# Multi-Access Edge Computing for Vehicular Networks: a Position Paper

Ridha Soua, Ion Turcanu, Florian Adamsky, Detlef Führer, and Thomas Engel
Interdisciplinary Centre for Security, Reliability and Trust (SnT),
University of Luxembourg, Luxembourg
{name.surname}@uni.lu

***Abstract*—With the emergence of self-driving technology and the ever-increasing demand of bandwidth-hungry applications, providing the required latency, security and computational capabilities is becoming a challenging task. Although being evolving, traditional vehicular radio access technologies, namely WLAN/IEEE 802.11p and cellular networks cannot meet all the requirements of future Cooperative, Connected and Automated Mobility (CCAM). In addition, current vehicular architectures are not sufficiently flexible to support the highly heterogeneous landscape of emerging communication technologies, such as mmWave, Cellular Vehicle-to-Everything (C-V2X), and Visible Light Communication (VLC). To this aim, Multi-access Edge Computing (MEC) has been recently proposed to enhance the quality of passengers experience in delay-sensitive applications. In this paper, we discuss the in-premises features of MEC and the need of supporting technologies, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), to fulfil the requirements in terms of responsiveness, reliability and resiliency. The latter is of paramount importance for automated services, which are supposed to be always-on and always-available. We outline possible solutions for mobility-aware computation offloading, dynamic spectrum sharing, and interference mitigation. Also, by revealing MEC-inherent security vulnerabilities, we argue for the need of adequate security and privacy-preserving schemes in MEC-enabled vehicular architectures.**

***Index Terms*—MEC, URLLC, V2X, SDN/NFV, Security, Privacy**

## I. Introduction

The recent progress on 5G's Ultra-Reliable and Low-Latency Communications (URLLC) for connected and Autonomous Vehicles (AVs) is unlocking new use cases and services, such as situation-aware driving, self-parking, and Vulnerable Road User (VRU) detection. In fact, 3GPP identified AVs as one of the use cases that should be addressed by 5G with the support of URLLC (1 millisecond end-to-end latency and packet loss rate as low as 1e-04 are required) [1]. A prerequisite for AVs is the high perception of their surrounding environment and awareness of the situation. To this end, AVs rely on a wide constellation of on-board sensors, but also on remote cloud services, such as high-definition maps, dynamic path planning, and guided parking. The main concern in the present vehicular communication landscape is that these automated driving services are time-varying, location-dependent, bandwidth-hungry, and delay-constrained. Automated driving sets very stringent networking performance requirements in terms of communication delay, reliability, and capacity to ensure innovative and diverse services. The most widely adopted Vehicle-to-Everything (V2X) networking solutions today are based on Dedicated Short-Range Communication (DSRC) [2], [3], Long Term Evolution (LTE) [4], or on heterogeneous approaches that aim at integrating the advantages from both DSRC and LTE [5], [6]. However, existing solutions can neither guarantee the end-to-end delay requirements nor the reliability of these emerging AV services, especially when considering the intermittent connectivity, high velocity, and dynamic nature of vehicular networks.

The Multi-access Edge Computing (MEC) paradigm is considered a potential solution towards achieving URLLC in vehicular networks. MEC was first introduced in 2014 with the purpose to provide cloud-computing capabilities within Radio Access Network (RAN) close to the mobile subscribers [7]. The MEC Industry Specification Group (ISG) of the European Telecommunications Standards Institute (ETSI) has provided the specification for MEC architecture based on use-case-driven requirements. In its white paper published in December 2017, the 5G Automotive Association (5GAA) outlined how MEC technology with its features (i.e., low latency, computation, and data storage close to end users) can be a supporting technology for multiple services for connected autonomous driving [8]. Specifically, it highlights several use cases where the use of MEC is relevant, such as intersection movement assist, real-time situational awareness, see-through, cooperative lane change, and VRU discovery. It also evaluates the gap from already defined MEC features and functions with respect to the new requirements in terms of new multi-access edge services, interfaces, and data models.

