Department of Computer Science

Submitted in part fulfilment for the degree of MSc

Why autonomous cars are not the technology of tomorrow?

Exam number: Y3864454

07 February 2019

Supervisor: Dr Katrina Attwood

ABSTRACT

The development of autonomous vehicles has significantly accelerated during the past years. Numerous experiments and researches have considerably contributed to the formation of the “appearance” of autonomous vehicles that we are having today. However, before self-driving cars appear on public roads, numerous safety challenges need to be addressed. This paper briefly summarizes key benefits which self-driving cars would provide us with, such as remove of spatial barriers for disabled people, reduce wasted fuel and environment pollution and, most importantly, reduce of traffic accidents and losses of lives. Additionally, the paper underlines the most significant challenges which prevent autonomous automobiles become available, including architecture design issues, security vulnerabilities, the way of interaction with the environment and the problem of storing an enormous amount of sensor data.

STATEMENT OF ETHICS

This literature review is organised by topic, i.e. sources are grouped by their themes and theoretical concepts. Referencing was conducted adequately and correctly represented the ideas and thoughts of other people. That is to say, each source was read and analysed appropriately, i.e. this paper represents the summary and main findings of different researches and studies. The style of referencing is IEEE with list of references in the end of this paper. The findings presented in this literature review do not have limits on their use.

TABLE OF CONTENTS

1 Introduction

Autonomous automobiles have been a dream since the invention of vehicles. Introducing new Intelligent Transportation System which takes into account environmental and ethical issues as well as safety factors is one of the considerable obstacles in developing an autonomous vehicle. Nevertheless, during the last years, several international companies and organisations tried to develop an autonomous automobiles which could dramatically change the future of the transportation system: the European Project Prometheus “which provided support for the development of many ground-breaking technologies that would eventually lead to the driver-assistance systems” [1], the European project Chauffeur [2] which aimed to develop a road train in which only the heading truck is driven by a human driver, the AHS (Advanced Cruise-Assist Highway System) project in Japan “aimed at improvement of road traffic safety, increase in transport efficiency, and alleviation of environmental problems” [3] and many others whose attempts significantly contributed to the formation of the “appearance” of autonomous vehicles that we have today.

The main reason why numerous projects and researchers are devoted to developing a self-driving car is that autonomous vehicles can solve a list of severe problems such as environmental issues (decrease the level of congestion, fuel consumption etc.), ethical challenges (e.g. remove of a spatial barriers for disabled people), but one of the most important problem is human’s safety. According to the World Health Organisation [4], more than 1.25 million people die each year as a result of road traffic accidents. Autonomous cars can, hypothetically, significantly reduce the number of people deaths, “crash rates and insurance costs by 90%” [5]. However, before self-driving cars appear on roads, numerous safety challenges and additional risks, which autonomous vehicles could introduce, need to be addressed.

There have been many studies on the numerous challenges related to self-driving cars such as ethical problems, social acceptance, environmental issues. However, since the focus of this research is on the safety challenges, these studies will not be reviewed in depth, and only referred to when appropriate. This literature review will focus on safety issues in the sense of whether the technology is safe enough for humans, including the safety design decisions which should inherit the principals of fault tolerance logic to prevent numerous potential hazards, cyber security safety, the way of communication between autonomous vehicles, and the issue related to processing and storing an enormous amount of data.

2 Review of Literature

In this section we firstly analyse the major advantages of self-driving cars, how it could change the way of people's lives and, secondly, underline the main challenges which prevent autonomous automobiles appear on roads.

2.1 Key benefits of autonomous vehicles

This chapter we describe the primary reasons why people need a different form of transportation and how it would contribute to their lives, including increased people' mobility, cutting environmental contamination and eliminating the human failure.

2.1.1 Increase mobility

One of the most significant advantage of self-driving cars is an increased mobility of disabled people which could eliminate social exclusion. Dana M. and Mele, J. in their study analyzed "quasi-autonomous" cars, its design solutions and evolution over the years and why such cars present potential advantages for both blind and sighted people. They concluded that introducing autonomous vehicles would "contribute to goals of independence and autonomy for individuals with disabilities and provide valuable innovative technologies to increase safety for all drivers" [6]. Another significant study conducted by scientist from the University of Florida examined 38 blind and low sighted participants in order to reveal their opinion regarding self-driving cars. The findings showed that "the majority of participant comments centered on the potential for increased independence, personal mobility and the potential for time savings versus participants' existing means of transportation" [7].

