Future connected vehicles: Communications demands, privacy and cyber-security

Citation for the original published paper (version of record):
Olovsson, T., Svensson, T., Wu, J. (2022). Future connected vehicles: Communications demands, privacy and cyber-security. Communications in Transportation Research, 2.
http://dx.doi.org/10.1016/j.commtr.2022.100056

(article starts on next page)

Communications in Transportation Research 2 (2022) 100056

Contents lists available at ScienceDirect

Communications in Transportation Research

journal homepage: www.journals.elsevier.com/communications-in-transportation-research

Editorial

Future connected vehicles: Communications demands, privacy and cyber-security

1. Introduction

With the advance of data collection, data processing, telecommunication and vehicular technologies, connected vehicles (CVs) have been emerging as a crucial branch of smart mobility (Olia et al., 2015; Li et al., 2021). Its basic idea is to realize real-time exchanges and processing of essential information, such as positions and destinations, among surrounding vehicles and infrastructures. With connected vehicles, we can expect a paradigm shift of traffic management from the traditional reactive approach to the more efficient proactive approach. Specifically, the merits and implications of CVs can be found in bringing new solutions to the most challenging and vital transportation problems, and from group-based management to more individualized management, including but not limited to congestion mitigation, energy minimization, and traffic safety improvement.

At the macroscopic level, CVs will be able to receive real-time route choice guidelines to avoid bottlenecks (Wang et al., 2021). Although there are already similar services such as Google Maps, the information only indicates aggregated traffic states. With information from CVs, the accuracy and usability of traffic state estimation will be considerably improved, which is pivotal for congestion mitigation. At the tactical level, taking signalized intersection control as an example, CVs could feed their positions and destinations to the traffic controller and receive driving guidelines from the controller to enhance the centralized control. At the microscopic level, vehicle-to-vehicle (V2V) communication techniques could preliminarily realize cooperative driving. Although the cooperation cannot be as advanced as that in autonomous driving cases, the benefits are still significant. Existing studies have demonstrated that, through basic communication, CVs could reduce travel time up to 50% at work zone areas and drive more safely in critical scenarios (Cao et al., 2021), as illustrated in Fig. 1.

Another immediate implication is to reinforce emergency vehicle (EV) preemptions (Wu et al., 2020). Emergency vehicles are critical in saving lives and avoiding property loss and thus have been the focus in post-accident management. In the current practice, emergency vehicles, i.e., fire trucks and ambulances, largely rely on the horns and obligations of surrounding vehicles, which are not only highly unreliable for EVs but also disruptive for normal traffic. It is commonly seen that an EV is blocked in the middle of a less-congested road only because surrounding vehicles are not able to clear one lane on such short notice of the horn. With V2V techniques, the communication between EVs and normal vehicles can be substantially extended and enable a more gradual and reliable clearance of the lane.

2. Communication demands

To realize the above possibilities, reliability, low latency, and secure connectivity will be a key enabler. The 5th generation of mobile communications (5G) technologies and beyond will enable road users and vehicles to be connected to the networks as well as to communicate directly with each other (Fallgren, 2020; Fallgren et al., 2018). With 5G and its evolutions, users will expect the connected society to be available with no limitations, and users will make use of bandwidth-demanding services like augmented reality and virtual office applications, also when on the move. The modern vehicle itself is also emerging as a heavy consumer and producer of information that constantly collects and receives information that could be highly valuable to support smart city, such as sensing air quality, monitoring noise levels, route guidance, etc.

In this context, future transportation system may also play an important role in wireless networks and thus become an integrated part of the communications infrastructure, thus forming integrated moving networks to improve capacity and coverage of the mobile networks. In return, vehicles would benefit from the additional capacity and reliability of the mobile network service for their own connectivity and sensing needs. Such steps are currently being taken within ongoing research towards the 6th generation of mobile communications (6G), in the area of joint communications and sensing (radar) and mapping (De Lima et al., 2021), as well as on the evolution of mobile edge computing towards a distributed platform hosting artificial intelligence based learning and inference services. There are also untapped possibilities to explore various kinds of situational awareness information to improve communications, like road infrastructure information, driving route information, positioning, and social networks.