An ongoing effort recently started by ETSI investigates innovative mechanisms to support connected cars' use cases [9]. MEC is considered by ETSI as a fundamental technology in the 5G ecosystem, not only to ensure URLLC for V2X communication, but also to deploy services at appropriate locations [10]. In accordance with ETSI vision, two research projects have been recently launched: the MEC-View project [11] targets connecting infrastructure sensors to AVs via a mobile network with pre-processing of object information on the MEC server; the second project, Car2MEC [12], aims to improve connectivity for safety applications by taking advantage of local processing capability of MEC servers and the combination of ad-hoc and infrastructure-based networks.

However, before embracing the MEC paradigm, a number of challenges have to be addressed. In particular, resiliency is a paramount concern for automated services, which are supposed to be always-on and always-available. MEC-enabled architectures must be able to adapt and dynamically react to node failures and communication link deterioration. Also, the plethora of wireless communication technologies in vehicular networks and the possibility to gain access to MEC servers and hence to rich-context information, create serious security and privacy concerns.

In this position paper, we focus on the soaring need to provide URLLC V2X communications for seamless access to automated driving services by exploiting the MEC paradigm, as well as other 5G-enabling technologies, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV). We argue that leveraging on the emerging MEC paradigm will enable the development of innovative solutions for 5G automotive systems. We also discuss security and privacy implications of moving the traditional cloud close to the edges of the network, as well as the need for new privacy-preserving techniques in MEC-enabled vehicular architectures. Finally, we claim that resilient mechanisms for V2X communications under interactions with various access technologies are necessary.

## II. MEC in Vehicular Networks: a Broad Overview

MEC is considered an enabler for URLLC within the context of Cooperative, Connected and Automated Mobility (CCAM). The main idea behind the MEC paradigm is to bring a cloud computing environment at the edge of the network and in proximity to the end-users. This can be done by coupling MEC servers with the existing network infrastructure, i.e., Base Stations (BSs), Road Side Units (RSUs), and other Access Points (APs). By integrating IT services and telecommunications networking, MEC enables the evolution of the mobile BSs and triggers the rapid deployment of innovative services and applications. The general MEC concept is based on a distributed pool of servers and resources able to process content and to provide proximity services.

Currently, there is no common agreement on how the MEC-enabled vehicular architecture for CCAM should look like. ETSI has defined a MEC framework where several MEC servers are implemented at the BSs [13]. Recent studies have proposed MEC-enabled architectures for V2X use cases [14]–[17]. While some studies have adopted the same architecture designed by ETSI, namely BSs or RSUs co-located with MEC servers [14], other assume edge servers being located between the core network and BSs [15]. Hence, they are deployed independently from the radio network elements. Other studies consider vehicles as edge servers connected to Evolved NodeBs (eNBs) through two-tier architecture [16]. The first tier is directly connected to the eNB and is responsible of content caching, data aggregation, and analysis. The connection to the eNB is carried out by a cluster head using licensed Sub-6 GHz link. The second tier is connected to the cluster head of the first tier via mmWave links.

Figure 1 depicts an example of a high-level MEC-enabled architecture for CCAM with different use-cases. The first use-case, namely *platooning*, describes a scenario in which a group of vehicles are coordinated to drive together with very small inter-vehicle distance and without human control. A platoon is usually coordinated by a platoon leader (i.e., the heading vehicle), who is in charge of deciding the main platoon configuration (e.g., inter-vehicle distance, platoon size, driving speed, etc.), by means of Vehicle-to-Vehicle (V2V) communication. A MEC-enabled CCAM architecture providing URLLC can improve platoon applications by minimizing the shock-wave effects and improving the platoon stability [18]. Additionally, such an architecture can enable the deployment of autonomous vehicular highway systems, where platoons can be remotely controlled and managed by traffic management operators. For instance, Huang et al. [18] use MEC technology to achieve real-time computing/processing in-proximity of platoon members and to allocate virtual machines instances of diverse applications to the platoon. Moreover, given that in a platoon vehicles are evolving in the same environment, Ferdowsi et al. [19] proposed that vehicles should collaboratively learn a shared prediction model while keeping all of the training data on their own. This can be achieved through collaborative edge analytics, such as federated learning. Hence vehicles forming the platoon are decoupled from cloud and less data is generated inside the platoon.