2.1.2 Cut environmental contamination

Environmental pollution and world' congestions are ones of the most significant problems of 21st century which could be partly solved with autonomous automobiles. According to the study conducted by A. C. Mersky and C. Samaras, "AV following algorithms designed without considering efficiency can degrade fuel economy by up to 3%" [8]. It means that not only environment congestion would be reduced, but also fuel consumption would be decreased which would result in improvements in fuel economy and, thus, low level of released CO_2 emissions which is a key factor of Global Warming and Climate Change problems [9].

2.1.3 Eliminate the human failure

A different form of transportation such as self-driving cars could significantly change the way of driving we are having today. As

Christoph Stiller (Senior Member IEEE) emphasizes, “it is expected that such cars will not only show quantitative effects on traffic, but in the long term will provide a new quality of traffic operation including concerted navigation for safe, comfortable, and efficient driving” [10]. What it means that with autonomous automobiles people would minimize the risk of hazard occurred due to the decrease of human failures such as age, fatigue, external distractions, mobile phone conversations and others. According to data published in “National Motor Vehicle Crash Causation Survey”, driver failure is the most common factor in vehicle accidents (95%). It could be significantly decreased or even eliminated if autonomous vehicles appear on public roads because their decisions based on accurate calculations are more reliable and precise in comparison with humans. What is more, N. Thomopoulos and M. Givoni [11] found in their study that young and elderly drivers are more likely to be involved in accidents and this fatality risk could be eliminated if autonomous vehicles would replace today’s car. Both studies revealed that humans error is the underlying cause of traffic crashes which lead to people’s deaths and autonomous automobiles could potentially prevent numerous traffic disasters.

2.2 Challenges in autonomous driving

However, before autonomous vehicles appear on public roads, some serious challenges need to be addressed. In this section we will look at the most significant obstacles which prevent autonomous automobiles become widely spread. Firstly, we will look at the existing hardware and software designs of the system and why they are still not enough safe for people. Secondly, we will focus on cyber security safety and on cryptography algorithms which could prevent a car being hijacked. Thirdly, we will analyze the way of communication and interaction between autonomous vehicles and what approaches have been proposed. Lastly, we will look at data maintenance and storage challenge and how developers can solve this issue.

2.2.1 Hardware and software design

In order to achieve safety in autonomous vehicles, numerous researches and studies have been undertaken with the focus on hardware and software design.

One of the most well-renowned research was conducted by the Defensive Advanced Research Projects Agency who opened the Grand Challenge and Urban Challenge competitions in the United States. The Grand Challenge competition focused on the development of autonomous cars that can traverse off-road terrain by themselves [12] while the Urban Challenge assisted at the promotion of

autonomous automobiles with urban driving technique. These researches helped to confirm the feasibility of the self-driving automobile realization. Based on the result elevated through beforementioned competitions, multiple universities, organizations and scientists tried to develop a design of an autonomous vehicle which could be able to operate safely in a range of environments including open roads, urban canyons, tunnels etc. As a result, basic hardware functions were developed which are shown in Figure 1.1 [13].

