounding traffic. The other type of alert regards the infrastructure where people need warnings of unsafe situations and road conditions, and connectedly how the unsafe spots might be detected, reported and disseminated to others.

Beaconing for increased awareness

The group worked through a design discussion to determine necessary considerations for making a beaconing system for VRUs. We discussed technology design regarding the radio and the protocols for beaconing. Firstly, the group discussed two options of communication: device-to-device communication (ad hoc) and of vehicle-to-infrastructure communication. The second option would use the mobile communication infrastructure (4G and beyond) with positioned users and processing in edge or cloud computing servers. For the D2D option, we discussed needed range and directionality of the transmissions and the position of the receivers, the potential contents of the beacons, the frequency of transmissions, and the use of standard radio technology, such as variants of Bluetooth, WiFi or even ZigBee. We considered a baseline design for a broad use based on radio interfaces in common mobile phones, which could be augmented by external devices (antennae, LIDAR and more), mounted on the vehicle, or on the road user (for instance on the helmet). The second compound of questions relates to the reception and processing of beacons. The contents of beaconing messages could include speed and speed variations, direction and steadiness, as well as type of vehicle and its dimensions. These messages, possibly received from many simultaneously approaching vehicles, should be compiled, prioritized, assessed, and formed into meaningful alerts or warning messages to the road user. This leads to the third topic of discussion: the interaction of the system with the human. We did not have any expert present on human-machine interaction and foresaw that it is a most germane area of research for the system. The alerts must be timely – allowing human reaction time; accurate – not causing false warnings; meaningful – leading to correct actions, and non-distracting – not causing dangerous situations.

Sensing and communication

The other area of safety concerns for VRUs relates to traffic intensity, road conditions, and design and state of the infrastructure (for instance, unsafe solutions, and broken traffic signals). Data for this area might need a centralized collection and compilation of reports from pedestrians and bikers as well as sensing data from the bikes (such as vibrations, and accelerometer measurements indicating sliding, heavy breaking, potholes, or falls). Similar to the beaconing, these messages need to be collected and compiled into meaningful alerts and warnings which have to be locally disseminated to where they have relevance to road users. Aggregated reports could also be provided to road authorities for improving the conditions or expediently removing dangers (for instance by sanding icy patches). For all

types of beaconing and reporting of unsafe spots, it is important that the users can remain anonymous and untraceable. Otherwise, a misuse of information endangering individuals might be possible. There are likely other security and privacy aspects that we did not have time to discuss.

Concluding remarks

The two discussion sessions were fruitful and we developed our own understanding of the issues by working through a self-defined scenario for bikers overtaking one another. It opened up suggestions for many additional options such as use of image sensors and radar, and various feedback to the user through smart glasses with displays, tactile signals as well as auditory signals and messages. Several participants in the two sessions were interested in conducting a preliminary study on the feasibility of some of the ideas generated with the hope of defining a larger design study for experimental evaluation. We are grateful for the possibility to meet at Dagstuhl for this engaging discussion around an important problem area.

4.5 Vehicle to cloud to vehicle communication

Michele Segata (University of Trento, IT) and Onur Altintas (Toyota Motor North America – Mountain View, US)

V2V communications and potential applications have been proposed and investigated for more than 20 years. Yet, despite the large effort by both academic and industry research communities, technologies like IEEE 802.11p and C-V2X, as well as the applications that are built on them have not seen widespread deployment. On the other hand, most automakers ship new vehicles with cellular modems to enable, for example, data collection for diagnostic purposes. There is the possibility to exploit such means to potentially realize inter-vehicle communication and applications. Data coming from vehicles to be processed by the car manufacturer is handled by cloud computing facilities, so we refer to this type of inter-vehicle communication as vehicle to cloud to vehicle (V2C2V).

The aim of the breakout session was the analysis of potential benefits and drawbacks of such an approach to inter-vehicle communications. In particular, the breakout group indicated that the first point to be addressed is finding out the set of applications for which V2C2V could actually bring benefits with respect to V2V. One example is data aggregation, where a cloud-supported centralized solution would be easier to implement and more efficient than a fully decentralized one. An additional use case could be the one of cooperative maneuvers in urban scenarios. A centralized approach might ease gathering data and compute the best coordination strategy to be then communicated back to the vehicles, whereas a decentralized V2V solution might incur communication challenges due to the harsh environment. The second point raised by the group is that different OEMs might rely on different mobile operators and, in addition, they might resort to different cloud computing facilities. This opens a problem of interoperability between different car manufacturers.

First of all, in such cases, which operator's resources should handle the communication? Which spectrum should be used? More than technological, this question is mainly answered by agreements and business policies, which can definitely slow down the adoption of such systems.