3. Cyber-security and privacy

Key challenges when implementing all these new services are how to guarantee privacy, security and implement authentication and owner protection of the information sources. Safety work for vehicles has in the past focused on hardware and software failures but with the increased

https://doi.org/10.1016/j.commtr.2022.100056
Received 19 January 2022; Received in revised form 10 February 2022; Accepted 10 February 2022
Available online xxxx

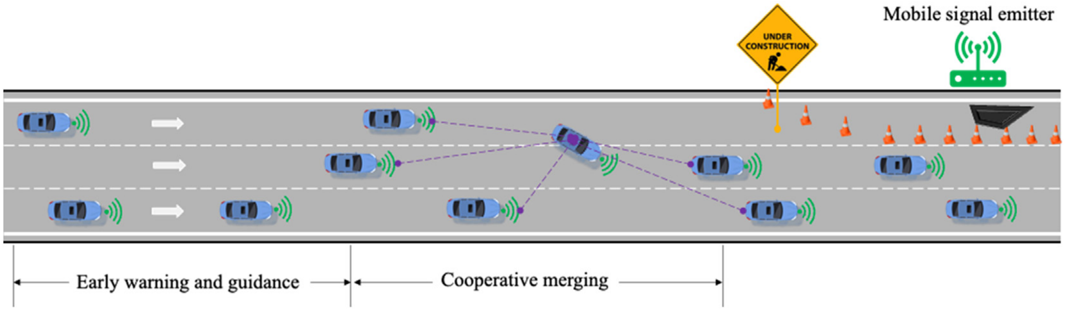

Fig. 1. Communication and cooperative driving in work zones.

connectivity, cyber-security is now of uttermost concern. Security should be there as an invisible component guaranteeing that all communication and exchanged information is authentic and correct.

Securing automated vehicles is much harder than it may seem. Vehicle complexity is constantly increasing and we are currently transitioning to massively parallel computers with thousands of processor cores offering various types of functionalities with both internal and external communication, such as Bluetooth, WLAN, IEEE 802.11p and mobile communication that are all susceptible to attacks. Since new threats constantly appear and new weaknesses are discovered, smart intrusion detection systems are needed to detect all deviations from normal behaviors. Detection is however not enough. Vehicles also need to take immediate action to limit possible consequences when a deviation is discovered. Therefore, they must be designed to be resilient and able to immediately reconfigure themselves while waiting for a software update to arrive (Rosenstatter et al., 2020).

Cyber-security is not only an issue for the vehicle or the vehicle owner. Fleet-wide attacks may be spawned and even worse. Attacks can be directed towards cloud-based services, for example, to disturb route selection. When information is exchanged, it is necessary to *authenticate* the sender using certificates, *authorization* to see if an entity is allowed to send a particular type of message, verification of the *authenticity* and *freshness* of every message which involves checking that it has not been altered or is a replay of an old message (Strandberg et al., 2018). In addition, to ease forensics investigations, *non-repudiation* is an important component to trace back the sources of all messages preceding an event. Key information may also have to be encrypted to preserve *confidentiality*. Finally, we also have to consider *privacy* issues since much data in and around vehicles reveal information about the driver and passengers. All these security functions for CVs will not come for free. Security makes communication more error-prone since more information is transmitted, more things may go wrong, and more recovery mechanisms have to be implemented. This can to some extent be mitigated by having good and reliable communication channels with low round-trip delays.

4. Conclusions

Connectivity is the indispensable component in the highly anticipated smart mobility, while communication and safety guarantees are the backbones paving the road towards this future. Without sufficiently fast, resilient, and robust network communication, critical tasks such as cooperative driving will be significantly hindered, and safety & privacy performance largely determines whether such techniques will eventually be put into practice. Although we highly value the merits of communication guarantees in this paper, there are also other key aspects that must be investigated in the development and implementation of connected vehicles, such as computation. When implementing CV services, it is necessary to decide where data should be processed. If computations are done by each vehicle, they need more computational resources and they will also perform duplicated work with finding solutions to the same problem. This will possibly result in different outcomes since we cannot guarantee that they will receive the same information due to message loss, corruption, or limited bandwidth. If computations instead are conducted by roadside servers or in the cloud, computations can be more efficient, and it is possible to make optimal decisions albeit being more dependent on good network coverage with high bandwidth and low delays. It is so far not obvious where these computations should be done and it may vary depending on the type and quality of service needed and on communication quality. In this regard, communication and computation are to some extent twisted, and the current solutions are far from satisfactory. In summary, more research is warranted before highly functional and safe connected vehicles can be eventually realized.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research is sponsored by Vinnova projects SoSer. We would like also to acknowledge the constructive discussions with the Editor-in-Chief.