The second use-case is *collaborative networking*. This latter can be carried out at different levels (e.g., Physical, MAC, Routing/ Forwarding) [20]. For instance, instead of using multiple antennas to achieve spatial diversity, neighbouring vehicles cooperate among themselves to enhance the reliability of a message by transmitting it through different communication channels. In this way, the obtained performances are similar to what is achieved by conventional MIMO systems. Space diversity can be also achieved at the routing layer by using cooperative routing protocols among nodes along the route. Hu et al. [16] integrate different V2X technologies (licensed Sub-6 GHz, IEEE 802.11p, and mmWave) to improve the content distribution and processing in vehicular networks. To this end, they developed a hierarchical MEC-enabled architecture composed of two different types of vehicular edges: tier-1 edges for data caching and aggregation, and tier-2 edges for data analysis. The presence of MEC servers close to the edge of the network enhances computation and processing capabilities of the network infrastructure. However, the computation time needed to execute certain tasks on a MEC server can be higher than the direct connectivity time of a vehicle with that server. Collaborative networking has been identified as a potential solution for predictive task offloading, where computation tasks can be relayed by means of multi-hop inter-vehicle communication [21]. Finally, collaborative networking improves situation awareness [20]. In this context, a MEC-based architecture can help to prevent accidents by signalling collision warnings faster because of URLLC capabilities. This can provide real-time alerts to vehicles in a local area. Additionally, it can deliver information about free parking space in-proximity which saves time and emissions.

The last use-case in Figure 1 is *VRU safety*. In this use-case the edge server is aware of other traffic participants in the

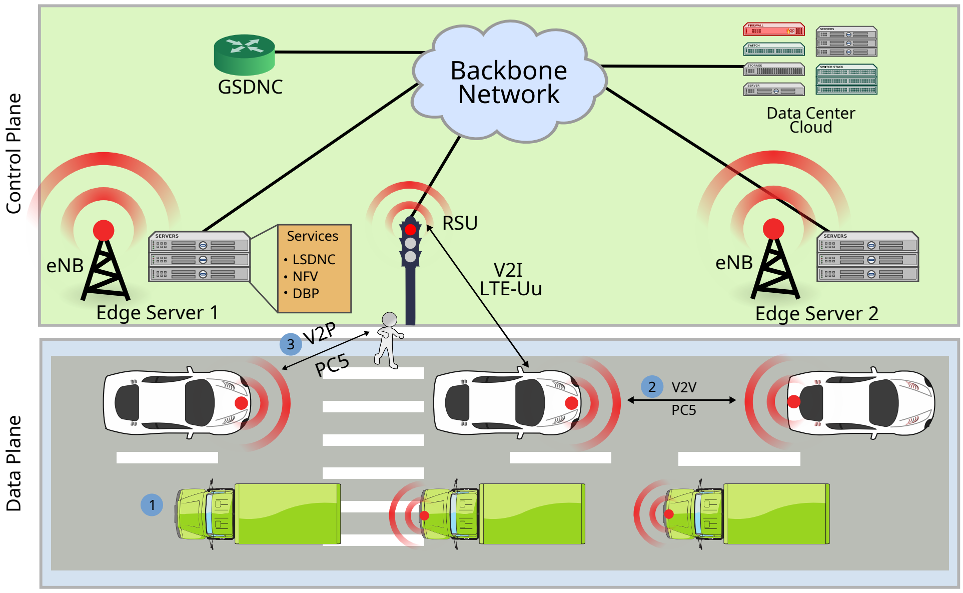

Figure 1. An example of MEC-enabled architecture with three use cases: (1) platooning, (2) collaborative networking and (3) VRU safety.

vicinity, such as pedestrians, cyclists, people with disabilities, and can signal cross-walk warnings to all approaching vehicles. Additionally, applications that allow vehicles themselves to send warning messages to VRUs, by means of Vehicle-to-Pedestrian (V2P) communication, can be developed. This can significantly improve the safety for VRUs. In this regard, MEC can play a key role by exploiting the local context and collected information to propose suitable manoeuvres in a timely manner. Recently, MEC ETSI group released a first set of APIs (Radio Network information, Location APIs, etc.) to improve the accuracy of the positioning information of all traffic participants [8]. Despite the advantages of MEC technology, there are several research challenges that needs to be addressed by the research community.