The group discussed potential solutions to this problem, one being peering agreements between operators. In such case one of the biggest problems would be performance guarantees. As in classical Internet routing, operators might give higher priority to traffic belonging to their customers, but especially for safety applications this might be unacceptable. To encourage operators to cooperate, one solution would be to dedicate a portion of the spectrum for safety-related V2C2V communications which all operators could use for free.

Second, data sharing across different manufacturers is a complex issue. One option could be to agree on minimum amount of safety-related information to be shared so that the safety applications can be deployed without compromise. This clearly requires to define what is the minimum amount of information to be shared that can effectively improve vehicular safety. Here, regulations and standards may play a vital role in determining the minimum necessary set of safety information to be shared among automakers.

Finally, the discussion touched upon issue of deciding who is paying for the service, which relates to the incentives that could be granted by governments. Differently from pure V2V communications such as IEEE 802.11p, the use of cellular technologies does not come for free. A car manufacturer might sell a cellular data plan included in the price of the vehicle, but only for a limited amount of time. If customers have to take over the expenses after this period expires, we incur the risk of them bailing out, with a potentially negatively impacting on safety.

In conclusion, V2C2V might provide benefits to the vehicular domain, but applications and requirements need to be well-defined. In addition, we believe the role of governments and regulators to be fundamental.

5 Open problems

5.1 Connecting Bikes

Ana Aguiar (Universidade do Porto, PT)

Joint work of Pedro Santos, Luís Pinto, José Pintor, Eduardo Soares, Pedro D'Orey, João Mesquita, Miguel Rosa, Luís Almeida

Main reference Luis Ramos Pinto, Pedro M. Santos, Luís Almeida, Ana Aguiar: "Characterization and Modeling of the Bicycle-Antenna System for the 2.4GHz ISM Band", in Proc. of the 2018 IEEE Vehicular Networking Conference, VNC 2018, Taipei, Taiwan, December 5-7, 2018, pp. 1–8, IEEE, 2018.

URL https://doi.org/10.1109/VNC.2018.8628395

Bicycles are a healthy and environmentally friendly transportation mode that is increasingly used for commuting. Connecting bicycles to other vehicles is an enabler for a large variety of services, from safety to infotainment. Conversely useful and comfortable applications could make cycling more attractive. This talk shows demonstrations of motivating applications supported by Bluetooth Low Energy (BLE): a stolen bike detection system [1], and a broadcast walkie-talkie for a platoon [2].

The talk evolves to explore connectivity aspects needed to support such applications, both to connect bicyles to one-another and to the infrastructure. A characterisation 2.4 GHz operating technologies on bike-to-bike links using commodity hardware shows that BLE range exceeds 50m at low packet loss rates [3]. A dependence on relative bike positions was identified. Anechoic chamber measurements with bikes allowed to characterise the dependence of bike-to-anything links on antenna position and bike material [4].

References

1 P. M. Santos, M. Rosa, L. R. Pinto and A. Aguiar, Cooperative Bicycle Localization System via Ad Hoc Bluetooth Networks, IEEE VNC 2020
2 E. Soares, P. Santos, L. Pinto, P. Brandão, R. Prior, A. Aguiar. Demo: VoIP System for Bicycle Platoons IEEE VNC 2018
3 P. Santos, L. Pinto, A. Aguiar, L. Almeida. A Glimpse at Bicycle-to-Bicycle Link Performance in the 2.4GHz ISM Band, IEEE PIMRC 2018
4 P. Santos, L. Pinto, L. Almeida , A. Aguiar. Characterization and Modeling of the Bicycle-Antenna System for the 2.4GHz ISM Band, IEEE VNC 2018

5.2 On Realistic Scenarios for Hazard Perception of Vulnerable Road Users

Jérôme Härri (EURECOM – Biot, FR)

Joint work of Ali Nadar, Mathis Lafon, Jérôme Härri
Main reference Ali Nadar, Mathis Lafon, Jérôme Härri, A RounD-like Roundabout Scenario in CARLA Simulator, in Proceedings of the 4th Symposium on Management of Future Motorway and Urban Traffic Systems (MFTS2022), Dresden, 2022.
URL https://gitlab.eurecom.fr/cats/carla/round-carla

Evaluating contextual hazard of vulnerable road users (VRUs) under realistic driving and sensory contexts are critical to the integration of VRU with legacy and automated vehicles. Over the last decades, various synthetic scenarios have been designed and calibrated for microscopic simulators for SUMO mostly focusing on vehicles. Realistic traffic datasets including VRU such as RounD have been used to extract and learn precise driving and hazard patterns but cannot be modified to evaluate the impact of C-ITS safety applications for VRU in the dataset environment. The driving simulator CARLA has been designed to model robotic and sensory context in highly precise driving environment, which makes it perfectly suitable to model VRU in mixed traffic scenarios. However, most of the studies using CARLA focuses primarily on the modeling or the perception of an ego-vehicle (or a VRU) either isolated or under unrealistic traffic. Considering that realistic traffic interacting with VRU is critical to identifying hazard contexts for VRUs, this talk presents an open-source CARLA [1] scenario reproducing the RounD dataset and discuss its benefit to integrate realistic perception of VRUs.

