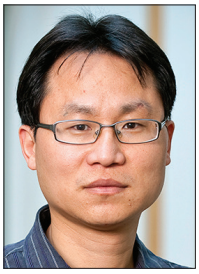
Reshaping Autonomous Driving for the 6G Era

Anwer Al-Dulaimi Xiaodong Lin

Autonomous vehicles are self-driving platforms that will transform the whole transportation system into a new form of connected intelligent ecosystem. However, vehicle automation will go through multiple evolution stages that start by partially automated driving where platforms are self-managed while driving decisions are made by humans, to the collaborative driving vehicles where humans intervene is needed during emergencies, and ultimately reaching fully automated vehicles that are completely driven by artificial intelligence (AI). Although fully automated vehicles are anticipated to operate as independent platforms, in-reality they are network-dependent systems that require continuous access to communication channels. The terrain data obtained from vehicle sensors are limited in distance and may not be able to capture the surrounding landscape for safe automated driving. Therefore, autonomous vehicles are dimensioning their roadways using data obtained through real-time connectivity with the cellular network. If any network connectivity interruptions occurred, the vehicle safety systems may switch the driving mode from full to partial automation. To this end, extensive network coverage and reliable connectivity are the key enablers to make vehicle automation complete and safe.

Vehicular networking may need to employ a more robust security system that protects both platforms and communications from hackers. For example, autonomous hacking defense and Tactics, Techniques and Procedures (TTPs) technologies is one system that improves the defense capabilities and resiliency of hyper-connected intelligent platforms. In addition, blockchains are widely accepted as a distributed ledger technology of a secure data structure solution that allows to exchange the data between vehicles. Considering cloud-based networks, blockchains should become a network service that stores and provides vehicle data. Those ledgers can be associated with either physical domains where vehicles interconnected with the same local network or logic networks that connect a selected set of local vehicles. These technologies and use cases will be key factors in defining any new vehicle-specific standards as part of the sixth generation (6G) networks. This opens the space for more discussions about 6G requirements for transport connectivity systems, security features, performance indicators, central vehicle monitoring and routing systems, and ultimately network-based vehicle automation.

This issue of the Vehicular Networking Series has four articles. The first article is entitled "Vehicular Communications for ITS: Standardization and Challenges" by Sherali Zeadally, Muhammad Awais Javed and Elyes Ben Hamida. The authors provide a review of the current standardization efforts for Dedicated Short-Range Spectrum (DSRC) and Cellular Vehicle-to-everything (C-V2X) technologies. The intention is to provide readers with insights about the evolution of Medium Access Control (MAC) and Physical (PHY) layers for both of the mentioned technologies. This article is very useful for readers since it also addresses the open challenges to improve these standards of the addressed technologies within the context of vehicular communications.

The next article, entitled "SDN-Sim: Integrating System Level Simulator with Software Defined Network" by Saptarshi Ghosh *et al.*, proposes an integrated framework of a system level simulator (SLS) with a software defined networking (SDN) infrastructure using a relational database as middleware. The aim is to reproduce SLS defined topology into an SDN emulator to evaluate the offloading of operations by computing routes in SDN and inject the outcomes back to the SLS. This article helps to predict the capabilities of future networks and evaluates the challenges ahead when accessing V2X functionaries at the edge clouds.

The third article, entitled "Supporting Vehicle-to-Everything (V2X) Services by 5G New Radio Release-16 Systems," is authored by Shehzad A. Ashraf, Ricardo Blasco, Hieu Do, Gábor Fodor, Wanlu Sun, and Congchi Zhang. The article studies the capabilities of the New Radio (NR) and how they support various advanced V2X scenarios. In particular, there is a ficus on the NR sidelink interface that is designed to enable platooning, advanced driving such as collision avoidance and cooperative lane change, extended sensors and remote driving use cases. The authors also provide analysis that demonstrates the performance of the resource allocation mechanism of transmission mode-2 of the NR sidelink.

The last article, entitled "Survey on Internet of Vehicles: Network Architectures and Applications" by Baofeng Ji *et al.*, provides a framework for a new network architecture employing Internet of Vehicles (IoV) for higher throughput, lower latency, robust security and massive connectivity. Besides a comprehensive survey on IoV, the authors show several network architectures and typical applications of IoV for Vehicular Ad-hoc Network (VANET) technology. The article studies different network elements and proposes a new four-layer network architecture that improves compatibility between VANET and IoV.

Biographies

Anwer Al-Dulaimi [M'11, SM'17] (anwer.al-dulaimi@exfo.com) received his Ph.D. degree in electronic and computer engineering from Brunel University, London, UK in 2012. Currently, he is a technical product owner (TPO) at the Center of Excellence at EXFO, Canada. His research interests include 5G and beyond, cloud networks, and V2X. He is the chair of IEEE 1932.1 Working Group "Standard for Licensed/Unlicensed Spectrum Interoperability in Wireless Mobile Network" and IEEE Distinguished Lecturer.

Xiaodong Lin [M'09, SM'12, F'17] (xlin08@uoguelph.ca) received his Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, China, and his Ph.D. degree (with the Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo. He is currently an associate professor in the School of Computer Science at the University of Guelph, Canada. His research interests include computer and network security, privacy protection, applied cryptography, computer forensics, and software security.