## III. Research Challenges in MEC-enabled Vehicular Networks

This section describes the open research challenges that are important to solve and to make MEC-enabled heterogeneous vehicular networks ready for CCAM.

**RC 1 URLLC, seamless connectivity and resiliency**

Many existing and emerging AV applications, such as safety, platooning, or Advanced Driver-Assistance Systems (ADAS), are only possible if URLLC among neighbouring vehicles and between vehicles and the infrastructure is guaranteed. Current V2X communication systems, namely IEEE 802.11p, Cellular Vehicle-to-Everything (C-V2X), mmWave, or Visible Light Communication (VLC), are normally used to obtain an enhanced perception of the surrounding environment. However, none of these communication technologies is able to fully satisfy latency and reliability requirements of AV applications. In addition, 5G networks envision deploying a large number of small cells to satisfy the seamless coverage. Consequently, a vehicle engaged in V2X communications and travelling across multiple cells needs to frequently perform horizontal and vertical handover procedures. It is crucial for some V2X applications to maintain the service continuity while performing seamless handover. Subsequently, resilient collaborative networking schemes are of paramount importance.

**RC 2 Resources Management & Orchestration**

5G networks are extremely heterogeneous (different communication technologies and mobile operators) and hence deploying resources and services at the edge of the network and in-proximity of end-users is too complex to manage. It is challenging to meet the Quality of Service (QoS) requirements (delay, throughput, etc.) and seamless service delivery without sophisticated resources management and orchestration schemes. V2X use cases will be a main part of the Mobile Network Operators (MNOs) targeted services and, therefore, they will face the challenge of orchestrating all their edges nodes to support new vertical segments (e.g., CCAM, industry4.0, public safety) in a single network infrastructure. These edge nodes are geographically distributed and will need standard-driven solution with reusing assets.

**RC 3 Cooperative Awareness**

A typical communication paradigm in vehicular networks consists in every vehicle periodically broadcasting Cooperative Awareness Messages (CAMs), containing basic state information, such as speed, location, driving direction, etc. This information must be shared among neighboring vehicles in order to enhance knowledge about the surrounding environment. Vehicles can cooperate either via V2V or Vehicle-to-Infrastructure (V2I). A reliable and low-latency exchange of such information is crucial for the operation of most vehicular safety applications. However, the heterogeneous nature of vehicular networks, i.e., the presence of multiple on-board vehicular communication technologies, makes this operation quite challenging. In addition, AVs are expected to push a large number of heavy computational tasks to edge nodes. Although these nodes are powerful, most of them do not offer the required capacity to carry out these tasks within the predefined QoS requirements of critical V2X uses cases where high reliability and low latency are of paramount importance.

**RC 4 Heterogeneity & Interferences**

Various heterogeneous wireless access technologies will exist in 5G vehicular networks sharing network infrastructures and spectrum resources. Given the high-mobility of vehicles, intermittent nature of V2X links, randomness in channel dynamics, and link interferences, this can lead to low Quality of Experience (QoE) of vehicle users and waste of the scarce spectrum resources. While MNOs are deploying small cells (e.g., Femto, Micro, Pico), interferences mitigation among tiers becomes extremely crucial due to the heterogeneity of networks. Therefore, how to provide resiliency for V2X applications and dynamic spectrum sharing solutions with URLLC requirement using the existing or future vehicular networks has become a major challenge. For instance, mmWave presents inherent propagation characteristics that need new solutions for spectrum sharing in 5G vehicular networks based on the context of the AVs and services' requirements.