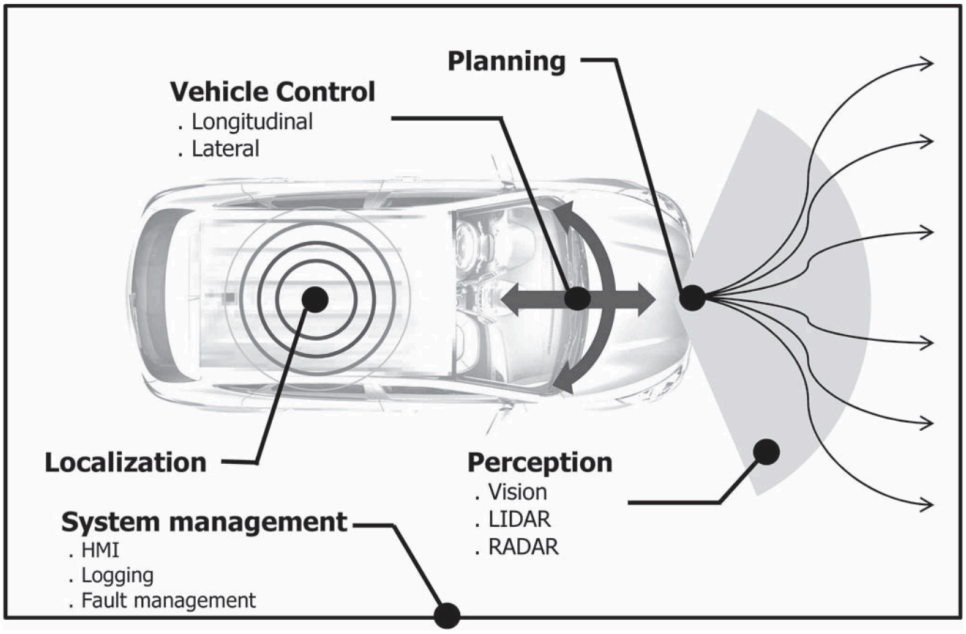

***Figure 2.1**: Basic architectural design of an autonomous vehicle*

However, despite the fact that the basic system design has already been developed, it is not safe enough for carrying people. According to J. Cui, “the complex interactions between these components inside the autonomous vehicle make it difficult to model the system, and to align the safety and security in an autonomous vehicle” [14]. This was demonstrated by the group of scientists under the Urban Challenge competition. They have developed an autonomous vehicle called Boss “capable of driving safely in traffic at speeds up to 48 km/h” [15]. However, after series of testing, they concluded that “no single sensor is capable of providing environmental data to sufficient range and with sufficient coverage to support autonomous urban driving” [15]. In other words, despite the fact that the automobile was able to drive on an public road, avoid obstacles and make right decisions, it is still not safe enough due to unpredictable environments which could cause the car’s delay in responding on a particular event and, thus, lead to a hazard.

Another problem associated with hardware and software design of the system is the ability of an autonomous car to be resilient. To achieve “centimeter-level accuracy that is robust against sensor failures and missing information” [16], the autonomous automobile should follow fault tolerance logic which means that “the failed sensor of one type, can be replaced by the functionality of a sensor of another type” [17]. It means that to achieve a fail-operation system, developers should design at least three redundant components which would be able to safely operate if one of them is destroyed. In the research conducted by P. Koopman and M. Wagner was concluded that introducing new components not only very expensive approach, but “there is also an issue of testing to make sure that failure detection and recovery works, assuring independence of failure, and ensuring that all redundant components are fault-free at the start of a driving mission” [18]. In other words, to ensure safety in autonomous automobiles redundancy can be avoided.

Despite all the beforementioned challenges, researches try to invent an autonomous automobile that satisfy all safety requirements. For example, during the research conducted by the scientists from Carnegie Mellon University [19], researchers have been able to develop an autonomous vehicle which meets the requirements of general autonomous driving (obstacle avoidance, detecting traffic lights and road signs, fault tolerance behavior etc). What is more, this autonomous automobile “has been tested extensively on both a closed test field and public roads” successfully [19]. Similarly, another significant project was implemented by German scientists who have developed an autonomous car called “Junior” [20]. This machine was able to “logged hundreds of miles of autonomous operation in a variety of real-life conditions” being resistant to bad weather conditions. However, both studies concluded that in order to prevent hazards, a safety driver should present during all rides and switch to manual control in the case of unpredictable events.

2.2.2 Cyber security safety

One of the most significant challenges in developing autonomous vehicles is cyber security safety because self-driving cars completely rely on software generated routing instructions. A self-driving automobile which cannot repel hackers attacks could be hijacked which would lead to numerous hazards and even losses of lives.

Nowadays researches concluded that the most suitable way of interaction between autonomous vehicles is through wireless communication technologies. “However, connecting wireless-enabled vehicles to external entities can make ITS applications vulnerable to various security threats, thus impacting the safety of drivers” [21]. To

enhance the security resistance of autonomous vehicles, researches from Qatar Mobility Innovations Center analyzed various intelligent transport system threats and their corresponding cryptographic counterblasts, security requirements and architecture decisions. Additionally, they analyzed and evaluated the European ETSI TC ITS standard [22]. The results revealed that available cyber security standards cannot manage secure V2X communications [21].