References

Cao, D., Wu, J., Wu, J., Kulcsár, B., Qu, X., 2021. A platoon regulation algorithm to improve the traffic performance of highway work zones. Comput. Aided Civ. Infrastruct. Eng. 36 (7), 941–956.

De Lima, C., Belot, D., Berkvens, R., Bourdoux, A., Dardari, D., Guillaud, M., Isomursu, M., Lohan, E.-S., Miao, Y., Barreto, A.N., Aziz, M.R.K., Saloranta, J., Sanguanpuak, T., Sarieddeen, H., Seco-Granados, G., Suutala, J., Svensson, T., Valkama, M., Van Liempd, B., Wymeersch, H., 2021. Convergent communication, sensing and localization in 6G systems: an overview of technologies, opportunities and challenges. IEEE Access 9, 26902–26925.

Fallgren, M., 2020. Cellular V2x for Connected Automated Driving. S.L.: Wiley-Blackwell.

Fallgren, M., Vilalta, R., Dillinger, M., Alonso-Zarate, J., Boban, M., Abbas, T., Manolakis, K., Mahmoodi, T., Svensson, T., Laya, A., 2018. Fifth-generation technologies for the connected car: capable systems for vehicle-to-anything communications. IEEE Veh. Technol. Mag. 13 (3), 28–38.

Li, H., Zhang, J., Zhang, Z., Huang, Z., 2021. Active lane management for intelligent connected vehicles in weaving areas of urban expressway. J. Intell. Connected Veh. 4 (2), 52–67.

Olia, A., Abdelgawad, H., Abdulhai, B., Razavi, S.N., 2015. Assessing the potential impacts of connected vehicles: mobility, environmental, and safety perspectives. J. Intell. Transport. Syst. 20 (3), 229–243.

Rosenstatter, T., Strandberg, K., Jolak, R., Scandariato, R., Olovsson, T., 2020. REMIND: a framework for the resilient design of automotive systems. In: 2020 IEEE Secure Development, pp. 81–95.

Strandberg, K., Olovsson, T., Jonsson, E., 2018. Securing the connected car: a security-enhancement methodology. IEEE Veh. Technol. Mag. 13 (1), 56–65.

Wang, C., Peeta, S., Wang, J., 2021. Incentive-based decentralized routing for connected and autonomous vehicles using information propagation. Transp. Res. Part B Methodol. 149, 138–161.

Wu, J., Kulcsár, B., Ahn, S., Qu, X., 2020. Emergency vehicle lane pre-clearing: from microscopic cooperation to routing decision making. Transp. Res. Part B Methodol. 141, 223–239.

Tomas Olovsson is an Associate Professor at the Department of Computer Science and Engineering at Chalmers University of Technology, Gothenburg, Sweden. He has been working actively with computer security for more than 25 years, both in the industry and in the academia. His research interests are communications and security and he is currently focusing on security and privacy for Internet-connected vehicles. This work includes secure internal network architectures and secure V2X communications.

Tommy Svensson is Full Professor in Communication Systems at Chalmers University of Technology in Gothenburg, Sweden, where he is leading the Wireless Systems research on air interface and wireless backhaul networking technologies for future wireless systems. He received a Ph.D. degree in Information theory from Chalmers in 2003, and he has worked at Ericsson AB with core networks, radio access networks, and microwave transmission products. He is heavily involved in European top research projects towards next generation mobile communications systems, from 4G, 5G to currently 6G. He has co-authored 5 books, and 230 journal/conference papers. He has been editor/organizer of several top IEEE journals, conferences and workshops, and chair of the awards winning IEEE Sweden joint Vehicular Technology/ Communications/ Information Theory Societies chapter.

Jiaming Wu is a researcher in the Department of Architecture and Civil Engineering. His research interests include cooperative control of connected and automated vehicles and emerging Mobility-as-a-Service systems. He is now leading and involved with several research projects regarding public transit systems, connected and automated vehicle control, and modular autonomous buses. He has published several research articles in top-tier journals such as TR-Part A, TR-Part B, TR-Part C, and CACAIE.

Tomas Olovsson
Department of Computer Science and Engineering, Chalmers University of Technology, Gothenburg, SE, 41296, Sweden
E-mail address: tomas.olovsson@chalmers.se.

Tommy Svensson
Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, SE, 41296, Sweden
E-mail address: tommy.svensson@chalmers.se.

Jiaming Wu[*]
Department of Architecture and Civil Engineering, Chalmers University of Technology, Gothenburg, SE, 41296, Sweden

[*] Corresponding author.
E-mail address: jiaming.wu@chalmers.se (J. Wu).