**RC 5 Security & Privacy**

Road users determine their own positions with Global Positioning System (GPS) or Dead Reckoning and broadcast their position to their neighbourhood. A malicious vehicle can easily broadcast forged location information and create a huge amount of damage. In this scenario, MEC could help to be a trusted entity and verify the location of each participant. Additionally, one of the principles of the MEC paradigm is that cloud computing capabilities are only provided to users in close proximity. A research challenge remains how an edge server can verify the location of the users in order to countermeasure the above mentioned attacks.

Since MEC-enabled architectures are quite new, investigation of security and privacy vulnerabilities is still nascent. Only few studies have analysed these threats. Shirazi et al. [22] and Roman et al. [23] summarized the security threats that can target the network infrastructure, edge data centre, core infrastructure, virtualisation infrastructure, and user devices. Attacks such as Denial-of-Service (DoS) can be carried out against the network infrastructure (e.g. Radio Frequency (RF) jamming), but also against the virtualized infrastructure. Rogue hard- and software could run in the gateway, edge data center and core infrastructure and hence an attacker is able to run Man-in-the-Middle (MitM) attacks. Both studies outline that privacy leakages can take place in the edge data centre, virtualized infrastructure and the user device itself.

Privacy is another crucial requirement for V2X communications and is currently solved with pseudonym schemes [24], [25]. The introduction of multiple access technologies in a MEC-enabled environment, however, increases the amount of physical information that can be used to create a unique fingerprint of a user, which can be used for tracking [26], [27]. Consequently, revealing the security challenges introduced by MEC-enabled platforms and proposing adequate countermeasures is mandatory. In addition, the capability of MEC nodes to store and analyse data, and execute complex computations, makes them attractive candidates for security attacks. Therefore, privacy-preserving schemes are needed, given that rich context-information is processed by MEC servers and malicious users or third-party stakeholders can gain access to edge servers and derive information regarding users in proximity.

## IV. Potential Solutions

In this section, we discuss potential solutions to the research challenges that we have described in Section III.

To address RC 1, a constellation of different communication technologies and links can be exploited. In particular, V2X communication systems include different information exchange paths: V2I, Vehicle-to-Network (V2N), V2P and V2V. MEC servers can help in selecting the best signalling path and the most suitable communication technology among the once available in order to ensure the most reliable and low-latency communication link. The multitude and variety of communication paths and technologies allows having backup links, which improves resiliency and provides seamless connectivity. Moreover, caching services and mobility prediction mechanisms can be implemented on the MEC servers side in order the guarantee resource and information availability in advance, which will improve URLLC, connectivity and resiliency.

A MEC-enabled architecture for CCAM requires coordination, management, and orchestration to use the resources efficiently, as pointed out in RC 2. Leveraging on the recent advances on SDN along with NFV, the two key 5G components, MEC could significantly improve the resource management and orchestration. Although there are some recent studies that have focused on integrating these technologies in the MEC architecture [17], [28], [29], the full potential of SDN and NFV is still to be discovered. RC 2 challenges can be tackled by concentrating the network intelligence at distributed software-based controllers. In this way, SDN can relieve edge devices from the burden of complex operation. At the same time, NFV comes to help by allowing network functions to be dynamically deployed and inter-connected. Thus, it is mandatory to conceptualize the 5G reference framework by integrating SDN and NFV with MEC and introduce a programmable, flexible, and controllable architecture that can meet the requirements of selected uses cases for CCAM [30].

Deployment of SDN controllers and Virtualized Network Function (VNF) instances should take into account traffic characteristics, wireless diversity (link quality, link correlation, etc.) and mobility pattern. Including these technologies in the MEC architecture will enable 5G-like functionalities over the existing 4G infrastructure.