Multiple studies have been undertaken to develop a security algorithms which would make an autonomous vehicle resistant to malicious hackers. One of them has developed a security toolbox [23] which consists of security tools such as event data recorder, secure positioning component, data correlation tool and others, which could prevent different cyber threats and potentially could be used by security architecture designers while developing an autonomous car's software design. Another research leaded by J. Kavitha found a vulnerable place in an autonomous automobile – the signal to and from satellites (GPS) can be hacked which would cause a car stopped because of the lack of maps and its current geo-referenced position. They proposed a Secret key Encryption method which is based on one-time pad concept "where the data is converted to cipher text and then it is going to be decrypted by the satellite" [24].

Despite of the range of different security algorithms and cryptography techniques, they are all still unable to defend autonomous cars from malicious hacker attacks. A recent research conducted in 2015 by the University of Los Angeles displayed how cyber-attacks influence the road congestion and cause traffic jams. Via simulations they showed that malicious attacks increase the trip time of the car which consequently impacts the entire urban grid. They concluded that "current countermeasures are not effective, and point to new possible defenses" [25].

Another study run by the University of California investigated how security attacks influence communication channel of connected vehicles. They classified the types of cyber security attacks (Application Layer Attacks, Network Layer Attacks, System Level Attacks, Privacy Leakage Attacks) in order to study the behavior of a self-driving car while being under one of this attack via simulation through VENTOS (Vehicular Network Open Simulator) platform. They also revealed that "cryptographic security in terms of digital signatures/certificates by itself will not be able to prevent the attack" [26]. What is more, they proposed some potential countermeasures for detecting malicious behavior: Local Plausibility Check which detects a faulty affected by hackers sensor, Wearables and Mobile Devices which acts "as a verifier for the sensing data generated or

received by the vehicle", Voting technique which forces nearby cars to groups and perform trust computation and, if the data of one of the vehicle is false, vote for/against keeping the vehicle in the group [26].

2.2.3 The way of communication

Another significant challenge that need to be overcame before autonomous vehicles penetrate on public market and become widely used is the way of communication. By today a lot of design decisions have been proposed to enable communication among autonomous vehicles. One of them is communication based on 5G network [27] which uses cloud software services in order to analyze data collected from different sensors and avoid obstacles. In this study researchers developed a testbed with autonomous cars communicating through 5G network which demonstrates "the capabilities of autonomous and connected cars and study the influence of various parameters on the traffic efficiency of the communicating cars" [27]. They concluded that "with use of the emulated 5G cmWave, it demonstrates the capability of 5G networks to be flexibly adapted to the needs of divergent services through consequent use of virtualization and SDN techniques" [27].

However, in the recent study [28] researches concluded that the problem of all existing data sharing standards is that "transmittability is limited at the megabit level" [28] which would result in inability to share data collected from sensors (LIDAR/ HD cameras which generate large amount of data every second) with other autonomous vehicles. Instead, they proposed the next-generation mobile technology Millimeter-Wave Wireless Communications [29] which they extended and adopted for self-driving vehicles. According to them, "potentially provide the ability of multi-gigabit transmission, which is the most effective and straightforward solution to support the communication for autonomous vehicles in the next few decades and beyond" [28]. Despite all advantages of this technology, significant drawbacks prevent it to be used in self-driving cars such as security and privacy algorithms, lack of an incentive mechanism which would enable pedestrians to notify vehicles about their intentions and others.

Another implementation decision which would enable car-to-car communication is "broadband vehicle-to-vehicle communication using an extended autonomous cruise control sensor". The study [30] explored the possibility of extending the functionality of autonomous cruise control equipment through introducing microwave radio path. The results showed that the current cruise control architecture could be modified to support this technique. Despite the high cost of the modifications, this could result in better conditions of communication between autonomous vehicles.

Interesting solution was proposed by the University of MIT. They proposed to use cloud-assisted system called Carcel [31] which collects sensor data from autonomous vehicles and aids self-driving cars to make proper planning trajectories. The cloud storages all this information and analyzes data about nearby objects, traffic lights, weather condition, road signs and obstacles, blind spots and build alternative paths for each vehicle who send a request to Carcel. After set of testing and evaluation, researchers concluded that such way of communication can “significantly improve the safety of autonomous driving, by providing vehicles greater access to critical information in their blind spots” [31]. However, this communication approach is also difficult to implement due to challenge in “ensuring low latency and high availability over an inherently unreliable wireless medium.” [31].