References

1 RounD scenario for CARLA, `https://gitlab.eurecom.fr/cats/carla/round-carla`

5.3 Joint Communication and Sensing for V2?

Renato Lo Cigno (University of Brescia, IT)

Joint Communication and Sensing (JCS) is a staple of 6G and future Wi-Fi systems. The idea is using SCI (Channel State Information) collected at the PHY layer for MIMO, equalization, and so forth, to *sense* or *sound* the environment. Sensing includes localization, motion

recognition and much more. Early works are promising, though not yet definitive, and focus mostly on indoor scenarios. The question is: can this technology be exported to vehicular environments and VRU protection too? Open question that I hope someone can tackle. One further question is if we can also protect the privacy of users against attacks based on EM fingerprinting at the PHY layer that cannot be countered with cryptographic techniques. Also this question has initial positive answers, but more research is needed.

5.4 Reconfigurable Intelligent Surfaces for Edge and Cooperative Driving

Michele Segata (University of Trento, IT)

Joint work of Marios Lestas, Paolo Casari, Taqwa Saeed, Dimitrios Tyrovolas, George Karagiannidis, Christos Liaskos

Reconfigurable Intelligent Surfaces (RIS) are communication devices capable of reflecting impinging wireless signals towards a certain direction, and the reflection angle can differ from the incidence one. These devices can be particularly useful in non-line-of-sight conditions, which are typical for mmWave communications. RIS could find application in vehicular communications to enable around-the-corner communications in the mmWave band, which could be especially beneficial for bandwidth-hungry applications such as cooperative perception or vehicular edge computing. The talk presents such opportunities but also the challenges connected to it, which include huge path loss due to the reflection, RIS scheduling, performance evaluation, and tracking of the users.

5.5 Performance Evaluation of Inter Vehicle Communication (IVC) for Vulnerable Road Users (VRUs)

Christoph Sommer (TU Dresden, DE)

Commoditization of system-level Inter Vehicle Communication (IVC) simulation has beneftitted research greatly. It commonly rests on three pillars: metrics, models, and scenarios. In the past few years, a rich set of all of these has slowly been made available for research on Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) use cases. This meant that high-fidelity experiments were no longer conditioned on the availability of resources for large field operational tests, nor was scale limited to just a few situations or vehicles, as afforded by hardware-in-the-loop type simulation. All of this has propelled research in the area of "traditional" Inter Vehicle Communication (IVC) forward. However, the case could be made that, while fragmented efforts exist [1, 2], a comprehensive set of generalizable metrics, models, and scenarios is still missing for researching Vulnerable Road Users (VRUs) centric use cases. We talk about how such a set might look like with a view towards generalizability and reproducibility of research.

References

1 L. Pinto, P. M. Santos, L. Almeida and A. Aguiar, "Characterization and Modeling of the Bicycle-Antenna System for the 2.4GHz ISM Band," 2018 IEEE Vehicular Networking Conference (VNC), 2018, pp. 1-8, doi: 10.1109/VNC.2018.8628395.

2 RounD scenario for CARLA, `https://gitlab.eurecom.fr/cats/carla/round-carla`

Participants

- Ana Aguiar
Universidade do Porto, PT
- Onur Altintas
Toyota Motor North America – Mountain View, US
- Khalil Ben Fredj
University of Twente – Enschede, NL
- Claudio Casetti
Polytechnic University of Turin, IT
- Carla-Fabiana Chiasserini
Polytechnic University of Turin, IT
- Klaus David
Universität Kassel, DE
- Falko Dressler
TU Berlin, DE
- Jérôme Härri
EURECOM – Biot, FR
- Geert Heijenk
University of Twente, NL
- Frank Kargl
Universität Ulm, DE
- Gunnar Karlsson
KTH Royal Institute of Technology – Stockholm, SE
- Florian Klingler
Universität Paderborn, DE
- Renato Lo Cigno
University of Brescia, IT
- Marie-Christin Hannah Oczko
Paderborn, DE
- Jörg Ott
TU München, DE
- Michele Segata
University of Trento, IT
- Gürkan Solmaz
NEC Laboratories Europe – Heidelberg, DE
- Christoph Sommer
TU Dresden, DE
- Lukas Stratman
TU Berlin, DE
- João P. Vilela
University of Porto, PT & INESC TEC – Porto, PT & CISUC – Coimbra, PT
- Lars Wolf
TU Braunschweig, DE