To address the challenges in RC 3, MEC servers could periodically collect data from vehicles related to the presence of different communication technologies on-board. Based on this information, the edge network will be used to create connectivity graphs, which will be periodically disseminated to vehicles and other road users, in order to enhance their knowledge about available on-board communication technologies and to improve vehicles' awareness. All this information exchange process in heterogeneous vehicular network must be efficiently coordinated. Compared to a resourceful cloud, a MEC server has limited resources. Operating alone, a MEC server cannot handle the burden of computation caching offloading from multiple AVs. To solve RC 3, we propose a dynamic orchestration of tasks computing and caching taking into account MEC-to-MEC communication and popularity patterns of computing tasks over large set of MEC servers. SDN and NFV could also be combined to enable dynamic orchestration of computing resources in order to enhance cooperative awareness. Deep reinforcement learning techniques could be investigated to obtain efficient resource-allocation policies.

RC 4 argues that radio spectrum is increasingly scarce, particularly in the "propagation-friendly" sub-6 GHz range. IEEE 802.11p-based ITS-G5 and 3GPP LTE-based C-V2X are the two major technologies competing for adoption in large-scale V2X deployment and the corresponding allocated frequency bands. Moreover, there are other incumbent services, such as Short Range Devices (SRD) and Fixed Wireless Access (FWA), operating in the same band. Harmful interference between these systems could have fatal consequences as pointed out in RC 4. To solve this issue, effective spectrum sharing mechanisms are necessary and therefore, it is necessary to study coexistence conditions between the different systems, in particular between ITS-G5 and C-V2X, and propose coexistence mechanisms or/and interference mitigation techniques. In a V2X system, dynamic spectrum maps could be generated utilizing miscellaneous data supplied from both mobile and fixed nodes and applying machine-learning techniques for data analysis. Such spectrum maps can be explored and, in combination with mobility models, employed to design a location-based dynamic spectrum access scheme for heterogeneous wireless vehicular networks.

An important aspect to be investigated is how MEC servers can act as trusted entities to provide accurate and trustworthy location information to road users, which we mentioned in RC 5. A possible solution is to use a Distance Bounding Protocol (DBP) [31], a cryptographic protocol which measures the signal propagation delay in order to verify the location of road users. However, since there are a number of DBPs and communication technologies which could be used, an evaluation is needed. Because the foundation of DBP is to measure the signal propagation delay, it is also mandatory to investigate appropriate techniques (e.g. invert non-uniform discrete Fourier transformation) to mitigate the multi-path problem inherent to DBP. Another not-well addressed security aspect from RC 5 is the vulnerability of MEC-enabled V2X systems to DoS attacks such as jamming, RF-based attacks, eavesdropping, and MitM attacks, taking into account recent advances in Software-defined Radio (SDR) and Unmanned Aerial Vehicle (UAV) technology which enable more sophisticated attacks on mobile targets. A possible solution to this problem is the usage of Frequency Hopping Spread Spectrum (FHSS) [32], a method in which the communication partners (AVs) changing the carrier frequency rapidly according to a pseudo-random scheme known to them. This makes it harder for the attacker, because the frequency must be known in order to jam it. Wide frequency jamming is technically a lot harder to do. Another possible solution is the usage of a new spread spectrum technique, such as Bandwidth Hopping Spread Spectrum (BHSS) [33]. In this technique, the transmitter randomly hopping the signal bandwidth to hamper the jamming attack.

As highlighted in RC 5, privacy-preserving V2X communications is a great concern for road users. Currently, in V2X, this problem is solved with pseudonymity schemes. However, the providers of the edge server could collect physical information from the multiple access technologies to create a unique end-user fingerprint, which then could be used for tracking. The authors of [34], [35] have shown that even physical information such as Channel State Information (CSI) of a wireless device are enough to create a unique fingerprint. Such investigations are needed for all access technologies used by the MEC architecture to protect users' privacy. It is important to investigate which physical information (e.g. phase shifting, amplitude, number of antennas, etc.) can be collected from the multiple access technologies. Appropriate machine-learning algorithms can be used to create unique device fingerprints. Based on these investigations, adequate countermeasures need to be developed to harden fingerprint generation.