The research conducted by H. Seif and X. Hu analyzed HD maps as a way of data sharing among autonomous vehicles. Scientists underlined that information obtained from sensors is “insufficient to enable fully autonomous driving” [32]. As a result, they proposed the following way of vehicle-to-vehicle communication: “the sensor data collected by thousands of cars allows the establishment of dynamic HD maps with high accuracy and real-time”. Communicating through HD maps, each car would be able to add essential information on HD maps (to a range of about 1 km) which will lead to multi-dimensional information with accuracy +/- 10cm. “This allows autonomous fast data acquisition, low errors, and dense point clouds for the realization of precise 3D maps” [33].

2.2.4 The storage of information

An autonomous automobile processes considerable amount of data collected from different sensors. What is more, the data from sensors is collected every X milliseconds. The problem arises when we talk about how to store this great amount of information and how to avoid “buffer overflowed” problem. Numerous proposals have been made how to achieve a consistent and coherent way of storing information. One study proposed to solve this problem by developing cloud-based self-driving cars [34]. The idea is to store all data in external databases – clouds – and request information only when is needed. It would enable autonomous vehicles obtain information only when it necessary which would allow them to not store all the information “on-board”. However, the challenge which prevents cloud-based cars appear on road is inability to reach stable connection. Thus, to introduce such way of storing data developers should overcome the problem with network.

According to an another significant recent research conducted in 2017, a typical autonomous vehicle generates immense amount of raw

information “which can exceed 2 Gbytes per second” [35]. In order to aid autonomous automobiles process such enormous amount of data, they introduced “a unified cloud infrastructure to provide distributed computing and storage capabilities for autonomous driving” [35] which is based on three technologies: “Apache Spark for distributed computing, Alluxio for in-memory storage, and OpenCL for heterogeneous computing acceleration” [35]. Such approach enables cars to have a consistent, low-latency and high-throughput cloud which would solve the problem of data storage and car’s memory capacity, performing heterogeneous parallel computations and HD map generation. What is more, they undertook evaluating of the cloud-architecture performance by processing a dataset with the total size more than 12 TBytes. The results showed that the combination of these technologies significantly increased the overall system performance. Both studies demonstrate the cloud-based approach of storing information which, as it was revealed in these researches, has numerous advantages in comparison with autonomous vehicle’s internal database information storage.

3 Conclusion

In summary, the main objective of this Literature Review was to investigate the safety challenges which prevent autonomous vehicle appear on public roads. While autonomous vehicles can provide us with many advantages such as independent mobility for non-drivers, decreased level of environment pollution, reduction in traffic accidents and increase in overall drivers safety, there are numerous challenges which prevent them to emerge on markets.

Despite the numerous hardware and software architectural approaches that have been proposed, they are all not able to process an enormous amount of data collected from different sensors and interpret it in a safe way. As a result, according to findings in experiments [19] [20] which successfully developed an autonomous automobile which meets the safety requirements, in order to ensure safe trip for people, safety driver should always accompany every ride and switch to manual control in the case of unpredictable events.

Similarly, many security algorithms and cryptography techniques have been developed in order to prevent an autonomous vehicle being hijacked. However, due to multiple types of cyber attacks which were classified in [24], [25], [26], current cryptography countermeasures cannot reflect different malicious cyber assaults and, thus, they need to be modified and enhanced appropriately.

One of the most significant challenges is the way of communication between autonomous vehicles. Different strategies of sharing data have been proposed such as communication based on 5G network [27], the next-generation mobile technology Millimeter-Wave Wireless Communications [29], cloud-assisted system called Carcel [31], communicating through HD maps [32]. However, to enable cars to communicate through wireless communication, as it was emphasized in the above studies, improved transmittability, low latency and high availability over a network should be provided. The same problems arise in storing and maintaining information in cloud databases, which were proposed in [34] and [35] in order to overcome the challenge of autonomous automobile's low-capacity internal storages which could be "overflowed" with enormous amount of sensor data.