## V. Conclusion

The rapid proliferation of connected cars and self-driving technology is posing severe demands on cloud infrastructure and vehicular access networks. Stringent requirements in terms of latency, reliability and seamless service delivery are calling for placing highly localized intelligence in close proximity to vehicle users. In light of this, this paper focused on the emerging MEC paradigm, considered as a key technology that can fulfil the requirements of future vehicular networks. MEC is considered by ETSI as a cornerstone for the execution of several delay-sensitive V2X use cases. However, the research on MEC-enabled vehicular networks is still in its early stage and therefore, a panoply of research challenges need to be addressed. Accordingly, we have outlined several research challenges that need to be taken into account when designing future MEC-enabled vehicular networks. Then, we highlighted potential solutions for resources management, low-latency computation and security using 5G key technologies.

## References

[1] 3GPP, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)," 3GPP, TR 22.892, Sep. 2016.

[2] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[3] European Telecommunications Standards Institute, "Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," ETSI, EN 302 663 V1.2.1, Jul. 2013.

[4] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for Vehicular Networking: A Survey," *IEEE Communications Magazine*, vol. 51, no. 5, pp. 148–157, May 2013.

[5] I. Turcanu, F. Klingler, C. Sommer, A. Baiocchi, and F. Dressler, "Duplicate suppression for efficient floating car data collection in heterogeneous LTE-DSRC vehicular networks," *Computer Communications*, vol. 123, pp. 54 –64, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0140366417304942.

[6] P. Salvo, I. Turcanu, F. Cuomo, A. Baiocchi, and I. Rubin, "Heterogeneous cellular and DSRC networking for Floating Car Data collection in urban areas," *Vehicular Communications*, vol. 8, pp. 21 –34, 2017, Internet of Vehicles. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S221420961630081X.

[7] ETSI, "Mobile-edge-computing- Introductory technical white paper," ETSI, White Paper, Sep. 2014 (accessed April, 2018). [Online]. Available: https://portal.etsi.org.

[8] 5GAA, "Toward fully connected vehicles: Edge computing for advanced automotive communications," White Paper, Dec. 2017 (accessed April, 2018). [Online]. Available: http://5gaa.org/news/toward-fully-connected-vehicles-edge-computing-for-advanced-automotive-communications.

[9] ETSI, "Multi-access Edge Computing (MEC); Study on MEC Support for V2X Use Cases," Tech. Rep., March 2018 (accessed April, 2018). [Online]. Available: https://portal.etsi.org/webapp/workProgram/Report_WorkItem.asp?wki_id=52949.

[10] F. Giust, V. Sciancalepore, D. Sabella, M. C. Filippou, S. Mangiante, W. Featherstone, and D. Munaretto, "Multi-access Edge Computing: The driver behind the wheel of 5G-connected cars," Mar. 2018 (accessed April, 2018). [Online]. Available: https://arxiv.org/abs/1803.07009.

[11] M.-V. project consortium. (). Mobile Edge Computing Based Object Detection for Automated Driving, [Online]. Available: http://www.mec-view.de/.

[12] F. Institute. (). Streamlined Development of Networked Vehicle Applications, [Online]. Available: www.ezcar2x.fraunhofer.de/en.html.

[13] ETSI, "Mobile Edge Computing (MEC); Framework and Reference Architecture," GS MEC 003 v1.1.1, Mar. 2016 (accessed April, 2018). [Online]. Available: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf.

[14] S. A. Ali Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for Vehicular Communications," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[15] L. Li, Y. Li, and R. Hou, "A Novel Mobile Edge Computing-Based Architecture for Future Cellular Vehicular Networks," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Mar. 2017, pp. 1–6.

[16] Q. Hu, C. Wu, X. Zhao, X. Chen, Y. Ji, and T. Yoshinaga, "Vehicular Multi-Access Edge Computing With Licensed Sub-6 GHz, IEEE 802.11p and mmWave," *IEEE Access*, vol. 6, pp. 1995–2004, 2018.

[17] A. Aissioui, A. Ksentini, A. M. Gueroui, and T. Taleb, "On Enabling 5G Automotive Systems Using Follow Me Edge-Cloud Concept," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5302–5316, Jun. 2018.

[18] R.-H. Huang, B.-J. Chang, Y.-L. Tsai, and Y.-H. Liang, "Mobile Edge Computing-Based Vehicular Cloud of Cooperative Adaptive Driving for Platooning Autonomous Self Driving," in *7th IEEE International Symposium on Cloud and Service Computing (SC2)*, Nov. 2017, pp. 32–39.

[19] A. Ferdowsi, U. Challita, and W. Saad, "Deep Learning for Reliable Mobile Edge Analytics in Intelligent Transportation Systems," *Http://arxiv.org/pdf/1712.04135v1*, 2017.

[20] E. Ahmed and H. Gharavi, "Cooperative Vehicular Networking: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 996–1014, Mar. 2018.

[21] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-Edge Computing for Vehicular Networks: A Promising Network Paradigm with Predictive Off-Loading," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 36–44, Jun. 2017.

[22] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog From a Security and Resilience Perspective," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2586–2595, Nov. 2017.

[23] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680 –698, 2018.

[24] D. Eckhoff and C. Sommer, "Readjusting the privacy goals in Vehicular Ad-Hoc Networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools," *Computer Communications*, vol. 122, pp. 118 –128, 2018.

[25] D. He, C. Chen, S. Chan, and J. Bu, "Secure and Efficient Handover Authentication Based on Bilinear Pairing Functions," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 48–53, Jan. 2012.

[26] N. T. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric Bayesian method," in *Proceedings IEEE INFOCOM*, Apr. 2011, pp. 1404–1412.

[27] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom '08)*, San Francisco, California, USA: ACM, 2008, pp. 116–127.

[28] J. Liu, J. Wan, B. Zeng, Q. Wang, H. Song, and M. Qiu, "A Scalable and Quick-Response Software Defined Vehicular Network Assisted by Mobile Edge Computing," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 94–100, 2017.

[29] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, "Exploring Mobile Edge Computing for 5G-Enabled Software Defined Vehicular Networks," *IEEE Wireless Communications*, vol. 24, no. 6, pp. 55–63, Dec. 2017.

[30] J. M. Duarte, E. Kalogeiton, R. Soua, G. Manzo, M. R. Palattella, A. D. Maio, T. Braun, T. Engel, L. A. Villas, and G. A. Rizzo, "A Multi-Pronged Approach to Adaptive and Context Aware Content Dissemination in VANETs," *Mobile Networks and Applications*, Jan. 2017. [Online]. Available: https://doi.org/10.1007/s11036-017-0816-y.

[31] S. Brands and D. Chaum, "Distance-Bounding Protocols," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed. Springer Berlin Heidelberg, 1994.

[32] S. Chang, Y. Hu, and N. Laurenti, "SimpleMAC: A jamming-resilient MAC-layer protocol for wireless channel coordination," in *Proceedings of the 18th Annual International Conference on Mobile Computing and Networking (MobiCom'12)*, Sep. 2012, pp. 77–88.

[33] D. Giustiniano, M. Schalch, M. Liechti, and V. Lenders, "Interference Suppression in Bandwidth Hopping Spread Spectrum Communications," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '18, Stockholm, Sweden: ACM, 2018, pp. 134–143. [Online]. Available: http://doi.acm.org/10.1145/3212480.3212484.

[34] J. Hua, H. Sun, Z. Shen, Z. Qian, and S. Zhong, "Accurate and Efficient Wireless Device Fingerprinting Using Channel State Information," in *Proceedings of the 37th IEEE International Conference on Computer Communication*, 2018.

[35] F. Adamsky, T. Retunskaia, S. Schiffner, C. Köbel, and T. Engel, "WLAN Device Fingerprinting Using Channel State Information (CSI)," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '18, Stockholm, Sweden: ACM, 2018, pp. 277–278. [Online]. Available: http://doi.acm.org/10.1145/3212480.3226099.