Bibliography

[1] M. Daily, S. Medasani, R. Behringer, and M. Trivedi, “Self-Driving Cars,” 2017.

[2] J. Goodrich, *Driving Miss Daisy: An Autonomous Chauffeur System*. 2013.

[3] H. Morimoto, M. Koizumi, H. Inoue, and K. Nitadow, “AHS Road-to-Vehicle Communication System,” pp. 327–334.

[4] “WHO | World Health Organization.” [Online]. Available: https://www.who.int/. [Accessed: 13-Jan-2019].

[5] D. J. Fagnant and K. Kockelman, “Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations,” *Transp. Res. Part A Policy Pract.*, vol. 77, pp. 167–181, 2015.

[6] D. M. Mele, “The Quasi-Autonomous Car as an Assistive Device for Blind Drivers: Overcoming Liability and Regulatory Barriers,” 2013.

[7] J. Brinkley, B. Posadas, J. Woodward, and J. E. Gilbert, “Opinions and Preferences of Blind and Low Vision Consumers Regarding Self-Driving Vehicles: Results of Focus Group Discussions Exploring the Policy and Practical Implications of the Martin-Zimmerman Encounter; The Co-Production of Campus Safety and Security View project Fully Autonomous or "Self-Driving" Vehicles and Persons with Disabilities View project Opinions and Preferences of Blind and Low Vision Consumers Regarding Self-Driving Vehicles: Results of Focus Group Discussions.”

[8] A. C. Mersky and C. Samaras, “Fuel economy testing of autonomous vehicles,” 2016.

[9] O. US EPA, “Overview of Greenhouse Gases.”

[10] Ü. Özgüner, C. Stiller, and K. Redmill, “Systems for safety and autonomous behavior in cars: The DARPA grand challenge experience,” *Proc. IEEE*, vol. 95, no. 2, pp. 397–412, 2007.

[11] N. Thomopoulos and M. Givoni, “The autonomous car—a blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes,” *Eur. J. Futur. Res.*, vol. 3, no. 1, p. 14, 2015.

[12] S. Thrun, M. Montemerlo, H. Dahlkamp, D. Stavens, A. Aron, J. Diebel, P. Fong, J. Gale, M. Halpenny, G. Hoffmann, K. Lau, C.

Oakley, M. Palatucci, V. Pratt, P. Stang, S. Strohband, C. Dupont, L.-E. Jendrossek, C. Koelen, C. Markey, C. Rummel, J. Van Niekerk, E. Jensen, P. Alessandrini, G. Bradski, B. Davies, S. Ettinger, A. Kaehler, A. Nefian, and P. Mahoney, "Stanley: The Robot that Won the DARPA Grand Challenge," *J. F. Robot.*, vol. 23, no. 9, pp. 661–692, 2006.

[13] K. Jo, C. Jang, M. Sunwoo, J. Kim, and D. Kim, "Development of Autonomous Car-Part I: Distributed System Architecture and Development Process," *IEEE Trans. Ind. Electron.*, vol. 61, no. 12, 2014.

[14] J. Cui and G. Sabaliauskaite, "On the Alignment of Safety and Security for Autonomous Vehicles," no. c, pp. 59–64, 2017.

[15] C. Urmson, J. Anhalt, D. Bagnell, C. Baker, R. Bittner, M. N. Clark, J. Dolan, D. Duggins, T. Galatali, C. Geyer, M. Gittleman, S. Harbaugh, M. Hebert, T. M. Howard, S. Kolski, A. Kelly, M. Likhachev, M. McNaughton, N. Miller, K. Peterson, B. Pilnick, R. Rajkumar, P. Rybski, B. Salesky, Y.-W. Seo, S. Singh, J. Snider, A. Stentz, Z. Wolkowicki, J. Ziglar, H. Bae, T. Brown, D. Demitrish, B. Litkouhi, J. Nickolaou, V. Sadekar, W. Zhang, J. Struble, M. Taylor, M. Darms, and D. Ferguson, "Autonomous Driving in Urban Environments: Boss and the Urban Challenge," *www.interscience.wiley.com). • J. F. Robot.*, vol. 25, no. 8, pp. 425–466, 2008.

[16] B. Shin and C. Sciences, "Fault Tolerant Control and Localization for Autonomous Driving : Systems and Architecture," 2016.

[17] C. A. Jerlin, "Fault Tolerance in Wireless Sensor," vol. 2, no. 2, pp. 142–146, 2015.

[18] P. Koopman and M. Wagner, "Challenges in Autonomous Vehicle Testing and Validation."

[19] J. Wei, J. M. Snider, J. Kim, J. M. Dolan, R. Rajkumar, and B. Litkouhi, "Towards a Viable Autonomous Driving Research Platform."

[20] J. Levinson, J. Askeland, J. Becker, J. Dolson, D. Held, S. Kammel, J. Z. Kolter, D. Langer, O. Pink, V. Pratt, M. Sokolsky, G. Stanek, D. Stavens, A. Teichman, M. Werling, and S. Thrun, "Towards Fully Autonomous Driving: Systems and Algorithms."

[21] E. Hamida, H. Noura, and W. Znaidi, "Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures," *Electronics*, vol. 4, no. 3, pp.

380–423, 2015.

[22] “ETSI - Automotive Intelligent Transport.” [Online]. Available: https://www.etsi.org/technologies/automotive-intelligent-transport. [Accessed: 07-Feb-2019].

[23] M. Raya, J.-P. Hubaux, M. Verità, and / Ascona, “Security Aspects of Inter-Vehicle Communications STRC 5 th Swiss Transport Research Conference Security Aspects of Inter-Vehicle Communications.”

[24] J. C. Kavitha, A. Venugopal, S. Pushparani, and A. Professor, *Algorithm for Security in Autonomous Cars*. 2016.

[25] M. T. Garip, E. Gursoy, P. Reiher, and M. Gerla, “Congestion Attacks to Autonomous Cars Using Vehicular Botnets,” 2015.

[26] E. Org, M. Amoozadeh, A. Raghuramu, C.-N. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, and K. Levitt, “Publication Date License CC BY-SA 4.0 Peer reviewed Security Vulnerabilities of Connected Vehicles Streams and their Impact on Cooperative Driving.”

[27] S. Pandi, F. H. P Fitzek, C. Lehmann, F. HPFitzek, D. Nophut, D. Kiss, V. Kovács, Á. Nagy, G. Csovási, M. Tóth, T. Rajacsics, H. Charaf, and R. Liebhart, “Joint Design of Communication and Control for Connected Cars in 5G Communication Systems.”

[28] L. Kong, M. K. Khan, F. Wu, G. Chen, and P. Zeng, “Millimeter-Wave Wireless Communications for IoT-Cloud Supported Autonomous Vehicles: Overview, Design, and Challenges,” 2017.

[29] N. Bahadori, N. Namvar, B. Kelley, and A. Homaifar, *Device-to-Device Communications in the Millimeter Wave Band: A Novel Distributed Mechanism*. 2018.

[30] M. Heddebaut, J. Rioult, J. P. Ghys, C. Gransart, and S. Ambellouis, “Broadband vehicle-to-vehicle communication using an extended autonomous cruise control sensor,” *Meas. Sci. Technol*, vol. 16, pp. 1363–1373, 2005.

[31] S. Gollakota, D. K. A, S. Kumar, and D. Katabi, “Cloud-Assisted Design for Autonomous Driving .” Proceedings of Accessed Citable Link Detailed Terms A Cloud-Assisted Design for Autonomous Driving,” 2018.

[32] H. G. Seif and X. Hu, “Autonomous Driving in the iCity—HD Maps as a Key Challenge of the Automotive Industry,” *Engineering*, vol. 2, no. 2, pp. 159–162, Jun. 2016.

[33] J. O'Neill-Dunne, "Image boost: drones produce sharper images for mapping," *Roads Bridg.*, 2015.

[34] N. S. Yeshodara, N. S. Nagojappa, and N. Kishore, "Cloud Based Self Driving Cars," in *2014 IEEE International Conference on Cloud Computing in Emerging Markets (CCEM)*, 2014, pp. 1–7.

[35] S. Liu, J. Tang, C. Wang, Q. Wang, and J.-L. Gaudiot, "A Unified Cloud Platform for Autonomous Driving," *Computer (Long. Beach. Calif).*, vol. 50, no. 12, pp. 42–49, Dec. 2017.